NAS ストレージ管理

ONTAP 9

NetApp
September 12, 2024

目次

NAS ストレージ管理

System Manager を使用して NAS プロトコルを管理します

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 以降のリリースの System Manager を使用して NAS 環境を構成および管理する方法を説明します。

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 構成の概要"
- "SMBセツテイノカイヨウ"

System Manager では、以下のワークフローがサポートされ

- NAS ファイルサービスに使用するクラスタの初期設定。
- ストレージニーズを変更するための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、またはその両方（NAS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およびTLSセキュリティ
- エクスポートと共有
- qtree
- ユーザと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。

を作成した後 "NFS 対応の Storage VM" System Manager で、 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、 VSC はの一部です "ONTAP Tools for VMware vSphere 仮想アプライアンス"で、 VSC 、 vStorage APIs for Storage Awareness （ VASA ） Provider 、および Storage Replication Adapter （ SRA ） for VMware vSphere の機能を使用できます。

必ずを確認してください "NetApp Interoperability Matrix を参照してください" 現在の ONTAP リリースと VSC

リリースの互換性を確認するため。

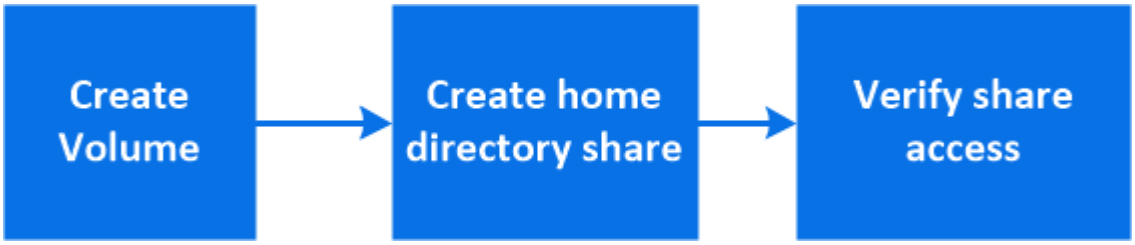
System Manager Classic（ONTAP 9.7以前のリリース）を使用してESXiホストからデータストアへのNFSアクセスを設定するには、を参照してください。 "VSCを使用したESXi向けのNFS設定の概要"

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

ホームディレクトリ用の **NAS** ストレージをプロビジョニングします

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

この手順は、上にホームディレクトリ用の新しいボリュームを作成します "SMB対応の既存のStorage VM"。ボリュームの構成時にシステムのデフォルトをそのまま使用することも、カスタム構成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、高い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には 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 を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"。

このボリュームの仕様は 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、編集できます"。

手順

1. SMB 対応 Storage VM に新しいボリュームを追加
   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。 を参照してください [ボリュームの設定をカスタマイズする]をクリックし、次の手順を実行するためにここに戻ります。
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 ）を使用して共有名が作成された場合は、解決済みの名前を使用してアクセスをテストする必要があります。

b. 新しく作成したドライブで、テストファイルを作成し、作成できたら削除します。

ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、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または FlexGroup ボリュームの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。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- 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 によるデータ保護（ローカルまたはリモート）を実行してから、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、に戻ります [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 を使用して **Linux** サーバ用の **NAS** ストレージをプロビジョニング

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。

この手順は、に新しいボリュームを作成します "NFS 対応の既存の Storage VM"。ボリュームの設定時にシステムのデフォルトをそのまま使用することも、カスタム構成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、高い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には 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 を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"。

このボリュームの仕様は 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、編集できます"。

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

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 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。

        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。 を参照してください [ボリュームの設定をカスタマイズする]をクリックし、次の手順を実行するためにここに戻ります。
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、テキストを書き込んでから、ファイルを削除します。

   アクセスを確認したら、を実行できます "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" 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。

ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、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または FlexGroup ボリュームの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。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- 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 によるデータ保護（ローカルまたはリモート）を実行してから、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、に戻ります [step2-complete-prov] NFS を使用して Linux サーバのプロビジョニングを完了する方法

ONTAP でこれを行うその他の方法

実行するタスク	参照先
System Manager Classic （ ONTAP 9.7 以前）	"NFS 構成の概要"
ONTAP コマンドラインインターフェイス（ CLI ）	"CLI を使用した NFS の設定の概要"

エクスポートポリシーを使用してアクセスを管理します

エクスポートポリシーを使用した NFS サーバへの Linux クライアントアクセスの有効化

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

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 を使用して Windows サーバ用の NAS ストレージをプロビジョニングする

ONTAP 9.7 以降で使用可能な 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。

この手順は、に新しいボリュームを作成します "SMB対応の既存のStorage VM" およびは、ボリュームのルート（ / ）ディレクトリ用の共有を作成します。ボリュームの構成時にシステムのデフォルトをそのまま使用することも、カスタム構成を指定することもできます。SMB の初期設定後に、追加の共有を作成したりプロパティを変更したりすることもできます。

FlexVol ボリュームを作成することも、高い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には 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 を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"。

このボリュームの仕様は 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、編集できます"。

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

作業を開始する前に

- 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 "File System Analytics を有効にします"。

手順

1. SMB 対応 Storage VM に新しいボリュームを追加
   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。 を参照してください [ボリュームの設定をカスタマイズする]をクリックし、次の手順を実行するためにここに戻ります。
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、テキストを書き込み、ファイルを削除します。

アクセスを確認したら、共有 ACL によってクライアントアクセスを制限し、マッピングされ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。を参照してください "SMB 共有を作成" を参照してください。

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することができます。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。

共有の設定時に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（ ONTAP 9.10.1 以降）の継続的可用性を有効にします。次も参照してください。
    - "Hyper-V over SMB での継続的な可用性を備えた共有の要件"
    - "SQL Server over SMB での継続的な可用性を備えた共有の要件"
  - この共有へのアクセス時に SMB 3.0 でデータを暗号化する。

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します
- 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て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）。
  - Access-Based Enumeration （ ABE ；アクセスベースの列挙）を有効にすると、ユーザのアクセス権限に基づいて共有リソースが表示されます。

の手順

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。

ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、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、デフォルト値の選択に加えて、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または FlexGroup ボリュームの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。そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- 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。そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。
- ボリュームが設定されているプロトコルに対するアクセス権限。
- SnapMirror によるデータ保護（ローカルまたはリモート）を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」をクリックしてボリュームを作成し、クラスタと Storage VM に追加します。

システムのデフォルトを受け入れる代わりに、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または FlexGroup ボリュームの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。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- 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 によるデータ保護（ローカルまたはリモート）を実行してから、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、に戻ります [step2-compl-prov-win] SMB を使用した Windows サーバのプロビジョニングの完了

ONTAP でこれを行うその他の方法

実行するタスク	参照先
System Manager Classic （ ONTAP 9.7 以前）	"SMBセツテイノカイヨウ"
ONTAP の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** の両方を使用して **Windows** と **Linux** の両方に **NAS** ストレージをプロビジョニングする

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。

この手順は、に新しいボリュームを作成します "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"。

> 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、高い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には FlexGroup ボリュームを作成することもできます。 を参照してください "FlexGroup を使用して大規模ファイルシステム用の NAS ストレージをプロビジョニング"。

このボリュームの仕様は 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、編集できます"。

手順

1. NFS と SMB の両方に対して有効になっている 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。

      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。エクスポートポリシーにはあとから制限付き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。ACL にはあとから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。

または、許可、サービス品質、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。を参照してください [ボリュームの設定をカスタマイズする]をクリックし、次の手順を実行するためにここに戻ります。

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、テキストを書き込んでから、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、テキストを書き込み、ファイルを削除します。

アクセスを確認したら、を実行できます "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、共有 ACL を使用してクライアントアクセスを制限します"をクリックし、エクスポートおよび共有ボリュームに対して必要な所有権と権限を設定します。

ボリュームの設定をカスタマイズする

システムのデフォルトを受け入れる代わりに、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または FlexGroup ボリュームの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。 そうしないと、追加するボリュームはデフォルトで FlexVol ボリュームになります。

- 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 によるデータ保護（ローカルまたはリモート）を実行してから、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、に戻ります [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するため。

ONTAP でこれを行うその他の方法

実行するタスク	参照するコンテンツ
System Manager Classic （ ONTAP 9.7 以前）	"SMB と NFS のマルチプロトコル構成の概要"
ONTAP の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 の設定の概要" • "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 を使用してクライアントアクセスを保護

NAS クライアントのストレージアクセスを保護するには、 Kerberos を有効にします。

この手順は、で有効になっている既存の Storage VM に Kerberos を設定します "NFS" または "SMB"。

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

手順

1. ONTAP コマンドラインで、 Storage VM ルートボリュームに対する 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	root または ID 0
GID	root 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、を使用します `volume modify` コマンドを使用して更新します。

2. Storage VM ルートボリュームに対する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 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**
NFS	500ドル	0
ルート	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、を使用します `vserver services name-service unix-user modify` コマンドを使用して更新します。

3. Storage VM ルートボリュームに対する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 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.
ルート	0

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

4. Kerberos を設定するには、 System Manager に切り替えてください
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 を追加します

     KDC ベンダーに応じて設定の詳細を入力します。

   - Realm にネットワークインターフェイスを追加します

     [* 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. [ストレージ]>[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** の下で、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。有効になっている既存のStorage VMでこの設定を行うことができます： "NFS"。

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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。

作業を開始する前に

を参照してください "要件" （NFS over TLSの場合）。

1. 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。
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を無効にする

転送中のデータのセキュリティを強化する必要がなくなった場合は、NFSクライアントのTLSを無効にすることができます。

手順

1. 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。
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 が LDAP または NIS を使用してホスト、ユーザ、グループ、またはネットグループ情報を検索し、 NAS クライアントを認証できるようにします。

この手順は、に対して有効になっている既存の Storage VM の LDAP または NIS の設定を作成または変更します "NFS" または "SMB"。

LDAP 構成の場合は、環境で必要な LDAP の設定の詳細が必要であり、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 のボリュームの表示を展開し、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、低レイテンシの高速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 "File System Analytics 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 を使用して、ホスト固有のユーザとグループを管理します

ONTAP 9.10.1 以降では、 System Manager を使用して、 UNIX または Windows ホストに固有のユーザとグループを管理できます。

次の手順を実行できます。

Windows の場合	「 UNIX 」
• Windows のユーザとグループを表示します • [add-edit-delete-Windows] • [manage-windows-users]	• UNIX ユーザおよびグループを表示します • [add-edit-delete-UNIX] • [manage-unix-users]

Windows のユーザとグループを表示します

System Manager では、 Windows 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 グループを追加、編集、または削除します

System Manager では、 Windows グループを追加、編集、削除することで、グループを管理できます。

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を表示します。
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. グループメンバーの指定（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の追加）
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 ユーザを管理します

System Manager では、 Windows ユーザを追加、編集、削除、有効化、無効化することで管理できます。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を表示します。
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. 有効にする各無効な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. 無効にする各有効な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を表示します

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、または削除します

System Manager では、 UNIX グループを追加、編集、または削除することで、それらのグループを管理できます。

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を表示します。

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）関連付けられた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、削除することで管理できます。

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を表示します。
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を監視します

ONTAP 9.8 以降では、クラスタ上で NFS のライセンスが有効になっている場合に、どの NFS クライアント接続がアクティブになっているかが表示されます。

この方法を使用すると、接続はされているがアイドル状態で切断されている Storage VM にアクティブに接続している NFS クライアントを簡単に確認できます。

各NFSクライアントのIPアドレスについて、* NFSクライアント*ディスプレイには次のように表示されます。
*最終アクセス時刻
*ネットワークインターフェイスのIPアドレス
* NFS接続のバージョン
* Storage VM名

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

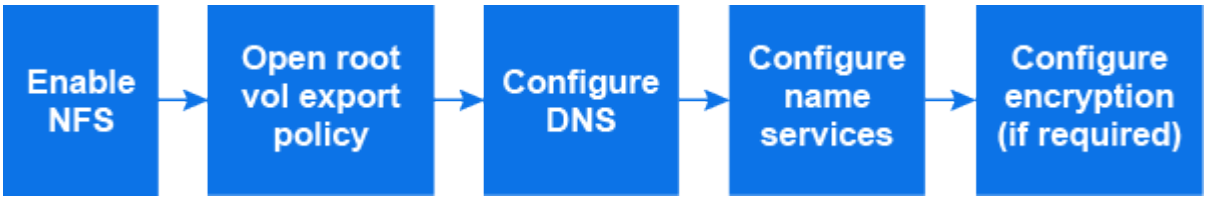
1. NFS クライアントアクティビティを表示します。 [*Hosts] > [NFS Clients] をクリックします。

NAS ストレージを有効にします

NFS を使用して **Linux** サーバ用の **NAS** ストレージを有効にします

Storage VMを作成または変更して、NFSサーバがLinux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、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。



作業を開始する前に

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を更新する（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. Storage > Volumes * をクリックし、 Storage VM のルートボリューム（デフォルトは _volume-name_root ）を選択して、 * Export Policy * に表示されるポリシーをクリックします。

b. ルールを追加するには、 [* 追加] をクリックします。

- 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. 必要に応じてネームサービスを設定

   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]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クライアント用の**TLS**の設定

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

手順

1. を参照してください "要件" （NFS over TLSの場合）を参照してください。
2. 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。
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

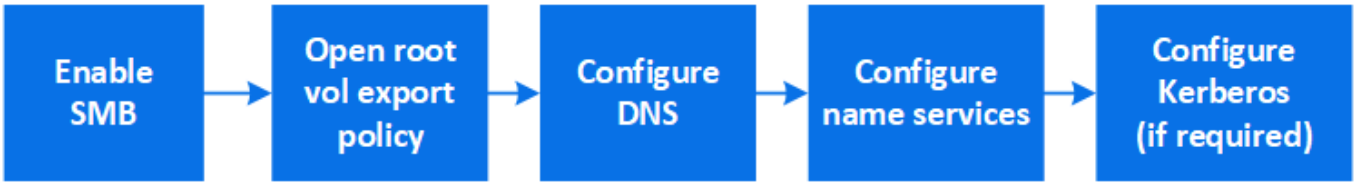
手順

1. 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。
2. [Kerberos]タイル内をクリックし、*[追加]*をクリックします。

SMB を使用して **Windows** サーバ用の **NAS** ストレージを有効にします

Storage VMを作成または変更して、SMBサーバで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 では、SMBプロトコル用の新規または既存のStorage VMを有効にします。ここでは、環境に必要なネットワークサービス、認証サービス、セキュリティサービスの構成の詳細を記載するものとします。



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
      - 組織単位を確認します。
      - DNS値を確認します。
      - 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を更新する（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. Storage > Volumes * をクリックし、 Storage VM のルートボリューム（デフォルトは *volume-name_root*） を選択し、 * Export Policy * に表示されるポリシーをクリックします。
   b. ルールを追加するには、 [* 追加] をクリックします。
      - 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。

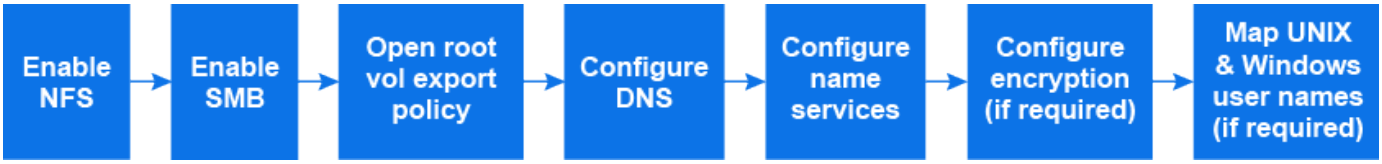
- フォワードルックアップ（A - アドレスレコード）とリバースルックアップ（PTR - ポインタレコード）のエントリを作成して、 SMB サーバ名をデータネットワークインターフェイスの IP アドレスにマッピングします。
- NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータネットワークインターフェイスの IP アドレスにマッピングします。

4. 必要に応じてネームサービスを設定
   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. 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。
   b. でをクリックし、[追加]*をクリックし → ます。

NFS と **SMB** の両方を使用して、 **Windows** と **Linux** の両方で **NAS** ストレージを有効にします

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

新規または既存のStorage VMが、この手順を使用して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。



作業を開始する前に

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を有効にする
   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. 組織単位を確認します。
   d. DNS値を確認します。
   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を更新する（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. Storage > Volumes * をクリックし、 Storage VM のルートボリューム（デフォルトは *volume-name_root*） を選択し、 * Export Policy * に表示されるポリシーをクリックします。

b. ルールを追加するには、 [* 追加] をクリックします。

- 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）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. 必要に応じてネームサービスを設定します。

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、[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クライアント用の**TLS**の設定

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

手順

a. を参照してください "要件" （NFS over TLSの場合）を参照してください。

b. 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。

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. 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。

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 2 組のユーザセットがある場合、ネームマッピングを設定する必要があります。

CLI で NFS を設定

CLI を使用した NFS の設定の概要

ONTAP 9 の 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。

次の手順に従って、ボリュームまたは qtree へのアクセスを設定します。

- 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 を使用する 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には、を参照してください "NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングする"。

- 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。

- 新しいボリュームを UNIX ファイル権限を使用して保護する。
- SVM 管理者権限ではなくクラスタ管理者権限を持っている。

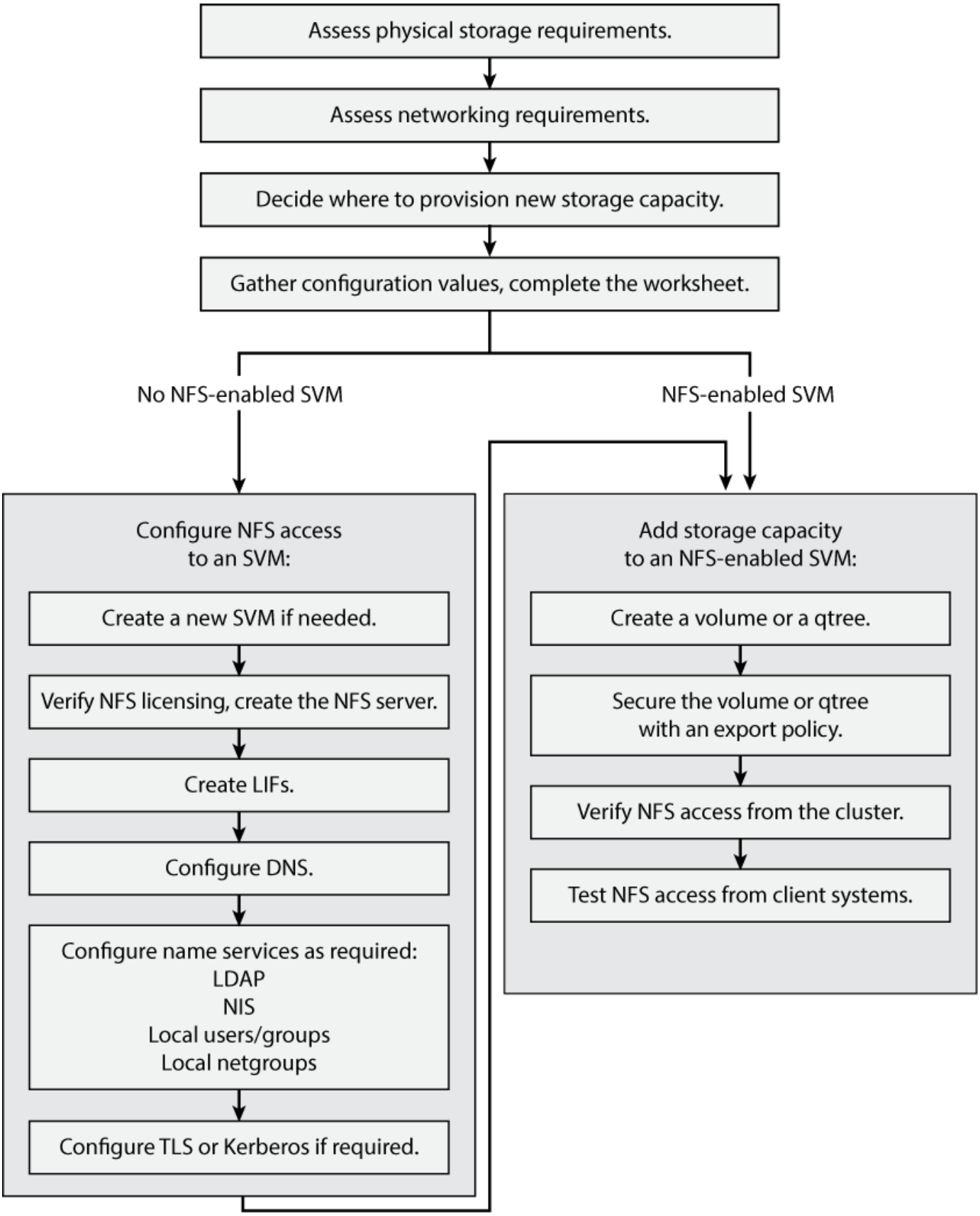
ONTAP NFS プロトコル機能の範囲の詳細については、を参照してください "NFS のリファレンスの概要"。

ONTAP でこれを行うその他の方法

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 を使用して Linux サーバ用の NAS ストレージをプロビジョニング"
System Manager Classic （ ONTAP 9.7 以前で使用可能	"NFS 構成の概要"

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を評価

クライアントの 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のため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、を使用して既存のアグリゲートにディスクを追加します `storage aggregate add-disks` コマンドを実行するか、を使用して新しいアグリゲートを作成します `storage aggregate create` コマンドを実行します

ネットワーク要件を評価

クライアントに NFS ストレージを提供する前に、 NFS 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。

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高であるポートを使用する必要があります。
   - 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。

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、を使用して作成されます `network subnet create` コマンドを実行します

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、を使用してIPv6を有効にできます `network options ipv6 modify` コマンドを実行します

新しい **NFS** ストレージ容量のプロビジョニング先を決定します

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。これにより、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ものの設定されていない既存の 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、「 SVM への NFS アクセスの設定」と「 NFS 対応 SVM へのストレージ容量の追加」の両方の手順を完了します。

  SVM への NFS アクセスを設定

  NFS対応SVMにNFSストレージを追加

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 上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」の手順を実行します。

  NFS 対応 SVM にストレージを追加

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 に対する 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 アクセスを設定する
- 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、次の作業のみを実行してください。

- NFS 対応 SVM へのストレージ容量の追加

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 **NFS** アクセスを設定

- SVM を作成するためのパラメータ *

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

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 *

では、次の値を指定します `vserver nfs create` コマンドは、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ときに使用します。

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。 ONTAP 9.8以降では、v4.2もサポートされます `v4.1` が有効になります。	
`-v4-id-domain`	ID マッピングのドメイン名を指定します。	
`-v4-numeric-ids`	所有者 ID 番号のサポート（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*

では、次の値を指定します `vserver nfs tls interface enable` コマンドを実行します

ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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 *

では、次の値を指定します `network interface create` コマンドを使用してLIFを作成します。

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`	でLIFが戻るノードを指定します `network interface revert` LIFに対してコマンドを実行します。	
`-home-port`	の場合に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` LIFに対してコマンドを実行します。	
`-address`	新しい LIF によるデータアクセスに使用されるクラスタ上の IPv4 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を指定します。	
-subnet	IP アドレスのプール。の代わりに使用されます -address および -netmask 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 *

では、次の値を指定します vserver services name-service dns create コマンドを使用してDNSを設定します。

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 アドレスを指定します。	

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 *

を使用してローカルユーザを作成する場合は、次の値を指定します vserver services name-service unix-user create コマンドを実行しますUniform Resource Identifier （ URI ）から UNIX ユーザを含むファイルをロードすることによっ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	一二三	100	ジョンミラー
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 *

を使用してローカルグループを作成する場合は、次の値を指定します `vserver services name-service unix-group create` コマンドを実行しますURI から UNIX グループを含むファイルをロードすることによっ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 *

では、次の値を指定します `vserver services name-service nis-domain create` コマンドを実行します

> ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-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 で名前検索に使用される 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*

では、次の値を指定します `vserver services name-service ldap client create` コマンドを実行します

また、自己署名ルートCA証明書も必要です `.pem` ファイル。

> ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-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`	デフォルトを使用します `3` このワークフローの秒数。	`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`。をに設定する必要があります `sasl` 署名と封印が設定されている場合。	
`-preferred-ad-servers`	カンマで区切った IP アドレスのリストによって、優先される Active Directory サーバを指定します。	
`-ad-domain`	Active Directory ドメインを指定します。	
`-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`	デフォルトのLDAPサーバポートを使用します `389` をクリックします。	`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を指定します。	
-base-dn	ベース識別名。デフォルトはです "" （ルート）。	
-base-scope	デフォルトのベース検索範囲を使用します subnet をクリックします。	subnet
-session-security	LDAP 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 *

では、次の値を指定します vserver nfs kerberos realm create コマンドを実行しますMicrosoft Active Directory をキー配布センター（ KDC ）サーバとして使用するか、 MIT やその他の UNIX KDC サーバとして使用するかによって、一部の値が異なります。

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可されているクロックスキューを指定します	
-kdc-ip	KDC の IP アドレスを指定します。	
-kdc-port	KDC のポート番号を指定します。	
-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 ベンダーを指定します。	{Microsoft
Other}	-comment	必要なコメントを指定します。

では、次の値を指定します vserver nfs kerberos interface enable コマンドを実行します

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 ）を指定します。	
-permitted-enc-types	Kerberos over NFSで許可されている暗号化タイプ。 aes-256 クライアントの機能に応じて推奨されます。	
-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を指定します。パスワードは必須です	
-keytab-uri	KDC 管理者のクレデンシャルを持っていない場合は、 SPN キーが含まれている KDC の keytab ファイルを指定します。	

-ou	Microsoft KDC の Realm を使用して Kerberos を有効にしたときに Microsoft Active Directory サーバアカウントが作成される組織単位（OU）を指定します。	

NFS 対応 SVM へのストレージ容量の追加

- 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 *

では、次の値を指定します `vserver export-policy create` コマンドを実行します

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。	

では、各ルールに次の値を指定します `vserver export-policy rule create` コマンドを実行します

フィールド	説明	あなたの価値
-clientmatch	クライアント一致条件	
-ruleindex	ルールの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	システム	65534
1.					
2.					
3.					
…					
N					

- ボリュームを作成するためのパラメータ *

では、次の値を指定します `volume create` コマンドは、qtreeの代わりにボリュームを作成する場合に使用します。

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`	新しいボリュームをマウントするルート（`/`）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 *

では、次の値を指定します `volume qtree create` コマンドは、ボリュームではなくqtreeを作成する場合に使用します。

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を指定します。	
`-qtree`	新しい qtree に対して、一意のわかりやすい名前を 64 文字以内で指定します。	
`-qtree-path`	qtreeパスの引数を指定します。形式はです `/vol/volume_name/qtree_name\>` ボリュームとqtreeを別 々 の引数として指定する代わりに指定できます。	
`-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。	

SVM への NFS アクセスを設定

SVM を作成します。

NFS クライアントへのデータアクセスを提供するための SVM がクラスタ内に 1 つもな

い場合は、作成する必要があります。

作業を開始する前に

- 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`*

   - にUNIX設定を使用します `-rootvolume-security-style` オプション
   - デフォルトのC.UTF-8を使用します `-language` オプション
   - 。 `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を含める必要があります。このリストはあとで編集できます。

   。 `Vserver Operational State` フィールドにはを表示する必要があります `running` 状態。が表示された場合 `initializing` 状態にすると、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 内に作成します。

```
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に追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含ま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を設定します。

SVM で **NFS** プロトコルが有効になっていることを確認します

SVM で NFS 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。

このタスクについて

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、を使用してあとから有効にすることができます `vserver add-protocols` コマンドを実行します

> 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。

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` コマンドを実行します

手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。

   `vserver show -vserver vserver_name -protocols`

   を使用することもできます `vserver show-protocols` コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示します。

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手順は次のとおりです。
     [+]
     `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、を追加することでNFS経由のアクセスを許可します `nfs` vs1というSVMで有効になっているプロトコルのリストに移動します。

```
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きます

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。

このタスクについて

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を使用するすべての NFS クライアントに対してアクセスが許可されていることを確認してから、ボリュームまたは qtree ごとにカスタムのエクスポートポリシーを作成して各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:  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に含める場合は、エクスポートルールオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5` または `krb5i`。例：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

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

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 サーバを作成します

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、を使用できます `vserver nfs create` コマンドを使用してSVMにNFSサーバを作成し、SVMがサポートするNFSのバージョンを指定します。

このタスクについて

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 以降をサポートする場合は、次の点に注意してください。

- NFSv4 ユーザ ID マッピングドメイン名が、 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が使用されていれば、 LDAP または NIS の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で NFSv4 数値 ID 設定がサポートされている必要があります。
- セキュリティ上の理由から、 NFSv4 環境では、 LDAP をネームサービスに使用する必要があります。

作業を開始する前に

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
   ```

   表示されない場合は、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 バージョンは任意の組み合わせで有効にすることができます。pNFSをサポートする場合は、両方を有効にする必要があります `-v4.1` および `-v4.1-pnfs` オプション（ Options ）

   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する必要があります。

   - `-v4-id-domain`

     （オプション）このパラメータは、 NFSv4 プロトコルの定義に応じて、ユーザ名およびグループ名の文字列形式のドメイン部分を指定します。デフォルト ONTAP では、 NIS ドメインが設定されている場合は NIS ドメインを、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ているドメイン名に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 所有者属性で数値文字列識別子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

ートすることを確認する必要があります。

NFSのその他の機能は、を使用してあとから有効にすることができます `vserver nfs modify` コマンドを実行します

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 を作成

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が管理用に設定されている必要があります `up` ステータス。
- 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。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理す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 はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じネットワークポート上に 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。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、 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にある指定したホームノード上のランダムな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 の LIF とネームスペースは、同じノードでホストする必要があります。
- 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を作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 `-data-protocol` パラメータは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 9.6以降）。

- `-home-node` は、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

  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` オプション

- `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
- でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
- 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。
- サブネットを使用せずに手動で IP アドレスを割り当てると、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。
- をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

  必要に応じて、カスタムファイアウォールポリシーをあとから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は廃止され、完全にLIFのサービスポリシー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できます。デフォルト設定はです `false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。

2. 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` コマンドを実行します
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
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

次のコマンドでは、を使用して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ます `-address` および `-netmask` パラメータ：

```
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 ）から割り当てています。

```
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 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、 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、に割り当てられたNASデータLIFを作成する方法を示しています `default-data-files` サービスポリシー：

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

ホスト名解決に使用する **DNS** を有効にします

を使用できます `vserver services name-service dns` 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します。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

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

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つだけの場合は警告が表示されます。

このタスクについて

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、 SVM vs1 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` コマンドは設定の自動検証を実行し、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を報告します。

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

   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
   ```

   次のコマンドは、 SVM vs1 の DNS 設定の詳細を表示します。

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

   。 `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

ネームサービスの概要を設定

ストレージシステムの構成によっては、クライアントに適切なアクセス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します

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。

このタスクについて

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、環境でNISが使用されていない場合は、を指定しないでください `-sources nis` オプション

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、を使用する必要があります `vserver services name-service ns-switch modify` または `vserver services name-service ns-switch delete` コマンド

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
```

完了後

- 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を設定する

ローカル **UNIX** ユーザおよびグループの概要を設定する

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** ユーザを作成します

を使用できます `vserver services name-service unix-user create` コマンドを使用してローカルUNIXユーザを作成します。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 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）からSVMにロードすることで、タスクを簡易化できます。 (`vserver services name-service unix-user load-from-uri`）。

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、UNIX内のユーザ情報が含まれている必要があります `/etc/passwd` 形式：

   `user_name: password: user_ID: group_ID: full_name`

   このコマンドにより、の値が破棄されます *`password`* フィールドと、の後のフィールドの値 *`full_name`* フィールド (*`home_directory`* および *`shell`*）。

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URIからロードします `ftp://ftp.example.com/passwd` vs1という名前のSVMに追加します。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** グループを作成します

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

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 文字以内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します

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

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** グループをロードします

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、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` コマンドを実行します

手順

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

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

   `group_name: password: group_ID: comma_separated_list_of_users`

   このコマンドにより、の値が破棄されます *`password`* フィールド。

   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、を設定する必要があります `-overwrite` パラメータの値 `true` 既存のすべてのエントリを新しいファイルで上書きするか、または既存のエントリと重複するエントリが新しいファイルに含まれていないことを確認します。

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 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した場合 `true`と指定ONTAP したSVMの既存のローカルUNIXグループデータベース全体が、ロードするファイルのエントリで置き換えられます。

例

次のコマンドは、ローカルUNIXグループのリストをURIからロードします `ftp://ftp.example.com/group` vs1という名前のSVMに追加します。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

ネットグループの概要の使用

ネットグループは、ユーザ認証に使用でき、また、エクスポートポリシールールでクライアントを照合するためにも使用できます。を使用して、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したり、Uniform Resource Identifier（URI）からSVMにネットグループをロードしたりできます `vserver services name-service netgroup load` コマンドを実行します

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。

  また、クライアントの IP アドレスが複数の PTR レコードを持つ場合は、それらすべてのホスト名がネットグループのメンバーであり、対応する A レコードを持っている必要があります。

- ネットグループ内のすべてのホストの名前が、そのソース（ NIS 、 LDAP 、またはローカルファイル）に関係なく、正しいスペルで、かつ大文字 / 小文字を正しく使用している必要があります。ネットグループで使用されているホスト名に不整合があると、エクスポートチェックの失敗など、予期しない動作が発生する可能性があります。
- ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 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。

  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。

このタスクについて

ネットグループについては次の処理を実行できます。

- を使用できます `vserver export-policy netgroup check-membership` 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するためのコマンド。
- を使用できます `vserver services name-service getxxbyyy netgrp` コマンドを使用して、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します。

  検索を実行する基盤となるサービスは、設定済みの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）を使用してSVMに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。

このタスクについて

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、数分かかる場合があります。

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

例

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

```
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状態を確認します

ネットグループをSVMにロードしたら、を使用できます `vserver services name-service netgroup status` ネットグループの定義のステータスを確認するコマンド。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します

現在の環境でネームサービスにNetwork Information Service（NIS；ネットワーク情報サービス）が使用されている場合は、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` コマンドを実行します

必要なもの

SVM に NIS ドメインを設定するためには、設定済みのすべての NIS サーバが使用可能でアクセスできる状態になっている必要があります。

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 エントリに依存したクライアントアクセスに失敗する可能性があります。

このタスクについて

複数の NIS ドメインを作成できます。ただし、に設定されているものだけを使用できます `active`。

NISデータベースにが含まれている場合 `netgroup.byhost` マップ、ONTAP は、検索を高速化するために使用できます。。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは常に同期されている必要があります。ONTAP 9.7以降ではNISが使用されます `netgroup.byhost` エントリはを使用してキャッシュできます `vserver services name-service nis-domain netgroup-database` コマンド

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 -active true -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、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-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、 IP アドレス 192.0.2.180 の NIS サーバを使用して、 vs1 という名前の SVM に、 nisdomain という NIS ドメインのアクティブな NIS ドメイン設定を作成します。

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

LDAP を使用する

LDAP の使用方法の概要

現在の環境で LDAP がネームサービス用に使用されている場合は、 LDAP 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 LDAP クライアントとして有効にする必要があります。

ONTAP 9.10.1 以降では、 LDAP チャネルバインドがデフォルトで Active Directory とネームサービスの両方の LDAP 接続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に設定されている場合にのみ、 LDAP 接続でチャネルバインドを試行します。ネームサーバとの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、を使用します `-try-channel-binding` パラメータと `ldap client modify` コマンドを実行します

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"。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント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 クライアント上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ている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされてい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 サーバに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（データの整合性チェックを提供）および LDAP の署名と封印（データの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、次のサービスが設定されている必要があります。
    - LDAP サーバで GSSAPI （ Kerberos ） SASL がサポートされている必要があります。
    - LDAP サーバに、 DNS A/AAAA レコード、および 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、 DNS サーバ上に存在する SRV レコードが必要です。
  - TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。
    - ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
    - LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
    - 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）、次の条件を満たしている必要があります。
    - 両方のドメインで、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。一次は紹介ドメインを信頼します

    - 親子
  - 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
  - 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サポートされません。
>
> - 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（ `-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しています。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。

- LDAP をホスト名解決に使用することはサポートされていません。

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 』"
- "自己署名ルート CA 証明書を SVM にインストールします"

新しい **LDAP** クライアントスキーマを作成します

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。

このタスクについて

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

- MS-AD-BIS （ほとんどの Windows Server 2012 以降の AD サーバで推奨されるスキーマ）
- AD-IDMU （ Windows Server 2008 、 Windows Server 2012 、およびそれ以降の AD サーバ）
- AD-SFU （ Windows Server 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 に用意されているデフォルトの LDAP スキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、そ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します

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、の適切な設定値を確認してください `vserver services name-service ldap client create` コマンドを実行します

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

        - を使用します `-ad-domain` Active DirectoryドメインでLDAPサーバ検出を有効にするオプション。

          - を使用できます `-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するオプション。このオプションを使用する場合は、CIFSのデフォルトサイトも指定する必要があります。 `-default-site`。

- を使用できます `-preferred-ad-servers` カンマで区切ってIPアドレスで1つ以上の優先Active Directoryサーバを指定するオプション。クライアントが作成されたら、を使用してこのリストを変更できます `vserver services name-service ldap client modify` コマンドを実行します
- を使用します `-servers` カンマで区切ってIPアドレスで1つ以上のLDAPサーバ（Active DirectoryまたはUNIX）を指定するオプション。

> 。 `-servers` オプションはONTAP 9.2で廃止されました。ONTAP 9.2以降では、`-ldap-servers` フィールドがに置き換わります `-servers` フィールド。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。その場合は、デフォルトスキーマ（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 を参照してください

  RFC 2307bis に基づいて、ほとんどの標準的な Windows 2012 以降の LDAP 環境で優先される 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 Server 2008 、 Windows Server 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 サーバで必要な場合は、 LDAP の署名と封印または LDAP over TLS を有効にすることができます。

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

  署名を有効にできます (`sign`、データ整合性）、署名と封印 (`seal`、データ整合性と暗号化）、またはどちらでもない `none`、署名または封印なし）。デフォルト値はです `none`。

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

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

  に設定すると **`true`** LDAPサーバがサポートしており、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でSMBサーバがドメインに追加されており、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、 `-session-security -for-ad-ldap` オプションを使用します `vserver cifs security modify` コマンドを実行します

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 を使用した LDAP 接続の保護を予定している場合は、デフォルトのポート 389 を使用する必要があります。Start TLS は LDAP のデフォルトポート 389 経由でプレーンテキスト接続として開始され、その後 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 は失敗します。

- `-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。デフォルト値はです `3` 秒。

- `-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 リファーラル追跡を有効にした場合など）。デフォルト値はです `""` （ルート）。

- `-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、 LDAP リファーラル追跡を有効にすると、必要なレコードが他の LDAP サーバにあることを示す 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 クライアントがそれらの LDAP サーバに対してルックアップ要求を実行することができます。デフォルト値はです **`false`**。

参照された LDAP サーバにあ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。LDAPサーバの検出は指定したドメインの特定の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 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 CN=Users,DC=addomain,DC=example,DC=com
```

次のコマンドは、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** に関連付けます

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

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ており、 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 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` コマンドは設定の自動検証を実行し、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を報告します。

次のコマンドは、「 vs1 」という SVM で LDAP を有効にし、「 ldap1 」という 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. 上の 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** ソースを確認します

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. を更新します `ns-switch` 必要に応じて入力：

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します

NFS での **Kerberos** 使用によるセキュリティ強化の概要

Kerberos を強力な認証に使用している環境では、 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設定を決定し、 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に従う必要があります。

- 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

  タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を回避するために必要です。

- ドメイン名解決（ DNS ）

  それぞれの UNIX クライアントおよび SVM LIF について、 KDC の前方参照ゾーンと逆引き参照ゾーンに適切なサービスレコード（ SRV ）が登録されている必要があります。すべてのコンポーネントを DNS で正しく解決できる必要があります。

Kerberos 設定の権限を確認します

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	root または ID 0
GID	root または ID 0

名前	設定
UNIX 権限	755

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

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（ **Comment** ）
NFS	500ドル	0	GSS INIT フェーズで必要。 NFS クライアントユーザの SPN の最初のコンポーネントがユーザとして使用されます。 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。
ルート	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、を使用できます `vserver services name-service unix-user modify` コマンドを使用して更新します。

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.
ルート	0

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

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、を使用する必要があります `vserver nfs kerberos realm create` SVMにKerberos Realm設定を作成するコマンド。

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. で指定する適切な設定値を決定するには、Kerberos管理者に問い合わせてください `vserver nfs kerberos realm create` コマンドを実行します
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 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 で許可されている暗号化タイプを設定する

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。を使用して、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` コマンドにを指定します `-permitted-enc-types` パラメータ

このタスクについて

クライアントの互換性を最大にするために、 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、セキュリティの向上を必要としていて環境でこの機能がサポートされている場合は、この手順を使用して、 DES と 3DES を無効にしてクライアントに 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 上で 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 上で Kerberos 構成を無効にすることが必要になるからです。

  この変更を行う前に、 SVM 上で NFS クライアントが AES 暗号化に依存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. 許可されている必要な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** を有効にします

を使用できます `vserver nfs kerberos interface enable` コマンドを使用してデータLIFでKerberosを有効にします。これにより、 SVM で NFS の Kerberos セキュリティサービスを使用できます。

このタスクについて

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、オプションのを指定できます `-ou` パラメータ

   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 が有効になっていることを確認します。

   `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 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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。ONTAPクラスタにCA署名済みサーバ証明書を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。

- 各証明書は、NFSサーバ（TLSを有効または設定するデータLIF）のFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を共通名（CN）として設定する必要があります。
- 各証明書には、サブジェクト代替名（SAN）としてNFSサーバ（またはその両方）のIPアドレスまたはFQDNを設定する必要があります。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。

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 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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。

作業を開始する前に

- を参照してください "要件" （NFS over TLSの場合）を参照してください。
- を参照してください "マニュアルページ" 詳細については、 `vserver nfs tls interface enable` コマンドを実行します

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

```
vserver nfs tls interface show
```

例

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

```
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を無効にする

転送中のデータのセキュリティを強化する必要がなくなった場合は、NFSクライアントのTLSを無効にすることができます。

> 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。

作業を開始する前に

を参照してください "マニュアルページ" 詳細については、 `vserver nfs tls interface disable` コマ

ンドを実行します

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

```
vserver nfs tls interface show
```

例

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

```
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

NFS over TLSの既存の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。

作業を開始する前に

を参照してください "マニュアルページ" 詳細については、 `vserver nfs tls interface modify` コマンドを実行します

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 `status` の `enable`を指定する必要があります。 `certificate-name` パラメータ括弧<>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. を使用します `vserver nfs tls interface show` コマンドを使用して結果を表示します。

```
vserver nfs tls interface show
```

例

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

```
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

NFS 対応 SVM の概要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。を使用できます `vserver export-policy create` コマンドを使用してエクスポートポリシーを作成します。

手順

1. エクスポートポリシーを作成する

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

   ポリシー名に指定できる文字数は最大 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含まれていないと、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種類を選択し、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、を使用できます `vserver export-policy rule create` 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します。

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うちどのセキュリティ方式が使用されているかを特定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）

このタスクについて

エクスポートポリシーの既存のルールがクライアント照合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、エクスポートルールオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5`、 `krb5i`または `krb5p`。

手順

1. クライアントと、新しいルールのクライアント照合形式を特定します。

   。 `-clientmatch` オプションは、ルールを適用するクライアントを指定します。クライアント照合の値は 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,...`
ピリオド区切りの形式の 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,...`

クライアント照合形式	例
ネットグループ名の前に @ 文字を付け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。たとえば、 `.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 のように、 IP アドレスの範囲を入力することはできません。

  この形式のエントリはテキスト文字列と解釈され、ホスト名として扱われます。

- 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. クライアント照合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対して、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に対する読み取り / 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に対する読み取り専用アクセスも許可した場合にのみ許可されます。読み取り専用パラメータで読み取り / 書き込みパラメータよりも限定的なセキュリティタイプを指定した場合、クライアントに対して読み取り / 書き込みアクセスが許可されない可能性があります。スーパーユーザアクセスの場合も同様です。

   カンマ区切りの形式を使用して、 1 つのルールに対して複数のセキュリティタイプを指定できます。セキュリティタイプとしてを指定する場合は `any` または `never`、その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てください。

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、常に実行されます。

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
none	単独で指定した場合、どのセキュリティタイプのクライアントにも匿名アクセスが許可されます。他のセキュリティタイプと一緒に指定した場合、指定したセキュリティタイプのクライアントにアクセスが許可され、それ以外のセキュリティタイプのクライアントには匿名アクセスが許可されます。
never	受信セキュリティタイプに関係なく、絶対に使用しないでください。
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 によって認証されます。

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

NFSv3でKerberosを使用する場合は、エクスポートポリシールールで許可する必要があります `-rorule` および `-rwrule` へのアクセス `sys` に加えて `krb5`。これは、 Network Lock Manager （ NLM ；ネットワークロックマネージャ）に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` option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 が pcuser というユーザに関連付けられています。ユーザIDが0のクライアントからのアクセスを無効にするには、の値を指定します `65535`。

4. ルールインデックスの順序を選択します。

。 `-ruleindex` optionには、ルールのインデックス番号を指定します。ルールはインデックス番号のリストの順序に従って評価され、インデックス番号の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	作業
最初のルールをエクスポートポリシーに追加します	入力するコマンド 1。
追加のルールをエクスポートポリシーに追加	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 任意のバージョンと一致します。 nfs3 および nfs4 特定のバージョンのみを照合します。

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`*

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

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 という名前の SVM 上のエクスポートルールを作成し、作成を確認します。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 内のどのクライアントとも一致します。すべての NFS アクセスを有効にしています。AUTH_SYS で認証されたユーザに対する読み取り専用および読み取り / 書き込みアクセスを有効にしています。UNIX ユーザ ID が 0 （ゼロ）のクライアントは、 Kerberos 以外で認証すると匿名化されます。

```
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。すべての NFS アクセスを有効にしています。AUTH_SYS によって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 / 書き込みおよびルートアクセスについては Kerberos 認証を要求します。UNIX ユーザ ID が 0 （ゼロ）のクライアントは、Kerberos 以外で認証すると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します

ボリュームを作成します

を使用して、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` コマンドを実行します

このタスクについて

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、新しいボリュームを作成するときに指定できます。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、を使用してSVMネームスペースにボリュームを_mount_する必要があります `volume mount` コマンドを実行します

作業を開始する前に

- 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トラッキングを有効にするには、を問題します `volume create` コマンドにを指定

します `-analytics-state` または `-activity-tracking-state` をに設定します `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 "File System Analytics を有効にします"。

手順

1. ジャンクションポイントを指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 `-junction-path` 次のようなものがあります。

   - 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。

     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、次のように指定します。 `/new_dir/new_vol` その後、SVMルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。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そのポリシーを指定できます。エクスポートポリシーは、を使用してあとから追加することもできます `volume modify` コマンドを実行します

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、で使用できます `/users`。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 」およびアグリゲート「 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 `/eng/` はvs1 SVMのネームスペースにすでに存在し、新しいボリュームはで使用できるようになります `/eng/home`をクリックします。これがのホームディレクトリになります `/eng/` ネームスペース：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です `volume` （デフォルト）。

```
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 を作成します

を使用して、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` コマンドを実行します

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、を使用してあとから追加することもできます `volume qtree modify` コマンドを実行します

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を作成します `/vol/data1`：

```
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て **NFS** アクセスを保護

エクスポートポリシーを使用して **NFS** アクセスを保護

エクスポートポリシーを使用することにより、ボリュームまたは qtree への NFS アクセスを特定のパラメータに一致するクライアントだけに制限することができます。新しいストレージをプロビジョニングするときに、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することができます。エクスポートポリシーの設定を確認することもできます

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、すべてのルール違反をエラールールリストに記録することができます。。 `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、構成を検証し、誤った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、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。

エクスポートルールの処理順序を管理します

を使用できます `vserver export-policy rule setindex` 既存のエクスポートルールのインデックス番号を手動で設定するコマンド。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。

このタスクについて

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
```

エクスポートポリシーをボリュームに割り当てます

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するための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。

このタスクについて

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
```

エクスポートポリシーを **qtree** に割り当てます

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。

このタスクについて

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を確認

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。を使用してクライアントアクセスを確認できます `vserver export-policy check-access` コマンドを実行し、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、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` コマンドを実行します

   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が示されます `exp-home-dir` アクセスは拒否されます

   ```
   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。

クライアントシステムからの **NFS** アクセスをテストします

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. 新しいフォルダを作成します。
      [+]
      `mkdir /mnt/folder`

   b. 次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. 入力するコマンド
[+]
`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。

追加情報の参照先

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構成

NFS アクセスについてさらに詳しく設定するには、以下の情報と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ています。

- "ネットアップ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。

- "ネットアップ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 ）サーバを使用する ONTAP の設定方法と、 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 ）を使用するための の設定方法について説明しています。

- "ネットアップテクニカルレポート 3580 ：『 NFSv4 の拡張内容とベスト・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 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、次の情報と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ています。

- "ネットアップ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ベストプラクティス』"

  ONTAP ネットワーク設定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およびベストプラクティスの推奨事項を提供しています。

- "ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

  認証用に LDAP 、 NIS 、 DNS 、およびローカルファイルの設定を行う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 の設定情報を使用できます。この情報は、複数のホストオペレーティングシステムに対応しています。

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 に対するネットアップ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消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 でのNFSエクスポートの実装方法に詳しくない場合は、7-ModeとONTAP のエクスポート設定ツール、およびサンプルの7-Modeを比較してください `/etc/exports` クラスタ化されたポリシーとルールを含むファイル。

ONTAP ではありません `/etc/exports` ファイルではありません `exportfs` コマンドを実行します代わりに、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 の場合とほとんど同じ方法でクライアントアクセスを制御できます。また、 1 つのエクスポートポリシーを複数のボリュームに再利用できるなどの機能も追加されています。

関連情報

"NFS の管理"

"ネットアップテクニカルレポート 4067 ：『 NFS Best Practice and Implementation Guide 』"

7-Mode と ONTAP のエクスポートの比較

ONTAP でのエクスポートは、定義方法と使用方法が 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	エクスポートはで定義されます `/etc/exports` ファイル。	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。 • で別のエントリを作成する必要があります `/etc/exports` ファイルパスまたはqtreeごとに指定します。 • エクスポートは、で定義されている場合にのみ保持されます `/etc/exports` ファイル。	• 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および 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。 • システムの再起動後も、すべてのエクスポートポリシーが永続します。

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、で各クライアントとその許可されているアクセスをリストする必要があります `/etc/exports` ファイル。	エクスポートポリシーは、多数のエクスポートルールで構成されています。エクスポートルールごとに、リソースに対する特定のアクセス権限が定義され、該当する権限を持つクライアントが一覧表示されます。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、特定のアクセス権限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として、ファイルパスとは異なる名前を選択できます。を使用する必要があります `-actual` でこのようなエクスポートを定義するときのパラメータ `/etc/exports` ファイル。	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、それぞれ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、マウント解除し、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、に表示される7-Modeエクスポートを示しています `/etc/export` ファイル：

```
/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（ **Element** ）	価値
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）
`-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、7-Modeを示しています `/etc/export` 10個のqtreeごとに1行で構成されるファイル：

```
/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2つのポリシーのうちの1つ（を含むルールが設定されたポリシー）が必要です `-clientmatch host1519s`、またはを含むルールを持つ1つ `-clientmatch host2057s`。

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 の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含まれています。NFS サーバおよびエクスポートボリュームまたは qtree を有効にすることができます。

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 ファイルアクセスを理解する

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

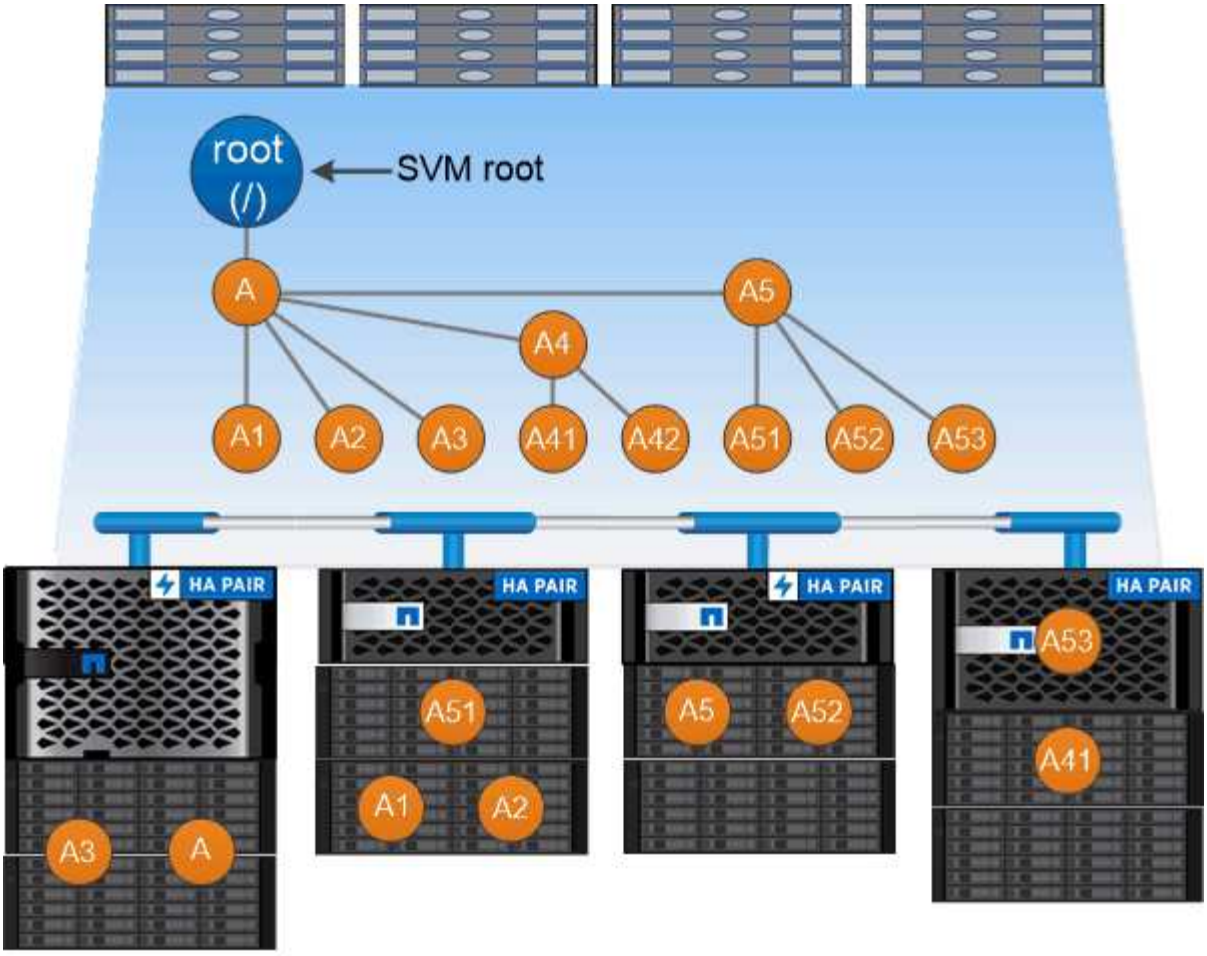
nas_namespace _ は、 _junction points_to によって結合されたボリュームを論理的にグループ化して、単一のファイルシステム階層を作成します。十分な権限を持つクライアントは、ストレージ内のファイルの場所を指定せずにネームスペース内のファイルにアクセスできます。ジャンクションされたボリュームはクラスタ内の任意の場所に配置できます。

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た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、になることがあります `/vol1/vol2/vol3` または `/vol1/dir2/vol3` あるいは `/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上に作成します `/eng/home`：

```
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わせて、ネームスペースアーキテクチャを選択できます。

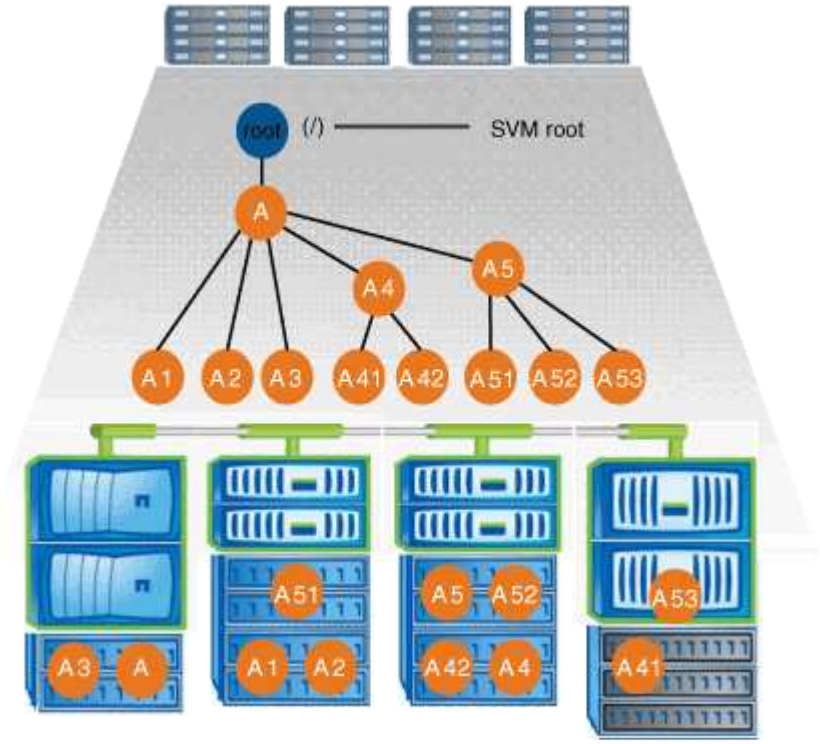
ネームスペースの最上位は常にルートボリュームであり、スラッシュ（ / ）で表されます。ルートの下位のネームスペースアーキテクチャは、次の 3 つの基本カテゴリに分類されます。

- ネームスペースのルートへのジャンクションポイントを 1 つ備えた単一のブランチツリー

- ネームスペースのルートへのジャンクションポイントを複数備えた複数分岐ツリー
- 複数のスタンドアロンボリュームがそれぞれ、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備えています

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は、結合されたボリュームまたはルートの下のディレクトリのどちらかになります。それ以外のすべてのボリュームは、単一の挿入ポイントの下のジャンクションポイント（ボリュームまたはディレクトリ）でマウントされます。

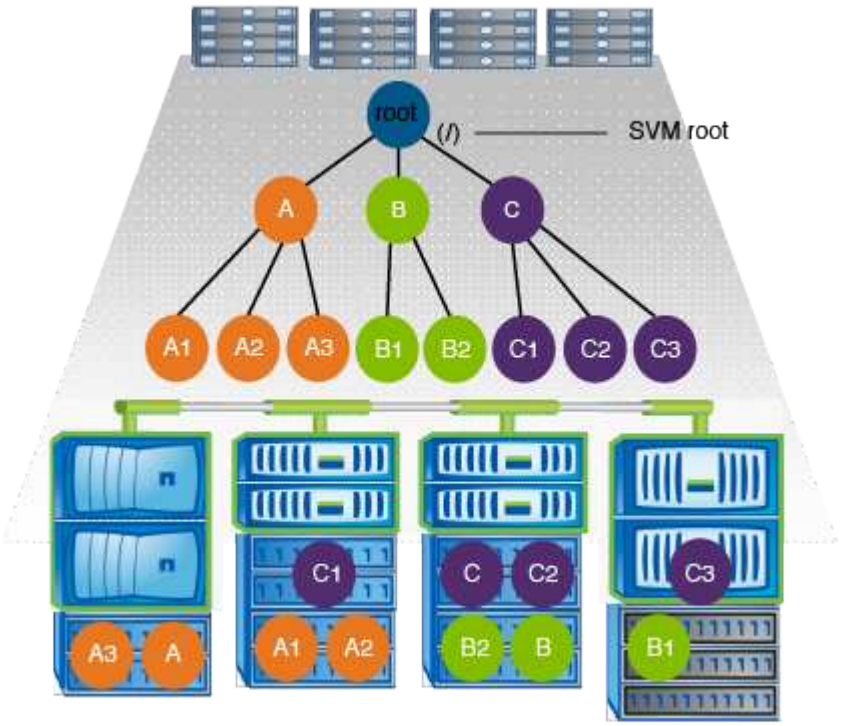


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、すべてのボリュームが単一の挿入ポイントの下で結合された以下のような構成になります。これは「 `d ATA` 」というディレクトリです。

```
                      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、ルート直下で結合されたボリュームまたはディレクトリのどちらかになります。それ以外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。

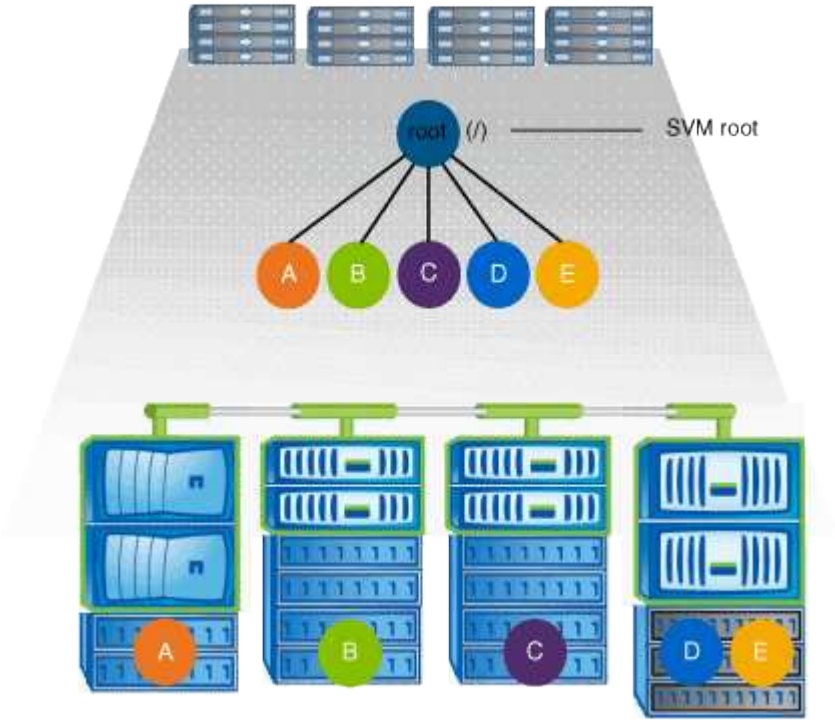


たとえば、上記のネームスペースアーキテクチャを使用する標準的なボリュームジャンクション構成は、SVM のルートボリュームへの 3 つの挿入ポイントがある以下のような構成になります。2 つの挿入ポイントは、「 `d ata" 」と「 projects' 」という名前のディレクトリです。挿入ポイントの 1 つは「 audit 」という名前の結合されたボリュームです。

```
                      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含むネームスペース

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。各ボリュームは一意のパスを持ち、ルート直下で結合されているか、ルートより下のディレクトリで結合されています。



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

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

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）。

- 承認

  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処理を実行する権限がエンティティにあるかどうかを判断します。アクセスは、 3 つのセキュリティレベルの評価後に有効な権限によって判断されます。

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

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

- ストレージレベルのアクセス保護のファイルおよびディレクトリセキュリティ

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

  > 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 のネイティブのファイルレベルのセキュリティ

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

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ためには、 NFS クライアントが正しく認証されている必要があります。ONTAP では、 UNIX クレデンシャルを設定されたネームサービスに照らしてチェックすることで、そのクライアントを認証します。

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

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

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およびクライアントに関する情報を取得します。ONTAP は、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うために、この情報を使用します。

ストレージシステムを設定するときに、 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 では、次のネームサービスをサポートしています。

- ローカルユーザ（ファイル）
- 外部 NIS ドメイン（ NIS ）
- 外部LDAPドメイン（LDAP）

を使用します `vserver services name-service ns-switch` ネットワーク情報を検索するソースとソースの検索順序をSVMに設定するコマンドファミリー。これらのコマンドは、と同等の機能を提供します `/etc/nsswitch.conf` UNIXシステム上のファイル。

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 がユーザクレデンシャルを適切にマッピングできるようにするには、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 "管理者認証と RBAC"。

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

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

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

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。その後、 ONTAP は、以降の参照用にこれらのクレデンシャルを内部のクレデンシャルキャッシュに格納します。NFS クレデンシャルキャッシュの仕組みを理解しておくと、パフォーマンスおよびアクセスに関する潜在的な問題に対処できます。

クレデンシャルキャッシュがないと、 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。
- ユーザの認証を行う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ち時間をなくすことで、ユーザアクセスが高速になります。

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、ユーザの最初の認証から 24 時間は、そのユーザからのすべてのアクセス要求で ONTAP はキャッシュされたクレデンシャルを使用します。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、次の 24 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

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、ユーザに対する最初のアクセス拒否から 2 時間は、そのユーザからのすべてのアクセス要求を ONTAP は拒否し続けます。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。それまでの 2 時間にネームサーバ上でクレデンシャルが変更された場合、 ONTAP は、次の 2 時間での使用に備えて、更新されたクレデンシャルをキャッシュします。

NAS ネームスペース内でデータボリュームを作成および管理します

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します

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。

作業を開始する前に

- 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トラッキングを有効にするには、を問題します `volume create` コマンドにを指定

します `-analytics-state` または `-activity-tracking-state` をに設定します `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 "File System Analytics を有効にします"。

> 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指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、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は任意です。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に適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームには適切でないセキュリティ形式である場合もあります。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、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。 `/ENG` はと同じです `/eng`。CIFS 共有を作成する場合、 Windows では、ジャンクションパスがあたかも大文字と小文字の区別があ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などです `/ENG`SMB共有のパスはで始まる必要があります `/ENG`ではありません `/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。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

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 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上に作成します `/eng/home`：

```
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

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、 NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

- 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トラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `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 "File System Analytics を有効にします"。

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に適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームには適切でないセキュリティ形式である場合もあります。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、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。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

2. ジャンクションポイントが設定されていないボリュームが作成されたことを確認します。

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data           RW_volume
vs1       home4       true     /eng/home       RW_volume
vs1       vs1_root    -        /               -
vs1       sales       -        -               -
```

NAS ネームスペース内の既存のボリュームをマウントまたはアンマウントします

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。ボリュームはアンマウントすることもできます。

このタスクについて

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。

> NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純に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、そのボリューム内のデータは失われません。また、既存のボリュームエクスポートポリシーおよびボリュームまたはディレクトリ上に作成された SMB 共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすれば、 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内のデータにアクセスできるようになります。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

ボリュームをアンマウントします	`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に関する情報を表示します

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。また、ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、 SVM ネームスペースを理解し、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、の有効なフィールドを表示できます `-fields` パラメータを指定するには、次のコマンドを使用します。 `volume show -fields ?` b. を使用して、必要な情報を表示します `-fields` パラメータ： `volume show -vserver vserver_name -fields fieldname,…`

例

次の例は、 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
```

セキュリティ形式を設定する

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、セキュリティ形式ごとに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	
混在	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
統合：（ONTAP 9.4以前のリリースでは、Infinite Volume のみ）。	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

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

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。

ONTAP 9.2以降では、 `show-effective-permissions` パラメータをに設定します `vserver security file-directory` コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindows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も指定します `-share-name` 有効な共有権限を表示できます。

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

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します

ボリュームで使用するセキュリティ形式を決定するには、 2 つの要素を考慮する必要が

あります。第 1 の要素は、ファイルシステムを管理する管理者のタイプです。第 2 の要素は、ボリューム上のデータにアクセスするユーザまたはサービスのタイプです。

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して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。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「 UNIX 」	• ファイルシステムが UNIX 管理者によって管理される。 • ユーザの大半が NFS クライアントである。 • データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。
NTFS	• ファイルシステムは 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、サービスアカウントとして Windows ユーザが使用される。
混在	• ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式は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て UNIX アクセス権を管理します

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 ルートボリュームのセキュリティ形式を設定する

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. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

   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、です `unix`、 `ntfs`または `mixed`。

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 ボリュームのセキュリティ形式を設定する

Storage Virtual Machine （ SVM ）の FlexVol 上のデータに使用するアクセス権のタイプを決定するには、 FlexVol のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	`volume create` を含めます `-security-style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume modify` を含めます `-security-style` セキュリティ形式を指定するパラメータ。

   FlexVol のセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs``または `mixed`。

   FlexVol ボリューム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。

   詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください "論理ストレージ管理"。

2. 作成した FlexVol ボリューム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 にセキュリティ形式を設定する

qtree 上のデータに使用するアクセス権のタイプを決定するには、 qtree のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
はまだ存在しません	`volume qtree create` を含めます `-security-style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume qtree modify` を含めます `-security-style` セキュリティ形式を指定するパラメータ。

   qtreeセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs``または `mixed`。

   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`。

詳細については、を参照してください `volume qtree create` または `volume qtree modify` コマンド、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 の概要を使用したファイルアクセスのセットアップ

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。環境の現在の設定によっては、さらにいくつかの手順を実行することもできます。

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

1. SVM で NFS プロトコルを有効にします。

   クライアントからの 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 サーバを作成します。

   NFS サーバは、 NFS 経由のファイル提供を可能にする 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。

   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には、エクスポートポリシーを設定する必要があります。

4. ネットワークおよびストレージの環境に応じて、適切なセキュリティおよびその他の設定を使用して NFS サーバを設定します。

   この手順には、Kerberosの設定、 "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。

エクスポートポリシーを使用して NFS アクセスを保護

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は、すべてのアクセスが暗黙的に拒否されます。

エクスポートポリシーは、 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、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ます `default` SVMのルートボリュームに対して実行します。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済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントにアクセスを許可するエクスポートルールが少なくとも 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に処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールの権限が使用され、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、クライアントの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。たとえば、 NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

  の最大サイズ `-clientmatch` フィールドは4096文字です。

- Kerberos v5 、 NTLM 、 AUTH_SYS など、クライアントが認証に使用するセキュリティタイプ。

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、すべてのルール違反をエラールールリストに記録することができます。。 `vserver export-policy config-checker` コマンドを実行するとチェッカーが呼び出されて結果が表示され、設定を検証したり、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、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv3 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.17.37 です。

クライアントアクセスプロトコルが一致していても、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アドレスとは別のサブネットに属しています。そのため、クライアントは一致しなくなり、このルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントの IP アドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。セキュリティタイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

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 アドレスは一致しています。読み取り専用パラメータでは、認証に使用する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。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、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

リストにないセキュリティタイプを使用するクライアントを管理します

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、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` にアクセスパラメータを指定します。

クライアントは、別のセキュリティタイプで認証されているか、まったく認証されていない（セキュリティタイプ AUTH_NONE ）場合に、アクセスパラメータで指定されていないセキュリティタイプを使用しているとみなされます。デフォルトでは、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、オプションは追加できます `none` をアクセスパラメータに追加します。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、拒否されずに匿名ユーザ ID にマッピングされます。。 `-anon` パラメータは、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。に指定されたユーザID `-anon` パラメータは、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。

に有効な値 `-anon` パラメータの範囲はからです `0` 終了： `65535`。

に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、このユーザに対して設定された権限に応じてアクセスできるようになります。
`65534`	クライアントアクセス要求はユーザ nobody にマッピングされ、このユーザに対して設定されたアクセス権に応じてアクセスできるようになります。これがデフォルトです。

に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
`65535`	この ID にマッピングされていて、クライアントがセキュリティタイプ AUTH_NONE を使用している場合、クライアントからのアクセス要求は拒否されます。ユーザ ID が 0 のクライアントからのアクセス要求は、この ID にマッピングされ、他のセキュリティタイプをクライアントが使用している場合、拒否されます。

オプションを使用する場合 `none`では、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。

読み取り専用にはが含まれます `none`	読み取り/書き込みに含まれます `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	はい。	最初に読み取り専用が処理されるため、拒否されました
はい。	いいえ	匿名として読み取り専用です
はい。	はい。	匿名として読み書き可能です

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

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

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、 AUTH_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り

専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスがすべてのセキュリティタイプに許可されていますが、この場合は、読み取り専用ルールですでにフィルタされている環境クライアントのみが許可されます。

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 / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

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

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、読み取り専用アクセスが、 AUTH_SYS で認証された、自身のユーザ ID を持つクライアントに許可されています。読み取り専用パラメータでは、ユーザ ID が 70 の匿名ユーザとしての読み取り専用アクセスが、他のセキュリティタイプを使用して認証されたクライアントに許可されています。読み取り / 書き込みパラメータでは、匿名ユーザとしてのみ読み取り / 書き込みアクセスが許可されています。

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

セキュリティタイプによるクライアントアクセスレベルの決定方法

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

アクセスレベルには、次の 3 つがあります。

1. 読み取り専用です
2. 読み書き可能です
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	読み取り専用です (`-rorule`)
標準ユーザの読み取り / 書き込み	読み取り専用です (`-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です	読み取り専用です (`-rorule`）および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`）および `-superuser`

次に、これらの 3 つのアクセスパラメータのそれぞれで有効なセキュリティタイプを示します。

- `any`
- `none`
- `never`

  このセキュリティタイプは、では使用できません `-superuser` パラメータ

- `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`。	で指定されたユーザIDを持つ匿名ユーザとして、そのレベルのアクセス権を取得します `-anon` パラメータ

クライアントのセキュリティタイプ	クライアント
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、には適用されません -superuser パラメータには常にが含まれているためです none 指定されていない場合でも。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

クライアント #1 は、 IP アドレスが 10.1.16.207 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

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

3 つすべてのクライアントで、クライアントアクセスプロトコルと IP アドレスは一致しています。読み取り専用パラメータでは、セキュリティタイプに関係なく、読み取り専用アクセスがすべてのクライアントに許可されています。読み取り / 書き込みパラメータでは、読み取り / 書き込みアクセスが、 AUTH_SYS または Kerberos v5 で認証された、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。スーパーユーザパラメータでは、スーパーユーザアクセスが、 Kerberos v5 で認証された、ユーザ ID が 0 のクライアントに許可されています。

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

スーパーユーザ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、は指定できます - superuser ユーザIDが0のクライアントの処理方法（セキュリティタイプに応じて）を決定す

るエクスポートルールのパラメータ。で有効なオプションは次のとおりです `-superuser` パラメータ：

- `any`
- `none`

  これは、を指定しない場合のデフォルト設定です `-superuser` パラメータ

- `krb5`
- `ntlm`
- `sys`

ユーザIDが0のクライアントは、に応じて2つの方法で処理されます `-superuser` パラメータ設定：

状況に応じて **-superuser** パラメータおよび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	で指定されたユーザIDを持つ匿名ユーザとしてアクセスを取得します `-anon` パラメータとその割り当てられた権限。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ません `none`。

クライアントがNTFSセキュリティ形式およびのボリュームにアクセスするためにユーザID 0を提示する場合 `-superuser` パラメータはに設定されます `none`ONTAP では、匿名ユーザがネームマッピングを使用して適切なクレデンシャルを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

クライアント#1は、IPアドレスが10.1.16.207、ユーザIDが746で、NFSv3プロトコルを使用してアクセス要求を送信し、Kerberos v5で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

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 アドレスは一致しています。読み取り専用パラメータでは、認証に使用する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。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、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。

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。代わりに、が原因で匿名にマッピングされます `-superuser` パラメータが指定されていません。つまり、デフォルトはです `none` ユーザID 0を匿名に自動的にマッピングします。また、クライアント #2 はセキュリティタイプが読み取り / 書き込みパラメータと一致しなかったため、読み取り専用アクセス権のみを取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

クライアント #1 は、 IP アドレスが 10.1.16.207 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 、ユーザ ID が 0 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、 AUTH_SYS で認証されます。

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 アドレスは一致しています。読み取り専用パラメータでは、認証に使用する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。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、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

このエクスポートルールでは、ユーザ ID が 0 のクライアントにスーパーユーザアクセスが許可されています。クライアント#1は、読み取り専用およびのユーザIDおよびセキュリティタイプと一致するため、スーパーユーザアクセスを取得します `-superuser` パラメータクライアント#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` パラメータ代わりに、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
にアクセスします	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
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を制御するパラメータがいくつかあります。これらのパラメータの仕組みを理解すると、各パラメータを変更してアクセスキャッシュを調整し、パフォーマンスと格納される情報の鮮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 へのアクセスを試みるクライアントに適用される 1 つ以上のエクスポートルールで構成され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定され、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を発生させなかったアクセスキャッシュエントリです。	最小値： 300 最大値： 86 、 400 デフォルト値は 3,600 です。

負のエントリ	クライアントへのアクセス拒否を発生させたアクセスキャッシュエントリです。	最小：60 最大値： 86 、 400 デフォルト値は 3,600 です。

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、エクスポートポリシールールに対するクライアントのマッチングを行い、クライアントがエクスポートポリシールール設定に基づいてアクセスを行っ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特定の期間使用されていない既存のアクセスキャッシュエントリをクリアするための追加のパラメータがあります。これ `-harvest-timeout` 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。これは、を使用して実行できます `volume qtree modify` コマンドにを指定します `-export-policy` パラメータと空の名前文字列（""）。

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 を検証します

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、を変更します `-validate-qtree-export` パラメータこのパラメータはデフォルトで有効になっています。

このタスクについて

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	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. admin 権限レベルに戻ります。

   ```
   set -privilege admin
   ```

FlexVol のエクスポートポリシーの制限とネストされたジャンクション

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

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

NFS で **Kerberos** を使用してセキュリティを強化する

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対して強力でセキュアな認証を提供します。認証により、ユーザおよびプロセスの ID をサーバで検証できます。ONTAP 環境では、 Storage Virtual Machine （ SVM ）と NFS クライアント間の認証を Kerberos で実行できます。

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 では、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）とデータ整合性に関する理由（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）の両方で有用です。

- プライバシーチェック機能を備えた Kerberos 5 認証（ krb5p ）

krb5p では、クライアントとサーバ間のすべてのトラフィックがチェックサムで暗号化されます。これにより、安全性が向上し、負荷も増加します。

- 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 設定に関してクラスタ管理者に頼る必要がなくなり、個別の Kerberos Realm 設定をマルチテナンシー環境で作成することができます。

NFS で **Kerberos** を設定するための要件

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

> 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 などのバージョンや種類によって異なります。これらのすべての変数については、本ドキュメントでは説明していません。詳細については、各コンポーネントの該当するドキュメントを参照してください。
>
> Windows Server 2008 R2 の Active Directory および Linux ホストを使用する環境での ONTAP と Kerberos 5 および NFSv3 / NFSv4 の設定方法に関する詳しい例については、テクニカルレポート 4073 を参照してください。

次の項目を最初に設定する必要があります。

ネットワーク環境の要件

- Kerberos

  Kerberos を Key Distribution Center （ KDC ；キー配布センター）で設定しておく必要があります（たとえば、 Windows Active Directory ベースの Kerberos または MIT Kerberos ）。

  NFSサーバはを使用する必要があります `nfs` マシンプリンシパルの主要コンポーネントとして使用します。

- 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する必要があります。

- NTP

  タイムサーバで NTP を実行している必要があります。これは、時刻のずれによる Kerberos 認証の失敗を回避するために必要です。

- ドメイン名解決（ DNS ）

  それぞれの UNIX クライアントおよび SVM LIF について、 KDC の前方参照ゾーンと逆引き参照ゾーンに適切なサービスレコード（ SRV ）が登録されている必要があります。すべてのコンポーネントを DNS で正しく解決できる必要があります。

- ユーザアカウント

  各クライアントについて、 Kerberos Realm のユーザアカウントが必要です。NFS サーバでは ' マシン・プリンシパルの主要コンポーネントとして NFS' を使用する必要があります

NFSクライアントの要件

- NFS

  NFSv3 または NFSv4 を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

  クライアントで RFC1964 および RFC2203 がサポートされている必要があります。

- Kerberos

  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。

    非常にセキュリティ性の高い 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：

  - 走らないでください `gssd` を使用 `-n` パラメータ
  - 走らないでください `kinit` をrootユーザとして指定します。

- 各クライアントは、最新かつ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 での AES 暗号化の互換性と信頼性が最大限確保されます。

- DNS

  DNS を使用して名前が正しく解決されるように各クライアントが適切に設定されている必要があります。

- NTP

  各クライアントが NTP サーバと同期されている必要があります。

- ホストおよびドメインの情報

  各クライアントの `/etc/hosts` および `/etc/resolv.conf` ファイルには正しいホスト名とDNS情報が格納されている必要があります。

- keytab ファイル

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

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

ストレージシステムの要件

- NFS ライセンス

  ストレージシステムに有効な NFS ライセンスがインストールされている必要があります。

- CIFSライセンス

  CIFS ライセンスはオプションです。マルチプロトコルのネームマッピングを使用する場合にのみ、Windows クレデンシャルをチェックする必要があります。純粋な UNIX のみの環境では必要ありません。

- SVM

  システムで SVM を少なくとも 1 つ設定しておく必要があります。

- SVM で DNS を設定します

  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得るために、 Kerberos で AES-256 暗号化のみを許可するように NFS サーバを設定する必要があります。

- SMBサアハ

  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。

- 個のボリューム

  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	root または ID 0
GID	root または ID 0
UNIX 権限	777

ルートボリュームとは異なり、データボリュームのセキュリティ形式は任意に設定できます。

- 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.
ルート	0
pcuser	65534 （ SVM を作成すると ONTAP で自動的に作成されます）

- UNIXユーザ

  SVM で次の UNIX ユーザを設定しておく必要があります。

ユーザ名	ユーザ **ID**	プライマリグループ **ID**	コメント（ **Comment** ）
NFS	500ドル	0	GSS INITフェーズで必要 NFS クライアントユーザの SPN の最初のコンポーネントがユーザとして使用されます。
pcuser	65534	65534	NFS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。

ユーザ名	ユーザ **ID**	プライマリグループ **ID**	コメント（ **Comment** ）
ルート	0	0	マウントに必要

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

- エクスポートポリシーとルール

  ルートボリュームと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、エクスポートルールのオプションを設定できます `-rorule`、 `-rwrule`および `-superuser` ルートボリュームのをに設定します `krb5` 、 `krb5i`または `krb5p`。

- Kerberos-UNIX ネームマッピング

  NFS クライアントユーザの SPN によって識別されたユーザに root 権限を持たせる場合は、 root に対するネームマッピングを作成する必要があります。

関連情報

"ネットアップテクニカルレポート 4073 ：『 Secure Unified Authentication 』"

"NetApp Interoperability Matrix Tool で確認できます"

"システム管理"

"論理ストレージ管理"

NFSv4 のユーザ ID ドメインを指定します

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

このタスクについて

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、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する必要があります。これは 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 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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。ONTAPクラスタにCA署名済みサーバ証明書を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。

- 各証明書は、NFSサーバ（TLSを有効または設定するデータLIF）のFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を共通名（CN）として設定する必要があります。
- 各証明書には、サブジェクト代替名（SAN）としてNFSサーバ（またはその両方）のIPアドレスまたはFQDNを設定する必要があります。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。

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。有効になっている既存のStorage VMでこの設定を行うことができます： "NFS"。

> ONTAP 9.15.1では、NFS over TLSがパブリックプレビューとして提供されています。プレビュー版として、ONTAP 9.15.1では本番ワークロードでNFS over TLSはサポートされていません。

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。

作業を開始する前に

- を参照してください "要件" （NFS over TLSの場合）を参照してください。
- 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。

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

```
vserver nfs tls interface show
```

例

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

```
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を無効にする

転送中のデータのセキュリティを強化する必要がなくなった場合は、NFSクライアントのTLSを無効にすることができます。

作業を開始する前に

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。

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

```
vserver nfs tls interface show
```

例

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

```
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

NFS over TLSの既存の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。

作業を開始する前に

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。

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 `status` の `enable`を指定する必要があります。 `certificate-name` パラメータ括弧<>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. を使用します `vserver nfs tls interface show` コマンドを使用して結果を表示します。

```
vserver nfs tls interface show
```

例

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

```
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.
```

ネームサービスを設定

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、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` UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

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番で参照するかを決定します。ONTAP では、 SVM ごとに個別のネームサービススイッチテーブルが保持されます。

データベースタイプ

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

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、 DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます

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
namemap	ユーザ名のマッピング	ファイル、 LDAP

ソースタイプ

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

ソースタイプ	情報の検索先	使用するコマンド

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

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

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります `files` また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

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へのアクセスに次のプロトコルを使用します。

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

例

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

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

ホストの IP アドレスの検索では、 ONTAP は最初にローカルのソースファイルを参照します。結果が返されない場合は、次に DNS サーバが照会されます。

ユーザまたはグループ情報の検索では、 ONTAP はローカルのソースファイルだけを参照します。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の検索では、 ONTAP が最初に外部 NIS サーバを参照し、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照会されます。

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含まれていません。そのため、 ONTAP はデフォルトでローカルのソースファイルだけを参照します。

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

LDAP を使用する

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 サーバに保存する場合、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。

- LDAP for ONTAP を設定する前に、サイト環境が LDAP サーバおよびクライアント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 クライアント上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ている LDAP ユーザパスワードハッシュタイプには、 ONTAP でサポートされてい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 サーバに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（データの整合性チェックを提供）および LDAP の署名と封印（データの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、次のサービスが設定されている必要があります。

- LDAP サーバで GSSAPI （ Kerberos ） SASL がサポートされている必要があります。
- LDAP サーバに、 DNS A/AAAA レコード、および 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、 DNS サーバ上に存在する SRV レコードが必要です。

◦ TLS または LDAPS を開始できるようにするには、次の点を考慮する必要があります。

- ネットアップでは、 LDAPS ではなく Start TLS を使用することを推奨します。
- LDAPS を使用している場合は、 ONTAP 9.5 以降で LDAP サーバの TLS または SSL が有効になっている必要があります。ONTAP 9.0~9.4 では SSL はサポートされません。
- 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）、次の条件を満たしている必要があります。

- 両方のドメインで、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。一次は紹介ドメインを信頼します
  - 親子
- 参照されているすべてのサーバ名を解決するように DNS が設定されていること。
- の認証では、ドメインパスワードが同じである必要があります `--bind-as-cifs-server` trueに設定します。

> 次の設定は LDAP リファーラル追跡でサポートされません。
>
> ◦ 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（ `-use-ldaps-for-ad-ldap` オプション）

- ONTAP 9.11.1以降では、を使用できます "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しています。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。

- LDAP をホスト名解決に使用することはサポートされていません。

追加情報の場合は、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 ）サーバへの照会に対する 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、シークレットキーの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`。テスト

SMBトラフィックに対するLDAPの署名と封印は、を使用してSVMで有効にします `-session-security -for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

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 は、 Active Directory 統合 LDAP サーバ間または UNIX ベース LDAP サーバ間の認証されたセッションの設定に Start TLS または LDAPS を使用できます。

用語集

ONTAP での LDAP 通信の保護に LDAPS を使用する方法に関して理解しておくべき用語があります。

- * LDAP *

  （ Lightweight Directory Access Protocol ）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です。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たり LDAP クライアントからの要求を満たしたりするディレクトリサービスも提供します。

- **SSL**

  （ Secure Sockets Layer ）インターネット上で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ました。

- * tls *

  （ Transport Layer Security ）従来の SSL 仕様に基づいた IETF 標準の追跡プロトコルです。SSL の後継にあたります。TLSはONTAP 9.5以降でサポートされます。

- * 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ます。

- ONTAP 9.5-9.8 では、 LDAPS はポート 636 でのみ有効にできます。そのためには、を使用します `-use-ldaps-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します
- 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。これを行うには、を設定します `-ldaps-enabled` パラメータの値 `true` そして目的のものを指定してください `-port` パラメータ詳細については、を参照してください `vserver services name-service ldap client create` のマニュアルページ

ネットアップでは、 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。この認証により、 SVM の LDAP クライアントは、バインド操作時に LDAP サーバの ID を確認できます。TLS に対応した LDAP クライアントは、公開鍵暗号化の標準的な技法を使用して、サーバの証明書および公開 ID が有効であり、かつクライアントの信頼できる Certificate Authority （ CA ；認証局）のリストにある CA によって発行されたものであるかどうかをチェックできます。

LDAP では、 TLS を使用した通信の暗号化方法として STARTTLS がサポートさ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 では次の機能がサポートされます

- Active Directory 統合 LDAP サーバと SVM の間の SMB 関連トラフィックに使用する LDAPS
- LDAPS ：ネームマッピングやその他の UNIX 情報で使用する LDAP トラフィックに使用します

  Active Directory 統合 LDAP サーバまたは UNIX ベース 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ユーザ、グループ、ネットグループなどのその他の UNIX 情報の格納に使用できます。

- 自己署名ルート CA 証明書

  Active-Directory 統合 LDAP を使用している場合は、 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自己署名ルート証明書が生成されます。UNIX ベースの LDAP サーバを LDAP ネームマッピングに使用している場合は、該当する LDAP アプリケーションに適切な手段を使用して、自己署名ルート証明書の生成と保存が行われます。

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 を使用するとともに、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を必要とする場合は、 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うち、使用するいずれか 1 つのコピーを作成しておく必要があります。

このタスクについて

LDAP クライアントスキーマでは、グループオブジェクトによって memberUid 属性が使用されます。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を一覧表示できます。RFC2307bis 対応の LDAP クライアントスキーマでは、グループオブジェクトによって 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 Distinguished Name （ DN ；識別名）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。

このユーザは、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 は、この 256 グループの上限を超えるグループをすべて無視します。

デフォルトでは、 RFC2307bis サポートが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 では RFC2307bis サポートが自動的に有効になります。

追加情報の場合は、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
```

LDAP ディレクトリ検索の設定オプション

環境にとって最も適切な方法で 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、およびネットグループ情報を含め、 LDAP ディレクトリ検索を最適化することができます。デフォルトの LDAP ベースおよびスコープ検索値で十分な状況や、カスタム値のほうが適切な場合に指定すべきパラメータを理解しておく必要があります。

ユーザ、グループ、およびネットグループ情報の LDAP クライアント検索オプションは、 LDAP クエリの失敗、ひいてはストレージシステムへのクライアントアクセスの失敗を回避するのに役立ちます。また、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、検索をできるだけ効率的に行うことができます。

デフォルトのベースおよびスコープ検索値です

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

カスタムベース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 クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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 クエリを実行するため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行われます。LDAP クエリによる検索範囲を、名前付きエントリのみ、 DN の 1 レベル下にあるエントリ、または DN の下にあるサブツリー全体のどれにするかが決定されます。

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、各クエリで DN の下にあるサブツリー全体が検索されます。これにより、 LDAP クエリが成功する見込みは最大になりますが、非効率的であったり、大規模な LDAP ディレクトリではパフォーマンスの大幅な低下につながったり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。クエリの検索ベースとクエリをこうした形で制限すると、検索対象が 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、パフォーマンスを大幅に向上させることができます。

カスタムベースおよびスコープ値を指定した場合、ユーザ、グループ、およびネットグループ検索の一般的なデフォルト検索ベースおよびスコープは無視されます。カスタムベースおよびスコープ値を指定するパラメータは、 advanced 権限レベルで使用できます。

LDAP クライアントパラメータ	カスタム指定要素
`-base-dn`	すべての LDAP 検索のベース DN 複数の値を必要に応じて入力できます（ ONTAP 9.5 以降のリリースで LDAP リファーラル追跡を有効にした場合など）。

`-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、環境ユーザ名マッピング検索も行います。
`-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、環境ユーザ名マッピング検索も行います。
`-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 ディレクトリが複雑な場合は、特定の情報を求めて 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 の指定が必要になることがあります。複数のユーザ、グループ、およびネットグループ DN パラメータを指定するには、各パラメータをセミコロン（ ; ）で区切り、 DN 検索リスト全体を二重引用符（ " ）で囲みます。DN にセミコロンが含まれている場合は、 DN 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。

scope 環境は、対応するパラメータに指定されている のリスト全体を表します。たとえば、 3 つの異なるユーザ DN のリストとサブツリーをユーザスコープで指定した場合は、 LDAP ユーザ検索により、指定された 3 つの DN のそれぞれでサブツリー全体が検索されます。

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、このリファーラルデータに記載されたサーバからターゲットオブジェクトを取得します。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は、（を使用して）リファーラル追跡が有効になっている場合にのみ検索されます `-referral-enabled true` オプション）LDAPクライアントの作成時または変更時

LDAP ディレクトリのホスト単位ネットグループ検索のパフォーマンスを向上させます

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することができます。これにより、ネットグループ検索の処理速度を大幅に引き上げ、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を減らすことができます。

必要なもの

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

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

ネットグループ内の IPv6 アドレスを指定するときは、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。

このタスクについて

NISサーバは、と呼ばれる3つの個別のマップにネットグループ情報を格納します `netgroup`、`netgroup.byuser`および `netgroup.byhost`。の目的 `netgroup.byuser` および `netgroup.byhost` マップはネットグループ検索を高速化するためのものです。ONTAP 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ディレクトリにはそのようなはありません `netgroup.byhost` NISサーバと同様のマッピングただし、サードパーティのツールを使用すると、NISをインポートできます `netgroup.byhost` LDAPディレクトリにマッピングして、ホスト単位の高速ネットグループ検索を有効にします。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、を使用してONTAP LDAPクライアントを設定できます `netgroup.byhost` ホスト単位のネットグループ検索を高速化するために、名前、DN、および検索範囲をマッピングします。

ホスト単位のネットグループ検索の結果をより迅速に受け取ることで、 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場合、より高速にエクスポートルールを処理できます。これにより、ネットグループ検索による遅延の問題によってアクセスが遅延する可能性が低下します。

手順

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

   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` の識別名を指定します `netgroup.byhost` LDAPディレクトリにマッピングします。これにより、ホスト単位のネットグループ検索のベース DN が無効になります。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、デフォルトのが使用されます `subtree`。

   LDAPクライアント設定がまだ存在しない場合は、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` コマンドを実行します

ONTAP 9.2以降では、フィールドが表示されます `-ldap-servers` フィールドを置き換えます `-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」という名前の既存のLDAPクライアント設定を変更して、を使用したホスト単位のネットグループ検索を有効にします `netgroup.byhost` 「`nisMapName="netgroup.byhost"`、`dc=corp`、`dc=example`、`dc=com`」という名前のマップとデフォルトの検索範囲 `subtree`：

```
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
```

完了後

。 `netgroup.byhost` および `netgroup` クライアントアクセスの問題を回避するために、ディレクトリ内のマップは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できます

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。

このタスクについて

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サーバで管理ユーザを認証します。この認証方式では、ONTAP がユーザまたはグループの名前を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、サーバのハッシュコードを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と比較します。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 はセキュアな接続を介してLDAPサーバにユーザクレデンシャル（ユーザ名とパスワード）のみを送信します。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、LDAPサーバでサポートされるすべての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。パスワードハッシュはLDAPサーバによって実行されるためです。

"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クライアントがTLSまたはLDAPS用に設定されていることを強く推奨します。設定されていない場合は、パスワードが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）データベースに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てnsswitch認証を行うには、ONTAP 管理者ユーザアカウントとグループ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管理者に確認してください。
2. ONTAP 管理者ユーザクレデンシャルがLDAPサーバで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リスト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. 確認してください `ldap` は、nsswitchに設定されているソースの1つです `passwd` データベースに次のように入力します

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

   "nsswitch設定の詳細は、こちらをご覧ください。"

4. 管理ユーザがnsswitchで認証されていること、およびアカウントでLDAP高速バインド認証が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、と入力します `security login modify` 次のパラメータ設定を確認します。

     ```
     -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統計を表示します。

ONTAP 9.2 以降では、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 LDAP 統計を表示することができます。

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、オブジェクトのパフォーマンスデータを表示します `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance “vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1”

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                              Value
-------------------------------- --------------------------------
instance_name                        vserverName:LDAP (NIS & Name
                                     Mapping):GetUserInfoFromName:
                                     1.1.1.1
last_modified_time                   1460610787
node_name                            nodeName
num_not_found_responses              1
num_request_failures                 1
num_requests_sent                    1
num_responses_received               1
num_successful_responses             0
num_timeouts                         0
operation                            GetUserInfoFromName
process_name                         secd
request_latency                      52131us
```

ネームマッピングを設定する

ネームマッピングの概要を設定する

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 環境を構成しており、ボリュームに対して SMB アクセスや 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ている場合。

  このシナリオでは、すべてのクライアントクレデンシャルを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ません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、 SALES という単語が先頭または末尾に付くすべての AD ユーザを、特定の UNIX ユーザおよびそのユーザの UID にマッピングできます。

ネームマッピングの仕組み

ONTAP がユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、 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 ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。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。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。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、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、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。

  マシンアカウントに定義されているネームマッピングがあっても無視されます。

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 に与える影響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 上の 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しています。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、ホームドメインと他方のドメインの間に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、ホームドメインが他方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

  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しているユーザを認証または認可できません。

  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のためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、 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容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（ **Pattern** ）	交換	結果
ルート	｛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。

パターン（ **Pattern** ）	交換	結果
*	｛Asterisk｝ ｛backslash｝ ｛backslash｝ ｛Asterisk｝	有効な UNIX ユーザは、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

マルチドメインの名前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方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

ユーザ名のドメインセクションにワイルドカードを使用して UNIX ユーザが Windows ユーザにマッピングされている場合、 Windows ユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先の Windows ユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザ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は、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` プログラム。

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュリティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

このタスクについて

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
   ```

   > 。 `-pattern` および `-replacement` ステートメントは正規表現として記述できます。を使用することもできます `-replacement` null置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント `" "` （スペース文字）。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

   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、優先順位リスト内での位置は 1 番目です。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
```

デフォルトユーザを設定します。

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

このタスクについて

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

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

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 ユーザを設定します	`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します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`

2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリ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します	`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します

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。

このタスクについて

デフォルトでは、 Windows NFSv3 クライアントサポートが無効になっています。

作業を開始する前に

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、を無効にします `-enable-ejukebox` および `-v3-connection-drop` パラメータ：

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

   これで、 Windows NFSv3 クライアントが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. 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` オプション

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します

NFSクライアントはを使用できます `showmount -e` 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します。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` のオプション `vserver nfs modify` コマンドは明示的に有効にする必要があります。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 を有効または無効にします

NFSv3を有効または無効にするには、を変更します `-v3` オプションこれにより、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 を有効にします	`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、 `-v4.0` オプションこれにより、 NFSv4.0 プロトコルを使用してクライアントがファイルにアクセスできるかどうかを指定できます。ONTAP 9.9.1では、NFSv4.0がデフォルトで有効になります。それより前のリリースでは、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、 `-v4.1` オプションこれにより、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、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を表示します

。`vserver nfs storepool show` コマンドは、消費されたストレージプール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. 管理者としてを実行します `vserver nfs storepool show` コマンドを使用してNFSv4クライアントのstorepool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.
```

ストレージプール制限の制御を有効または無効にします

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します	`vserver nfs storepool config modify -limit-enforce enabled`
ストレージプール制限の制御を無効にします	`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します

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. を使用します `vserver nfs storepool blocked-client show` コマンドを使用してNFSv4ブロッククライアントリストを表示します。

ブロックされたクライアントリストからクライアントを削除します

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. を使用します `vserver nfs storepool blocked-client flush -client-ip <ip address>` コマンドを実行して、storepoolブロックされたクライアントキャッシュをフラッシュします。
2. を使用します `vserver nfs storepool blocked-client show` コマンドを使用して、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 を有効または無効にします

pNFS は、 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し、ボトルネックとなる可能性がある NFS サーバをバイパスできるようにすることで、パフォーマンスを向上します。pNFS（Parallel NFS）を有効または無効にするには、を変更します `-v4.1-pnfs` オプション

ONTAP リリースの種類	**pNFS** のデフォルト値
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 を有効にします	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
pNFS を無効にします	`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** アクセスを制御します

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、を変更します `-tcp` および `-udp` パラメータを指定します。これにより、環境で 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。

このタスクについて

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

> コマンドの失敗を防ぐために、 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、コマンドを使用します `vserver snapdiff-rpc-server off -vserver vserver name`。

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** 要求を制御します

非予約ポートからのNFSマウント要求を拒否するには、を有効にします `-mount-rootonly` オプション非予約ポートからのすべてのNFS要求を拒否するには、を有効にします `-nfs-rootonly` オプション

このタスクについて

デフォルトでは、オプションです `-mount-rootonly` はです `enabled`。

デフォルトでは、オプションです `-nfs-rootonly` はです `disabled`。

これらのオプションは、 NULL 手順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します	`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します	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
非予約ポートからのすべての NFS 要求を許可します	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
非予約ポートからのすべての NFS 要求を拒否します	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

不明な **UNIX** ユーザ向けに、 **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。ONTAP は、セキュリティを厳しくするためにそのようなユーザに対してアクセスを拒否するように設定することも、そうしたユーザをデフォルトの Windows ユーザにマッピングしてすべてのユーザに最小限のレベルのアクセスを保証するように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。

このタスクについて

UNIX ユーザが NTFS セキュリティ形式のボリュームまたは qtree へのアクセスを試みる場合、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その UNIX ユーザの名前を検索できなかった場合、特定の Windows ユーザにその UNIX ユーザを明示的にマッピングすることができません。このような不明な UNIX ユーザの処理方法は、次の方法で決定できます。

- 不明な UNIX ユーザに対してアクセスを拒否する。

  この場合、 NTFS ボリュームまたは qtree へのアクセス権を取得するためにすべての UNIX ユーザに明示的なマッピングを要求することで、より厳しい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する。

  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	`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注意事項

。 `-mount-rootonly` 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、オプションを無効にする必要があります。Hummingbird クライアントや Solaris NFS / IPv6 クライアントがこれに該当します。

状況に応じて `-mount-rootonly` オプションが有効になっている場合、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クライアントでNFSエクスポートをマウントすることはできません。

ドメインを検証してネットグループのより厳密なアクセスチェックを実行します

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。

このタスクについて

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、を変更します `-netgroup-dns -domain-search` パラメータ。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。

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	`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 サービスで使用され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経由で NFS クライアントと通信します。デフォルトポートは、ほとんどの NFS 環境で正しく機能するので変更する必要はありませんが、別の NFS ネットワークポートを NFSv3 環境で使用する場合はそうすることができます。

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、変更に先立ってこの情報をユーザに伝えておく必要があります。

このタスクについて

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 （ NSM ；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	デフォルトのポート
`-mountd-port`	NFS マウントデーモン	635
`-nlm-port`	Network Lock Manager の略	4045
`-nsm-port`	Network Status Monitor サービスの略	4046
`-rquotad-port`	NFS クォータデーモン	4049

   デフォルトポートに加えて、 1 、 024~65 、 535 の範囲のポート番号を使用できます。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. を使用します `network connections listening show` ポート番号の変更を確認するコマンド。
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 サーバを管理するためのコマンドです

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 サーバを作成します	`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`

を非表示にします `.snapshot` NFSv3マウントポイント下のディレクトリリスト への明示的なアクセス `.snapshot` このオプションが有効になっていても、ディレクトリは許可されます。	`vserver nfs` を使用したコマンド `-v3-hide-snapshot` オプションを有効にします

詳細については、各コマンドのマニュアルページを参照してください。

ネームサービスの問題をトラブルシューティングする

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、を使用できます `vserver services name-service getxxbyyy` さまざまなネームサービス検索を手動で実行し、検索の詳細と結果を調べてトラブルシューティングに役立てるためのコマンドファミリー。

このタスクについて

- 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、想定されるネームサービス設定問題の検索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IDごとのグループのメンバー	`vserver services name-service getxxbyyy getgrbygid`

グループ名ごとのグループのメンバー	`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）
ユーザ名別のユーザ情報	`vserver services name-service getxxbyyy getpwbyname` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
ユーザIDごとのユーザ情報	`vserver services name-service getxxbyyy getpwbyuid` RBACユーザの名前解決をテストするには、を指定します `-use-rbac` パラメータの形式 `true`。
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、正しくない結果が得られました	DNS設定
検索で間違った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 、ルートなど）
ホスト名の検索に失敗したかタイムアウトになり、DNS の短縮名（例： host1 ）が DNS サーバで解決されない	Top-Level Domain（TLD；最上位レベルのドメイン）クエリのDNS設定。を使用して、TLDクエリを無効にできます `-is-tld-query-enabled false` オプションをに設定します `vserver services name-service dns modify` コマンドを実行します

関連情報

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスの接続を確認

ONTAP 9.2 以降では、 DNS ネームサーバと LDAP ネームサーバが ONTAP に接続されているかどうかを確認できます。これらのコマンドは admin 権限レベルで使用できます。

このタスクについて

DNS または LDAP ネームサービスの設定が有効かどうかは、必要に応じてネームサービス設定チェックを使用して確認できます。この検証チェックは、コマンドラインまたは System Manager で実行できます。

DNS 設定の場合、すべてのサーバがテストされ、設定が有効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 設定の場合は、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では、以外の設定チェックが適用されます `skip-config-validation` フィールドはtrue（デフォルトはfalse）です。

ステップ

1. 適切な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".                                              |
```

設定されているサーバ（ 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れば、設定の検証は成功です。到達不能なサーバがある場合は、警告が表示されます。

ネームサービススイッチエントリを管理するコマンド

ネームサービススイッチエントリは、作成、表示、変更、および削除することで管理できます。

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します	`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

"ネットアップテクニカルレポート 4668 ：『 Name Services Best Practices Guide 』"

ネームサービスキャッシュを管理するコマンド

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がキャッシュに保持される期間です。

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します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`
2 つのネームマッピングの位置を入れ替えます 注：ネームマッピングにIP修飾子エントリ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します	`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。

ローカル **UNIX** ユーザを管理するためのコマンド

ONTAP には、ローカル UNIX ユーザを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX ユーザを作成します	`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 ユーザを表示します	`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** グループを管理するためのコマンド

ONTAP には、ローカル UNIX グループを管理するための固有のコマンドが用意されています。

状況	使用するコマンド
ローカル UNIX グループを作成します	`vserver services name-service unix-group create`
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`
URI からローカル UNIX グループをロードします	`vserver services name-service unix-group load-from-uri`
ローカル UNIX グループを表示します	`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します	`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でき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	デフォルトの制限です	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。

このタスクについて

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`

状況	使用するコマンド
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`
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

URI からのロード、ノード間でのステータスの確認、表示、削除を行うことで、ローカルネットグループを管理できます。

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

詳細については、各コマンドのマニュアルページを参照してください。

NIS ドメイン設定を管理するコマンドです

ONTAP には、 NIS ドメイン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
NIS ドメイン設定を作成します	`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します	`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 権限レベル以上で使用できます。
NIS の統計を消去します	`vserver services name-service nis-domain clear-statistics` advanced 権限レベル以上で使用できます。
NIS ドメイン設定を変更する	`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でのキャッシュを有効にします	`vserver services name-service nis-domain netgroup-database config modify` advanced 権限レベル以上で使用できます。

詳細については、各コマンドのマニュアルページを参照してください。

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したり削除したりできません。

状況	使用するコマンド
LDAP クライアント設定を作成します	`vserver services name-service ldap client create`
LDAP クライアント設定を表示します	`vserver services name-service ldap client show`
LDAP クライアント設定を変更します	`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します	`vserver services name-service ldap client modify-bind-password`
LDAP クライアント設定を削除します	`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 設定を管理するためのコマンド

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 設定を作成します	`vserver services name-service ldap create`
LDAP 設定を表示します	`vserver services name-service ldap show`
LDAP 設定を変更します	`vserver services name-service ldap modify`
LDAP 設定を削除します	`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を管理するためのコマンド

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したり削除したりできません。

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

詳細については、各コマンドのマニュアルページを参照してください。

NFS Kerberos インターフェイス設定を管理するコマンドです

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 を有効にします	`vserver nfs kerberos interface enable`
NFS Kerberos インターフェイスの設定を表示します	`vserver nfs kerberos interface show`
NFS Kerberos インターフェイスの設定を変更します	`vserver nfs kerberos interface modify`
LIF で NFS Kerberos を無効にします	`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 設定を管理するコマンド

ONTAP には、 NFS Kerberos Realm の設定を管理するための固有のコマンドが用意されています。

状況	使用するコマンド
NFS Kerberos Realm の設定を作成します	`vserver nfs kerberos realm create`
NFS Kerberos Realm の設定を表示します	`vserver nfs kerberos realm show`
NFS Kerberos Realm の設定を変更します	`vserver nfs kerberos realm modify`
NFS Kerberos Realm の設定を削除します	`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を管理するためのコマンド

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します	`vserver export-policy show`
エクスポートポリシーの名前を変更します	`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を管理するためのコマンド

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します	`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を照合する同一のエクスポートルールが複数設定されている場合は、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必ず維持するようにしてください。

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を設定する

NFS クレデンシャルキャッシュの **Time-To-Live** を変更する理由

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

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 を長くして、 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これまで拒否されていた NFS ユーザに対してアクセスを許可する変更を行った。	キャッシュされている拒否されたクレデンシャルに対する TTL を短くして、 ONTAP ユーザ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 ユーザがアクセスできるようになるまでの待機時間を短縮します。
ネームサーバ管理者がこれまで許可されていた NFS ユーザに対してアクセスを拒否する変更を行った。	キャッシュされている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

受理および拒否のクレデンシャルをキャッシュしておく期間を個別に変更することができます。ただし、こうした変更の長所と短所の両方に注意する必要があります。

状況	利点は ...	欠点は ...
クレデンシャルのキャッシュ時間を長くしてください	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。	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が長くなります。
受理されたクレデンシャルのキャッシュ時間を短くします	それまではアクセスが許可されていたが今後は許可されなくなる NFS ユーザに対し、アクセスを拒否するのにかかる時間が短くなります。	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。	それまで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 ユーザに対し、アクセスを許可するのにかかる時間が長くなります。
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	それまで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 ユーザに対し、アクセスを許可するのにかかる時間が短くなります。	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** を設定してください

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である Time-To-Live （ TTL ）を設定できます。これにより、ネームサーバの高負荷に関する問題や、 NFS ユーザアクセスに影響を及ぼすクレデンシャルの変更に関する問題を軽減できます。

このタスクについて

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 の測定単位はミリ秒です。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。
拒否のクレデンシャルです	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL の測定単位はミリ秒です。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します

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します (`vserver export-policy cache flush`)古い可能性がある情報を削除し、ONTAP が適切な外部リソースから最新情報を取得するように強制します。これは、 NFS エクスポートへのクライアントアクセスに関するさまざまな問

題の解決に役立ちます。

このタスクについて

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
- ネームサーバでホスト名レコードが最近変更された
- ネームサーバでネットグループエントリが最近変更された
- ネットグループの完全なロードを妨げていたネットワーク停止からのリカバリが発生しました

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` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。
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` オプションのを指定できます `-node` アクセスキャッシュをフラッシュするノードを指定するパラメータ。

フラッシュ対象	入力するコマンド
ホスト名キャッシュ	`vserver services name-service cache hosts forward-lookup delete-all`
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ネットグループのキューとキャッシュを表示します

ONTAP では、ネットグループのインポート時および解決時にネットグループキューを使用し、結果として得られる情報を格納するためにネットグループキャッシュを使用します。エクスポートポリシーのネットグループ関連の問題をトラブルシューティングする場合は、を使用できます `vserver export-policy netgroup queue show` および `vserver export-policy netgroup cache show` ネットグループキューのステータスおよびネットグループキャッシュの内容を表示するコマンド。

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します

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場合は、を使用できます `vserver export-policy netgroup check-membership` 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するためのコマンド。

このタスクについて

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。を使用します `vserver export-policy netgroup queue show` ネットグループのロードを監視し、完了後にチェックを再試行するコマンド。

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。

このタスクについて

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、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、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 クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、 SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、 `rmdir`および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、 SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、 NFS の書き込みの処理はエラーになります。

UNIX セキュリティ形式のボリュームでは、 NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、 SMB のロック状態が考慮されます。

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 クライアントがこ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 では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因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原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって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。

の詳細を確認してください "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します

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。

このタスクについて

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` 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. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

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
```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。 `vserver locks break` コマンドは、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、を使用します `vserver locks show` コマンドを実行します

   詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、 LIF 名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロック ID	`vserver locks break -lockid UUID`

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 / 書き込み処理が監視対象イベントの場合、読み取り / 書き込み要求のトラフィックが多いと NFS クライアントで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に対して I/O を実行する際に、ファイルのハンドルを取得します。このハンドルは、サーバとクライアントのリブート後も有効なままになる場合があります。このため、クライアントはハンドルを自由にキャッシュし、ハンドルを再取得しなくても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。これらのすべての要求につい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。

- 追加の通知処理により負荷が増大し、応答時間が長くなります。
- サーバに影響のない通知も含め、多数の通知が FPolicy サーバに送信される。

クライアントから特定のファイルに対する最初の読み取り / 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 / 書き込みの数が増分されます。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要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` FPolicyが処理される初回読み取り要求は、設定によって決まります。

- first-write ：初回書き込みのクライアント要求をフィルタリングします。

  このフィルタはNFSイベントに使用されます `-file-session-io-grouping-count` および `-file-session-io-grouping-duration` 設定により、FPolicyが処理された初回書き込み要求が決まります。

NFS サーバのデータベースには、次のオプションが追加されます。

```
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。

このタスクについて

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 にアクセスします
NFSv4.1 実装 ID の名前	`-v4.1-implementation-name`	クラスタバージョンの名前
NFSv4.1 実装 ID - 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`

変更する **NFSv4.1** 実装 **ID** のオプション	入力するコマンド
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 ACLs を管理します

NFSv4 ACL を有効化する利点

NFSv4 ACL を有効化すると多くの利点を得られます。

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 セキュリティが向上します
- 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 が設定されているディレクトリ内にファイルやサブディレクトリを新しく作成すると、新しいファイルやサブディレクトリには、その ACL 内の ACE のうち、該当する継承フラグが指定された ACL エントリ（ACE ）がすべて継承されます。

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

- 要求に ACL が含まれる場合は、その ACL が使用されます。
- 要求に標準 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のタグが付けられていれば、それらの ACE が新しいファイルやディレクトリに継承されます。

> 親ACLは、の場合でも継承されます `-v4.0-acl` がに設定されます `off`。

- 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。

> 状況に応じて `-chown-mode` パラメータがに設定されました `restricted` でコマンドを使用します `vserver nfs` または `vserver export-policy rule` ファミリーの場合、NFSv4 ACLで設定されたディスク上の権限でroot以外のユーザがファイル所有権を変更できる場合でも、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します

ONTAP がを受信したとき `chmod` ACLが設定されたファイルまたはディレクトリに対するコマンド。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。を無効にすることができます `-v4-acl-preserve` 代わりにACLをドロップする場合に動作を変更するパラメータ。

このタスクについて

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 ファイルアクセス権が保持されるか破棄されるかの指定も行います。

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、モードビットを変更するときに NFSv4 ACL を破棄します	`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します

NFSv4 ACLを有効または無効にするには、を変更します `-v4.0-acl` および `-v4.1-acl` オプション（ Options ）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。

このタスクについて

。 `-v4.0-acl` 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。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	作業
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。この制限を引き上げることで、 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できるようになります。

このタスクについて

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
   ```

   の有効な範囲

   `max_ace_limit` はです `192` 終了： `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には、を変更します `-v4.0-read-delegation`または オプション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。

このタスクについて

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	作業
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の変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 書き込みファイル委譲を有効または無効にします

書き込みファイル委譲を有効または無効にするには、を変更します `-v4.0-write-delegation`または オプション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。

このタスクについて

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	作業
NFSv4 書き込み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 -v4.0 -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する	次のコマンドを入力します。 `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`

状況	作業
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の変更はすぐに反映されます。NFS のリブートやリスタートは必要ありません。

NFSv4 ファイルおよびレコードロックを設定する

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。

"ネットアップテクニカルレポート 3580 ：『 NFSv4 の拡張内容とベスト・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します

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、を変更します `-v4-lease-seconds` オプション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。

このタスクについて

デフォルトでは、このオプションはに設定されています `30`。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。この期間は、で設定できます `locking.lease_seconds` オプション

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 ロック猶予期間を指定します

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、を変更します `-v4-grace-seconds` オプション

このタスクについて

デフォルトでは、このオプションはに設定されています `45`。

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、 NFSv4 要求を受け取ったクラスタノードが、 NFSv4 クライアントに Storage Virtual Machine （ SVM ）の別の論理インターフェイス（ LIF ）を紹介します。

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します

Storage Virtual Machine（SVM）でNFSv4リファーラルを有効にするには、オプションを有効にします `-v4-fsid-change` および `-v4.0-referrals`または。NFSv4 リファーラルを有効にすると、この機能をサポートする NFSv4 クライアントのデータへのアクセス速度を向上させることができます。

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

   ```
   statistics catalog object show -object nfs*
   ```

2. を使用します `statistics start` およびオプションです `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

例：**NFSv3**のパフォーマンスの監視

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、正常に行われた読み取り要求および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. を使用します `statistics catalog object show` コマンドを使用して、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. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

DNS 統計を監視しています

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 / タイムアウトになった 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 クエリに対し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 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. を使用します `statistics catalog object show` コマンドを使用して、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. を使用します `statistics start` および `statistics stop` 1つ以上のオブジェクトからデータサンプルを収集するコマンド。
3. を使用します `statistics show` コマンドを使用してサンプルデータを表示します。

NIS 統計を監視する

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 / タイムアウトになった 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 クエリに対し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 がサポートされるようになりました

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

サポートされている機能

次の機能がサポートされます。

- コピーオフロード

  ESXi ホストで、仮想マシンや仮想マシンディスク（ VMDK ）のコピーを、ホストを介さずにソースとデスティネーションのデータストア間で直接実行できます。これにより、 ESXi ホストの CPU サイクルやネットワーク帯域幅を節約できます。ソースボリュームがスパースボリュームの場合、コピーオフロードでスペース効率が保持されます。

- スペースリザベーション

  スペースをリザーブして VMDK ファイル用のストレージスペースを確保します。

制限

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

- 次の場合にコピーオフロード処理が失敗することがあります。
  - ソース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可能性があります。

  qtree のエクスポートを現在行っているか、以前行っていた SVM から、これまでに qtree をエクスポートしたことがない SVM へのデータのコピーを試みます。上記の制限を回避するために、デスティネーション SVM で少なくとも 1 つの qtree をエクスポートすることができます。

関連情報

"Data ONTAP では、 VAAI オフロード処理はどのようにサポートされていますか。"

VMware vStorage over NFS を有効または無効にします

を使用して、Storage Virtual Machine（SVM）でVMware vStorage over NFSのサポートを有効または無効にできます `vserver nfs modify` コマンドを実行します

このタスクについて

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 での現在の vStorage のサポートステータスを表示します。

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

2. 次のいずれかを実行します。

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

完了後

この機能を使用する前に、 NFS Plug-in for VMware VAAI をインストールしておく必要があります。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

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

rquota のサポートを有効または無効にします

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、を使用します `vserver nfs modify` コマンドを実行します

このタスクについて

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 転送サイズを変更することで **NFSv3 / NFSv4** のパフォーマンスが向上します

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 と **NFSv4** の **TCP** 最大転送サイズを変更する

を変更できます `-tcp-max-xfer-size` NFSv3およびNFSv4.xプロトコルを使用するすべてのTCP接続の最大転送サイズを設定するオプション。

このタスクについて

これらのオプションは Storage Virtual Machine （ SVM ）ごとに変更できます。

ONTAP 9以降では、を参照してください `v3-tcp-max-read-size` および `v3-tcp-max-write-size` オプションは廃止されました。を使用する必要があります `-tcp-max-xfer-size` 代わりにオプション。

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

> 最大転送サイズには、 4KB （ 4096 バイト）の倍数を入力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. を使用します `vserver nfs show -fields tcp-max-xfer-size` コマンドを使用して変更を確認します。
4. 静的マウントを使用しているクライアントがある場合、新しいパラメータサイズを有効にするには、いったんアンマウントしてから再度マウントします。

例

次のコマンドは、 vs1 という SVM で NFSv3 と NFSv4.x の TCP 最大転送サイズを 1 、 048 、 576 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** の数を設定します

ONTAP は、 Kerberos （ RPCSEC_GSS ）認証を使用して NFS ユーザクレデンシャルを処理する場合、デフォルトで最大 32 個のグループ ID をサポートしています。AUTH_SYS 認証を使用する場合は、 RFC 5331 で定義されているとおり、グループ ID のデフォルトの最大数は 16 個です。デフォルト数を超えるグループに属しているユーザがいる場合は、この最大数を 1 、 024 まで増やすことができます。

このタスクについて

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、そのユーザが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発生する可能性があります。SVM あたりの最大グループ数は、環境内の最大グループ数と同じ数に設定する必要があります。

次の表に、の2つのパラメータを示します `vserver nfs modify` 3つの設定例でグループIDの最大数を決定するコマンド。

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 に設定されます	`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. を確認します `-extended-groups-limit` AUTH_SYSが拡張グループを使用し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

次の例は、拡張されたグループを AUTH_SYS 認証で有効にし、 AUTH_SYS 認証と RPCSEC_GSS 認証の両方で拡張グループの最大数を 512 に設定します。これらの変更は、 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 セキュリティ形式データへのアクセスを許可したりするように ONTAP を設定することができます。NFS データストアで NTFS セキュリティ形式を使用する際には、 root ユーザによるアクセスの処理方法を決定し、それに応じて Storage Virtual Machine （ SVM ）を設定する必要があります。

このタスクについて

root ユーザが NTFS セキュリティ形式のデータにアクセスする際には、次の 2 つのオプションがあります。

- 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する。
- NTFS ACL を無視してフルアクセスを root に対して提供する。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 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 ユーザにマッピングする	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
NT ACL チェックをバイパスします	`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存在しない場合、 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
```

サポート対象の**NFS**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 でサポートされる NFS のバージョンとクライアントを確認しておく必要があります。

この表は、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ONTAP でデフォルトでサポートされる場合を示しています。デフォルトでは、このNFSプロトコルをサポートするONTAP の最も古いバージョンがサポートされているわけではありません。

バージョン	サポートされます	導入済み
NFSv3	はい。	すべてのONTAPリリース
NFSv4.0	はい。	ONTAP 8
NFSv4.1	はい。	ONTAP 8.1
NFSv4.2	はい。	ONTAP 9.8
pNFS	はい。	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 で確認できます"

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

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

- 委譲機能はすべてのクライアントタイプ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 以外の文字が含まれている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 NFSv4 を使用してマウントされたボリュームはこの制限を受けなくなります。

- すべてのファイルハンドルは永続的です。サーバは揮発性のファイルハンドルを提供しません。
- 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の負荷共有ミラーのソースにルーティングします。

- 名前付き属性はサポートされていません。
- 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`

> ただし、はサポートされていません `quota*` 属性では、ONTAP はRQUOTA側のバンドプロトコルを介し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

ONTAP 9.8 以降では、 NFSv4.1 が有効になっている場合、 nconnect 機能がデフォルトで使用できます。

以前の NFS クライアント実装では、マウントを使用する TCP 接続は 1 つだけです。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ことがあります。ただし、 nConnect 対応クライアントでは、 1 つの NFS マウントに複数の TCP 接続（最大 16 個）を関連付けることができます。このような NFS クライアントは、ファイル操作を複数の TCP 接続にラウンドロビン方式で多重化し、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を取得します。nConnect は、 NFSv3 マウントと NFSv4.1 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、を指定して有効にすることができました `-v4.1` オプションを選択し、に設定します `enabled` Storage Virtual Machine（SVM）にNFSサーバを作成する場合。

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。

ONTAP 9.9.1 以降では、 NFSv4 4.2 がデフォルトで有効になっています。ONTAP 9.8では、 `-v4.1` オプションを選択し、に設定します `enabled` Storage Virtual Machine（SVM）にNFSサーバを作成する場合。NFSv4.1 を有効にすると、クライアントが v4.2 としてマウントされた状態で NFSv4.1 の機能を使用することもできます。

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。

先頭のドキュメント	**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
ONTAP 9.9.1	NFSとラベルされた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 ）対応であり、クライアントから送信された sec_label 属性を保存および取得します。

詳細については、を参照してください "RFC 7240"。

ONTAP 9.12.1以降では、NDMPダンプ処理でNFS v4.2セキュリティラベルがサポートされます。以前のリリースのファイルまたはディレクトリでセキュリティラベルが検出された場合、ダンプは失敗します。

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する：

```
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、で定義される標準のNFS属性です "RFC 8276" 最新のNFSクライアントで有効になっています。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。

現在のところ、NDMPダンプ処理では、NFS拡張属性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た場合'ダンプは続行されますが'こ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、を使用します `vserver nfs modify -v4.2-xattrs disabled` コマンドを実行します

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 と SMB のファイルとディレクトリの命名規則

NFSと**SMB**のファイルとディレクトリの命名規則について説明します

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のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、 ONTAP のリリースに応じて、ファイル、ディレクトリ、 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。この違いがマルチプロトコル環境に及ぼす影響と、 SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `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した場合 `TESTDIR`を指定することはできません。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ます。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場合 `TESTDIR`では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および `TESTDIR`ディレクトリ名では大文字と小文字が区別されるためです。
- SMB クライアントでは、 2 つのディレクトリを区別するために 8.3 形式の名前が使用されます。1 つのディレクトリには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、が表示されます `testdir` および `TESTDI~1`。

- ONTAP によってが作成されます `TESTDI~1` 2つのディレクトリを区別するディレクトリ名。

  この場合、 Storage Virtual Machine （ SVM ）での共有の作成時または変更時に共有パスを指定するときは、 8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `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した場合 `Test.txt`を指定することはできません。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ます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt`では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、 `test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMB クライアントでは、 2 つのファイルを区別するために 8.3 形式の名前が使用されます。1 つのファイルにはベースファイル名が付けられます。追加のファイルには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
  - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。

> 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 による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とします `specifications.html`ONTAP で作成される`8.3`形式のファイル名はです `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名前の別のファイルを作成したとします `specifications_new.html`、8.3形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、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 エンコード形式の名前がサポートされるようになり、 Basic Multilingual Plane （ BMP ；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。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には、でnew_utf8mb4_言語コードを使用できます `vserver` および `volume` コマンド・ファミリー。

- 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。
- ボリュームを設定しています `-language` 明示的なオプション：

  ```
  volume create -language utf8mb4 {…}
  ```

- ボリュームを継承しています `-language` オプションを指定して作成または変更したSVMから、次のオプションを選択します。

  ```
  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設定のままです。

[+]

> 現在のところ、 4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、 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 ）、 NFS ファイルシステムでは 8-bit Unicode Transformation Format （ UTF-8 ）を使用して表現されます。

  ONTAP 9.5 よりも前のリリースでは、 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 UTF-16 に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作成したファイル名に有効な追加文字が含まれている場合や無効な追加文字が含まれている場合、 ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

  この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は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。

Unicode 文字は qtree 名で使用できます。

- どちらかを使用できます `volume qtree` 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を使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、 BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。

> ONTAP 9.5 よりも前のリリースでは、 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 名や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、 qtree が utf8mb4 に対応したボリュームに含まれていれば、 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を設定します

NFS クライアントは、 SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

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 はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロン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、長いファイル名に重要な情報を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を使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、 SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、 SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に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をまたいで適用されません。

  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。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

  たとえば ' コロン (:) をハイフン (-) にマッ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てもまだマッピングに無効な Windows 文字が含まれている場合、 ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、 NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。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ません。ただし、 8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙（「 dir 」）を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ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（「 . 」または空白で終わる場合など）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 進数値で入力された Unicode 文字です。例： 3C ： E03C

   それぞれの最初の値 `mapping_text` コロンで区切られたペアは、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。マッピングのペアは一意である必要があります（ 1 対 1 のマッピングが存在する必要があります）。

   - ソースマッピング

     次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

Unicode 文字	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	>	が次の値より大きい
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を管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	`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します	`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。

NFSトランキングの概要

ONTAP 9.14.1以降では、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るため、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。

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。

ONTAP 9.14.1では、トランキングは1つのノードのLIFに制限されます。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

ONTAP 9.8 以降では、 NFSv4.1 が有効になっている場合、 nconnect 機能がデフォルトで使用できます。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。

の詳細を確認してください "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

トランキングが有効な**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。

作業を開始する前に

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
   ```

   の詳細を確認してください "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
   ```

   の詳細を確認してください "NFSサーバの設定"

完了後

必要に応じて次のサービスを設定します。

- "DNS"
- "LDAP"
- "Kerberos"

ネットワークをトランキング用に準備する

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。

このタスクについて

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。

作業を開始する前に

- 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
  ```

の詳細を確認してください "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。

     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` オプション

   - `-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。
   - でIPアドレスを指定できます `-address` および `-netmask` オプション（ではなく） `-subnet` オプション
   - 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、デフォルトのポリシーが自動的に割り当てられます。を使用します `network interface service-policy show` 使用可能なサービスポリシーを確認するためのコマンド。
   - `-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。

     次のコマンドを実行すると、 `lif-A` SVM用 `vs1`、ポート `e0c` ノード `cluster1_01`：

     ```
     network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
     -node cluster1_01 -home-port e0c -address 192.0.2.0
     ```

の詳細を確認してください "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
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

クライアントアクセス用のデータのエクスポート

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する

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

   ポリシー名に指定できる文字数は最大 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
   ```

。 `-clientmatch` パラメータには、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。

の詳細を確認してください "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指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
   ```

クライアントマウントの作成

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 "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
```

バージョン (`vers`）の値は次のとおりです。 `4.1` 以降が必要です。

。 `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の接続に対応します。

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適応の概要

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、エクスポートしたボリュームを `max_connect` オプション

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
   ```

   の詳細を確認してください "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
   ```

トランキングのため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。

このタスクについて

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。

作業を開始する前に

- 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。

     ポートは次の形式で追加されます。 *`node_name:port_number`*`例えば、 `node1:e0c`。

     次のコマンドは、フェイルオーバーグループを作成します。 `fg3` SVM vs1にポートを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
     ```

   の詳細を確認してください "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。

     LIFをホームノードと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には、 `-auto -revert` オプション

   - `-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。
   - でIPアドレスを指定できます `-address` および `-netmask` オプション（ Options ）
   - 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、デフォルトのポリシーが自動的に割り当てられます。を使用します `network interface service-policy show` 使用可能なサービスポリシーを確認するためのコマンド。
   - `-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
```

の詳細を確認してください "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
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

クライアントアクセス用のデータエクスポートを変更します。

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、 `-clientmatch` パラメータを指定すると、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クライアントが正しく識別されます。

調整が必要な場合は、 `vserver export-policy rule modify` コマンドを実行するか、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
```

の詳細を確認してください "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
```

クライアントマウントの再確立

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 "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` 値は次のでなければなりません： `4.1` 以降が必要です。

。 `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

RDMA経由のNFS

NFS over RDMA は RDMA アダプタを使用し、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は発生しません。

NFS over RDMA 構成は、レイテンシの影響を受けやすいワークロードや、マシンラーニングや分析などの広帯域幅ワークロードを使用するお客様向けに設計されています。NVIDIA は、 GPU Direct Storage （ GDS ）を有効にするために RDMA 経由の NFS を拡張しました。GDSはRDMAを使用してストレージシステムとGPUメモリ間でデータを直接転送することで、CPUとメインメモリを完全にバイパスすることで、GPU対応のワークロードをさらに高速化します。

ONTAP 9.10.1以降では、Mellanox CX-5アダプタまたはCX-6アダプタを使用すると、NFSv4.0プロトコルでNFS over RDMA構成がサポートされます。このアダプタを使用すると、バージョン2のRoCEプロトコルを使用した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 ファミリー GPU のみを使用してサポートされます。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RDMA経由のNFS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RDMA上のNFSを設定する必要があります。
- HAペアの両方のノードのバージョンを同じにする必要があります。
- ストレージシステムコントローラにはRDMAがサポートされている必要があります。

ONTAPで開始しています…	次のコントローラが**RDMA**をサポートしています…
9.10.1以降	• AFF A400 • AFF A700の略 • AFF A800
ONTAP 9.14.1以降	• AFF Cシリーズ • AFF A900 の略

- RDMAでサポートされるハードウェア（例 Mellanox CX-5またはCX-6）
- RDMA をサポートするには、データ LIF を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。

> インターフェイスグループはNFS over RDMAではサポートされません。

次のステップ

- NFS over RDMA 用に NIC を設定します
- NFS over RDMA 用に LIF を設定します
- 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 用に NIC を設定します

NFS over RDMA 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に NIC を設定する必要があります。

ストレージプラットフォームの構成

サーバに X1148 RDMA アダプタをインストールする必要があります。HA 構成を使用している場合は、フェイルオーバーパートナーに対応する X1148 アダプタを用意して、フェイルオーバー中も RDMA サービスを継続できるようにする必要があります。NIC は ROCE 対応である必要があります。

ONTAP 9.10.1以降では、次のコマンドを使用して、RDMA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（例 X1148 ）および Mellanox OFED ネットワークソフトウェア。サポートされ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、すべてのスイッチでプライオリティフロー制御が有効であることを確認します。

この設定を確認したら、 NFS をマウントできます。

System Manager の略

System Managerを使用してRDMA経由のNFSで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. のワークフローに従ってください NFS を使用して Linux サーバ用の NAS ストレージを有効にします 新しいNFSサーバを設定します。

   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で、このオプションを選択します。

CLI の使用

1. 次の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` を有効にする必要があります。サポートされていない場合は、 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. クライアントを RDMA 経由で NFSv4.0 にマウントします。
   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、を使用します `proto=rdma`。IPv6の場合は、 `proto=rdma6`。
   b. NFSターゲットポートをと指定します `port=20049` 標準ポート2049ではなく、次の手順を実行します。

      ```
      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、コマンドを実行します `unmount mount_path`

詳細情報

- NFS サーバを作成します
- NFS を使用して Linux サーバ用の NAS ストレージを有効にします

NFS over RDMA 用に LIF を設定します

NFS over RDMAを利用するには、LIF（ネットワークインターフェイス）をRDMA互換性を確保す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がRDMAをサポートしている必要があります。

新しい LIF を作成

System Manager の略

System ManagerでRDMA経由のNFS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. 選択するオプション + 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 RoCE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 の使用

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
```

   - サービスポリシーには、 default-data-files または dataNFS-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を指定する必要があります。
   - 。 `-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。いつ `roce` また、LIFはRoCEオフロードをサポートしているポートでのみ設定でき、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 の略

System ManagerでRDMA経由のNFS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、その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 の使用

1. LIFのステータスは、で確認できます `network interface show` コマンドを実行しますサービスポリシーに 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` リストにはと入力します `roce`。上記のいずれかの条件に該当しない場合は、 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 を変更した場合に、そのプロトコルをサポートするポートに LIF が割り当てられていないとエラーが発生します。

LIF を移行

ONTAP では、RDMAを介した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で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と、ポートがRoCEに対応しているかどうかが指定されます。

次の場合にのみ、LIFをNFS over RDMA構成に移行できます。

- 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。

詳細情報

- LIF を作成
- LIF を作成
- LIF を変更する
- LIF を移行

NFS 設定を変更します

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 の移行に関する問題に対処するには、 NFSv4 の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以降の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 ロック猶予期間を指定します。

CLI を使用して SMB を設定します

CLIヲシヨウシタSMBセツテイノカイヨウ

ONTAP 9 の 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。

次の手順に従って、ボリュームまたは qtree への SMB アクセスを設定します。

- SMB のバージョン 2 以降を使用する必要がある。
- NFS クライアントではなく、 SMB クライアントのみを対象とする（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 管理者権限ではなくクラスタ管理者権限を持っている。

  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。

  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には、を参照してください "NFS と SMB の両方を使用して Windows と Linux の両方に NAS ストレージをプロビジョニングする"。

- 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。

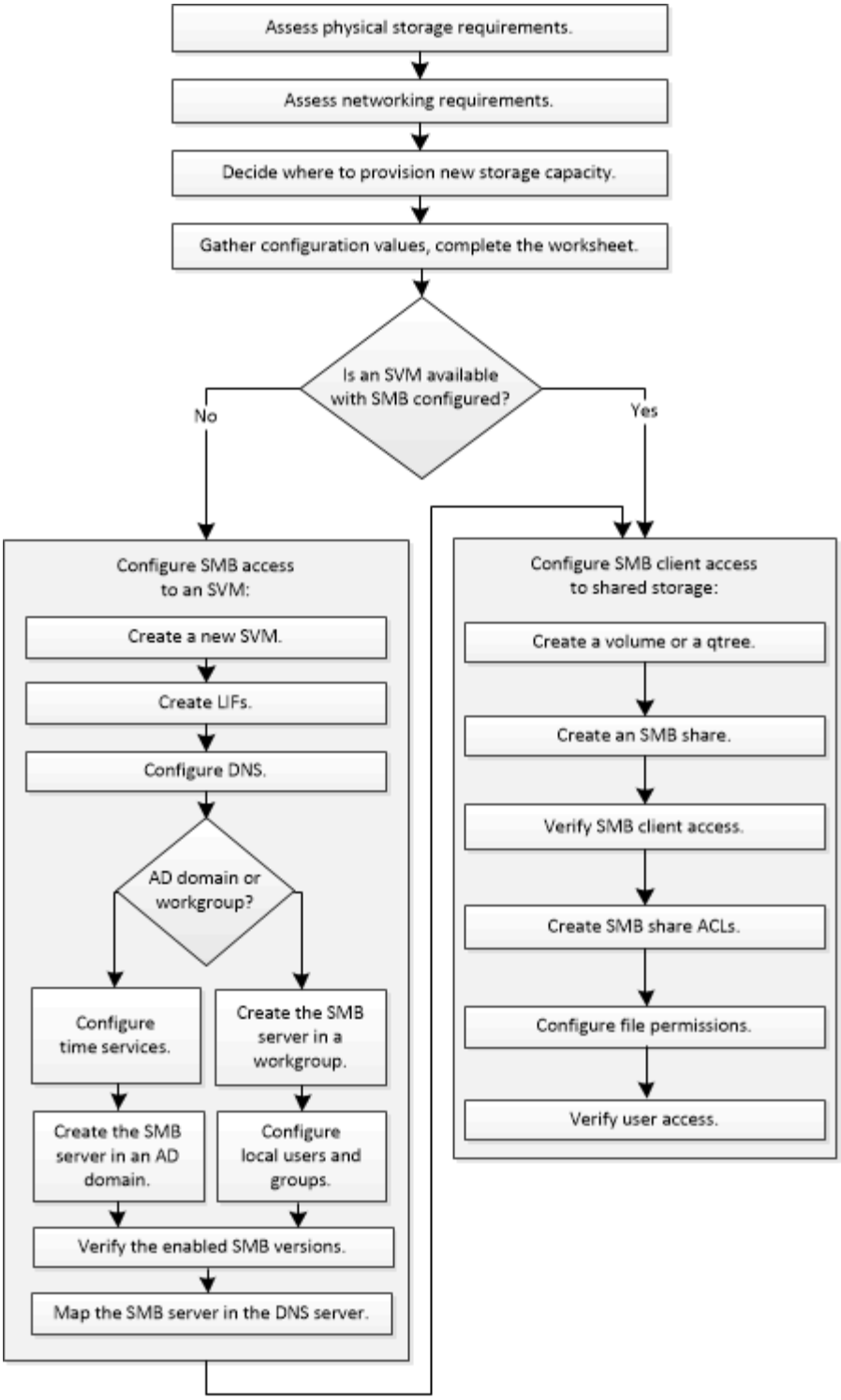
ONTAP の SMB プロトコル機能の範囲の詳細については、を参照してください "SMB リファレンスの概要"。

ONTAP でこれを行うその他の方法

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 を使用して Windows サーバ用の NAS ストレージをプロビジョニングする"
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 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 を追加するかによってワークフローが異なります。



準備

物理ストレージ要件を評価

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、を使用して既存のアグリゲートにディスクを追加します `storage aggregate add-disks` コマンドを実行するか、を使用して新しいアグリゲートを作成します `storage aggregate create` コマンドを実行します

ネットワーク要件を評価

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。

作業を開始する前に

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高であるポートを使用する必要があります。
- 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。

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、を使用して作成されます `network subnet create` コマンドを実行します

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、を使用してIPv6を有効にできます `network options ipv6 modify` コマンドを実行します

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。これにより、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 *

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

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`

フィールド	説明	あなたの価値
`-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`	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 *

では、次の値を指定します `network interface create` コマンドを使用してLIFを作成します。

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SMBプロトコルのみを使用します。	`cifs`
`-home-node`	でLIFが戻るノードを指定します `network interface revert` LIFに対してコマンドを実行します。	
`-home-port`	の場合に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` LIFに対してコマンドを実行します。	
`-address`	新しい LIF によるデータアクセスに使用されるクラスタ上の IPv4 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を指定します。	
`-subnet`	IP アドレスのプール。の代わりに使用されます `-address` および `-netmask` アドレスとネットマスクを自動的に割り当てます。	

フィールド	説明	あなたの価値
`-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`
`-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 *

では、次の値を指定します `vserver services name-service dns create` コマンドを使用してDNSを設定します。

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 アドレスを指定します。	

Active Directory ドメインで **SMB** サーバをセットアップする

- タイムサービス設定のパラメータ *

では、次の値を指定します `cluster time-service ntp server create` コマンド（タイムサービスを設定する場合）。

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 *

では、次の値を指定します `vserver cifs create` コマンドは、新しいSMBサーバを作成し、ドメイン情報を指定するときに使用します。

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。	

フィールド	説明	あなたの価値
`-cifs-server`	SMB サーバの名前（最大 15 文字）を指定します。	
`-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、この SMB サーバ概要を確認できます。	

ワークグループに **SMB** サーバをセットアップする

- 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 *

では、次の値を指定します `vserver cifs create` コマンドは、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ときに使用します。

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、この SMB サーバ概要を確認できます。	

- ローカルユーザー作成用のパラメータ *

を使用してローカルユーザを作成する場合は、次の値を指定します `vserver cifs users-and-groups local-user create` コマンドを実行しますこれらの値は、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る場合は、フルネームを 2 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。概要にスペースが含まれる場合は、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 *

を使用してローカルグループを作成する場合は、次の値を指定します `vserver cifs users-and-groups local-group create` コマンドを実行します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。概要にスペースが含まれる場合は、パラメータを引用符で囲みます。	

- ボリュームを作成するためのパラメータ *

では、次の値を指定します `volume create` コマンドは、qtreeの代わりにボリュームを作成する場合に使用します。

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`	新しいボリュームをマウントするルート（/）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 *

では、次の値を指定します `volume qtree create` コマンドは、ボリュームではなくqtreeを作成する場合に使用します。

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を指定します。	
`-qtree`	新しい qtree に対して、一意のわかりやすい名前を 64 文字以内で指定します。	

フィールド	説明	あなたの価値
-qtree-path	qtreeパスの引数を指定します。形式はです /vol/volume_name/qtree_name\> ボリュームとqtreeを別 々 の引数として指定する代わりに指定できます。	

- SMB 共有作成のパラメータ *

では、次の値を指定します vserver cifs share create コマンドを実行します

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。デフォルト設定はです oplocks、 browsable、 changenotify`および `show-previous-versions。	
-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 *

では、次の値を指定します vserver cifs share access-control create コマンドを実行します

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。	

フィールド	説明	あなたの価値
`-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`
`-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 を作成します。

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。

作業を開始する前に

- 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`*
    - のNTFS設定を使用します。 `-rootvolume-security-style` オプション
    - デフォルトのC.UTF-8を使用します `-language` オプション

- 。 `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CIFSを含める必要があります。このリストはあとで編集できます。

   。 `Vserver Operational State` フィールドにはを表示する必要があります `running` 状態。が表示された場合 `initializing` 状態にすると、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内に作成します `ipspaceA`：

```
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に追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含ま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を設定します。

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。

このタスクについて

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、を使用してあとから有効にすることができます `vserver add-protocols` コマンドを実行します

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。

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` コマンドを実行します

手順

1. 現在 SVM で有効になっているプロトコルと無効になっているプロトコルを確認します。 `vserver show -vserver vserver_name -protocols`

   を使用することもできます `vserver show-protocols` コマンドを使用して、クラスタ内のすべてのSVMで現在有効になっているプロトコルを表示します。

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 / 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、を追加してSMB経由のアクセスを許可します `cifs` vs1というSVMで有効になっているプロトコルのリストに移動します。

```
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きます

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。

このタスクについて

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 アクセスが許可されていることを確認してから、ボリュームまたは qtree ごとにカスタムのエクスポートポリシーを作成して各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. を使用してルールの作成を確認します `vserver export-policy rule show` コマンドを実行します

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 SMB クライアントからアクセスできるようになります。

LIF を作成

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。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。
- 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。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理す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 はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、 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にある指定したホームノード上のランダムな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 9.6以降）。
   - 。 `-data-protocol` サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。ONTAP 9.5以前を使用している場合 `-data-protocol` パラメータは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。
   - `-home-node` は、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

     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` オプション

- `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
- でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
- 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。
- サブネットを使用せずに手動で IP アドレスを割り当てると、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。
- をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

  必要に応じて、カスタムファイアウォールポリシーをあとから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は廃止され、完全にLIFのサービスポリシー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できます。デフォルト設定はです `false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。

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
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドでは、を使用して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ます `-address` および `-netmask` パラメータ：

```
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

）から割り当てています。

```
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 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、 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、に割り当てられたNASデータLIFを作成する方法を示しています `default-data-files` サービスポリシー：

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

ホスト名解決に使用する **DNS** を有効にします

を使用できます `vserver services name-service dns` 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します。ホスト名は外部DNS サーバを使用して解決されます。

作業を開始する前に

ホスト名を検索するために、サイト規模の DNS サーバが使用可能である必要があります。

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つだけの場合は警告が表示されます。

このタスクについて

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、 SVM vs1 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` コマンドは設定の自動検証を実行し、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を報告します。

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

   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
```

次のコマンドは、 SVM vs1 の DNS 設定の詳細を表示します。

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

   。 `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 ドメイン内に **SMB** サーバをセットアップする

タイムサービスを設定

Active Directory 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 サーバが所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。

このタスクについて

Active Directory ドメインと同じ NTP サーバを使用して時刻を同期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。

ONTAP 9.5 以降では、対称認証を使用するように NTP サーバをセットアップできます。

手順

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

   `cluster time-service ntp server show`

   ```
   Server                          Version
   ------------------------------- -------
   10.10.10.1                      auto
   10.10.10.2                      auto
   ```

NTP サーバの対称認証を管理するコマンドです

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 鍵を使用した対称認証機能が含まれ、ネットワークセキュリティが強化されます。

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 サーバに対して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`

作業	使用するコマンド
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 サーバで同じである必要があります
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 でサーバを設定する。	`cluster time-service ntp server create -server server_name -key-id key_id` キー ID 、タイプ、および値が、 NTP サーバで設定されたキー ID 、タイプ、および値と同じである必要があります。
対称認証を無効にします	`cluster time-service ntp server modify -server server_name -authentication disabled`

Active Directory ドメイン内に **SMB** サーバを作成します

を使用できます `vserver cifs create` コマンドを使用してSVM上にSMBサーバを作成し、所属先のActive Directory（AD）ドメインを指定します。

作業を開始する前に

データ処理に使用している 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 サーバの追加先となる 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ユーザなら誰でも、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、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

このタスクについて

Activity Directory ドメインで SMB サーバを作成する場合の条件は次のとおりです。

- 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。
- を使用して、SMBサーバを別の組織単位（OU）に追加することもできます `-ou` オプション
- 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 個）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 サーバに統合して、 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。

。 `vserver cifs` マニュアルページには、追加のオプションパラメータと命名要件が記載されています。

> ONTAP 9.1 以降では、 SMB 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。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、 SMB 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 では、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` オプションはに設定されています `true`;デフォルトはです `false`。このオプションを設定すると、 SMB3 でのみ暗号化がサポートされるため、 SMB3 プロトコルのみが使用されます。。

"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ます。 "ONTAP One"。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. を使用してSMBサーバの設定を確認します `vserver cifs show` コマンドを実行します

   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との暗号化通信を有効にします（ONTAP 9.8以降）。 `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。。 `-domain` optionは、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。。 `username` オプションは、信頼できるドメインの管理者を指定します。

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

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

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

SMB 認証用の keytab ファイルを作成します

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;ユニフォームリソース識別子）としてONTAP 管理者が使用できるようにします。このファイルは、に指定します `vserver cifs` コマンドを実行するには、ADドメインとのKerberos認証が必要です。

AD管理者は、標準のWindows Serverを使用してkeytabファイルを作成できます `ktpass` コマンドを実行しますこのコマンドは、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ていません。

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。したがって、管理者ユーザのパスワードを変更した場合は、そのたびに新しい 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。

ワークグループ内に **SMB** サーバをセットアップする

ワークグループの概要で **SMB** サーバをセットアップする

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。

ワークグループ内に **SMB** サーバを作成

を使用できます `vserver cifs create` コマンドを使用して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します。

作業を開始する前に

データ処理に使用している 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。

このタスクについて

ワークグループモードの SMB サーバでは、次の SMB 機能はサポートされません。

- SMB3 監視プロトコル
- 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 ）

。 `vserver cifs` 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、マニュアルページ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ます。 "ONTAP One"。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. を使用してSMBサーバの設定を確認します `vserver cifs show` コマンドを実行します

   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: -
```

完了後

ワークグループ内の CIFS サーバについては、 SVM 上でローカルユーザ、およびオプションで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を作成します

SVM に格納されたデータへの SMB 接続によるアクセスの許可に使用できるローカルユーザアカウントを作成できます。ローカルユーザアカウントは、 SMB セッションを作成する際の認証にも使用できます。

このタスクについて

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`

     ローカルユーザの概要。

   - `-is-account-disabled {true|false}`

     ユーザアカウントが有効になっているか無効になっているかを示します。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を入力するように求められます。

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
```

ローカルグループを作成します

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。

このタスクについて

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概要。

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
```

完了後

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の管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに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。

このタスクについて

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[,...]`

     カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。

   - 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[,...]`

     カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

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
```

有効な **SMB** のバージョンを確認

ONTAP 9 のリリースによって、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 のバージョンが決まります。ご使用の環境で必要なクライアントと機能を、 SMB サーバがサポートしていることを確認する必要があります。

このタスクについて

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ために、可能なかぎり SMB 2.0 以降を有効にする必要があります。セキュリティ上の理由から、 SMB 1.0 の使用は避け、お使いの環境で不要であることを確認した場合は無効にする必要があります。

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っていますが、デフォルトで有効になっている SMB 1.0 のバージョンは ONTAP 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。

  。 `-smb1-enabled` オプションをに設定します `vserver cifs options modify` コマンドは、SMB 1.0を有効または無効にします。

- ONTAP 9.3 以降では、新しい SVM で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、ドメインコントローラ（ DC ）に接続するために SMB 2.0 を有効にすることができます。DC 上で SMB 1.0 を無効にしている場合は、この処理は必須です。ONTAP 9.2 以降では、 SMB 2.0 が DC 接続用にデフォルトで有効になります。

> 状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true`ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、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に関する詳細が記載されています。

手順

1. 権限レベルを advanced に設定します。

   ```
   set -privilege advanced
   ```

2. 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には：

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     に指定できる値 `smb_version`：

     - `-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には：

     ```
     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。

作業を開始する前に

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。

このタスクについて

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を設定します

共有ストレージへの SMB クライアントアクセスを設定します

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。

作業を開始する前に

- 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します

ボリュームを作成します

を使用して、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` コマンドを実行します

このタスクについて

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、新しいボリュームを作成するときに指定できます。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、を使用してSVMネームスペースにボリュームを_mount_する必要があります `volume mount` コマンドを実行します

作業を開始する前に

- 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トラッキングを有効にするには、を問題します `volume create` コマンドにを指定します `-analytics-state` または `-activity-tracking-state` をに設定します `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 "File System Analytics を有効にします"。

手順

1. ジャンクションポイントを指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 `-junction-path` 次のようなものがあります。

   - 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。

   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、次のように指定します。 `/new_dir/new_vol`その後、SVMルートボリュームにジャンクションされた新しい親ボリュームを作成しておく必要があります。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、で使用できます `/users`。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 `/eng/` はvs1 SVMのネームスペースにすでに存在し、新しいボリュームはで使用できるようになります `/eng/home`をクリックします。これがのホームディレクトリになります `/eng/` ネームスペース：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です `volume` （デフォルト）。

```
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 を作成します

を使用して、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` コマンドを実行します

作業を開始する前に

- 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 である必要があります。また、 SMB 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 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. 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を作成します `/vol/data1`：

```
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、を使用してディレクトリパス構造を指定します `-path` のオプションを選択します `vserver cifs share create` クライアントがアクセスするコマンド）。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は 255 文字以内で指定します。
- 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"`）。
- UNCパスの場合 (`\\servername\sharename\filepath`（UNCパスの先頭のを除く）が256文字を超えている場合、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 問題ではなく Windows クライアント問題です。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です `oplocks`、 `browsable`、 `changenotify`および `show-previous-versions`。
- 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。を使用する場合 `-share-properties` パラメータ共有を作成するときは、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、を使用します `homedirectory` プロパティ。

  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、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` コマンドを実行します
- の値で指定したホームディレクトリ共有 `homedirectory` をクリックします `-share-properties` パラメータにはを含める必要があります `%w` （Windowsユーザ名）共有名の動的変数。

  共有名にはさらにを含めることができます `%d` （ドメイン名）動的変数（例： `%d/%w`）または共有名の静的な部分（例： `home1_%w`）。

- 共有が他のユーザのホームディレクトリに接続するために管理者またはユーザによって使用されている場合（のオプションを使用） `vserver cifs home-directory modify` 動的な共有名のパターンの前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` マニュアルページには追加情報 があります。

SMB 共有を作成

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。

作業を開始する前に

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。

このタスクについて

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。

   。 `vserver cifs share create` コマンドはで指定されたパスをチェックします `-path` オプション（共有の作成時）。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上に作成します `vs1.example.com`。ディレクトリパスはです `/users`をクリックすると、デフォルトのプロパティで作成されます。

```
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を確認

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、作成できたら削除します。

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を作成

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。

作業を開始する前に

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。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名を使用して共有レベルの ACL を設定できます。

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ます `Everyone / Full Control`は、セキュリティリスクをもたらします。

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. 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` コマンドを実行します

例

次のコマンドは、を示しています `Change` 「vs1.example.com`"SVM:」上の「sales」共有に対する「Sales Team」Windowsグループへの権限

```
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
```

以下のコマンドで説明します `Change` 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 `Full_Control` SVM「vs1」の「datavol5」共有に対する「Sue Chang」という名前のWindowsローカルユーザの権限：

```
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
```

共有内で **NTFS** ファイル権限を設定する

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許可するには、Windows クライアントで、その共有内のファイルおよびディレクトリに対して NTFS フ

ァイルアクセス権を設定する必要があります。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

"SMBの管理" また、標準および詳細な NTFS アクセス権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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

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	実行する処理
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（ Add ）] 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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

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 リファレンスの概要

SMB プロトコルで ONTAP ファイルアクセス機能を使用できます。CIFS サーバを有効にしたり、共有を作成したり、 Microsoft サービスを有効にしたりできます。

> *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。

これらの手順は、次のような状況で使用する必要があります。

- ONTAP の SMB プロトコル機能の範囲について理解する必要がある。
- SMB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。

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 ）上で 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 は、必ずしも同じドメインにバインドする必要はありません。
- 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 を設定しておく必要があります。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。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

"Network Management の略"

SMB サーバを変更

"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 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 のバージョンがサポートされますが、デフォルトである SMB 1.0 がサポートされるかどうかは 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 の 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を切り替えることができます。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
はデフォルトで有効になっています	はい。	はい。	はい。	いいえ
有効または無効にすることができます	いいえ	はい * 9.1 P8 以降が必要です。	はい。	はい。

SMB 1.0 および 2.0 のドメインコントローラへの接続に関するデフォルト設定も ONTAP のバージョンによって異なります。詳細については、を参照してください `vserver cifs security modify` のマニュアルページ。既存の CIFS サーバで SMB 1.0 を実行している環境では、できるだけ早く最新の SMB バージョンに移行して、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、ネットアップの担当者にお問い合わせください。

次の表に、 SMB でサポートされる機能と対応するバージョンを示します。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

* 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。 *				
複合操作			X	X	X	X
非同期操作			X	X	X	X
読み取り / 書き込みバッファのサイズが増加します			X	X	X	X
拡張性の向上			X	X	X	X
SMB 署名	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
共有の継続的な可用性	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

* 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。 *				
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
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 を介したデータ転送での SMB サーバの SMB 暗号化要求の設定

"ネットアップの相互運用性"

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 に **NIS** または **LDAP** ネームサービスを設定します

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

作業を開始する前に

ネームサービスデータベース設定をネームサービスインフラに合わせてカスタマイズしておく必要があります。

このタスクについて

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番を決定します。ns-switch ソースには、「 files 」、「 nis 」、または「 ldap 」を任意に組み合わせて使用できます。グループデータベースの場合、 ONTAP は設定されたすべてのソースからグループメンバーシップを取得し、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いずれかのソースを使用できないと、 ONTAP は完全な UNIX クレデンシャルを取得できず、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 設定に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必ず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ます `passwd` データベース：デフォルトの設定を使用する場合、 SMB アクセスに対する、 NIS または LDAP UNIX ユーザおよびグループのネームサービスまたは LDAP ユーザマッピングの設定は省略可能です。

手順

1. UNIX ユーザ、グループ、ネットグループ情報が NIS ネームサービスによって管理されている場合、 NIS ネームサービスを次のように設定します。

   a. を使用して、ネームサービスの現在の順序を確認します `vserver services name-service ns-switch show` コマンドを実行します

      この例では、3つのデータベースを示します (`group`、 `passwd`および `netgroup`を使用できます `nis` ネームサービスソースがのみを使用している `files` 情報源として

      ```
      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
```

を追加する必要があります `nis` を参照してください `group` および `passwd` データベース、およびオプションでにアクセスできます `netgroup` データベース：

b. 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序で調整します `vserver services name-service ns-switch modify` コマンドを実行します

パフォーマンスを最大にするためには、 SVM に設定する予定のないネームサービスデータベースには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、変更するそれぞれのネームサービスデータベースに対して別々にコマンドを実行する必要があります。

この例では、 `nis` および `files` は、のソースとして設定されています `group` および `passwd` この順番でデータベースを作成します。その他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. 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ます `vserver services name-service ns-switch show` コマンドを実行します

`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,… -active true+`

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

> ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-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、アクティブになっ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              Active Server
------------- ------------------- ------ ---------------
vs1           example.com         true   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、格納されている情報を使用して LDAP ネームサービスを設定します "NFS の管理"。

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、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` UNIXシステム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

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番で参照するかを決定します。ONTAP では、 SVM ごとに個別のネームサービススイッチテーブルが保持されます。

データベースタイプ

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

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、 DNS
グループ	ユーザグループ情報を検索しています	files 、 nis 、 ldap が表示されます
パスワード	ユーザ情報を検索しています	files 、 nis 、 ldap が表示されます

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
ネットグループ	ネットグループ情報の検索	files 、 nis 、 ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、 LDAP

ソースタイプ

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

ソースタイプ	情報の検索先	使用するコマンド

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

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

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります `files` また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

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へのアクセスに次のプロトコルを使用します。

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

例

次の例は、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
```

ユーザまたはグループ情報の検索では、 ONTAP はローカルのソースファイルだけを参照します。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の検索では、 ONTAP が最初に外部 NIS サーバを参照し、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照会されます。

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含まれていません。そのため、 ONTAP はデフォルトでローカルのソースファイルだけを参照します。

SMB サーバを管理します

SMB サーバを変更

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` コマンドを実行します

このタスクについて

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 サーバを移動するには、次の手順を実行します。 `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限がある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` 内のコンテナ *`example`*.comドメイン。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

- 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。

  - の該当するパラメータを使用して、他の属性を変更します `vserver cifs modify` コマンドを実行します

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について検討する場合は、使用できるオプションを把握しておくと便利です。一部のオプションは汎用的なものですが、 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複数あります。SMBサーバオプションは、で制御します `vserver cifs options modify` オプション

以下に、 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を秒数で指定できます。アイドルセッションとは、ユーザがクライアントでファイルもディレクトリも開いていないセッションのことです。デフォルト値は900秒です。

- * デフォルトの UNIX ユーザーの構成 *

  このオプションでは、 SMB サーバで使用されるデフォルトの UNIX ユーザを指定できます。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）。このため、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、ファイルへの読み取り権限を持つ SMB クライアントに許可するかどうかを指定できます。このオプションは、デフォルトで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すると、読み取り専用属性が設定されたファイルやフォルダの削除を NFS クライアントに許可するかどうかを指定できます。NTFS の削除では、読み取り専用属性が設定されたファイルやフォルダの削除は許可されません。UNIX の削除では読み取り専用ビットが無視され、ファイルやフォルダを削除できるかどうかは親ディレクトリの権限によって判断されます。デフォルト設定はです `disabled`これにより、NTFSの削除セマンティクスが発生します。

- * Windows Internet Name Service サーバーアドレスの設定 *

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

以下に、 advanced 権限レベルで使用できる 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 *

このオプションは、ファイルの所有者ではない 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、このパラメータがに設定されます `true`をクリックすると、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、このパラメータがに設定されます `false`を指定すると、通常の`UNIX`ルールを適用してファイル権限が付与されます。このパラメータは、権限がに設定されている`UNIX`セキュリティ形式のファイルに適用されます `mode bits` 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 9.3 で SMB サーバが作成された SVM では、 SMB 1.0 がデフォルトで無効になります。

  > ONTAP 9.3 以降では、 ONTAP 9.3 で新しく作成された SMB 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。できるだけ早く最新の SMB バージョンに移行して、セキュリティとコンプライアンスを強化してください。詳細については、ネットアップの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 を無効にした場合、 ONTAP では SMB 3.x も自動的に無効になります

  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ります

- * 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。Windows Server 2012 および Windows 8 は、 SMB 3.0 をサポートする Windows の最小バージョンです。

  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ります

- * SMB 3.1 を有効または無効にします

  Windows 10 は、 SMB 3.1 をサポートする Windows の唯一のバージョンです。

  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ります

- * 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は、コピー中のファイル変更を禁止するモードで Windows クライアントがコピー元のファイルを開こうとした場合に、コピーオフロード処理のパフォーマンスを向上させます。デフォルトでは、直接コピーメカニズムは有効になっています。

- * 自動ノードリファ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 接続のみで有効です。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ります

- * 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によって、 Hyper-V over SMB 解決策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ります

- * シャドウ・コピーのディレクトリ階層の設定 *

  このオプションでは、シャドウコピー機能を使用するときに、シャドウコピーを作成するディレクトリの最大階層を定義できます。

  このオプションは、 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ります

- * マルチドメインネームマッピングの検索機能の有効化または無効化 *

  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。ホームドメインとは、 SMB サーバのコンピュータアカウントが含まれるドメインです。

  双方向の信頼関係が確立されたすべてのドメインを検索する代わりに、信頼できるドメインのリストを設定することもできます。このオプションを有効にして、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ために優先リストが使用されます。

  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 から SMB クライアントに報告されるファイルシステムセクターサイズをバイト単位で設定できます。このオプションには2つの有効な値があります。 `4096` および `512`。デフォルト値はです `4096`。この値をに設定する必要がある場合があります `512` 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。

- * 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を含めて、ダイナミックアクセス制御を使用して SMB サーバのオブジェクトを保護できます。このオプションは、デフォルトでは無効になっています。

  このオプションは 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 ） *

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

- * UNIX 対応のセキュリティ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が SMB クライアントに表示される方法を指定します。有効 ONTAP にすると、 UNIX セキュリティ形式のボリューム内のファイルやフォルダは、 NTFS ACL を使用する NTFS ファイルセキュリティが設定されたファイルやフォルダとして SMB クライアントに表示されます。無効 ONTAP にすると、 UNIX セキュリティ形式のボリュームは、ファイルセキュリティのない FAT ボリュームとして表示されます。デフォルトでは、ボリュームは NTFS ACL を使用する NTFS ファイルセキュリティが設定されたボリュームとして表示されます。

- * SMB 擬似オープン機能の有効化または無効化 *

  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て、 SMB 2.x および SMB 3.0 のパフォーマンスが向上します。デフォルトでは、 SMB 擬似オープン機能は有効になっています。このオプションは、 SMB 2.x 以降を使用する接続にのみ有効です。

- * UNIX 拡張の有効化または無効化 *

  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、 UNIX ベースの SMB クライアントが環境内にある場合は、 UNIX 拡張を有効にしてください。UNIX 拡張を有効にすると、 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場合の検索では、長いファイル名に加えて 8.3 形式のファイル名も照合されます。このパラメータのデフォルト値はです `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 では、 SMB アクセス用のシンボリックリンクの実装で DFS リファーラルが使用されます。有効にすると、シンボリックリンクアクセスが有効かどうかに関係なく、 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以降ではを設定します `-max-credits` オプションを使用すると、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、SMB接続に付与するクレジットの数を制限できます。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 *

  を有効にします `-is-multichannel-enabled` ONTAP 9.4以降のリリースのオプションを使用すると、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、次のパラメータも指定できます。

  - 各マルチチャネルセッション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。
  - 各マルチチャネルセッションで通知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 権限レベルで設定します	`vserver cifs options modify -vserver` *`vserver_name options`*
advanced 権限レベルで設定します	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、のマニュアルページを参照してください `vserver cifs options modify` コマンドを実行します

SMBユーザへのUNIXグループ権限付与の設定

このオプションを使用すると、ファイルの所有者でない SMB ユーザもファイルやディレクトリにアクセスする権限をグループに付与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. 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は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しないようにします	`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`

匿名ユーザのアクセス制限を設定します

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。

このタスクについて

。 `-restrict-anonymous` SMBサーバオプションはに対応します `RestrictAnonymous` Windowsのレジストリエントリ。

匿名ユーザは、ユーザ名、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。次の 3 つのうち、いずれかのアクセス制限設定を指定して、匿名ユーザのアクセスを制御することができます。

価値	説明
`no-restriction` （デフォルト）	匿名ユーザにアクセス制限を設定しません。
`no-enumeration`	匿名ユーザに対して列挙だけを制限します。

価値	説明
`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の概要で、ファイルセキュリティが **SMB** クライアントにどのように提供されるかを管理します

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によって、 UNIX セキュリティ形式のデータに対するファイルセキュリティの SMB クライアントへの提供方法を選択できます。それぞれの設定には利点があり、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 クライアントからアクセス権を変更することはできません。たとえば、所有していないファイルの所有権を変更することはできません。これは、UNIX システムではこ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。

- ユーザは、 Microsoft Office などの特定の Windows アプリケーションを使用して UNIX セキュリティ形式のボリューム上でファイルを編集および保存します。 ONTAP では、保存処理中に UNIX アクセス権を保持する必要があります。
- 使用するファイルの NTFS ACL を読み取ることを想定した特定の Windows アプリケーションが環境にある場合。

状況によっては、 NTFS ACL としての UNIX アクセス権の提供を無効にすることもできます。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のは、次のような場合です。

- UNIX アクセス権の変更は、マウントを使用して UNIX クライアントでのみ行うことができます。

SMB クライアントで UNIX セキュリティ形式のボリュームがマッピングされている場合は、 Security タブを使用できません。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たドライブとして表示されます。

- SMB を使用するアプリケーションでアクセスするファイルやフォルダに NTFS ACL を設定しており、データが UNIX セキュリティ形式のボリュームにあると失敗する可能性がある場合。

  ONTAP がボリュームを FAT として報告する場合、アプリケーションは ACL の変更を試みません。

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します

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。

このタスクについて

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て UNIX アクセス権を管理します

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。ドメインユーザの認証に使用されるデフォルトの方法は Kerberos です。

Kerberos 認証

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

Kerberos は Active Directory のプライマリ認証サービスです。Kerberos サーバの Kerberos Key Distribution Center （ KDC ；キー配布センター）サービスは、 Active Directory に対してセキュリティプリンシパルに関する情報の格納や取得を行います。NTLM モデルとは異なり、 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、直接 KDC にアクセスしてセッションの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を共有し、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たSVMを作成する前に（を参照） `-identity-preserve` オプションはに設定されています `false` （SnapMirror構成の場合）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について理解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。この情報は、セキュリティ設定が正しいかどうかを確認する際に役立ちます。

このタスクについて

表示されるセキュリティ設定は、そのオブジェクトのデフォルト値か、 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。

を使用しないでください `vserver cifs security show` 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サーバに対してコマンドを実行します。

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
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`*

表示する情報	入力するコマンド
SVM の特定のセキュリティ設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 入ることができます `-fields ?` 使用できるフィールドを決定します。

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 設定に関する情報を表示します

ローカル **SMB** ユーザに対するパスワードの複雑さの要件を有効または無効にします

パスワードの複雑さの要件を有効にすると、 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。

作業を開始する前に

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。

このタスクについて

を使用しないでください `vserver cifs security modify` 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サーバに対してコマンドを実行します。

手順

1. 次のいずれかを実行します。

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

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

ローカルユーザパスワードの要件

ローカルユーザのアカウントパスワードを変更しています

CIFS サーバの **Kerberos** セキュリティ設定を変更します

Kerberos クロックスキュー時間の許容最大値、 Kerberos チケットの有効期間、チケットの更新日の最大数など、 CIFS サーバの Kerberos セキュリティ設定の一部を変更できます。

このタスクについて

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

手順

1. 次の操作を 1 つ以上実行します。

状況	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`* デフォルトの設定は 5 分です。
Kerberos チケットの有効期間を時間で指定します。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` デフォルトの設定は 10 時間です。
チケットの更新日の最大数を指定します。	`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 のソケットのタイムアウトを指定します。この時間を過ぎるとすべての KDC が到達不能とマークされます。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* デフォルトの設定は 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を表示する"

"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サーバの最小認証セキュリティレベルを設定する

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。

このタスクについて

- 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ません。
- LMCompatibilityLevel は SMB クライアント認証にのみ適用され、 admin 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うちの 1 つに設定することができます。

価値	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 暗号化を有効または無効にします

AES 暗号化を使用して **Kerberos** ベースの通信のセキュリティを強化できます

Kerberos ベースの通信による最も強固なセキュリティを実現するために、 AES-256 暗号化と AES-128 暗号化を SMB サーバで有効にすることができます。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 セッションの設定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
- DES （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するようになります。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。を使用できます `-advertised-enc-types` 推奨される暗号化タイプを有効にするオプション。また、弱い暗号化タイプを無効にする場合にも使用できます。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 で利用可能な Intel AES New Instructions （ Intel AES NI ）は AES アルゴリズムの改良版で、サポート対象のプロセッサファミリーでのデータ暗号化処理を高速化します。 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 暗号化を有効または無効にします

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。 Active Directory （ AD ） KDC との Kerberos ベースの通信に AES 暗号化タイプを SMB サーバで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、および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	デフォルトでは	はい。
9.12.1:	手動で実行する	はい。
9.11.1以前	手動で実行する	いいえ

ONTAP 9.12.1以降では、を使用してAES暗号化を有効または無効にします `-advertised-enc-types` オプション。AD KDCにアドバタイズする暗号化タイプを指定できます。デフォルト設定はです `rc4` および `des` ただし、`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`暗号化タイプと`DES`暗号化タイプを明示的に無効にすることもできます。`ONTAP 9.11.1`以前では、 `-is-aes-encryption-enabled` AES暗号化を有効または無効にするオプションを指定できません。また、暗号化タイプは指定できません。

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

IDが保持されないディザスタリカバリデスティネーションとしてSVMが設定されている場合（ `-identity-preserve` オプションはに設定されています `false` SnapMirrorの設定では、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	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

注： `-is-aes-encryption-enabled` オプションはONTAP 9.12.1では廃止され、以降のリリースでは削除される可能性があります。

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields 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 サーバを含む 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	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. AES暗号化が設定どおり有効または無効になっていることを確認します。 `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

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

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 サーバを含む 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 署名を使用してネットワークのセキュリティを強化します

SMB 署名を使用してネットワークセキュリティの概要を強化します

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ることのないようにします。デフォルト ONTAP では、クライアントから要求されたときに SMB 署名がサポートされます。ストレージ管理者は、必要に応じて、 SMB 署名を必須にするように SMB サーバを設定できます。

SMB 署名ポリシーが **CIFS** サーバとの通信に与える影響

CIFS サーバの SMB 署名セキュリティ設定に加えて、クライアントと 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。この設定をクライアントで無効にすると、クライアントの CIFS サーバとの通信は、 CIFS サーバ上の SMB 署名の設定によって異なります。

- `Microsoft network client: Digitally sign communications (always)`

  この設定は、クライアントがサーバとの通信に SMB 署名を必要とするかどうかを制御します。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に基づきます `Microsoft network client: Digitally sign communications (if server agrees)` およびCIFSサーバの設定。

> 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
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
署名が無効になっており、必要です	署名	署名
署名が有効になっており、必要です	署名	署名

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
署名が必要です	署名	署名

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	はい。	はい。	有効（不要）	無効（不要）	必須
SMB 2.x	HMAC SHA-256	いいえ	はい。	必要ありません	必要ありません	必須
SMB 3.0	AES-CMAC ：	いいえ	はい。	必要ありません	必要ありません	必須

Microsoftではの使用を推奨していません `Digitally sign communications (if client agrees)` または `Digitally sign communications (if server agrees)` グループポリシーの設定。Microsoftでは、の使用も推奨していません `EnableSecuritySignature` レジストリ設定。これらのオプションはSMB 1の動作にのみ影響し、で置き換えることができます `Digitally sign communications (always)` グループポリシー設定または `RequireSecuritySignature` レジストリ設定。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、 Windows クライアントとのすべての SMB 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上のノード）の両方に影響します。

パフォーマンスへの影響は、 CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

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、新しい暗号化の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が向上します。SMB 署名オフロードは、 SMB 署名が有効になっている場合にデフォルトで有効になります。

SMB 署名のパフォーマンスを向上させるには、 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 署名のパフォーマンスへの影響には幅があるため、影響の程度はご使用のネットワーク環境でのテストによってのみ検証可能です。

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

SMB 署名の設定に関する推奨事項

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

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

状況	推奨事項
クライアントとサーバの間の通信のセキュリティを強化する必要がある	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)` クライアントのセキュリティ設定。
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 のマニュアル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サーバに複数のが含まれています `A` CIFSサーバのエントリを記録します。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サーバのDNSは次のようになります `A` レコードエントリ：

```
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SMB署名要求で同じ共有に接続します `S:\` （パスを使用して接続を維持します `O:\`）。
4. その結果、両方でデータにアクセスするときにSMB署名が使用されます `O:\` および `S:\` ドライブ。

受信 **SMB** トラフィックの **SMB** 署名要求を有効または無効にします

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 署名要求を無効にできます。

このタスクについて

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。
>
> このような場合は、サポートされているバージョンの ONTAP で最初に行われた SMB 署名の設定が、リバートとその後のアップグレードを通して維持されます。

Storage Virtual Machine（SVM）ディザスタリカバリ関係を設定する際にで選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、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を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` （ID保持）。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。

を設定した場合は `-identity-preserve` オプションをに設定します `false` （ID保持なし）。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ている場合は、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	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. での値を確認して、SMB署名要求が有効か無効かを確認します `Is Signing Required` 次のコマンドの出力のフィールドは、目的の値に設定されます。 `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

例

次の例は、 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を確認します

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

手順

1. 次のいずれかを実行します。

表示する情報	入力するコマンド
指定した Storage Virtual Machine （ SVM ）上の署名されたすべてのセッション	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`

表示する情報	入力するコマンド
SVM 上の指定したセッション ID を持つ署名されたセッションの詳細です	`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
```

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

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

関連情報

SMB 署名済みセッションの統計を監視します

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

このタスクについて

。 `statistics` advanced権限レベルでコマンドを実行すると、が表示されます `signed_sessions` 署名済みSMBセッションの数を監視するために使用できるカウンタ。。 `signed_sessions` カウンタには、次の統計オブジェクトがあります。

- `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。

  SMB 3.0の統計はの出力に表示されます `smb2` オブジェクト。

署名されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `signed_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

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、サンプルが固定された状態になります。データ収集を停止しないと、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、傾向を確認するのに役立ちます。

手順

1. 権限レベルをadvancedに設定+
   `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`*`]`

   指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、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. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 署名統計情報を表示します。

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

表示する情報	入力するコマンド
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、オプションのを指定します `-node` パラメータ

5. admin権限レベルに戻ります。+
   `set -privilege admin`

例

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

次のコマンドは、 advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

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

次のコマンドは、サンプルのデータ収集を停止します。

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

次のコマンドは、ノードが署名した SMB セッションと確立されたセッションをサンプルから表示します。

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

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

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

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

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

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

    Counter                                                  Value
    -------------------------------- -------------------------
    node_name                                                node2
    signed_sessions                                              1
```

次のコマンドは、 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に必要な **SMB** 暗号化を **SMB** サーバで設定します

SMB暗号化の概要

SMB を介したデータ転送での SMB 暗号化は、 SMB サーバで有効化または無効化できるセキュリティ強化です。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 暗号化が提供する高度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。

暗号化された 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。Windows Server 2012 および Windows 8 以降の Windows クライアントでは、 SMB 暗号化がサポートされます。

SVM での SMB 暗号化は、次の 2 つの設定によって制御されます。

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

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

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

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
正しいです	いいえ	SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、 SMB セッション全体で暗号化が行われます。
正しいです	正しいです	共有レベルの暗号化には関係なく SVM のすべての共有でサーバレベルの暗号化が有効です。この設定では、 SMB セッション全体で暗号化が行われます。
いいえ	正しいです	特定の共有で共有レベルの暗号化が有効です。この設定では、ツリー接続から暗号化が行われます。

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
いいえ	いいえ	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、 Windows クライアントとのすべての SMB 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上のノード）の両方に影響します。

パフォーマンスへの影響は、 CPU 使用率の増加としてクライアントとサーバの両方に表示されますが、ネットワークトラフィックの量は変わりません。

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、新しい暗号化のオフロードアルゴリズムによって、暗号化された SMB トラフィックのパフォーマンスが向上します。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に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高めるには、 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可能です。

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 暗号化を有効にすると、 ONTAP はすべての要求に対して要求を復号化して応答を暗号化する必要があります。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** 暗号化要求を有効または無効にします

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。

このタスクについて

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に選択した値 `-identity-preserve` のオプション `snapmirror create` コマンドは、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を決定します。

を設定した場合は `-identity-preserve` オプションをに設定します `true` （ID保持）では、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。

を設定した場合は `-identity-preserve` オプションをに設定します `false` （ID保持なし）。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	`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` フィールドが表示されます `true` CIFSサーバおよびでSMB暗号化要求が有効になっている場合 `false` 無効になっている場合。

例

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

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

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

クライアントが暗号化 **SMB** セッションを使用して接続しているかどうかを確認します

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。

このタスクについて

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 暗号化統計情報を監視する

SMB 暗号化の統計を監視し、確立されたセッションおよび共有接続のうち、暗号化されたものと暗号化されていないものを区別できます。

このタスクについて

。 `statistics` advanced権限レベルでコマンドを実行する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
`rejected_unencrypted_sessions`	クライアントに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数を示します
`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。

  SMB 3.0の統計はの出力に表示されます `cifs` オブジェクト。 暗号化されたセッションの数をセッションの合計数と比較する場合は、の出力を比較できます `encrypted_sessions` の出力でカウンタに設定します `established_sessions` カウンタ。

  暗号化された共有接続数を共有接続の合計数と比較する場合は、の出力を比較します `encrypted_share_connections` の出力でカウンタに設定します `connected_shares` カウンタ。

- `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、サンプルが固定された状態になります。データ収集を停止しないと、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、傾向を確認するのに役立ちます。

手順

1. 権限レベルをadvancedに設定+
   `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`*`]`

   指定しない場合は、を実行します `-sample-id` パラメータを指定すると、サンプルIDが生成され、このサンプルがCLIセッションのデフォルトのサンプルとして定義されます。の値 `-sample-id` はテキスト文字列です。同じCLIセッションでこのコマンドを実行する場合に、を指定しないでください `-sample-id` パラメータを指定すると、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. を使用します `statistics stop` サンプルのデータ収集を停止するコマンド。
4. SMB 暗号化統計情報を表示します。

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*]`
暗号化されていないセッションは	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒否された暗号化されていない
`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、オプションのを指定します `-node` パラメータ

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 の暗号化統計情報を監視する方法を示します。

次のコマンドは、 advanced 権限レベルへの変更を行います。

```
cluster1::> set -privilege advanced

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

次のコマンドは、新しいサンプルのデータ収集を開始します。

```
cluster1::*> statistics start -object 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 セッション数と確立されたセッション数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、接続された SMB 共有数と暗号化された SMB 共有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 ）サーバへの照会

に対する 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、シークレットキーの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`。

SVMでCIFSトラフィックに対するLDAPの署名と封印が `-session-security-for-ad-ldap` オプションをに設定します `vserver cifs security modify` コマンドを実行します

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。

作業を開始する前に

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}`

   署名を有効にできます (`sign`、データ整合性）、署名と封印 (`seal`、データ整合性と暗号化）、またはどちらでもない `none`、署名または封印なし）。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、で対応する設定を有効にする必要があります `-session-security` のオプション `vserver services name-service ldap client modify` コマンドを実行します

LDAP over TLS を設定する

自己署名ルート **CA** 証明書のコピーをエクスポートします

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

作業を開始する前に

Active Directory 証明書サービスがすでにインストールされ、 CIFS サーバが属しているドメイン用に設定されている必要があります。Active Directory 証明書サービスのインストールと設定の詳細については、Microsoft TechNet ライブラリを参照してください。

"Microsoft TechNet ライブラリ： technet.microsoft.com"

ステップ

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

   "Microsoft TechNet ライブラリ： technet.microsoft.com"

完了後

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** にインストールします

LDAP サーバにバインドするときに TLS を使用した LDAP 認証が必要な場合は、まず自己署名ルート CA 証明書を SVM にインストールする必要があります。

このタスクについて

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、 Online Certificate Status Protocol （ OCSP ）を使用してデジタル証明書の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. 証明書を開きます `.pem` ファイルテキストエディタを使用して、で始まる行を含めて証明書をコピーします `-----BEGIN CERTIFICATE-----` で終わる `-----END CERTIFICATE-----`をクリックし、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ていることを確認します。 `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。

ONTAP 9.10.1 以降では、 Active Directory （ AD ）とネームサービスの両方の LDAP 接続で、 LDAP チャネルバインドが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に設定されている場合にのみ、 LDAP 接続でチャネルバインドを試行します。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、を使用します `-try-channel-binding-for-ad-ldap` パラメータと `vserver cifs security modify` コマンドを実行します

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"。

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ます `true`： `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、も変更する必要があります `-use-start-tls` オプションを使用します `vserver services name-service ldap client modify` コマンドを実行します

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

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することができます。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。

作業を開始する前に

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。

このタスクについて

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 *

クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされます。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の 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`

  各マルチチャネルセッション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、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

- `-max-lifs-per-session`

  各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 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して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 が割り当てられた 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 **Windows** ユーザから **UNIX** ユーザへのマッピングを設定する

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。

このタスクについて

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する必要があります。このオプションを null 文字列に設定すると、どのユーザも UNIX デフォルトユーザとして CIFS サーバにアクセスできません。つまり、 CIFS サーバにアクセスするためには、各ユーザがパスワードデータベースにアカウントを持つ必要があります。

ユーザがデフォルトの 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 ユーザを無効にします	`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** ユーザを設定します

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）。

このタスクについて

ゲスト UNIX アカウントを設定する場合は、次の点に注意する必要があります。

- CIFS サーバがホームドメインまたは信頼できるドメインのドメインコントローラ、ローカルデータベースのどちらかに対してユーザを認証できず、このオプションが有効である場合、 CIFS サーバはユーザをゲストユーザとみなし、そのユーザを指定した UNIX ユーザにマッピングします。
- 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 ユーザを設定します	`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           : -
   ```

Administrators グループをルートにマッピングします

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。

このタスクについて

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` ディレクトリには、AdministratorsグループがONTAP 構成ファイルにアクセスできるようにするファイルレベルのACLが設定されています。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`
2. 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	作業
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` がなくても、Administratorsグループ内のすべてのアカウントはrootとみなされます `/etc/usermap.cfg` アカウントをrootにマッピングするエントリ。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します

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。

このタスクについて

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

をクリックします `vserver cifs options modify` コマンドを使用すると、Windowsクライアントのリソース消費を制御できます。ファイルオープン、セッションオープン、変更通知要求が異常に多い場合など、正常な範囲を超えてリソースを消費しているクライアントがある場合に便利です。

には次のオプションがあります `vserver cifs options modify` Windowsクライアントのリソース消費を制御するコマンドが追加されました。これら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で設定された上限の 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 ツリーあたりの同じファイルの最大オープン数

- `-max-same-user-sessions-per-connection`

  同じユーザが接続ごとに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*）

デフォルトの制限および現在の設定を表示する方法については、マニュアルページを参照してください。

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側で開始され、サーバ側で制御されます。

SMB接続で許可できる未処理要求の最大数は、で制御されます `-max-credits` オプション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のパフォーマンスを向上

従来の **oplock** および **oplock** リースの概要でクライアントのパフォーマンスを向上

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。これにより、クライアントは、目的のファイルへのアクセス要求をサーバに定期的に通知しなくても、ファイルの読み書きを実行できます。これにより、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 リースでは、クライアントが、自身による複数の SMB オープンにおいてキャッシュ状態を取得し、保持できます。

oplock は次の 2 つの方法で制御できます。

- 共有プロパティで、を使用します `vserver cifs share create` 共有の作成時にコマンドを実行するか、またはを実行します `vserver share properties` 作成後のコマンド。
- qtreeプロパティ。を使用します `volume qtree create` コマンドを使用してqtreeを作成するか、コマンドを使用します `volume qtree oplock` 作成後のコマンド。

oplock を使用するときの書き込みキャッシュデータ消失に関する考慮事項

状況によっては、あるプロセスがファイルに対して排他的な oplock を保持している場合に、別のプロセスがそのファイルを開こうとすると、最初のプロセスはキャッシュされたデータを無効にし、書き込みとロックをフラッシュする必要があります。クライアントは oplock を放棄し、ファイルにアクセスする必要があります。このフラッシュ時にネットワーク障害が発生すると、キャッシュされた書き込みデータが失われる可能性があります。

- 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

  キャッシュ自体にはエラー処理がありません。アプリケーションがエラー処理を行います。アプリケーションがキャッシュへの書き込みを行うと、書き込みは常に完了します。キャッシュがネットワーク経由でターゲットシステムに書き込みを行う場合、書き込みは完了していると仮定する必要があります。これは、完了していない場合、データが失われるためです。

SMB 共有の作成時に oplock を有効または無効にします

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。Storage Virtual Machine （ SVM ）上にある SMB 共有では、 oplock が有効になっています。場合によっては、 oplock の無効化が必要になることがあります。oplock は共有ごとに有効または無効にできます。

このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームの oplock の設定よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。

oplock 共有プロパティに加えて、その他の共有プロパティをカンマで区切って指定できます。その他の共有パラメータを指定することもできます。

手順

1. 該当する操作を実行します。

状況	作業
共有の作成時に共有で oplock を有効にします	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,...]` 共有にデフォルトの共有プロパティのみを設定する場合は、です `oplocks`、 `browsable`および `changenotify` 有効にすると、を指定する必要はありません `-share-properties` SMB共有を作成するときのパラメータ。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、を指定する必要があります `-share-properties` パラメータに指定し、その共有に使用する共有プロパティのリストを指定します。
共有の作成時に共有で oplock を無効にします	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、を指定することはできません `oplocks` プロパティ。

関連情報

既存の SMB 共有で oplock を有効または無効にします

oplock ステータスを監視しています

ボリュームおよび **qtree** で **oplock** を有効または無効にするためのコマンド

oplock を使用すると、クライアントによってファイルがロックされてコンテンツがローカルにキャッシュされるため、ファイル操作のパフォーマンスが向上します。ボリュームや qtree の oplock を有効または無効にするためのコマンドを理解しておく必要があります。また、いつボリュームおよび qtree で oplock を有効または無効にできるかについても理解しておく必要があります。

- ボリュームではデフォルトで oplock が有効になっています。

- ボリュームの作成時に 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のデフォルトの 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 設定を継承します。この設定はデフォルトで有効になっています。ただし、新しい qtree に oplock 設定を指定すると、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 の oplock を有効にします	`volume qtree oplocks` を使用 `-oplock-mode` パラメータをに設定します `enable`
ボリュームまたは qtree の oplock を無効にします	`volume qtree oplocks` を使用 `-oplock-mode` パラメータをに設定します `disable`

関連情報

oplock ステータスを監視しています

既存の **SMB** 共有で **oplock** を有効または無効にします

Storage Virtual Machine （ SVM ）上の SMB 共有では、 oplock がデフォルトで有効になっています。場合によっては、 oplock の無効化が必要になることがあります。または、以前に共有で oplock を無効にした場合に、 oplock を再度有効にすることもできます。

このタスクについて

共有を含むボリュームで oplock が有効になっているが、その共有の oplock 共有プロパティが無効になっている場合、その共有の oplock は無効になります。共有での oplock の無効化は、ボリュームでの oplock の有効化よりも優先されます。共有で oplock を無効にすると、便宜的 oplock と oplock リースの両方が無効になります。既存の共有での oplock の有効化と無効化はいつでも実行できます。

ステップ

1. 該当する操作を実行します。

状況	作業
既存の共有を変更して、共有で oplock を有効にします	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、共有プロパティの既存のリストに追加されます。以前に指定した共有プロパティは有効なままです。
既存の共有を変更して共有で oplock を無効にします	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、削除しなかった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 共有の作成時における oplock の有効化と無効化

oplock ステータスを監視しています

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 ステータスを監視します

oplock ステータスについて、情報を監視、表示できます。この情報を使用して、 oplock が設定されたファイル、 oplock のレベルや oplock の状態レベル、 oplock リースの使用の有無を確認できます。また、手動での解除が必要となる可能性のあるロックについて、情報を確認することもできます。

このタスクについて

すべての oplock についての情報を要約形式または詳細なリスト形式で表示できます。オプションのパラメータを使用すると、既存のロックの一部について情報を表示することもできます。たとえば、クライアントの IP アドレスやパスを指定して、該当するロックのみを返すように指定できます。

従来の oplock および oplock リースについて、次の情報を表示できます。

- oplock が有効な SVM 、ノード、ボリューム、 LIF
- ロック UUID
- oplock が有効なクライアントの IP アドレス
- oplock が有効なパス
- ロックのプロトコル（ SMB ）およびロックのタイプ（ oplock ）
- ロックの状態
- oplock レベル
- 接続の状態および SMB の有効期限
- oplock リースが許可されている場合は、 Open Group ID

を参照してください `vserver oplocks show` 各パラメータの詳細な概要 のマニュアルページ

手順

1. を使用してoplockステータスを表示します `vserver locks show` コマンドを実行します

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は、で許可されています `read-batch` oplockレベル：

```
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`。を使用してファイルにoplockリースが許可されています `batch` IPアドレスがのクライアントに対するoplockレベル `10.3.1.3`：

> 詳細情報を表示する場合に、このコマンドを使用すると、 oplock の情報と共有ロックの情報を別々に表示できます。この例では、 oplock の情報のみが表示されています。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

関連情報

SMB 共有の作成時における oplock の有効化と無効化

既存の SMB 共有で oplock を有効または無効にします

ボリュームおよび qtree で oplock を有効または無効にするためのコマンド

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の説明を参照してください

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 Universally Unique Identifier （ UUID ）一覧

関連情報

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

"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。

- 高度な監査ポリシー設定：

  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。

  を使用して設定します `Audit Central Access Policy Staging` を設定します `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO：

  > 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

    を使用して設定します `Registry` GPO：

- グループポリシーの更新間隔のランダムオフセット

  を使用して設定します `Registry` GPO：

- BranchCache のハッシュの発行

  BranchCache のハッシュの発行 GPO は、 BranchCache の動作モードに対応します。次の 3 つの動作モードがサポートされています。

  - 共有ごと
  - all-shares
  - 無効
    を使用して設定します `Registry` GPO：

- 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
    を使用して設定します `Registry` GPO：

> BranchCache GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で BranchCache を構成する必要があります。SVM で BranchCache が構成されていない場合、 GPO 設定は適用されず、破棄されます。

- セキュリティ設定

  - 監査ポリシーとイベントログ

    - 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となるログオンイベントの種類を指定します。

      - 監査しないでください
      - 成功イベントのみ監査
      - 障害イベントの監査
      - 成功イベントと失敗イベントの両方を監査します
        を使用して設定します `Audit logon events` を設定します `Local Policies/Audit Policy` GPO：

        > 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となるオブジェクトアクセスの種類を指定します。

- 監査しないでください
- 成功イベントのみ監査
- 障害イベントの監査
- 成功イベントと失敗イベントの両方を監査します
  を使用して設定します `Audit object access` を設定します `Local Policies/Audit Policy` GPO：

> 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
  - イベントログを上書きしない（手動でログを消去）
    を使用して設定します `Retention method for security log` を設定します `Event Log` GPO：

- 最大ログサイズ

  監査ログの最大サイズを指定します。

  を使用して設定します `Maximum security log size` を設定します `Event Log` GPO：

> 監査ポリシーとイベントログ GPO 設定を使用するには、その設定を適用する CIFS 対応の SVM 上で監査を構成する必要があります。SVM で監査が構成されていない場合、GPO 設定は適用されず、破棄されます。

◦ ファイルシステムのセキュリティ

GPO を通してファイルセキュリティを適用するファイルまたはディレクトリのリストを指定します。

を使用して設定します `File System` GPO：

> SVM 内にファイルシステムセキュリティ GPO を構成するボリュームパスが存在している必要があります。

◦ Kerberos ポリシー

- 最大クロックスキュー

  コンピュータクロック同期の最大許容誤差を分単位で指定します。

  を使用して設定します `Maximum tolerance for computer clock synchronization` を設定します `Account Policies/Kerberos Policy` GPO：

- 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。

を使用して設定します `Maximum lifetime for user ticket` を設定します `Account Policies/Kerberos Policy` GPO：

- チケットの更新の有効期間

  ユーザチケットの更新の最大有効期間を日単位で指定します。

を使用して設定します `Maximum lifetime for user ticket renewal` を設定します `Account Policies/Kerberos Policy` GPO：

- ユーザ権限の割り当て（権限）

  - 所有権を取得します

    セキュリティ保護が可能なオブジェクトの所有権を持つユーザとグループのリストを指定します。

    を使用して設定します `Take ownership of files or other objects` を設定します `Local Policies/User Rights Assignment` GPO：

  - セキュリティ権限

    ファイル、フォルダ、 Active Directory オブジェクトなどの個々のリソースへのオブジェクトアクセスの監査オプションを指定できるユーザとグループのリストを指定します。

    を使用して設定します `Manage auditing and security log` を設定します `Local Policies/User Rights Assignment` GPO：

  - 通知権限の変更（トラバースチェックのバイパス）

    ユーザとグループがトラバースするディレクトリに対する権限を持っていなくても、ディレクトリツリーをトラバースできるユーザとグループのリストを指定します。

ファイルやディレクトリの変更通知を受け取るユーザにも同じ権限が必要です。を使用して設定します `Bypass traverse checking` を設定します `Local Policies/User Rights Assignment` GPO：

- 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。

を使用して設定します `Microsoft network server: Digitally sign communications (always)` を設定します `Security Options` GPO：

- restrict anonymous （匿名の制限

匿名ユーザの制限内容に次の 3 つの GPO 設定を指定します。

  - Security Account Manager （ SAM ）アカウントを列挙しない：

このセキュリティ設定は、コンピュータへの匿名接続に付与される追加の権限を決定します。このオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts` を設定します `Local Policies/Security Options` GPO：

- 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、匿名による SAM アカウントと共有の列挙を許可するかどうかを決定します。このオプションはと表示されます `no-enumeration` ONTAP （有効になっている場合）。

  を使用して設定します `Network access: Do not allow anonymous enumeration of SAM accounts and shares` を設定します `Local Policies/Security Options` GPO：

- 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。このオプションはと表示されます `no-access` ONTAP （有効になっている場合）。

  を使用して設定します `Network access: Restrict anonymous access to Named Pipes and Shares` を設定します `Local Policies/Security Options` GPO：

  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は、 `Resultant restriction for anonymous user` Output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されます。表示される可能性がある制限結果は、次のとおりです。

- `no-access`

  匿名ユーザは、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。この制限結果は、の場合に表示されます `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが有効になっている。

- `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 アカウントと共有は列挙できません。この制限は、次の両方の条件に該当する場合に適用されます。

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
  - またはをクリックします `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、列挙できます。この制限は、次の両方の条件に該当する場合に適用されます。

  - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPOが無効になっています。
  - 両方とも `Network access: Do not allow anonymous enumeration of SAM accounts`

および `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO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、組み込みまたはユーザ定義のグループのメンバーシップを一元管理することができます。グループポリシーを通して制限されたグループを適用する場合、CIFS サーバローカルグループのメンバーシップは、適用されるグループポリシーで定義されているメンバーリスト設定に一致するように自動的に設定されます。

を使用して設定します `Restricted Groups` GPO：

- 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 サーバ上で GPO サポートを有効または無効にします

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

"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

匿名ユーザのアクセス制限を設定します

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、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ます。 "ONTAP One"。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 ドメインに参加している必要があります。
- SMB サーバ管理ステータスがオンになっている必要があります。
- 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 サーバでグループポリシーオブジェクト（ GPO ）のサポートを有効または無効にできます。CIFS サーバ上で GPO のサポートを有効にすると、グループポリシー（ CIFS サーバコンピュータオブジェクトを含む組織単位に適用されるポリシー）に定義されている該当する GPO が CIFS サーバに適用されます。

このタスクについて

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
GPOs を有効にします。	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`
GPOs 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 サーバ上の GPO 設定を手動で更新します

GPO 設定に関する情報を表示します

CIFS サーバでの GPO の更新方法の概要

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 分に 1 回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、新しい GPO ポリシー設定を適用するには、ONTAP コマンドを使用して CIFS サーバで手動更新をトリガーします。

- デフォルトでは、すべての GPO を 90 分に 1 回確認し、必要に応じて更新。

  この間隔は設定可能で、を使用して設定できます `Refresh interval` および `Random offset` GPO設定。

  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 を 16 時間に 1 回更新。

  ONTAP は、変更の有無にかかわらず、 16 時間に 1 回セキュリティ設定の GPO を取得して適用します。

  > 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手動ですべての GPO を更新。

  このコマンドは、ウィンドウをシミュレートします `gpupdate.exe`/force`コマンド。

関連情報

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバ上の GPO 設定を手動で更新します

CIFS サーバの Group Policy Object （ GPO ；グループポリシーオブジェクト）設定を直ちに更新するには、設定を手動で更新します。変更された設定のみを更新することも、以前に適用されていて変更されていない設定を含めてすべての設定を強制的に更新することもできます。

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`*

更新する項目	入力するコマンド
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

GPO 設定に関する情報を表示します

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。

このタスクについて

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か、または 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ができます。

手順

1. 次のいずれかの操作を実行し、 GPO 設定に関する情報を表示します。

情報を表示するグループポリシー設定	入力するコマンド
Active Directory で定義されています	`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、 vs1 という CIFS 対応の 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 サーバ上で GPO サポートを有効または無効にします

制限されたグループの **GPO** に関する詳細情報を表示します

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。

このタスクについて

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
- グループポリシーのバージョン
- リンク

  グループポリシーを設定するレベルを指定します。出力される値は次のとおりです。

  - `Local` グループポリシーがONTAP で設定されている場合

- `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組織単位（OU）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です
- 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、ここに記載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もできます。

ステップ

1. 次のいずれかの操作を実行し、制限されたグループのすべての GPO に関する情報を表示します。

情報を表示する制限されたグループのすべての **GPO**	入力するコマンド
Active Directory で定義されています	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

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、グループポリシーオブジェクト（ GPO ）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。

このタスクについて

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
- 修正日時
- メンバールール

> ワークグループモードの CIFS サーバについては、 GPO をサポートしていないため情報は表示されません。

ステップ

1. 次のいずれかの操作を実行し、集約型アクセスポリシーに関する情報を表示します。

情報を表示するすべての集約型アクセスポリシー	入力するコマンド
Active Directory で定義されています	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
CIFS サーバに適用されます	`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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

Active Directory で定義されている集約型アクセスポリシーに関連付けられた集約型アクセスポリシールールに関する詳細情報を表示できます。また、集約型アクセスポリシーの GPO （グループポリシーオブジェクト）を介して CIFS サーバに適用されている集約型アクセスポリシールールに関する情報も表示できます。

このタスクについて

定義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 名です
- 集約型アクセスルールの名前
- 説明
- 作成時間
- 修正日時
- 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 で定義されています	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
CIFS サーバに適用されます	`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たすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: 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、クラスタ上で Storage Virtual Machine （ SVM ）に適用されている集約型アクセスポリシーに関連付けられたすべての集約型アクセスポリシールールの情報を表示します。

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: 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

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

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
ドメインアカウントのパスワードを変更またはリセットします。パスワードがわかっている場合	`vserver cifs domain password change`
ドメインアカウントパスワードをリセットします。パスワードがわからない場合	`vserver cifs domain password reset`
コンピュータアカウントパスワードの自動変更を行うために SMB サーバを設定する	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
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を管理します

検出されたサーバに関する情報を表示します

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 サーバを停止または起動しています

サーバをリセットおよび再検出します

CIFS サーバでサーバのリセットと再検出を行うと、 LDAP サーバおよびドメインコントローラに格納されている情報が CIFS サーバに破棄されます。サーバの情報が破棄されたあと、それらの外部サーバに関する最新の情報が再取得されます。これは、接続されているサーバが適切に応答しない場合に役立ちます。

手順

1. 次のコマンドを入力します。 `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. 再検出されたサーバに関する情報を表示します。 `vserver cifs domain discovered-servers show -vserver vserver_name`

例

次の例は、 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を表示する

CIFS サーバを停止または起動しています

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。サイトまたは優先 DC のプールに検出を制限できるため、環境によってはパフォーマンスの向上につながります。

このタスクについて

デフォルトでは、任意の優先 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 を含めて、使用可能なすべての DC 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は、検出方法を変更できます。

ONTAP 9.3以降のリリースでは、 `discovery-mode` のパラメータ `cifs domain discovered-servers` コマンドでは、次のいずれかの検出オプションを選択できます。

- ドメイン内のすべての DC が検出されます。
- ローカルサイト内の DC だけが検出されます。

  。 `default-site` SMBサーバのパラメータは、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。

- サーバの検出は実行せず、優先 DC のみを使用するように SMB サーバを設定します。

  このモードを使用するには、最初に SMB サーバに対して優先 DC を定義する必要があります。

作業を開始する前に

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}`

   のオプション `mode` パラメータ：

   - `all`

     使用可能なすべての DC を検出します（デフォルト）。

   - `site`

     DC の検出対象をサイトに制限します。

   - `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を追加する

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ドメインコントローラを追加することができます。

このタスクについて

指定したドメインに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、新しいリストが既存のリストに統合されます。

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*`はい。 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の追加、表示、削除を行うコマンドについて説明します。

状況	使用するコマンド
優先ドメインコントローラを追加する	`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** 接続を有効にします

ONTAP 9.1 以降では、 SMB 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。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、 SMB2 がデフォルトで有効になります。

このタスクについて

。 `smb2-enabled-for-dc-connections` コマンドオプションを使用すると、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 が有効、 SMB 2.0 が無効になります。ONTAP 9.2 のシステムデフォルトでは、 SMB 1.0 が有効になり、 SMB 2.0 が有効になります。ドメインコントローラは、最初に SMB 2.0 をネゴシエートし、失敗した場合は 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 では、SMB 1.0 を無効にした場合、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。

詳細情報：

- "有効なSMBのバージョンの確認"。
- "サポートされる SMB のバージョンと機能"。

> 状況 `-smb1-enabled-for-dc-connections` がに設定されます `false` 間 `-smb1-enabled` がに設定されます `true`ONTAP では、クライアントとしてのSMB 1.0の接続は拒否されますが、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. を使用して、該当するコマンドを実行します `smb2-enabled-for-dc-connections` オプション

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	`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します

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。

このタスクについて

ONTAP では、ドメインコントローラ（DC）通信の暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`;デフォルトはです `false`。このオプションを設定すると、 SMB3 でのみ暗号化がサポートされるため、 SMB3 プロトコルのみが使用されます。

暗号化されたDC通信が必要な場合は、を参照してください `-smb2-enabled-for-dc-connections` ONTAP はSMB3接続のみをネゴシエートするため、この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** 環境の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

非 **Kerberos** 環境でストレージにアクセスする場合は、 **null** セッションを使用します

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実現方法

null セッション共有には認証が必要ないため、 null セッションアクセスが必要なクライアントは、その IP アドレスがストレージシステムにマッピングされている必要があります。

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、共有の列挙など一部の 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 は、でWindows RestrictAnonymousレジストリ設定値をサポートしています `-restrict-anonymous` オプションこれにより、マッピングされていない null ユーザが表示またはアクセスできるシステムリソースの範囲を制御できます。たとえば、共有の一覧や 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できます。。 `vserver cifs options modify` および `vserver cifs options show` の詳細については、のマニュアルページを参照してください `-restrict-anonymous` オプション

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たり、null セッションクライアントのみに適用されるストレージシステムリソース権限を設定したりできます。

ONTAP には、マッピング構文が用意されています `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アドレスを指定するコマンドセット。null ユーザ用のグループを作成したら、 null セッションのみに適用されるストレージシステムリソースのアクセス制限およびリソース権限を指定できます。null ユーザは匿名ログオンとみなされます。null ユーザは、ホームディレクトリに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なアクセスを防止するため、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

匿名ユーザのアクセス制限を設定します

null ユーザにファイルシステム共有へのアクセスを許可します

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に使用するグループを割り当てて null セッションクライアントの IP アドレスを記録し、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リストにその IP アドレスを追加します。

手順

1. を使用します `vserver name-mapping create` IP修飾子を使用して、nullユーザを任意の有効なWindowsユーザにマッピングするコマンド。

   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. を使用します `vserver name-mapping show` コマンドを入力し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. を使用します `vserver cifs options modify –win-name-for-null-user` nullユーザにWindowsメンバーシップを割り当てるコマンド。

   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. を使用します `vserver cifs options show` コマンドを使用して、nullユーザのWindowsユーザまたはグループへのマッピングを確認します。

```
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 エイリアスの概要を管理します

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 サーバに統合して、 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。

SMB サーバの作成時または SMB サーバ作成後の任意の時点で、 NetBIOS エイリアスのリストを指定できます。リストへの NetBIOS エイリアスの追加や削除は、いつでも行うことができます。SMB サーバには NetBIOS エイリアスリスト内のどの名前を使用しても接続できます。

関連情報

NetBIOS over TCP 接続に関する情報を表示する

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。

このタスクについて

- NetBIOS エイリアス名は 15 文字以内にする必要があります。
- 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。
   - 現在のリストが空である場合、 NetBIOS エイリアスの新しいリストが作成されます。
2. NetBIOSエイリアスが正しく追加されたことを確認します。 `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   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を表示する

NetBIOS エイリアスリストから **NetBIOS** エイリアスを削除します

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。

このタスクについて

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。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 - をの値として指定します `-netbios-aliases` パラメータ

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`

表示する情報	入力するコマンド
NetBIOS エイリアスのリストを含む詳細な CIFS サーバ情報	`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 CIFS サーバの詳細情報の一部として表示します。

```
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を確認します

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、接続の問題のトラブルシューティングを行う場合に役立ちます。

このタスクについて

を使用する必要があります `-instance` SMB接続に関連付けられているNetBIOSエイリアス（ある場合）を表示するためのパラメータ。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は、

の出力が表示されます `NetBIOS Name` フィールドはです `-` （ハイフン）。

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、セッション ID 1 の SMB 接続に使用されている NetBIOS エイリアスに関する情報を表示します。

```
vserver cifs session show -session-id 1 -instance
```

```
                          Node: node1
                       Vserver: vs1
                    Session ID: 1
                 Connection ID: 127834
 Incoming Data LIF IP Address: 10.1.1.25
                   Workstation: 10.2.2.50
     Authentication Mechanism: NTLMv2
                  Windows User: EXAMPLE\user1
                     UNIX User: user1
                   Open Shares: 2
                    Open Files: 2
                    Open Other: 0
                Connected Time: 1d 1h 10m 5s
                     Idle Time: 22s
             Protocol Version: SMB3
       Continuously Available: No
            Is Session Signed: true
        User Authenticated as: domain-user
                  NetBIOS Name: ALIAS1
        SMB Encryption Status: Unencrypted
```

その他の **SMB** サーバタスクを管理します

CIFS サーバを停止または起動します

ユーザが SMB 共有を介してデータにアクセスしていない間に作業を行う場合は、 SVM 上の CIFS サーバを停止すると便利です。SMB アクセスを再開するには、 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 サーバを停止します	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	CIFS サーバを起動します
`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。省略した場合、このパラメータはに設定されます `true`コマンドはフォアグラウンドで実行されます。

2. 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` コマンドを実行します

例

次のコマンドは、 SVM vs1 の 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を表示する

サーバのリセットおよび再検出

CIFS サーバを別の OU に移動します

CIFS サーバの create 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 Organizational Unit （ OU ；組織単位） CN=Computers が使用されます。CIFS サーバはセットアップ後でも別の OU に移動できます。

手順

1. Windows サーバーで、 * 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 オブジェクトを見つけます。
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 オブジェクトが移動します。

SMB サーバを移動する前に、 SVM 上の動的 DNS ドメインを変更します

SMB サーバを別のドメインに移動する際に、 SMB サーバの DNS レコードが Active Directory に統合された DNS サーバによって DNS に動的に登録されるようにするには、SMB サーバを移動する前に Storage Virtual Machine （ SVM ）上の動的 DNS （ DDNS ）を変更する必要があります。

作業を開始する前に

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。

このタスクについて

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 サービスを設定する"

SVM を Active Directory ドメインに追加します

を使用してドメインを変更すると、既存のSMBサーバを削除することなくStorage Virtual Machine（SVM）をActive Directoryドメインに追加できます `vserver cifs modify` コマンドを実行します現在のドメインに参加しなおすことも、新しいドメインに参加することもできます。

作業を開始する前に

- 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 およびドメインコントローラサーバのサービスロケーションレコード（ SRV ）が含まれている必要があります。

このタスクについて

- 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、のマニュアルページを参照してください `vserver cifs modify` コマンドを実行します新しいドメイン用にDNSを再設定する必要がある場合は、のマニュアルページを参照してください `vserver dns modify` コマンドを実行します

   SMBサーバのActive Directoryマシンアカウントを作成するには、にコンピュータを追加するための十分な権限がある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` 内のコンテナ *example*.comドメイン。

   ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、 keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

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します

NetBIOS over TCP （ NBT ）接続に関する情報を表示できます。これは、 NetBIOS に関連する問題のトラブルシューティングを行う場合に役立ちます。

ステップ

1. を使用します `vserver cifs nbtstat` NetBIOS over TCP接続に関する情報を表示するコマンド。

   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	`vserver cifs stop`
SMB サーバを起動	`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にローカルユーザとローカルグループが受ける影響"

NetBIOS ネームサービスを有効にします

ONTAP 9 以降では、 NetBIOS ネームサービス（ NBNS 、 Windows Internet Name Service 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。NBNS が必須の構成でのみこのブロードキャストが送信されるようにするには、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。

作業を開始する前に

- すでに NBNS を使用しているシステムを ONTAP 9 にアップグレードした場合、このタスクを実行する必要はありません。NBNS はそれまでと同様に機能します。
- NBNS は UDP （ポート 137 ）経由で有効になります。
- 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 を使用します

IPv6 を使用するための要件

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 ライセンスの要件：

SMB のライセンスがあれば、 IPv6 を使用するために特別なライセンスは必要ありません。SMBライセンスはに含まれています。 "ONTAP One"。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 ONTAP は、すべてのバージョンの SMB プロトコルで IPv6 がサポートされます。

> 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 では、 IPv6 をサポートする Windows サーバおよびクライアントをサポートしています。次に、 Microsoft Windows クライアントおよびサーバによる IPv6 の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、 DNS 、 LDAP 、 CLDAP 、 Kerberos サービスなどの Active Directory 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 サービスに対してデフォルトで IPv6 が使用されます。IPv6 接続による NTLM 認証と Kerberos 認証の両方がサポートされます。

ONTAP でサポートされる Windows クライアントでは、いずれも IPv6 アドレスを使用して SMB 共有に接続できます。

ONTAPがサポートするWindowsクライアントに関する最新情報については、を参照してください。 "互換性マトリックス"。

NT ドメインは IPv6 ではサポートされません。

その他の **CIFS** サービスもサポートされます

ONTAP では、 SMB ファイル共有と Active Directory サービスに加え、以下に対しても IPv6 をサポートしています。

- クライアント側のサービス：オフラインフォルダ、移動プロファイル、フォルダリダイレクト、以前のバージョン機能など
- サーバ側のサービス：動的ホームディレクトリの有効化（ホームディレクトリ機能）、シンボリックリンクとワイドリンク、 BranchCache 、 ODX コピーオフロード、自動ノードリファーラル、 および以前のバージョン
- ファイルアクセス管理用のサービス： Windows のローカルユーザやローカルグループを使用したアクセス制御と権限の管理、 CLI を使用したファイル権限や監査ポリシーの設定、セキュリティトレース、ファイルロックの管理、 SMB アクティビティの監視などが可能です
- NAS のマルチプロトコルの監査
- FPolicy の
- 共有の継続的な可用性、監視プロトコル、およびリモート VSS （ Hyper-V over SMB 構成で使用）

ネームサービスおよび認証サービスのサポート

次のネームサービスとの通信が IPv6 でサポートされます。

- ドメインコントローラ
- DNS サーバ
- LDAPサーバ
- KDCサアハ
- NISサーバ

CIFS サーバが **IPv6** を使用して外部サーバに接続する方法

要件に対応した設定を作成するには、 CIFS サーバが外部サーバへの接続を確立するときに IPv6 がどのように使用されるかを確認しておく必要があります。

- 送信元アドレスの選択

  外部サーバへの接続を試行する場合、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なければなりません。たとえば、 IPv6 アドレスに接続する場合、 CIFS サーバをホストする Storage Virtual Machine （ SVM ）には、送信元アドレスとして使用する IPv6 アドレスを持つデータ LIF または管理 LIF が必要です。同様に、 IPv4 アドレスに接続する場合、 SVM には、送信元アドレスとして使用する IPv4 アドレスを持つデータ LIF または管理 LIF が必要です。

- DNS を使用して動的に検出されるサーバの場合、サーバ検出は次のように実行されます。
  - クラスタで IPv6 が無効になっている場合は、 IPv4 サーバアドレスのみが検出されます。
  - クラスタで IPv6 が有効になっている場合は、 IPv4 と IPv6 の両方のサーバアドレスが検出されます。アドレスが属するサーバが適切かどうかと、 IPv6 または IPv4 のデータ LIF または管理 LIF が使用可能かどうかに応じて、いずれかのタイプが使用されます。
    動的サーバ検出は、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 サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、 DNS ネームサービスの設定で IPv4 アドレスを使用できます。DNS ネームサービスの設定時に、 IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。

- LDAPサアハセツソク

  SVM が LDAP サーバに接続するときに IPv6 を使用するかどうかは、 LDAP クライアントの設定によって決まります。IPv6 アドレスを使用するように LDAP クライアントが設定されている場合は、 IPv6 を使用して接続が確立されます。必要に応じて、 LDAP サーバへの接続に引き続き IPv4 アドレスが使用されるようにするため、 LDAP クライアントの設定で IPv4 アドレスを使用できます。LDAP クライアントの設定時に、 IPv4 アドレスと IPv6 アドレスを組み合わせて指定できます。

  > LDAP クライアントの設定は、 UNIX ユーザ、グループ、およびネットグループのネームサービス用に LDAP を設定するときに使用されます。

- NISサーバへの接続

  SVMがNISサーバに接続するときにIPv6を使用するかどうかは、NISネームサービスの設定によって決まります。IPv6アドレスを使用するようにNISサービスが設定されている場合は、IPv6を使用して接続が確立されます。必要に応じて、NISサーバへの接続で引き続き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は有効になりません。SMB で IPv6 を使用するには、クラスタのセットアップ後にクラスタ管理者が IPv6 を有効にする必要があります。クラスタ管理者が IPv6 を有効にすると、 IPv6 はクラスタ全体で有効になります。

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 が有効になっている。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

"Network Management の略"

SMB で IPv6 を無効にします

クラスタで IPv6 を有効にするにはネットワークオプションを使用しますが、同じコマンドを使用して SMB での IPv6 を無効にすることはできません。代わりに、クラスタ管理者がクラスタで最後に IPv6 を有効にしたインターフェイスを無効にすると、 ONTAP は IPv6 を無効にします。IPv6 を有効にしたインターフェイスの管理については、クラスタ管理者と連絡を取る必要があります。

クラスタでの IPv6 の無効化の詳細については、 _ ネットワーク管理ガイド _ を参照してください。

関連情報

"Network Management の略"

IPv6 SMB セッション情報を監視および表示します

IPv6 ネットワークで接続されている SMB セッション情報を監視および表示できます。この情報は、 IPv6 SMB セッションに関する他の有用な情報と同様、 IPv6 を使用して接続するクライアントを決定する上で役に立ちます。

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ます	`vserver cifs session show -vserver` *`vserver_name`* `-instance`

確認する項目	入力するコマンド
特定の LIF アドレスにより、 SMB セッションに IPv6 を使用します	`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をセットアップする

セキュリティ形式を設定する

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、セキュリティ形式ごとに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	
混在	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.x ACL		
		NTFS ACL	NTFS	
統合：（ONTAP 9.4以前のリリースでは、Infinite Volume のみ）。	NFS または SMB	NFSv3 モードビット	「 UNIX 」	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

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

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。

ONTAP 9.2以降では、 `show-effective-permissions` パラメータをに設定します `vserver security file-directory` コマンドを使用すると、指定したファイルまたはフォルダパスに対してWindows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も指定します `-share-name` 有効な共有権限を表示できます。

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

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します

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

ボリュームのセキュリティ形式を設定するときは、最適なセキュリティ形式を選択して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。決定時には次の点を考慮すると役立ちます。

セキュリティ形式	以下の場合に選択
「 UNIX 」	• ファイルシステムが UNIX 管理者によって管理される。 • ユーザの大半が NFS クライアントである。 • データにアクセスするアプリケーションで、サービスアカウントとして UNIX ユーザが使用される。

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、サービスアカウントとして Windows ユーザが使用される。
混在	ファイルシステムが UNIX 管理者と Windows 管理者の両方によって管理され、ユーザが NFS クライアントと SMB クライアントの両方で構成される。

セキュリティ形式の継承の仕組み

新しい FlexVol または qtree の作成時にセキュリティ形式を指定しない場合、セキュリティ形式は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て **UNIX** アクセス権を管理します

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 ルートボリュームのセキュリティ形式を設定する

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. を使用します `vserver create` コマンドにを指定します `-rootvolume-security-style` セキュリティ形式を定義するパラメータ。

   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、です `unix`、 `ntfs``または `mixed。

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 ボリュームのセキュリティ形式を設定する

Storage Virtual Machine （ SVM ）の FlexVol 上のデータに使用するアクセス権のタイプを決定するには、 FlexVol のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

FlexVol ボリュームの状況	使用するコマンド
はまだ存在しません	`volume create` を含めます `-security-style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume modify` を含めます `-security-style` セキュリティ形式を指定するパラメータ。

FlexVol のセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs`または `mixed`。

FlexVol ボリューム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。

詳細については、を参照してください `volume create` または `volume modify` コマンド、を参照してください "論理ストレージ管理"。

2. 作成した FlexVol ボリューム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 にセキュリティ形式を設定する

qtree 上のデータに使用するアクセス権のタイプを決定するには、 qtree のセキュリティ形式を設定します。

手順

1. 次のいずれかを実行します。

qtree の有無	使用するコマンド
はまだ存在しません	`volume qtree create` を含めます `-security -style` セキュリティ形式を指定するパラメータ。
はすでに存在します	`volume qtree modify` を含めます `-security -style` セキュリティ形式を指定するパラメータ。

qtreeセキュリティ形式に指定できるオプションは、です `unix`、 `ntfs`または `mixed`。

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`。

詳細については、を参照してください `volume qtree create` または `volume qtree modify` コマンド、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 ネームスペース内でデータボリュームを作成および管理します

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およびジャンクションポイントを管理する必要があります。これには、ネームスペースアーキテクチャの計画、ジャンクションポイントが設定されたボリュームまたは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します

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。

作業を開始する前に

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指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、ディレクトリおよび結合されたボリュームを含むことができます。ジャンクションパスにボリュームの名前を含める必要はありません。ジャンクションパスはボリューム名に依存しません。

   ボリュームのセキュリティ形式の指定は任意です。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に適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、作成するデータボリュームには適切でないセキュリティ形式である場合もあります。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、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。 `/ENG` はと同じです `/eng`。CIFS 共有を作成する場合、 Windows では、ジャンクションパスがあたかも大文字と小文字の区別があ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などです `/ENG`、CIFS共有のパスは次の文字で始まる必要があります。 `/ENG`ではありません `/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。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

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 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上に作成します `/eng/home`：

```
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

ジャンクションポイントを指定せずにデータボリュームを作成できます。作成したボリュームは自動的にはマウントされず、 NAS アクセス用の設定に使用することはできません。ボリュームの SMB 共有または NFS エクスポートを設定する前に、ボリュームをマウントする必要があります。

作業を開始する前に

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に適用されている形式と同じセキュリティ形式を使用してボリュームを作成します。ただし、ルートボリュームのセキュリティ形式が、データボリュームには適切でないセキュリティ形式である場合もあります。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、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。これらの機能の詳細については、のマニュアルページを参照してください `volume create` コマンドを実行します

2. ジャンクションポイントが設定されていないボリュームが作成されたことを確認します。 `volume show -vserver vserver_name -volume volume_name -junction`

例

次の例は、ジャンクションポイントにマウントされない「 sales 」という名前のボリュームを SVM vs1 上に作成します。

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ---------- -------- --------------- -----------
vs1       data        true     /data            RW_volume
vs1       home4       true     /eng/home        RW_volume
vs1       vs1_root    -        /                -
vs1       sales       -        -                -
```

NAS ネームスペース内の既存のボリュームをマウントまたはアンマウントします

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。ボリュームはアンマウントすることもできます。

このタスクについて

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。

> NAS クライアントからのボリュームへのアクセスを中止するには、ボリュームを単純に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およびボリュームまたはディレクトリ上に作成された SMB 共有、およびアンマウントされたボリューム内のジャンクションポイントは保持されます。アンマウントしたボリュームを再マウントすれば、 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内のデータにアクセスできるようになります。

手順

1. 必要な操作を実行します。

状況	入力するコマンド
ボリュームをマウント	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

ボリュームをアンマウントします	`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
```

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。また、ジャンクションポイントにマウントされていないボリュームを確認することもできます。この情報を使用して、 SVM ネームスペースを理解し、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、の有効なフィールドを表示できます `-fields` パラメータを指定するには、次のコマンドを使用します。 `volume show -fields ?` b. を使用して、必要な情報を表示します `-fields` パラメータ：volume show -vserver vserver_name -fields fieldname、……

例

次の例は、 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
```

ネームマッピングを設定する

ネームマッピングの概要を設定する

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

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 環境を構成した場合、ボリュームに対して CIFS アクセスまたは NTFS セキュリティ形式を使用する予定はありません。
- 代わりにデフォルトユーザを使用するように設定している場合。

  このシナリオでは、すべてのクライアントクレデンシャルを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ません。

ただし、個々のユーザのグループを特定のユーザにマッピングすることはできます。たとえば、 SALES とい

う単語が先頭または末尾に付くすべての AD ユーザを、特定の UNIX ユーザおよびそのユーザの UID にマッピングできます。

ネームマッピングの仕組み

ONTAP がユーザのクレデンシャルをマッピングする必要がある場合、最初に、ローカルのネームマッピングデータベースおよび LDAP サーバで既存のマッピングの有無をチェックします。一方をチェックするか両方をチェックするか、およびそのチェック順序は、 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 ドメインで有効なユーザ名かどうかをチェックします。設定されている場合は、デフォルトの UNIX ユーザが使用されます。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。正しく設定されていない場合は、デフォルトの SMB ユーザが使用されます。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、デフォルトでは、指定したデフォルトの UNIX ユーザにマッピングされます。デフォルトの UNIX ユーザを指定しないと、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。

  マシンアカウントに定義されているネームマッピングがあっても無視されます。

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 に与える影響を理解しておく必要があります。CIFS サーバのホームドメインとの Active Directory 信頼関係は、双方向の信頼にすることも、インバウンドとアウトバウンドの 2 つのタイプがある単一方向の信頼のどちら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しています。CIFS サーバのホームドメインが別のドメインと双方向の信頼関係にある場合、このホームドメインは信頼できるドメインに属しているユーザを認証および認可でき、その反対に、この信頼できるドメインはホームドメインに属しているユーザを認証および認可することができます。

UNIX ユーザから Windows ユーザへのネームマッピング検索は、ホームドメインと他方のドメインの間に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、ホームドメインが他方のドメインを信頼しています。この場合、ホームドメインはアウトバウンドの信頼できるドメインに属しているユーザを認証および認可できます。

  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、 CIFS サーバのホームドメインが他方のドメインによって信頼されています。この場合、ホームドメインはインバウンドの信頼できるドメインに属しているユーザを認証または認可できません。

  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のためのマルチドメイン検索の設定

マルチドメインネームマッピング検索は、 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容易になります。次の表に、マルチドメイン検索を有効にするためにネームマッピングエントリのドメイン部にワイルドカードを使用する方法を示します。

パターン（ **Pattern** ）	交換	結果
ルート	• \\ 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。

パターン（ **Pattern** ）	交換	結果
*	\ * \\ *	有効な UNIX ユーザは、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

マルチドメインの名前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方法は 2 つあります。

- ONTAP で作成された自動検出された双方向の信頼リストを使用します
- 自分で作成した信頼できる優先ドメインリストを使用します

ユーザ名のドメインセクションにワイルドカードを使用して UNIX ユーザが Windows ユーザにマッピングされている場合、 Windows ユーザはすべての信頼できるドメインで次のように検索されます。

- 信頼できるドメインの優先リストが設定されている場合、マッピング先の Windows ユーザはこの検索リスト内でのみ順に検索されます。
- 信頼できるドメインの優先リストが設定されていない場合は、ホームドメインと双方向の信頼関係にあるすべてのドメインで Windows ユーザの検索が行われます。
- ホームドメインと双方向の信頼関係にあるドメインが存在しない場合、ホームドメインでユーザ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は、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` プログラム。

ネームマッピングを作成します

を使用できます `vserver name-mapping create` コマンドを使用してネームマッピングを作成します。ネームマッピングを使用すると、 Windows ユーザから UNIX セキュ

リティ形式のボリュームへのアクセスおよびその逆方向のアクセスが可能になります。

このタスクについて

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`

> 。 `-pattern` および `-replacement` ステートメントは正規表現として記述できます。を使用することもできます `-replacement` null置換文字列を使用してユーザへのマッピングを明示的に拒否するステートメント " "（スペース文字）。を参照してください `vserver name-mapping create` のマニュアルページを参照してください。

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、優先順位リスト内での位置は 1 番目です。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
```

デフォルトユーザを設定します。

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

このタスクについて

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

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

手順

1. 次のいずれかを実行します。

状況	入力するコマンド
デフォルトの UNIX ユーザを設定する	`vserver cifs options modify -default -unix-user` *`user_name`*
デフォルトの Windows ユーザを設定します	`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します	`vserver name-mapping create`
特定の位置にネームマッピングを挿入します	`vserver name-mapping insert`
ネームマッピングを表示します	`vserver name-mapping show`
2 つのネームマッピングの位置を入れ替えます 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交換できません。	`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`

状況	使用するコマンド
ネームマッピングが正しいことを確認します	`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を設定する

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します

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。

このタスクについて

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	`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をリセットして再検出します

すべての信頼できるドメインを強制的に再検出することができます。これは、信頼できるドメインサーバが適切に応答しない場合や、信頼関係が変更された場合に役立ちます。CIFS サーバのコンピュータアカウントを含むドメインであるホームドメインと双方向の信頼が確立されたドメインのみが検出されます。

ステップ

1. を使用して信頼できるドメインをリセットし、再検出します `vserver cifs domain trusts rediscover` コマンドを実行します

   ```
   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を表示する

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

CIFS サーバのホームドメインで検出された信頼できるドメインに関する情報を表示できます。ホームドメインとは、 CIFS サーバのコンピュータアカウントが含まれるドメインです。これは、検出される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把握する場合に役立ちます。

このタスクについて

ホームドメインと双方向の信頼関係が確立されたドメインのみが検出されます。ホームドメインのドメインコントローラ（ DC ）は信頼できるドメインのリストを DC が決めた順序で返すため、リスト内のドメインの順序は予測できません。信頼できるドメインのリストを表示すると、マルチドメインネームマッピングの検索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. 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` コマンドを実行します

   ```
   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に含まれる信頼できるドメインを追加、削除、または置換します

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関係にあるドメインの代わりにこのリストが使用されます。

このタスクについて

- 信頼できるドメインを既存のリストに追加すると、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、双方向の信頼関係にあるドメインのみ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にある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します	`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します	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
既存のリストを変更します	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

例

次のコマンドは、 SVM vs1 が使用す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
```

次のコマンドを実行すると、 SVM vs1 で使用されるリストから信頼できるドメインが 2 つ削除されます。

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

次のコマンドは、 SVM vs1 で使用されてい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を表示する

信頼できるドメインの優先リストに関する情報を表示します

信頼できるドメインの優先リストに含まれる信頼できるドメインに関する情報、およびマルチドメインネームマッピングの検索が有効な場合の信頼できるドメインの検索順序に関する情報を表示できます。自動検出された信頼できるドメインの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 ）ごとにグループ化されたクラスタ内のすべての信頼できる優先ドメイン	`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を指定します	`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に含まれる信頼できるドメインの追加、削除、または置換

SMB 共有を作成および設定

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 共有とは、ボリューム内に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 および SQL Server 向けの SMB の設定"

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を設定します

デフォルトの管理共有とは

Storage Virtual Machine（SVM）上にCIFSサーバを作成すると、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は作成されなくなりました。

- IPC $
- admin$（ONTAP 9.7以前のみ）
- c$

末尾が $ 文字である共有は非表示の共有であるため、デフォルトの管理共有はマイコンピュータには表示されませんが、共有フォルダを使用して表示することはできます。

ipc$** および **admin$ デフォルト管理共有の用途

ipc$ および admin$ 共有は ONTAP が使用するものであり、 Windows 管理者が SVM 上にあるデータにアクセスするために使用することはできません。

- ipc$ 共有

  ipc$ 共有は、プログラム間通信に必要な名前付きパイプを共有するリソースです。ipc$ 共有はコンピュータのリモート管理や、コンピュータの共有リソースを表示する際に使用されます。ipc$ 共有の共有設定、共有プロパティ、 ACL は変更できません。また、 ipc$ 共有の名前の変更や削除もできません。

- admin$共有（ONTAP 9.7以前のみ）

  > ONTAP 9.8以降では、admin$共有はデフォルトでは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$ 共有の名前の変更や削除もできません。

c$ デフォルト共有の用途

c$ 共有は、クラスタまたは SVM の管理者が SVM のルートボリュームへのアクセスおよび管理に使用できる管理共有です。

c$ 共有には、次のような特徴があります。

- この共有へのパスは、常に SVM ルートボリュームへのパスで、変更することはできません。
- c$ 共有のデフォルト ACL は、 Administrator / Full Control です。

  このユーザは、 BUILTIN\administrator です。デフォルトで、 BUILTIN\administrator を共有にマッピングでき、マッピングされたルートディレクトリ内のファイルやフォルダの表示、作成、変更、削除が可能です。このディレクトリ内のファイルおよび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$ 共有の設定や共有プロパティは変更できます。

- c$ 共有は削除できません。
- SVM 管理者は、ネームスペースジャンクションを横断することによって、マッピングされた c$ 共有から残りの SVM ネームスペースにアクセスできます。
- c$ 共有には、 Microsoft 管理コンソールを使用してアクセスできます。

関連情報

Windows ノセキュリティタブヲシヨウシタショウサイナ NTFS ファイルアクセスケンノセッテイ

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 の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あり、次の要件が含まれています。

- 共有名は SMB サーバでそれぞれ一意にする必要があります。
- 共有名では大文字と小文字は区別されません。
- 共有名の最大長は 80 文字です。
- 共有名では Unicode がサポートされます。
- $ 記号で終わる共有名は非表示の共有です。
- ONTAP 9.7以前の場合、admin$、ipc$、c$管理共有は、すべてのCIFSサーバ上に自動的に作成され、共有名が予約されます。ONTAP 9.8以降では、admin$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 ONTAP_ADMIN$ という共有名は使用できません。
- 共有名ではスペースの使用がサポートされます。
  - 共有名の先頭または末尾の文字をスペースにすることはできません。
  - スペースを含む共有名は引用符で囲む必要があります。

    単一引用符は共有名の一部とみなされ、引用符の代わりに使用することはできません。

- SMB 共有の名前では次の特殊文字の使用がサポートされます。

  ！@ #$%&'__ 。~ （） ｛｝

- SMB 共有の名前では次の特殊文字の使用はサポートされません。
  - "/\\:;|<> 、 ？* =

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す `/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 共有プロパティの概要を使用する

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を使用することを指定します。これはクライアント側キャッシュとも呼ばれます。
`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	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。各ユーザのアクセス権に基づいて ABE フィルタを適用した共有フォルダがユーザに表示され、そのユーザがアクセス権を持たないフォルダやその他の共有リソースは表示されないようにします。
namespace-caching	このプロパティは、この共有に接続する SMB クライアントが、 CIFS サーバから返されたディレクトリの列挙結果をキャッシュできることを指定します。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 暗号化の使用を義務付けます。SMB データへのアクセスで暗号化をサポートしていない SMB クライアントは、この共有にアクセスできません。

既存の **SMB** 共有に対する共有プロパティを追加または削除します

共有プロパティを追加または削除することで、既存の SMB 共有をカスタマイズできます。この方法は、環境内での要件の変化に合わせて共有の設定を変更する場合に便利です。

作業を開始する前に

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。

このタスクについて

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。

- カンマで区切って指定することで、 1 つ以上の共有プロパティを追加できます。
- 以前に指定した共有プロパティは有効なままです。

  新しく追加したプロパティは、共有プロパティの既存のリストに追加されます。

- 共有にすでに適用されている共有プロパティに新しい値を指定した場合は、元の値が新たに指定した値に置き換えられます。
- 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` コマンドを実行します

  を使用できます `vserver cifs share properties remove` 共有プロパティを削除するコマンド。

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。

- カンマで区切って指定することで、 1 つ以上の共有プロパティを削除できます。
- 以前に指定した共有プロパティは、削除しないかぎり有効なままです。

手順

1. 適切なコマンドを入力します。

状況	入力するコマンド
共有プロパティを追加します	`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します	`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

次のコマンドは、を追加します `showsnapshot` SVM vs1上の「`share1`」という名前の共有に共有プロパティを設定します。

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

次のコマンドでは、が削除されます `browsable` SVM vs1上の「`share2`」という名前の共有から共有プロパティを指定します。

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

関連情報

SMB 共有の管理用コマンド

force-group 共有設定を使用して、 **SMB** ユーザアクセスを最適化します

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確実にアクセスできるようになります。

force-group の指定は、共有が UNIX または mixed qtree 内にある場合にのみ有効です。NTFS セキュリティ形式のボリュームまたは qtree にある共有内のファイルへのアクセスは、 UNIX の GID ではなく Windows の権限によって判断されるため、これらの共有に 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、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、通常はプライマリ GID または UID を使用してアクセスできないファイルにこの共有内のファイルにアクセスできるようになります。

- SMB ユーザがこの共有内に作成するすべてのファイルは、ファイル所有者のプライマリ GID に関係なく、同じフォースグループに属します。

SMB ユーザが、 NFS ユーザによって作成されたファイルにアクセスしようとすると、 SMB ユーザのプライマリ GID によって、権限があるかどうかが判断されます。

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を与えません。NFS ユーザが作成したファイルは、ファイル所有者から GID を取得します。アクセス権限の決定は、ファイルにアクセスしようとしている NFS ユーザの UID およびプライマリ GID に基づきます。

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確実にアクセスできるようになります。たとえば、会社の Web ページを保存する共有を作成し、 Engineering グループと Marketing グループのユーザに書き込みアクセス権を付与する必要がある場合、共有を作成して、「 webgroup1 」という名前の 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。そのため、 Engineering グループと Marketing グループのユーザの権限を管理しなくても、すべてのユーザがこの共有に書き込むことができます。

関連情報

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** 共有を作成します

UNIX ファイルセキュリティ形式のボリュームや qtree にあるデータにアクセスする SMB ユーザが、同じ UNIX グループに属していると ONTAP で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`*

   UNCパスの場合 (`\\servername\sharename\filepath`）が256文字を超えています（先頭の「`\\`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 問題ではなく Windows クライアント問題です。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、共有をいつでも変更し、の値として空の文字列（""）を指定できます `-force-group-for-create` パラメータ共有を変更して 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

次のコマンドを実行すると、でWebからアクセスできる「'webpages'」共有が作成されます `/corp/companyinfo` 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ているディレクトリ：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
```

```
/corp/companyinfo -force-group-for-create webgroup1
```

関連情報

force-group 共有設定を使用して、 SMB ユーザアクセスを最適化します

MMC を使用して **SMB** 共有情報を表示します

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。

このタスクについて

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

この処理がサポートされていない場合は、が表示されることがあります `remote procedure call failed` エラー。

"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

を使用します `vserver cifs share` および `vserver cifs share properties` SMB共有を管理するコマンド。

状況	使用するコマンド
SMB 共有を作成	`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します	`vserver cifs share properties remove`
共有プロパティに関する情報を表示します	`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 を使用してファイルアクセスを保護

SMB 共有レベル ACL の管理に関するガイドラインを次に示します

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。

共有を作成すると、共有レベルの ACL のデフォルトでは、 Everyone という名前の標準グループに読み取りアクセス権が与えられます。ACL に読み取りアクセス権が設定されているため、ドメイン内およびすべての信頼できるドメイン内のすべてのユーザに共有への読み取り専用アクセス権が与えられます。

共有レベルの ACL を変更するには、 Windows クライアントの Microsoft 管理コンソール（ MMC ）または ONTAP コマンドラインを使用します。

MMC を使用する際には、次の点に留意してください。

- 指定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を作成

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。

このタスクについて

ローカルまたはドメインの Windows ユーザまたはグループ名、あるいは UNIX ユーザまたはグループ名を使用して共有レベルの ACL を設定できます。

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ます `Everyone / Full Control`は、セキュリティリスクをもたらします。

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_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. 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` コマンドを実行します

例

次のコマンドは、を示しています `Change` SVM「vs1.example.com」上の「sales」共有に対する「Sales Team」Windowsグループへの権限：

```
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、を示しています `Read` SVM「vs2.example.com」上の「eng」共有の「engineering」UNIXグループへの権限：

```
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
```

以下のコマンドで説明します `Change` 「Tiger Team」という名前のローカルWindowsグループおよびへの権限 `Full_Control` SVM「vs1」の「datavol5」共有に対する「Sue Chang」という名前のWindowsローカルユーザの権限：

```
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

アクセス制御リスト（ACL）の作成、表示、変更、削除など、 SMB の ACL 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てファイルアクセスを保護

Windows のセキュリティタブを使用して、詳細な **NTFS** ファイル権限を設定します

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。

作業を開始する前に

このタスクを実行する管理者は、選択したオブジェクトに対する権限を変更するための十分な NTFS 権限を持っている必要があります。

このタスクについて

NTFS ファイル権限を設定するには、 Windows ホストで、 NTFS セキュリティ記述子に関連付けられている NTFS Discretionary Access Control List （ DACL ；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。これらのタスクは Windows GUI によって自動的に処理されます。

手順

1. Windows 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. [* フォルダー *] ボックスに、許可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て使用可能な状態になり、共有内に格納されているファイルやフォルダが Windows エクスプローラウィンドウに表示されます。

3. NTFS ファイル権限を設定するファイルまたはディレクトリを選択します。
4. ファイルまたはディレクトリを右クリックし、 * 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、ユーザーおよびグループに割り当てられている既存のファイルアクセス権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。

   [アクセス権] 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	実行する処理
新しいユーザまたはグループの詳細な NTFS 権限を設定します	a. [追加（ Add ）] 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 アクセス権を変更します	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。
      次の詳細な権限に関する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を選択できない場合、その権限は親オブジェクトから継承されます。

11. このオブジェクトのサブフォルダ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、 1 つのファイルに NTFS ファイルアクセス権を設定する場合は、 [アクセス権] ボックスには表示されません。

      > この設定を選択する場合は注意が必要です。この設定を選択すると、すべての子オブジェクトの既存の権限がすべて削除され、このオブジェクトの権限設定に置き換えられます。削除する必要がなかった権限が誤って削除される可能性があります。これは、 mixed セキュリティ形式のボリュームまたは qtree でアクセス権を設定する場合に特に重要です。子オブジェクトが UNIX 対応のセキュリティ形式を使用している場合に、このような子オブジェクトに NTFS 権限を適用すると、 ONTAP によってこれらのオブジェクトが UNIX セキュリティ形式から NTFS セキュリティ形式に変更され、これらの子オブジェクトのすべての UNIX 権限が NTFS 権限に置き換えられます。

    - 両方のボックスを選択します。
    - どちらのボックスも選択しない。
14. **OK** をクリックして、 *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 を使用して、 NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

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を表示する

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を表示する

ONTAP CLI を使用して NTFS ファイル権限を設定します

ONTAP CLI を使用して、ファイルおよびディレクトリに対して NTFS ファイル権限を設定できます。これにより、 Windows クライアントで SMB 共有を使用してデータに接続することなく NTFS ファイル権限を設定できます。

NTFS ファイル権限を設定するには、 NTFS セキュリティ記述子に関連付けられている NTFS Discretionary Access Control List （ DACL ；随意アクセス制御リスト）にエントリを追加します。その後、セキュリティ記述子を NTFS ファイルおよびディレクトリに適用します。

コマンドラインで設定できるのは NTFS ファイルアクセス権だけです。CLI で 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/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 ファイルアクセス権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。

DAC （ダイナミックアクセス制御）を使用したファイルアクセスの保護

Dynamic Access Control （ **DAC** ；ダイナミックアクセス制御）の概要を使用したファイルアクセスの保護

ダイナミックアクセス制御を使用してアクセスを保護できます。 Active Directory で集約型アクセスポリシーを作成し、適用された GPO を使用して 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 クレデンシャルの追加

ダイナミックアクセス制御が導入される前は、 CIFS クレデンシャルにセキュリティプリンシパル（ユーザ）の ID と Windows グループメンバーシップが含まれていました。ダイナミックアクセス制御では、デバイス ID 、デバイスの信頼性、ユーザの信頼性という 3 種類の情報がクレデンシャルに追加されます。

- デバイス ID

  ユーザ ID 情報に似ていますが、ユーザがログインに使用しているデバイスの ID とグループメンバーシップは例外です。

- デバイスの信頼性

  デバイスのセキュリティプリンシパルに関するアサーションです。たとえば、デバイスの信頼性として特定の OU のメンバーであることなどがあります。

- ユーザの信頼性

  ユーザのセキュリティプリンシパルに関するアサーションです。たとえば、ユーザの信頼性として AD アカウントが特定の OU のメンバーであることなどがあります。

集約型アクセスポリシー

ファイルの集約型アクセスポリシーを使用すると、ユーザグループ、ユーザの信頼性、デバイスの信頼性、およびリソースのプロパティを使用した条件式を含む許可ポリシーを一元的に導入して管理できます。

たとえば、ビジネスへの影響が大きいデータにアクセスする場合、ユーザー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。

高度な監査機能を備えた集約型アクセスポリシーのステージング

集約型アクセスポリシーは「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。ポリシーが適用されていた場合の結果と、現在の設定との違いが、監査イベントとして記録されます。管理者は、実際にポリシーを有効にする前に、監査イベントログを使用してアクセスポリシーの変更による影響を確認できます。アクセスポリシーの変更による影響を評価したあと、ポリシーを目的の SVM に GPO 経由で導入できます。

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 サーバ上で GPO サポートを有効または無効にします

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

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を表示する

"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 サーバ上で DAC （ダイナミックアクセス制御）を使用する場合、 Active Directory 環境での ONTAP によるダイナミックアクセス制御機能のサポートについて理解しておく必要があります。

ダイナミックアクセス制御でサポートされます

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。

機能性	コメント
ファイルシステムへの請求	請求とは、ユーザに関する何らかの真実を表す単純な名前と値のペアです。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集中管理	集約型アクセスポリシーは、ファイルへのタグ付けが可能な Active Directory 内に格納される一種の ACL です。ファイルへのアクセスは、ディスク上のセキュリティ記述子とタグ付きの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、管理者はディスク上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	を拡張します `vserver security file-directory show` 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するコマンド。
集約型アクセスポリシーを含むセキュリティトレース	を拡張します `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するコマンドファミリー。

ダイナミックアクセス制御ではサポートされません

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。

機能性	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。

機能性	コメント
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概要を有効または無効にします

Dynamic Access Control （ DAC ；ダイナミックアクセス制御）を使用して CIFS サーバ上のオブジェクトを保護するオプションは、デフォルトでは無効になっています。CIFS サーバでダイナミックアクセス制御を使用する場合は、このオプションを有効にする必要があります。CIFS サーバに格納されたオブジェクトの保護にダイナミックアクセス制御を使用する必要がなくなった場合は、このオプションを無効にすることができます。

このタスクについて

ダイナミックアクセス制御を有効にすると、ダイナミックアクセス制御関連のエントリを使用する ACL をファイルシステムに含めることができます。ダイナミックアクセス制御を無効にすると、現在のダイナミックアクセス制御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	`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 が割り当てられたリソースがある場合に Storage Virtual Machine （ SVM ）でダイナミックアクセス制御を無効にすると、ダイナミックアクセス制御 ACE を削除するまではそのリソースの非ダイナミックアクセス制御 ACE を管理できません。

このタスクについて

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します

集約型アクセスポリシーを使用した CIFS サーバ上のデータへのアクセスを保護するためには、 CIFS サーバでの Dynamic Access Control （ DAC ；ダイナミックアクセス制御）の有効化、 Active Directory での集約型アクセスポリシーの設定、 GPO を使用した 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 GPO を有効にします。

作業を開始する前に

- 集約型アクセスポリシーを使用するには、 Active Directory を設定する必要があります。

- 集約型アクセスポリシーを作成し、 CIFS サーバを含むコンテナに GPO の作成と適用を行うには、 Active Directory ドメインコントローラに対して十分なアクセスが必要です。
- 必要なコマンドを実行するためには、 Storage Virtual Machine （ SVM ）で十分な管理アクセスが必要です。

このタスクについて

集約型アクセスポリシーは、 Active Directory のグループポリシーオブジェクト（ GPO ）に対して定義および適用されます。集約型アクセスポリシーと GPO の設定については、 Microsoft TechNet ライブラリを参照してください。

"Microsoft TechNet ライブラリ"

手順

1. 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、有効にします `vserver cifs options modify` コマンドを実行します

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 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、有効にします `vserver cifs group-policy modify` コマンドを実行します

   ```
   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 サーバコンピュータアカウントが存在するコンテナに GPO を適用します。
6. 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` コマンドを実行します

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. を使用して、GPO集約型アクセスポリシーがCIFSサーバ上のリソースに適用されていることを確認します `vserver cifs group-policy show-applied` コマンドを実行します

   次の例は、デフォルトのドメインポリシーに、 CIFS サーバに適用される 2 つの集約型アクセスポリシーがあることを示しています。

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
   ```

```
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
```

```
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

関連情報

GPO 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

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します

NTFS ボリューム、および mixed セキュリティ形式のボリューム上の NTFS 対応セキュリティを使用するデータについて、ダイナミックアクセス制御（ DAC ）セキュリティに関する情報を表示できます。これには、条件付き ACE 、リソース ACE 、および集約

型アクセスポリシー ACE に関する情報が含まれます。この結果を使用して、セキュリティ設定の検証や、ファイルアクセスに関する問題のトラブルシューティングを行うことができます。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

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
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細が表示されます	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
出力は、グループ SID とユーザ SID とともに表示されます	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
16 進数のビットマスクをテキスト形式に変換するファイルと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

次の例は、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` SVM vs1：

```
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 設定に関する情報を表示します

集約型アクセスポリシーに関する情報を表示します

集約型アクセスポリシールールに関する情報を表示します

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。
- を含むクラスタで監査の設定を変更する必要があります `cap-staging` のみを使用するイベントタイプ `file-op` イベントタイプ。

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方法および使用方法に関する追加情報の参照先

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際には、参考資料を利用することができます。

Active Directory のダイナミックアクセス制御と集約型アクセスポリシーの設定方法についての情報は、Microsoft TechNet ライブラリにあります。

"Microsoft TechNet ：「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およびサポートするように SMB サーバを設定するには、次の参考資料を使用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アクセスに関するエクスポートポリシーが有効になっている場合は、SMBクライアントによるSVMボリュームへのアクセスを制御するときにエクスポートポリシーが使用されます。データにアクセスするには、 SMB アクセスを許可するエクスポートポリシーを作成し、 SMB 共有を含むボリュームにそのポリシーを関連付けます。

エクスポートポリシーには 1 つ以上のルールが適用されており、このルールで、データへのアクセスを許可されるクライアントと、読み取り専用アクセスと読み取り / 書き込みアクセスでサポートされる認証プロトコルを指定します。エクスポートポリシーを設定して、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 認証と NTLM 認証の両方を使用した認証を許可できます。

ONTAP でエクスポートポリシーに適用されたすべてのエクスポートルールを処理したら、クライアントアクセスを許可するかどうか、および許可するアクセスのレベルを決定できます。エクスポートルールは、Windows のユーザとグループではなくクライアントマシンに適用されます。エクスポートルールは、Windows のユーザおよびグループベースの認証と許可に代わるものではありません。共有とファイルのアクセス権限に加えて、エクスポートルールはもう 1 つのアクセスセキュリティレイヤを提供します。

ボリュームへのクライアントアクセスを設定するには、ボリュームごとに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、名前や内容は変更できます。デフォルトでは、 SVM 上の各ボリュームはデフォルトのエクスポートポリシーに関連付けられています。SVM で SMB アクセスのエクスポートポリシーが無効になっている場合、「 default 」エクスポートポリシーは SMB アクセスには影響しません。

NFS ホストと SMB ホストの両方にアクセスを提供するルールを設定し、そのルールをエクスポートポリシーに関連付けることができます。このポリシーを、 NFS ホストと SMB ホストの両方がアクセスする必要があるデータを含むボリュームに関連付けることができます。または、 SMB クライアントのみがアクセスする必要があるボリュームがある場合は、 SMB プロトコルを使用したアクセスのみを許可するルール、および読み取り専用アクセスと書き込みアクセスの認証に Kerberos または NTLM のみ（あるいはその両方）を使用するルールを含むエクスポートポリシーを設定できます。その後、このエクスポートポリシーを SMB アクセスのみが必要なボリュームに関連付けます。

SMB に関するエクスポートポリシーが有効になっている場合に、クライアントが適用可能なエクスポートポリシーで許可されていないアクセス要求を行うと、権限拒否のメッセージが表示され、その要求は失敗します。クライアントがボリュームのエクスポートポリシーのどのルールにも一致しない場合、アクセスは拒否さ

れます。エクスポートポリシーが空の場合は、すべてのアクセスが暗黙的に拒否されます。これは、共有とファイルの権限によってアクセスが許可されている場合にも当てはまります。つまり、 SMB 共有を含むボリュームで少なくとも以下を許可するようにエクスポートポリシーを設定する必要があります。

- すべてのクライアント、またはクライアントの適切なサブセットへのアクセスを許可します
- SMB 経由のアクセスを許可する
- Kerberos 認証または NTLM 認証（あるいはその両方）を使用した適切な読み取り専用アクセスと書き込みアクセスを許可する

詳細はこちら "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済みの特定のパラメータと照合され、クライアントアクセス要求の処理方法が決定されます。

エクスポートポリシーには、クライアントにアクセスを許可するエクスポートルールが少なくとも 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に処理されます。ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールの権限が使用され、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、クライアントの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。たとえば、 NFSv4 や SMB などです。
- ホスト名や IP アドレスなどのクライアント識別子。

  の最大サイズ `-clientmatch` フィールドは4096文字です。

- Kerberos v5 、 NTLM 、 AUTH_SYS など、クライアントが認証に使用するセキュリティタイプ。

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、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求は NFSv3 プロトコルを使用して送信され、クライアントの IP アドレスは 10.1.17.37 です。

クライアントアクセスプロトコルが一致していても、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アドレスとは別のサブネットに属しています。そのため、クライアントは一致しなくなり、この

ルールはこのクライアントに適用されません。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

クライアントアクセス要求はNFSv4プロトコルを使用して送信され、クライアントのIPアドレスは10.1.16.54です。

クライアントアクセスプロトコルが一致し、クライアントの IP アドレスが指定したサブネット内にあります。そのため、クライアントは一致し、このルールはこのクライアントを環境します。セキュリティタイプに関係なく、クライアントは読み取り / 書き込みアクセス権を取得します。

例

エクスポートポリシーに、次のパラメータが指定されたエクスポートルールが含まれています。

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

クライアント #1 は、 IP アドレスが 10.1.16.207 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、Kerberos v5 で認証されます。

クライアント #2 は、 IP アドレスが 10.1.16.211 で、 NFSv3 プロトコルを使用してアクセス要求を送信し、AUTH_SYS で認証されます。

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 アドレスは一致しています。読み取り専用パラメータでは、認証に使用する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。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、認証に承認されたセキュリティタイプ Kerberos v5 を使用したためです。クライアント #2 は読み取り / 書き込みアクセス権を取得できません。

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。それ以外の場合は、受信します `access denied` エラー。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を有効または無効にします

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。

作業を開始する前に

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。

このタスクについて

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てファイルアクセスを保護

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

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

ストレージレベルのアクセス保護の動作

- 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。

  このセキュリティは、有効な権限を決定するために、ストレージオブジェクトレベルで適用され、メタデータ内に格納されます。

- システム（ Windows または UNIX ）管理者であっても、ストレージレベルのセキュリティをクライアントから取り消すことはできません。

  このセキュリティは、ストレージ管理者のみが変更できるように設計されています。

- ストレージレベルのアクセス保護は、 NTFS または mixed セキュリティ形式のボリュームに適用できます。
- ストレージレベルのアクセス保護を UNIX セキュリティ形式のボリュームに適用できるのは、そのボリュームが含まれている 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 のファイルやフォルダの Access Control List （ ACL ；アクセス制御リスト）、 NFSv4 ACL 、または UNIX モードのビット

ストレージレベルのアクセス保護の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

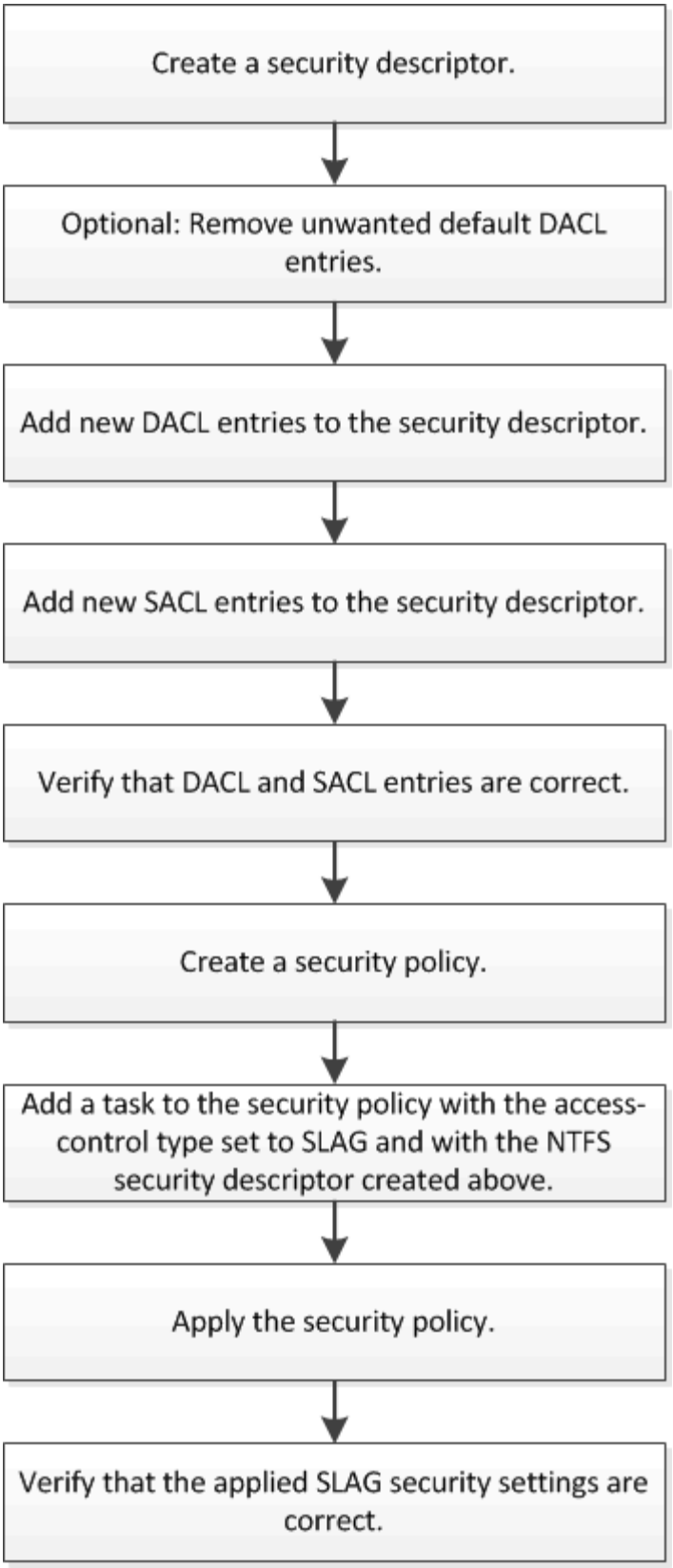
クトップから取り消すことはできません。一部のユースケースでは、ストレージレベルでアクセス制御を行える機能が役立ちます。

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を設定するためのワークフロー

ストレージレベルのアクセス保護（ SLAG ）を設定するワークフローでは、 NTFS ファイル権限や監査ポリシーを設定する際に使用する 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ためには、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を提供します。環境がすべての NAS プロトコルからその適用先のストレージオブジェクトにアクセスするセキュリティを提供します。

手順

1. を使用して、セキュリティ記述子を作成します `vserver security file-directory ntfs create` コマンドを実行します

   `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 アクセス制御エントリ（ ACE ）を持つように作成されます。

   ```
   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を設定するとき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に設定したくないデフォルトの DACL ACE を削除します。

a. を使用して、不要なDACL ACEを削除します `vserver security file-directory ntfs dacl remove` コマンドを実行します

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. 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` コマンドを実行します

この例では、コマンドからの出力により、セキュリティ記述子から 3 つのデフォルト DACL ACE が削除され、 NT AUTHORITY\SYSTEM のデフォルト DACL ACE エントリのみが残されていることを確認できます。

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 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` コマンドを実行します

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. 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` コマンドを実行します

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. を使用して、DACLおよびSACLのACEが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` および `vserver security file-directory ntfs sacl show` コマンドを指定します。

   この例では、次のコマンドはセキュリティ記述子「`d1"」の DACL エントリに関する情報を表示します。

   ```
   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. を使用して、セキュリティポリシーを作成します `vserver security file-directory policy create` コマンドを実行します

   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. 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` コマンドを実行します

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. を使用して、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` コマンドにを指定します `-access-control` パラメータをに設定します `slag`。

   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これはに割り当てられます `/datavol1` アクセス制御タイプが「`slag`」に設定されているパス。

   ```
   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. 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` コマンドを実行します

   ```
   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. を使用して、ストレージレベルのアクセス保護セキュリティポリシーを適用します `vserver security file-directory apply` コマンドを実行します

    ```
    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. を使用して、適用されたストレージレベルのアクセス保護セキュリティ設定が正しいことを確認します `vserver security file-directory show` コマンドを実行します

    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 Full Control を許可するデフォルト DACL は残っていますが、ストレージレベルのアクセス保護セキュリティによって、ストレージレベルのアクセス保護設定で定義されたグループにアクセスが制限（および監査）されます。

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                 Vserver: vs1
               File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

関連情報

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

ストレージレベルのアクセス保護を設定するためのワークフロー

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 の適用に関する一覧表

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します

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。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

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
要約形式で表示されます	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細が表示されます	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例は、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` SVM vs1：

```
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
```

次の例は、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` （SVM vs1）。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を削除します

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. 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` コマンドを実行します

   ```
   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. 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` コマンドを実行します

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. 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` コマンドを実行します

   ```
   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

ローカルユーザおよびローカルグループを使用して認証と許可を行います

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

ローカルユーザとローカルグループを設定して使用するかどうかを決定する前に、ローカルユーザとローカルグループの定義を理解し、基本的ないくつかの情報を理解しておく必要があります。

- * ローカルユーザー *

  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します。

  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。そのグループを作成した SVM 上でのみ認識が可能です。グループには一連のメンバーが含まれます。メンバーは、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です。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 によりバインドされています。ローカルドメインの名前は CIFS サーバの名前です。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に含まれています。

- * Security Identifier （ SID ；セキュリティ識別子） *

  SID は、 Windows 形式のセキュリティプリンシパルを識別する可変長の数値です。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 サーバ上のユーザの認証で使用される、 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のインスタンスを持つ複製されたデータベース。ローカルユーザとローカルグループのオブジェクトは、 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 ）を使用できないときでも、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。ローカルグループを使用して権限を割り当てる場合や、 SMB サーバがワークグループにある場合もあります。

ローカルユーザアカウントを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメインユーザを使用できない。

  ワークグループ設定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ときに、 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でも、ローカルユーザであれば、 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。ユーザに権限を割り当てるには、ユーザのアカウントにそれらの権限を割り当てるか、ユーザをそれらの権限が割り当てられたローカルグループのメンバーにします。

ローカルグループを作成する理由には、次のようなものがあります。

- SMB サーバがワークグループにあり、ドメイングループを使用できない。

  ワークグループにローカルグループを設定する必要はありませんが、設定するとローカルワークグループユーザのアクセス権限を管理するのに役立ちます。

- 共有やファイルアクセスの制御にローカルグループを使用して、ファイルやフォルダのリソースへのアクセスを制御する。
- カスタマイズした _ ユーザ権限の管理 _ 権限を持つローカルグループを作成する。

  権限があらかじめ定義された組み込みのユーザグループがいくつか用意されています。カスタマイズした一連の権限を割り当てるには、ローカルグループを作成し、そのグループに必要な権限を割り当てます。その後、ローカルグループにローカルユーザ、ドメインユーザ、およびドメイングループを追加します。

関連情報

ローカルユーザ認証の仕組み

サポートされる権限のリスト

ローカルユーザ認証の仕組み

CIFS サーバのデータにアクセスする前に、ローカルユーザは認証されたセッションを作成する必要があります。

SMB はセッションベースであるため、ユーザの ID は、最初にセッションがセットアップされたときに一度だけ確認できます。CIFS サーバでは、ローカルユーザの認証時に NTLM ベースの認証が使用されます。NTLMv1 と NTLMv2 の両方がサポートされています。

ONTAP では、 3 つの事例でローカル認証が使用されます。各事例は、ユーザ名のドメイン部分（ DOMAIN\user 形式）が CIFS サーバのローカルドメイン名（ CIFS サーバ名）と一致するかどうかによって異なります。

- ドメイン部分が一致します

  データへのアクセスを要求するときにローカルユーザクレデンシャルを指定したユーザが、 CIFS サーバでローカルに認証されます。

- ドメイン部分が一致しません

  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は、認証が失敗した理由によって次の動作が異なります。

  たとえば、ユーザは Active Directory 内に存在するが、パスワードが無効であるか期限切れになっている

場合は、 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。その他にも、 ONTAP が CIFS サーバ上の対応するローカルアカウントを使用している場合、そのアカウントが存在するときは、 NetBIOS ドメイン名が一致していなくても認証に使用するケースがあります。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。

- ドメイン部分は指定されません

  ONTAP はまず、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は、 ONTAP が、 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したら、 ONTAP でローカルグループメンバーシップおよび権限が考慮される完全なユーザアクセストークンが構成されます。

ローカルユーザの NTLM 認証の詳細については、 Microsoft Windows のマニュアルを参照してください。

関連情報

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はです `Domain Users` （RID 513）。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に対する影響

CIFS サーバを作成すると、デフォルトの一連のローカルユーザとローカルグループが作成され、 CIFS サーバをホストする Storage Virtual Machine （ SVM ）に関連付けられます。SVM 管理者は、ローカルユーザやローカルグループをいつでも作成することができます。CIFS サーバを削除するときは、それを実行した場合のローカルユーザとローカルグループに対する影響について理解しておく必要があります。

ローカルユーザとローカルグループは SVM に関連付けられます。そのため、セキュリティの観点から、CIFS サーバを削除してもそれらが削除されることはありません。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、表示されなくなります。SVM で CIFS サーバを再作成するまで、表示したり管理したりすることはできません。

CIFS サーバの管理ステータスは、ローカルユーザやローカルグループが表示されるかどうかには影響しません。

Microsoft 管理コンソールでのローカルユーザとローカルグループの情報の表示

Microsoft 管理コンソールを使用して、ローカルユーザとローカルグループのそれぞれの情報を表示できます。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

サポートされる権限のリスト

ONTAP には、一連のサポートされる権限があらかじめ定義されています特定の事前定義されたローカルグループには、これらの権限の一部がデフォルトで追加されています。事前定義グループの権限は追加または削除できます。また、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、そのグループや、既存のドメインユーザおよびグループに権限を追加することもできます。

次の表に、 Storage Virtual Machine （ SVM ）でサポートされる権限の一覧と、その権限が割り当てられている BUILTIN グループを示します。

権限の名前	デフォルトのセキュリティ設定	説明
`SeTcbPrivilege`	なし	オペレーティングシステムの一部として機能します
`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します
`SeRestorePrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	ファイルおよびディレクトリをリストアし、 ACL を上書きすべての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します
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	ファイルまたはその他のオブジェクトの所有権を取得します
`SeSecurityPrivilege`	`BUILTIN\Administrators`	監査の管理 これには、セキュリティログの表示、ダンプ、およびクリアが含まれます。

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

- ローカル権限を割り当てます
- トラバースチェックのバイパスの設定

権限を割り当てます

ローカルユーザまたはドメインユーザに権限を直接割り当てることができます。また、ユーザに付与する権限と一致する権限が割り当てられているローカルグループにユーザを割り当てることもできます。

- 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。

  その後、ユーザに付与する権限が割り当てられているグループにユーザを追加します。

- また、ローカルユーザおよびドメインユーザを、デフォルトの権限がユーザに付与する権限と一致している事前定義グループに割り当てることもできます。

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に対する権限の追加
- ローカルまたはドメインのユーザまたはグループの権限を削除しています
- ローカルまたはドメインのユーザまたはグループの権限をリセットしています
- 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を次に示します

BUILTIN グループとローカル管理者アカウントを使用する場合は、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 アカウントは、名前の変更は可能ですが、削除はできません。
- Administrator アカウントは BUILTIN\Administrators グループから削除できません。
- BUILTIN グループは、名前の変更は可能ですが、削除はできません。

  BUILTIN グループの名前を変更したあと、よく知られた名前を使用して別のローカルオブジェクトを作成できますが、そのオブジェクトには新しい RID が割り当てられます。

- ローカルゲストアカウントがありません。

関連情報

事前定義の BUILTIN グループとそのデフォルトの権限

ローカルユーザパスワードの要件

デフォルトでは、ローカルユーザのパスワードは複雑さの要件を満たしている必要があります。パスワードの複雑さの要件は、 Microsoft Windows_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 種類のうちの 3 種類以上の文字を含める必要があります。
  - 大文字のアルファベット（ A~Z ）
  - 小文字のアルファベット（ a~z ）
  - 数字（ 0~9 ）
  - 特殊文字：

    ~@ # $ % ｛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を表示する

ローカルユーザのアカウントパスワードを変更しています

事前定義の **BUILTIN** グループとそのデフォルトの権限

ローカルユーザまたはドメインユーザのメンバーシップを、 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、事前定義された権限が割り当てられ

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\Administrators`544番 最初に作成されたとき、ローカル `Administrator` RIDが500のアカウントは、自動的にこのグループのメンバーになります。Storage Virtual Machine（SVM）がドメインに参加している場合は、`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た場合は `domain\Domain Admins` グループがグループから削除されます。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`547番地 このグループには、最初に作成された時点ではメンバーはありません。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に追加することはできません `BUILTIN\Administrators` グループ：	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`住所は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はありません。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\Users`RID 545 最初に作成された時点では、このグループには（暗黙の以外に）メンバーはありません `Authenticated Users` 特殊グループ）。SVMがドメインに参加すると、が表示されます `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た場合は `domain\Domain Users` グループがこのグループから削除されます。	`SeChangeNotifyPrivilege`
`Everyone`SID 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（ただし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を次に示します

サポートされる権限のリスト

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を有効または無効にします

ローカルユーザとローカルグループ機能の概要を有効または無効にします

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の明示的な無効化に加えて、 ONTAP では、クラスタ内のノードがローカルユーザとローカルグループ機能をサポートしていないリリースの ONTAP にリバートされた場合にその機能が無効になります。クラスタ内のすべてのノードでその機能をサポートするバージョンの 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します

ローカルグループを変更します

ローカルまたはドメインのユーザまたはグループに権限を追加します

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します

Storage Virtual Machine （ SVM ）での SMB アクセスに使用するローカルユーザとローカルグループを有効または無効にすることができます。ローカルユーザとローカルグループ機能はデフォルトで有効になっています。

このタスクについて

SMB 共有および NTFS ファイル権限の設定時にローカルユーザとローカルグループを使用でき、必要に応じて、 SMB 接続の作成時の認証のためにローカルユーザを使用できます。認証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	`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を有効または無効にします

ローカルユーザアカウントを有効または無効にします

ローカルユーザ認証を有効または無効にします

Storage Virtual Machine （ SVM ）での SMB アクセスに関するローカルユーザ認証を有効または無効にすることができます。デフォルトでは、ローカルユーザ認証は許可されます。これは、 SVM がドメインコントローラにアクセスできない場合、またはドメインレベルのアクセス制御を使用しない場合に役立ちます。

作業を開始する前に

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。

このタスクについて

ローカルユーザ認証はいつでも有効または無効にできます。SMB 接続の作成時の認証のためにローカルユーザを使用する場合は、 CIFS サーバのローカルユーザとローカルグループオプションも有効にする必要があります。

手順

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	`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します

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` 概要 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します	`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します

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を有効または無効にします

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。

このタスクについて

ユーザアカウントを変更してローカルユーザを有効にします。

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します	`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します	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

ローカルユーザのアカウントパスワードを変更する

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を表示する

ローカルユーザに関する情報を表示します

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には、そのユーザの詳細なアカウント情報、および複数のユーザのアカウント情報を表示します。この情報は、ユーザの設定を変更する必要があるかどうかを判断する場合に加えて、認証やファイルアクセスに関する問題のトラブルシューティングを行う場合にも役立ちます。

このタスクについて

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 ）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`*

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します

ローカルユーザが属しているローカルグループに関する情報を表示できます。この情報を使用して、ユーザに付与する必要があるファイルやフォルダへのアクセスを確認できます。この情報は、ユーザに付与する必要があるファイルやフォルダへのアクセス権や、ファイルアクセスに関する問題のトラブルシューティングを行うタイミングを判断するのに役立ちます。

このタスクについて

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に関する情報を表示します	`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に関する情報を表示します	`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に関する情報を表示する	`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します

CIFS サーバに対するローカル 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、 Storage Virtual Machine （ SVM ）から削除することができます。

このタスクについて

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。

  このユーザを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- ローカルユーザへのすべての参照がメンバーシップおよび権限のデータベースから削除されます。
- Administrator などの標準的な既知のユーザは削除できません。

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

ローカルグループを変更します

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` 概要 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します

クラスタまたは指定した Storage Virtual Machine （ SVM ）で設定されているすべてのローカルグループの一覧を表示できます。この情報は、 SVM に格納されているデータに対するファイルアクセスに関する問題や、 SVM のユーザ権限に関する問題のトラブルシューティングに役立ちます。

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、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに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。

このタスクについて

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を次に示します。

- 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。
- ローカルグループにユーザを追加する前に、あらかじめそのグループが存在している必要があります。
- ローカルグループにユーザを追加する前に、あらかじめそのユーザが存在している必要があります。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、 Data ONTAP で名前を 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を次に示します。

- 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。
- 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 に対して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
グループに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[,...]` カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。
グループから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[,...]` カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

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を表示する

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

クラスタまたは指定した Storage Virtual Machine （ SVM ）で設定されているローカルグループのすべてのメンバーの一覧を表示できます。この情報は、ファイルアクセスに関する問題やユーザ権限に関する問題のトラブルシューティングに役立ちます。

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決定するのに必要なくなった場合や、 SVM ユーザ権限をグループメンバーに割り当てるのに必要なくなった場合は、 SVM からローカルグループを削除できます。

このタスクについて

ローカルグループを削除する場合は、次の点に注意してください。

- ファイルシステムは変更されません。

  このグループを参照するファイルやディレクトリに対する Windows セキュリティ記述子は調整されません。

- 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のドメインユーザおよびグループ名を更新します

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することができます。これらのドメインオブジェクトは、クラスタのローカルデータベースに登録されます。ドメインオブジェクトの名前を変更した場合は、ローカルデータベースを手動で更新する必要があります。

このタスクについて

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について、正常に更新されたものと更新できなかったものを表示する	`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について、正常に更新されたものを表示する	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
更新できなかったドメインユーザとドメイングループのみを表示します	`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します	`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およびグループの名前を更新します。前回の更新に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
```

ローカル権限を管理します

ローカルまたはドメインのユーザまたはグループに権限を追加します

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。

作業を開始する前に

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。

このタスクについて

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。
- ドメインユーザまたはグループへの権限の追加時、 ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。

  ONTAP からドメインコントローラに接続できない場合、コマンドが失敗することがあります。

手順

1. ローカルまたはドメインのユーザまたはグループに1つ以上の権限を追加します。 `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or -group-name name -privileges _privilege_[,...]`
2. 必要な権限がオブジェクトに適用されていることを確認します。 `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

例

次の例は、 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またはグループから権限を削除します

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。

作業を開始する前に

権限を削除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。

このタスクについて

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。
- ドメインのユーザまたはグループの権限を削除する場合、 ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。

  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つ以上の権限を削除します。 `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 必要な権限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権限をリセットします

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。

このタスクについて

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権限をリセットします。 `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. オブジェクトの権限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します

ドメインまたはローカルのユーザアカウントまたはグループに割り当てられているカスタムの権限に関する情報を表示できます。この情報は、必要なユーザ権限が適用されているかどうかを確認するのに役立ちます。

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 ）上のすべてのドメインおよびローカルのユーザとグループのカスタム権限	`vserver cifs users-and-groups privilege show -vserver` *`vserver_name`*
SVM 上の特定のドメインまたはローカルのユーザとグループのカスタム権限	`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

次のコマンドを実行すると、 SVM vs1 のローカルまたはドメインのユーザとグループに明示的に関連付けられているすべての権限が表示されます。

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ----------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

トラバースチェックのバイパスを設定する

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 でチェックされないで、ファイルへのアクセスの可否が判別されます。
- 拒否した場合、 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を設定する

ONTAP CLI を使用するか、 Active Directory グループポリシーにこのユーザ権限を設定すると、トラバースチェックのバイパスを設定できます。

。 `SeChangeNotifyPrivilege` 権限は、ユーザ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を拒否できます。

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割り当てられています。

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`

- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

これらのいずれかのグループのメンバーにトラバースチェックのバイパスを許可したくない場合は、グループからこの権限を削除する必要があります。

CLI を使用して SVM 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、を追加する必要があります `SeChangeNotifyPrivilege` そのグループへの特権。
- 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する場合に、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ときは、を追加できます `SeChangeNotifyPrivilege` そのユーザアカウントに対する権限。
- ローカルまたはドメインのユーザまたはグループのトラバースチェックのバイパスを無効にするには、を削除します `SeChangeNotifyPrivilege` いつでも特権。

> 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、も削除する必要があります `SeChangeNotifyPrivilege` 権限を取得します `Everyone` グループ：

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します

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を設定します

SMB 共有のアクセス制御リストを作成

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

サポートされる権限のリスト

ローカルまたはドメインのユーザまたはグループに権限を追加します

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ユーザにない場合でも、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、を追加します `SeChangeNotifyPrivilege` Storage Virtual Machine（SVM）上のローカルSMBユーザまたはグループに対する権限。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。

作業を開始する前に

- 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。
- が格納されているローカルまたはドメインのユーザまたはグループ `SeChangeNotifyPrivilege` 追加する権限はすでに存在している必要があります。

このタスクについて

ドメインユーザまたはグループへの権限の追加時、 ONTAP では、ドメインコントローラに接続してそのドメインユーザまたはグループを検証することがあります。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. を追加して、トラバースチェックのバイパスを有効にします `SeChangeNotifyPrivilege` ローカルまたはドメインのユーザまたはグループに対する権限： `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   の値 `-user-or-group-name` パラメータは、ローカルユーザまたはローカルグループ、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'」グループに属するユーザがを追加して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ます `SeChangeNotifyPrivilege` グループに対する権限：

```
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を禁止する

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します

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ために、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ないようにするには、を削除します `SeChangeNotifyPrivilege` Storage Virtual Machine（SVM）上のローカルSMBユーザまたはグループからの権限。

作業を開始する前に

権限を削除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。

このタスクについて

ドメインのユーザまたはグループの権限を削除する場合、 ONTAP でそれらのユーザやグループを検証するために、ドメインコントローラに接続することがあります。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. 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、を削除します `SeChangeNotifyPrivilege` 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の権限 `-user-or-group-name name` パラメータ

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を許可する

ファイルセキュリティと監査ポリシーに関する情報を表示します

ファイルセキュリティと監査ポリシーの概要に関する情報を表示します

Storage Virtual Machine （ SVM ）上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を表示する

次のセキュリティ形式のボリュームと（ FlexVol の） qtree 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 」
- 混在

監査ポリシーに関する情報を表示する

次の NAS プロトコルを介した FlexVol ボリューム上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 に対応している

Storage-Level Access Guard （ SLAG ；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

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 および qtree オブジェクトに適用できます。

- NTFS
- 混在
- UNIX （ボリュームが含まれる SVM で CIFS サーバが設定されている場合）

ダイナミックアクセス制御（ **DAC** ）セキュリティに関する情報を表示する

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 ボリューム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、 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。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、 NTFS ファイルアクセス権と Windows のユーザおよびグループのみを使用してファイルアクセス権を決定するため、 UNIX 関連の出力フィールドには表示専用の UNIX ファイルアクセス権情報が格納されます。
- 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
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細が表示されます	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスに関するセキュリティ情報を表示します `/vol4` SVM vs1：

```
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
```

次の例は、マスクを展開してパスに関するセキュリティ情報を表示します `/data/engineering` SVM vs1：

```
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
```

次の例は、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` SVM vs1：

```
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を表示する

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、 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。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

- mixed セキュリティ形式のボリュームおよび qtree には、 UNIX ファイル権限、モードビットまたは NFSv4 ACL 、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。
- mixed セキュリティ形式のボリュームの最上位には、 UNIX 対応のセキュリティまたは NTFS 対応のセキュリティを設定できます。
- ACL 出力は、 NTFS または NFSv4 セキュリティが適用されたファイルとフォルダについてのみ表示されます。

  このフィールドは、モードビットのアクセス権のみ（ NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよび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
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細が表示されます	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスに関するセキュリティ情報を表示します `/projects` マスクを展開した形式でSVM vs1に格納します。この mixed セキュリティ形式のパスには、 UNIX 対応のセキュリティが設定されています。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

次の例は、パスに関するセキュリティ情報を表示します `/data` （SVM vs1）。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
```

次の例は、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` （SVM vs1）。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を表示する

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。

このタスクについて

Storage Virtual Machine （ SVM ）の名前、およびファイルまたはディレクトリのセキュリティ情報を表示するデータのパスを入力する必要があります。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、ファイルアクセス権の決定時に、 UNIX ファイルアクセス権のみが使用されます。モードビットまたは NFSv4 ACL です。
- 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、モードビットのアクセス権のみ（ NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびディレクトリでは空になります。

- ACL 出力の所有者とグループの出力フィールドは、 NFSv4 セキュリティ記述子には該当しません。

  これらのフィールドが意味があるのは、 NTFS セキュリティ記述子の場合のみです。

- ストレージレベルのアクセス保護セキュリティは、SVMでCIFSサーバが設定されている場合、UNIXのボリュームまたはqtreeでサポートされるため、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` パラメータ

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
要約形式で表示されます	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
詳細が表示されます	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

例

次の例は、パスに関するセキュリティ情報を表示します `/home` SVM vs1：

```
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: -
```

次の例は、パスに関するセキュリティ情報を表示します `/home` マスクを展開した形式のSVM vs1：

```
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を表示する

CLI を使用して、 **FlexVol** の **NTFS** 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、適用されているアクセス権、システムアクセス制御リストに関する情報など、 FlexVol の NTFS 監査ポリシーに関する情報を表示できます。この結果を使用して、セキュリティ設定の検証や、監査に関する問題のトラブルシューティングを行うことができます。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

- NTFS セキュリティ形式のボリュームおよび qtree では、 NTFS の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およびフォルダには、 NTFS 監査ポリシーを適用できます。

  mixed セキュリティ形式のボリュームおよび qtree には、 UNIX ファイル権限、モードビットまたは NFSv4 ACL 、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- mixed セキュリティ形式のボリュームの最上位では、 UNIX または NTFS 対応のセキュリティを有効にすることができ、そこには NTFS SACL が格納されている場合も、格納されていない場合もあります。
- 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の NTFS SACL の両方が表示される場合があります。
- 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は表示専用の UNIX ファイル権限情報が格納されます。

  ファイルアクセス権の決定時、 NTFS セキュリティ形式のファイルおよびフォルダでは、 NTFS ファイルアクセス権と Windows ユーザおよびグループのみが使用されます。

- ACL 出力は、 NTFS または NFSv4 セキュリティ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、モードビットのアクセス権のみ（ NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者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
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細なリストとして	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスの監査ポリシーの情報を表示します `/corp` （SVM vs1）。パスで NTFS 対応のセキュリティが有効になっています。NTFS セキュリティ記述子には、 SUCCESS および SUCCESS/FAIL SACL エントリの両方が含まれています。

```
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、パスの監査ポリシーの情報を表示します `/datavol1` （SVM vs1）。このパスには、標準ファイルおよびフォルダの SACL とストレージレベルのアクセス保護の SACL の両方が格納されています。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

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。

このタスクについて

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。出力は要約形式または詳細なリストで表示できます。

- UNIX セキュリティ形式のボリュームおよび qtree では、監査ポリシーに NFSv4 SACL のみが使用されます。
- mixed セキュリティ形式のボリュームにある UNIX セキュリティ形式のファイルとディレクトリには、NFSv4 監査ポリシーを適用できます。

  mixed セキュリティ形式のボリュームおよび qtree には、 UNIX ファイル権限、モードビットまたは NFSv4 ACL 、および NTFS ファイル権限を使用する一部のファイルおよびディレクトリを含めることができます。

- 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、モードビットのアクセス権のみ（ NFSv4 ACL はなし）が適用されている UNIX セキュリティ形式のファイルおよびフォルダでは空になります。

- ACL 出力の所有者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、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` パラメータ

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
要約形式で表示されます	`vserver security file-directory show -vserver vserver_name -path path`
詳細が表示されます	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

例

次の例は、パスに関するセキュリティ情報を表示します `/lab` （SVM vs1）。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

次のコマンドにワイルドカード文字を指定すると、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ます `/1/` SVM vs1：

```
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、パスの下に「*」という名前のファイルの情報を表示します `/vol1/a` SVM vs1の。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場合、リモートクライアントを使用せずにファイルセキュリティを管理できます。CLI を使用すると、多数のファイルやフォルダに対してセキュリティを適用する場合でも 1 つのコマンドで実行できるため、所要時間を大幅に短縮できます。

ONTAP から SVM ボリュームに適用されるもう 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環境は、すべての NAS プロトコルからストレージレベルのアクセス保護が適用されているストレージオブジェクトへのアクセスを保護します。

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。また、 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。システム（ Windows または UNIX ）管理者であっても、ストレージレベルのアクセス保護セキュリティをクライアントから取り消すことはできません。そのため、ストレージレベルのアクセス保護は、ストレージ管理者が独立して設定および管理できるセキュリティレイヤをデータアクセスに追加で提供します。

ストレージレベルのアクセス保護では NTFS のアクセス権のみがサポートされます。ただし、ストレージレベルのアクセス保護が適用されているボリューム上のデータへの NFS 経由のアクセスに対しても、そのボリュームを所有する SVM 上の Windows ユーザに UNIX ユーザがマッピングされている場合は、 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はすべて、 NTFS 対応のセキュリティが有効になります。を使用できます `vserver security file-directory` 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するためのコマンドファミリー。

- ボリュームに格納されてい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および qtree には、 UNIX 対応のセキュリティを備え、 UNIX ファイルアクセス権を使用する一部のファイルおよびフォルダ、モードビットまたは NFSv4.x ACL と NFSv4.x 監査ポリシー、および NTFS 対応のセキュリティを有効にして NTFS ファイルアクセス権と監査ポリシーを使用する一部のファイルおよびフォルダを含めることができます。を使用できます `vserver security file-directory` 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するコマンドファミリー。

- mixed 形式のボリュームや qtree での NTFS 対応のセキュリティ形式のファイルおよびフォルダに対するファイル権限と監査ポリシー
- ストレージレベルのアクセス保護： NTFS 対応または UNIX 対応の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

UNIX セキュリティ形式のボリュームと 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 ）を備えたファイルとフォルダが含まれます。を使用する場合は、次の点に注意する必要があります `vserver security file-directory` 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コマンドファミリー：

- 。 `vserver security file-directory` UNIXセキュリティ形式のボリュームおよびqtreeでは、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。
- を使用できます `vserver security file-directory` UNIXセキュリティ形式のボリュームを含むSVMにCIFSサーバが含まれている場合に、そ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するコマンドファミリー。

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します

CLI を使用して、 NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

CLI を使用して、 NTFS ファイルおよびフォルダに対して監査ポリシーを設定および適用する

ストレージレベルのアクセス保護を使用してファイルアクセスを保護

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

ファイルおよびフォルダのセキュリティ設定で CLI を使用する際には、一定の制限事項を知っておく必要があります。

- 。 `vserver security file-directory` コマンドファミリーはNFSv4 ACLの設定をサポートしていません。

  NTFS のセキュリティ記述子は NTFS ファイルと NTFS フォルダにのみ適用できます。

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、指定されたファイルまたはフォルダに対してオブジェクト（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す。セキュリティ記述子が適用されるファイルまたはフォルダに対してユーザ、グループ、またはコンピュータオブジェクトが実行できる操作に関する情報が含まれます。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操作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 内の個々のエントリです。

  - DACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトに対して許可または拒否されるアクセス権を指定します。
  - SACL アクセス制御エントリは、特定のユーザ、グループ、またはコンピュータオブジェクトによって実行される指定された操作の監査時にログに記録される成功または失敗イベントを指定します。

- * 権限の継承 *

  権限の継承は、セキュリティ記述子で定義された権限が親オブジェクトからオブジェクトにどのように伝播されるかを示します。子オブジェクトには継承可能な権限のみが継承されます。親オブジェクトのアクセス権を設定する際に、フォルダ、サブフォルダ、およびファイルがそのアクセス権を継承できるかどうかを「適用先」で決定することができます `this-folder`、 `sub-folders`、および`files``」を指定します。

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に対する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がセキュリティ記述子、 DACL 、 SACL エントリのいずれかでローカルユーザまたはグループを使用する場合、 ID 破棄設定の Storage Virtual Machine （ SVM ）ディザスタリカバリデスティネーションでファイルとディレクトリのポリシーを適用する前に注意すべきいくつかの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（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` コマンドファミリー）。

たとえば、「vs1」の場合、が配置されているDACLエントリを設定しているとします `-account` パラメータが「CIFS1\user1」に設定されている場合、デスティネーションSVMでデスティネーションのCIFSサーバ名が反映されて設定が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
```

を使用する必要があります `vserver security file-directory modify` 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コマンド

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。を使用できます `vserver security file-directory ntfs modify` コマンドを使用してアカウント名に必要な変更を行います。

- DACL エントリ

  各 DACL エントリは、アカウントと関連付ける必要があります。ローカルユーザまたはグループアカウントを使用する DACL は、すべてデスティネーション SVM 名を使用するように変更する必要があります。既存の DACL エントリのアカウント名は変更できないため、ローカルユーザまたはグループが設定されたすべての DACL エントリをセキュリティ記述子から削除し、訂正したデスティネーションアカウント名を設定した新しい DACL エントリを作成し、その新しい DACL エントリを適切なセキュリティ記述子と関連付ける必要があります。

- SACLエントリ

  各SACLエントリは、アカウント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 を使用して、 **NTFS** ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

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。

このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

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（ Allow ）	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（ Allow ）	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可（ Allow ）	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（ Allow ）	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。

このタスクについて

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、その DACL に新しい ACE が追加されます。

必要に応じて、で指定したアカウントに対して許可または拒否する権限を指定することで、DACLエントリをカスタマイズできます `-account` パラメータ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。

- 権利
- 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ます `Full Control`。

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。

このタスクについて

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 SVM にそれぞれ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します

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。

このタスクについて

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 つのタイプがあります。

- 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、のデフォルト値です `-access-control` パラメータ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。

このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、 FlexVol ボリューム（ NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。

> 監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。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してください。

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
```

ポリシーを適用する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します

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。

このタスクについて

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、を使用します `-instance` パラメータ

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を確認します

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。

このタスクについて

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。オプションのを使用できます `-expand-mask` セキュリティ設定に関する詳細情報を表示するためのパラメータ。

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 の概要を使用して、 **NTFS** ファイルおよびフォルダに対して監査ポリシーを設定および適用する

ONTAP CLI を使用して NTFS ファイルおよびフォルダに監査ポリシーを適用するには、いくつかの手順を実行する必要があります。まず、 NTFS セキュリティ記述子を作成し、 SACL をセキュリティ記述子に追加します。次に、セキュリティポリシーを作成してポリシータスクを追加します。その後、 Storage Virtual Machine （ SVM ）にセキュリティポリシーを適用します。

このタスクについて

セキュリティポリシーを適用したら、セキュリティポリシージョブを監視して、適用した監査ポリシーの設定を確認することができます。

監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。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してください。

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 を使用して、 NTFS ファイルおよびフォルダに対してファイルセキュリティを設定および適用します

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。

このタスクについて

NTFS セキュリティ形式のボリューム内に存在するファイルやフォルダ、または mixed セキュリティ形式のボリューム上に存在するファイルやフォルダに対して、 NTFS セキュリティ記述子を作成できます。

デフォルトでは、セキュリティ記述子を作成すると、 Discretionary Access Control List （ DACL ；随意アクセス制御リスト）の 4 つの Access Control Entry （ ACE ；アクセス制御エントリ）がそのセキュリティ記述子に追加されます。4 つのデフォルトの ACE は次のとおりです。

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（ Allow ）	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（ Allow ）	フルコントロール	このフォルダ、サブフォルダ、ファイル
作成者の所有者	許可（ Allow ）	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（ Allow ）	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に **NTFS SACL** アクセス制御エントリを追加します

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。

このタスクについて

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ている SACL に既存の ACE がある場合は、新しい ACE が SACL に追加されます。セキュリティ記述子に SACL が含まれていない場合は、 SACL が作成され、その SACL に新しい ACE が追加されます。

SACLエントリを設定するには、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ます `-account` パラメータ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。

- 権利
- 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、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ます `apply to` パラメータ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。

このタスクについて

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 Storage Virtual Machine （ 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します

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。

このタスクについて

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 つのタイプがあります。

- 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、のデフォルト値です `-access-control` パラメータ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。

このタスクについて

セキュリティポリシーに定義されているセキュリティ設定を、 FlexVol ボリューム（ NTFS または mixed セキュリティ形式）内の NTFS ファイルおよびフォルダに適用できます。

> 監査ポリシーと関連する SACL を適用すると、既存の DACL は上書きされます。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してください。

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`

   ポリシーを適用する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します

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。

このタスクについて

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、を使用します `-instance` パラメータ

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
```

適用した監査ポリシーを確認します

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。

このタスクについて

を使用します `vserver security file-directory show` コマンドを使用して監査ポリシーの情報を表示します。データが格納されている SVM の名前、およびファイルまたはフォルダの監査ポリシーの情報を表示するデータのパスを指定する必要があります。

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の管理に関する考慮事項

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を管理するコマンド

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に関する情報を作成、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`

のマニュアルページを参照してください `vserver security file-directory ntfs` 詳細情報を表示するコマンドです。

NTFS DACL アクセス制御エントリを管理するコマンド

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、 NTFS DACL の ACE に関する情報を変更、削除、表示するなどで、既存の DACL を管理できます。

状況	使用するコマンド
ACE 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`

のマニュアルページを参照してください `vserver security file-directory ntfs dacl` 詳細情報を

表示するコマンドです。

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、 NTFS SACL の ACE に関する情報を変更、削除、表示するなどで、既存の SACL を管理することができます。

状況	使用するコマンド
ACE 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`

のマニュアルページを参照してください `vserver security file-directory ntfs sacl` 詳細情報を表示するコマンドです。

セキュリティポリシーを管理するためのコマンド

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を変更することはできません。

状況	使用するコマンド
セキュリティポリシーを作成する	`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`

のマニュアルページを参照してください `vserver security file-directory policy` 詳細情報を表示するコマンドです。

セキュリティポリシータスクを管理するコマンド

ONTAP には、セキュリティポリシータスクを追加、変更、削除、および関連する情報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`

のマニュアルページを参照してください `vserver security file-directory policy task` 詳細情報を表示するコマンドです。

セキュリティポリシージョブの管理用コマンド

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`

のマニュアルページを参照してください `vserver security file-directory job` 詳細情報を表示するコマンドです。

SMB 共有のメタデータキャッシュを設定します

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ングを有効にします

SMB メタデータのキャッシングを有効にすることで、 SMB 1.0 クライアントの SMB パフォーマンス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します	`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

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

SMB メタデータキャッシュエントリの有効期間を設定します

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。

作業を開始する前に

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
共有を作成します	`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、あるユーザが以前に開いていたファイルに別のユーザがアクセスするのを防ぐために、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 クライアントである場合、ロックは任意に設定します。クライアントが SMB クライアントである場合、ロックは必須となります。

NFS ファイルと SMB ファイルのロックの違いのため、 SMB アプリケーションですでに開いているファイルに NFS クライアントからアクセスすると、エラーになる場合があります。

NFS クライアントが SMB アプリケーションによってロックされたファイルにアクセスすると、次のいずれかの状態になります。

- mixed形式またはNTFS形式のボリュームでは、などのファイル操作が行われます `rm`、 `rmdir`および `mv` NFSアプリケーションが失敗するように原因 できますか。
- NFS の読み取りと書き込みの処理は、 SMB の読み取り拒否および書き込み拒否のオープンモードによってそれぞれ拒否されます。
- また、ファイルの書き込み対象となる範囲が、排他的な SMB バイトロックでロックされている場合も、NFS の書き込みの処理はエラーになります。
- 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ます。

    ファイルは最後に閉じた後に削除されます。
  - NFSのリンク解除処理はサポートされていません。

    NTFSセマンティクスとSMBセマンティクスが必要であり、NFSでは前回の削除時のクローズ処理がサポートされないため、この処理はサポートされません。
  - 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ます。

    NFSとUNIXのセマンティクスが必要なため、サポートされています。
- 名前を変更する
  - NTFSファイルシステムの場合、デスティネーションファイルがSMBまたはCIFSから開かれていれば、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。

    NTFSセマンティクスとSMBセマンティクスが必要なため、サポートされていません。

UNIX セキュリティ形式のボリュームでは、 NFS のリンク解除および名前変更の処理で SMB のロック状態が無視され、ファイルへのアクセスが許可されます。UNIX セキュリティ形式のボリュームでのその他すべての NFS 処理では、 SMB のロック状態が考慮されます。

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 クライアントがこ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 では、ファイルが開いているときにそのファイルのパスの各コンポーネントがロックされません。この動作は SMB 共有パスにも影響します。

ONTAP 原因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原因の問題が発生したり、SMB 構成の共有パスを無効な名前に変更したりすることができます。原因によって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、ユーザまたはアプリケーションが重要なディレクトリの名前を変更できないようにするセキュリティ設定を適用します。

ロックに関する情報を表示します

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。

このタスクについて

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` 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. を使用して、ロックに関する情報を表示します `vserver locks show` コマンドを実行します

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
```

ロックを解除します

ファイルロックが原因でクライアントがファイルにアクセスできなくなっている場合は、現在有効なロックの情報を表示して、特定のロックを解除することができます。ロックの解除が必要になるケースとしては、アプリケーションのデバッグなどが挙げられます。

このタスクについて

。 `vserver locks break` コマンドは、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、を使用します `vserver locks show` コマンドを実行します

   詳細については、コマンドのマニュアルページを参照してください。

2. 権限レベルを advanced に設定します。 `set -privilege advanced`
3. 次のいずれかを実行します。

ロックを解除するための指定項目	入力するコマンド
SVM 名、ボリューム名、 LIF 名、およびファイルパス	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
ロック ID	`vserver locks break -lockid UUID`

4. admin 権限レベルに戻ります。 `set -privilege admin`

SMB のアクティビティを監視する

SMB セッション情報を表示します

SMB 接続、 SMB セッション ID 、セッションを使用しているワークステーションの IP アドレスなど、確立された SMB セッションに関する情報を表示できます。セッションの SMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

このタスクについて

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。

- オプションのを使用できます `-fields` 選択したフィールドに関する出力を表示するためのパラメータ。

  入ることができます `-fields ?` 使用できるフィールドを決定します。

- を使用できます `-instance` 確立されたSMBセッションに関する詳細情報を表示するためのパラメータ。
- を使用できます `-fields` パラメータまたは `-instance` パラメータのみ、または他のオプションパラメータと組み合わせて指定します。

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を要約形式で表示します	`vserver cifs session show -vserver vserver_name`
指定した接続 ID のセッション	`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 アドレスからのセッションです	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定した LIF IP アドレスのセッションを表示します	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
指定したノード上のセッションを表示します	`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です
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	を指定します
`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セッションです	`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利用できます。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に設定します `SMB3` 以降が必要です。 ====
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 `Partial`つまり、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。を使用できます `vserver cifs sessions file show` コマンドを使用して、確立されたセッションのどのファイルが継続的可用性を備えた保護で開かれていないかを確認します。 ====
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。この接続はドメインアカウントを使用して確立されています。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドは、 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情報を表示します。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ためには、 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を表示する

開いている **SMB** ファイルに関する情報を表示します

SMB 接続、 SMB セッション ID 、ホスティングボリューム、共有名、共有パスなど、開いている SMB ファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報を表示できます。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確認するのに役立ちます。

このタスクについて

確立された SMB セッションで開いているファイルに関する情報を表示できます。これは、 SMB セッション内の特定のファイルに関する SMB セッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、開いているファイルの一部が継続的可用性を備えた保護を使用して開いている場合と、残りのファイル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場合（の値）`-continuously-available` フィールドに入力します `vserver cifs session show` コマンド出力はです `Partial`）の場合は、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。

を使用して、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` オプションのパラメータを指定しないコマンド。

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。

- オプションのを使用できます `-fields` 選択したフィールドの出力を表示するためのパラメータ。

  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。

- を使用できます `-instance` 開いているSMBファイルに関する詳細情報を表示するためのパラメータ。

  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
をクリックします	`vserver cifs session file show -vserver vserver_name`
指定したノード上のセッションを表示します	`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 セッション ID のファイル
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホスティング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です
`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 パスのオブジェクト
`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ファイル
`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 `No`つまり、これらの開いているファイルは、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は対応していません。また、可用性の高い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。 ====
指定した再接続の状態のファイル	`vserver cifs session file show -vserver vserver_name -reconnected {No

ほかにも、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統計カウンタを確認します

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ときの、クラスタ内の CIFS および SMB アクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

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
```

次のコマンドは、の一部のカウンタに関する情報を表示します `cifs` advanced権限レベルで表示されるオブジェクト。

この例では、で使用可能なカウンタの一部が表示されているわけではありません `cifs` オブジェクト。出力は切り捨てられます。

```
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 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

統計情報を表示します

統計情報を表示します

CIFS と SMB 、監査、および BranchCache ハッシュに関する統計など、さまざまな統計を表示して、パフォーマンスを監視し、問題を診断することができます。

作業を開始する前に

を使用してデータサンプルを収集しておく必要があります `statistics start` および `statistics stop` オブジェクトに関する情報を表示する前のコマンド。

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 と 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 統計を表示します

統計を使用した自動ノードリファーラルのアクティビティの監視

"Microsoft Hyper-V および SQL Server 向けの SMB の設定"

"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ます

オフラインファイルを使用して、オフラインで使用するためのファイルのキャッシュの概要を確認します

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るファイルでも作業を継続できます。

Windows のユーザドキュメントやプログラムを共有に自動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。オフラインで利用可能となったファイルは、 Windows クライアントのローカルディスクと同期されます。同期は、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およびフォルダに対するアクセス権限は CIFS サーバに保存されているファイルおよびフォルダと同じであるため、オフラインのファイルおよびフォルダに対して処理を実行するには、 CIFS サーバに保存されているファイルおよびフォルダに対する十分な権限が必要です。

ユーザとネットワーク上の他のユーザが同じファイルに変更を加えた場合、ユーザはネットワークにローカルバージョンのファイルを保存するか、別のバージョンを保持するか、または両方を保存できます。両方のバージョンを残す場合は、ローカルユーザが変更した新しいファイルがローカルに保存され、キャッシュされたファイルは CIFS サーバに保存されたバージョンの変更が反映されて上書きされます。

オフラインファイルは、共有ごとに共有の設定を行うことができます。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が共有に自動的にキャッシュされるようにします。ローカルにキャッシュされるのは、アクセスしたファイル、フォルダ、およびプログラムだけです。また、この設定を有効にすると、ネットワークに接続されている場合でも、クライアントはローカルにキャッシュされた実行フ

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を参照してください

が搭載された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ます `showsnapshot` ホームディレクトリに設定された共有プロパティ。

状況に応じて `showsnapshot` 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、Windowsクライアントはすべての Snapshotコピーをの下にキャッシュします `~snapshot` ユーザのホームディレクトリ内のフォルダ。

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。

  の内容 `~snapshot` ホームディレクトリ内のフォルダが含まれ、オフラインで使用できるようになります。

- ユーザは、などのフォルダを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ます `My Documents` CIFSサーバ共有上のホームディレクトリのルートに移動します。

  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は `~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。

> ファイル導入をオフラインにします `~snapshot` フォルダはオフラインファイルに含まれないようにしてください。内のSnapshotコピー `~snapshot` フォルダには、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格納されます。そのため、のオフラインコピーを作成します `~snapshot` フォルダは、クライアント上のローカルストレージを大量に消費し、オフラインファイルの同期中にネットワーク帯域幅を消費します。また、オフラインファイルの同期にかかる時間も長くなります。

CLI を使用して **SMB** 共有でオフラインファイルサポートを設定します

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、 ONTAP CLI を使用して、 4 つのオフラインファイル設定のいずれかを指定することによって、オフラインファイルのサポートを設定できます。手動オフラインファイルのサポートがデフォルト設定です。

このタスクについて

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の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、キャッシュしたプログラムファイルをオフラインモードで使用できます。

選択できるオフラインファイル設定は 1 つだけです。既存の SMB 共有でオフラインファイル設定を変更する

と、元の設定が新しいオフラインファイル設定に置き換えられます。その他の既存の SMB 共有設定および共有プロパティは、削除も置換もされません。明示的に削除または変更しないかぎり、有効なままです。

手順

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

次のコマンドでは、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` ファイルモードとディレクトリモードの作成マスクの値を追加します。

```
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** を使用して、 **SMB** 共有でオフラインファイルサポートを設定します

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 ）ホスト名と同じである場合は、 SVM 名を入力し

ます。CIFS サーバの名前が SVM ホスト名と異なる場合は、 CIFS サーバの名前を入力します。

5. [OK] をクリックします。
6. コンソールツリーで、 * システムツール * > * 共有フォルダー * 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すると、 **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できます

移動プロファイルを使用すると、 **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できます

ONTAP では、 Windows の移動プロファイルの格納をサポートしており、それらを Storage Virtual Machine （ SVM ）に関連付けられた CIFS サーバに格納することができます。ユーザ移動プロファイルを設定すると、ユーザはログイン先に関係なく自動でリソースを利用できるようになります。また、移動プロファイルを使用すると、ユーザプロファイルの管理と管理が簡単になります。

移動ユーザプロファイルには、次のような利点があります。

- 自動でリソースを利用できる

  Windows 8 、 Windows 7 、 Windows 2000 、または Windows XP を実行しているコンピュータであれば、ネットワーク上のどのコンピュータにログインしても、各ユーザの一意のプロファイルを自動的に利用できます。ネットワーク上で使用するコンピュータごとにプロファイルを作成する必要はありません。

- コンピュータの交換が簡単

  ユーザのプロファイル情報はすべてネットワークに別途保存されるため、交換後の新しいコンピュータにユーザのプロファイルを簡単にダウンロードできます。ユーザが新しいコンピュータに初めてログインしたときに、サーバに保存されているユーザのプロファイルが新しいコンピュータにコピーされます。

関連情報

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

移動プロファイルを使用するための要件

CIFS サーバで Microsoft の移動プロファイルを使用する前に、この機能をサポートする 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 ONTAP ）については、すべてのバージョンの SMB で移動プロファイルがサポートされます。

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 で確認できます"

移動プロファイルを設定する

ネットワーク上の任意のコンピュータにユーザがログオンするときに、そのユーザのプロファイルを自動的に使用できるようにするには、 Active Directory ユーザとコンピュータ MMC スナップインを使用して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したとき、 `%username%` がユーザの名前に置き換えられます。

   > パス内 `\\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ある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します

フォルダリダイレクトを使用して、 SMB サーバの概要にデータを格納します

ONTAP では、 Microsoft のフォルダリダイレクトをサポートしています。ユーザや管理者は、この機能を使用して、ローカルフォルダのパスを CIFS サーバの場所にリダイレクトできます。リダイレクトされたフォルダは、データが SMB 共有に格納されていても、ローカルの Windows クライアントに格納されたフォルダのように扱うことができます。

フォルダリダイレクトは、主に、ホームディレクトリをすでに導入しており、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、各自の Windows クライアントからフォルダをリダイレクトできます。
- 管理者は、 Active Directory 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。
- 移動プロファイルを設定している場合は、管理者がユーザデータとプロファイルデータを分けることができます。
- 管理者は、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、ローカルフォルダのデータストレージを CIFS サーバにリダイレクトし、ユーザはコンテンツをローカルにキャッシュできます。

関連情報

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を設定します

Windows の [プロパティ] ウィンドウを使用して、フォルダリダイレクトを設定できます。この方法を使用する利点は、 Windows ユーザが SVM 管理者のサポートがなくてもフォルダリダイレクトを設定できることです。

手順

1. エクスプローラで、ネットワーク共有にリダイレクトするフォルダを右クリックします。
2. * プロパティ * をクリックします。

   選択した共有のプロパティが表示されます。

3. [* ショートカット *] タブで、 [* 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、フォルダをにリダイレクトする場合などです `data` 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:\`、を指定します `Q:\data` ターゲットとして。

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 を使用する **Windows** クライアントから **~snapshot** ディレクトリにアクセスします

へのアクセスに使用する方法 `~snapshot` SMB 2.xを使用するWindowsクライアントのディレクトリは、SMB 1.0の場合とは異なります。にアクセスする方法を理解しておく必要があります `~snapshot` 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場合のディレクトリ。

SVM管理者は、Windowsクライアントのユーザがに表示およびアクセスできるかどうかを制御します `~snapshot` 共有上のディレクトリを有効または無効にします `showsnapshot` vserver cifs share properties familiesコマンドを使用した共有プロパティ。

をクリックします `showsnapshot` 共有プロパティが無効になっているため、SMB 2.xを使用するWindowsクライアントのユーザはを表示できません `~snapshot` ディレクトリにあり、内のSnapshotコピーにはアクセスできません `~snapshot` ディレクトリ（へのパスを手動で入力した場合も含む） `~snapshot` またはディレクトリ内の特定のSnapshotコピーにコピーします。

をクリックします `showsnapshot` 共有プロパティが有効になっています。SMB 2.xを使用するWindowsクライアントのユーザは引き続きを表示できません `~snapshot` 共有のルート、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。ただし、共有に接続したユーザは非表示のにアクセスできます `~snapshot` ディレクトリを手動で追加します `\~snapshot` 共有パスの末尾に移動します。隠れた者だ `~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。

- を共有のルートに追加します
- を共有スペースのすべてのジャンクションポイントでクリックします

隠れた者だ `~snapshot` 共有内のジャンクション以外のサブディレクトリからディレクトリにアクセスすることはできません。

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にアクセスできます `~snapshot` ディレクトリを手動で追加します `\~snapshot` を共有パス（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）に設定します。隠れた者だ `~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てファイルとフォルダをリカバリする

以前のバージョン機能の概要を使用したファイルとフォルダのリカバリ

Microsoft の以前のバージョン機能は、 Snapshot コピーを何らかの形でサポートしているファイルシステムで、それらが有効になっている場合に使用できます。Snapshot テクノロジは 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 Microsoft の以前のバージョン機能を使用する前に、この機能をサポートする ONTAP および SMB のバージョンと Windows クライアントの種類について確認しておく必要があります。また、 Snapshot コピーの設定の要件についても確認しておく必要があります。

ONTAP のバージョンの要件

は、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 ONTAP ）については、すべてのバージョンの SMB で以前のバージョン機能がサポートされます。

Windows クライアントの要件

ユーザが以前のバージョン機能を使用して Snapshot コピー内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 で確認できます"

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 コピー内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ようになっていて、 Snapshot コピーが存在している必要があります。

Snapshot コピーのデータを表示および管理するには、イゼンノバージョンタブを使用します

Windows クライアントマシンのユーザは、 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 ）管理者を介さずに Snapshot コピーに格納されたデータをリストアできます。

このタスクについて

管理者が共有を含むボリュームで Snapshot コピーを有効にしている場合、および管理者が Snapshot コピー

を表示するように共有を設定している場合は、以前のバージョンタブで SVM に格納されているデータの Snapshot コピーのデータを表示および管理することしかできません。

手順

1. エクスプローラで、 CIFS サーバに格納されたデータのマッピングされたドライブの内容を表示します。
2. Snapshot コピーを表示または管理するマッピングされたネットワークドライブのファイルまたはフォルダを右クリックします。
3. * プロパティ * をクリックします。

   選択したファイルまたはフォルダのプロパティが表示されます。

4. [以前のバージョン *] タブをクリックします。

   選択したファイルまたはフォルダの使用可能な Snapshot コピーのリストが [フォルダバージョン：] 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できます。

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	実行する処理
Snapshot コピーのデータを表示します	• 開く * をクリックします。
Snapshot コピーからデータのコピーを作成します	[* 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] タブにリストされているファイルやフォルダを変更する場合は、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、コピーを変更する必要があります。

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て Snapshot データを表示および管理する方法の詳細については、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/"

Snapshot コピーが以前のバージョン機能で使用できるかどうかを確認します

有効な Snapshot ポリシーが共有を含むボリュームに適用されていて、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にのみ、以前のバージョンタブで Snapshot コピーを表示できます。Snapshot コピーの使用可否を確認すると、以前のバージョン機能を使用してアクセス可能かどうか確認できます。

手順

1. 共有データが存在するボリュームで自動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 ポリシーおよび 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"

以前のバージョン機能のアクセスを有効にする **Snapshot** 設定を作成します

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、常に以前のバージョン機能を使用できます。Snapshot コピーの設定がこれらの要件を満たしていない場合は、要件を満たすように Snapshot コピーの設定を作成できま

す。

手順

1. [以前のバージョン機能]からのアクセスを許可する共有が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、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` コマンドを実行します

   を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

2. を使用して、Snapshotコピーへのアクセスを有効にします `volume modify` コマンドを使用してを設定します `-snap-dir` オプションをに設定します `true`。

   を使用する方法の詳細については、を参照してください `volume modify` コマンドについては、マニュアルページを参照してください。

3. 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` および `volume snapshot policy show` コマンド

   を使用する方法の詳細については、を参照してください `volume show` および `volume snapshot policy show` コマンドについては、マニュアルページを参照してください。

   Snapshot ポリシーおよび 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、が表示されてリストアに失敗することがあります `Access Denied` エラー。

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は、を使用して確認できます `vol show` コマンドにを指定します `-parent` オプションを使用することもできます `vserver security trace` ファイルおよびフォルダのアクセス問題に関する詳細なログを作成するコマンド。

関連情報

NAS ネームスペース内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を導入

ホームディレクトリを管理します

ONTAP で動的ホームディレクトリを有効にする方法

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/`%w` または `%u` 変数（Variable）：共有名には両方を使用できます `%d` および/`%w` 変数（例： `%d/%w`` または、共有名に静的な部分と変数の部分（`home_`など）を含めることができます/%w`）。

- * 共有パス *

  共有によって定義される、つまり、共有名の 1 つに関連付けられる相対パスです。各検索パスに付加されて、 SVM のルートからのユーザのホームディレクトリの完全パスを生成します。静的（例： `home`）、動的（例： `%w`）、または2つの組み合わせ（例： `eng/%w`）。

- * 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。を使用して、1つ以上の検索パスを指定できます `vserver cifs home-directory search-path add` コマンドを実行します複数 ONTAP の検索パスを指定すると、有効なパスが見つかるまで、指定された順に各検索パスが試行されます。

- * ディレクトリ *

  ユーザに対して作成する、そのユーザのホームディレクトリです。通常、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ます `\\vs1\home_jsmith`。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ます `jsmith`。ONTAP がというディレクトリを検索するようになりました `jsmith` 各検索パスを順にチェックするには、次の手順に従います。

- `/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：ユーザーがに接続する `\\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ます `acme/jsmith`。ONTAP がというディレクトリを検索するようになりました `acme/jsmith` 各検索パスを順にチェックするには、次の手順に従います。

- `/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します

SMB ホームディレクトリ機能を使用する場合、共有プロパティにホームディレクトリプロパティを含む共有を少なくとも 1 つ追加する必要があります。

このタスクについて

ホームディレクトリ共有は、共有の作成時にを使用して作成できます `vserver cifs share create` コマンドを入力するか、を使用して、既存の共有をいつでもホームディレクトリ共有に変更できます `vserver cifs share modify` コマンドを実行します

ホームディレクトリ共有を作成するには、を含める必要があります `homedirectory` の値 `-share -properties` オプションは、共有を作成または変更するときに使用します。共有名と共有パスは変数を使用して指定できます。変数はユーザがそれぞれのホームディレクトリに接続するときに動的に変換されます。パスで使用できる変数はです `%w`、 `%d`および `%u`Windowsユーザ名、ドメイン、マッピングされたUNIXユーザ名にそれぞれ対応します。

手順

1. ホームディレクトリ共有を追加：+
   `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。

共有名にリテラル文字列が含まれている場合は、必須の変数の1つに加えて、必要な変数も含まれています `%w`、 `%u`または `%d`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には、リテラル文字列の前に`%`（パーセント）文字を付ける必要があります（例： `%%w`）。

- 共有名にはどちらかを使用する必要があります `%w` または `%u` 変数（Variable）：
- 共有名にはさらにを含めることができます `%d` 変数（例： `%d/%w`）または共有名の静的な部分（例：home1_/`%w`）。
- 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` は、を設定してこのアクセスを有効にする場合に使用します `-is-home-dirs-access-for-admin-enabled` オプションをに設定します `true`）またはadvancedオプションを設定します `-is-home-dirs-access-for-public-enabled` 終了： `true`。

`-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。を指定する必要があります `homedirectory` 価値。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. 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` コマンドを実行します

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ます `%w`。。 `oplocks`、 `browsable``および `changenotify` 共有プロパティは、に加えて設定します `homedirectory` 共有プロパティ。

この例で表示されているのは、 SVM の共有の出力の一部です。出力は省略されています。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

関連情報

ホームディレクトリ検索パスを追加しています

[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には、一意なユーザ名が必要です

を使用してホームディレクトリ共有を作成する場合は、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` （Windowsユーザ名）または `%u` （UNIXユーザ名）変数。共有を動的に生成します。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。

- ユーザがを使用してクラスタ上の共有のリストを表示したとき `net view` コマンドを実行すると、同じユーザ名を持つ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。
- 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ます `%w` 共有名との競合を回避するためのパラメータ。

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のどちらかが含まれている必要があります `%w` または `%u` 動的変数。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、どちらも含まない新しいホームディレクトリ共有を作成することはできません `%w` または `%u` 変数（Variable）：

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、どちらかを含む名前に変更できます `%w` または `%u` 変数（Variable）：

ホームディレクトリ検索パスを追加します

ONTAP の SMB ホームディレクトリを使用する場合は、ホームディレクトリ検索パスを少なくとも 1 つ追加する必要があります。

このタスクについて

を使用して、ホームディレクトリ検索パスを追加できます `vserver cifs home-directory search-`

path add コマンドを実行します

。 vserver cifs home-directory search-path add コマンドはで指定されたパスをチェックします -path オプション（コマンド実行時）。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。お前が選べ y または n。をクリックします y 続行するには、ONTAP が検索パスを作成します。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、あらかじめディレクトリ構造を作成しておく必要があります。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、を再実行できます vserver cifs home-directory search-path add コマンドを実行します

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. を使用して、検索パスが正常に追加されたことを確認します vserver cifs home-directory search-path show コマンドを実行します

例

次の例は、パスを追加します /home1 SVM vs1のホームディレクトリ設定に移動します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

次の例は、パスの追加を試みます /home2 SVM vs1のホームディレクトリ設定に移動します。パスが存在しません。続行しないように選択します。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

関連情報

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の設定を作成します

を使用して、ホームディレクトリ設定を作成できます %w および %d 変数。ユーザは、動的に作成された共有を使用してホームディレクトリ共有に接続できます。

手順

1. 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. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
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。ユーザがホームディレクトリに接続すると、ONTAP によって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。を指定する必要があります `homedirectory` 価値。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. 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` コマンドを実行します
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. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory search-path show` コマンドを実行します
8. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。

   たとえば、パスがのqtreeを作成したとします `/vol/vol1/users` ディレクトリを作成するユーザ名はmydomain\user1で、次のパスでディレクトリを作成します。 `/vol/vol1/users/mydomain/user1`。

   にマウントされた「home1」という名前のボリュームを作成した場合 `/home1`では、次のパスでディレクトリを作成します。 `/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、ユーザがホームディレクトリ共有に正常に接続できることを確認します。

   たとえば、ユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順8で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

例

次の例のコマンドでは、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ために使用される検索パス `/home1`、は、NTFSセキュリティ形式で設定されているボリュームです。
- 設定は SVM vs1 上に作成されます。

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には、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 ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が Windows ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合にも、このような設定を使用できます。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

関連情報

%u 変数を使用してホームディレクトリを設定します

追加のホームディレクトリの設定

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する

%u 変数を使用してホームディレクトリを設定します

を使用して、ホームディレクトリの設定を作成し、共有名を指定できます `%w` 変数ですが、を使用します `%u` ホームディレクトリ共有の相対パスを指定する変数。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ディレクトリ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. 適切なセキュリティ形式がqtreeで使用されていない場合は、を使用してセキュリティ形式を変更します `volume qtree security` コマンドを実行します
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。

   > を使用することもできます `%u` の変数 `-share-name` オプションこれにより、マッピング先の UNIX ユーザ名を使用して相対共有パスが作成されます。

   `-path %u` 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な要素も含めることができます。例： `eng/%u`。

   `-share-properties homedirectory\[,...\]` その共有の共有プロパティを指定します。を指定する必要があります `homedirectory` 価値。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. 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` コマンドを実行します
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. を使用して、検索パスが正常に追加されたことを確認します `vserver cifs home-directory`

`search-path show` コマンドを実行します

8. UNIXユーザが存在しない場合は、を使用してUNIXユーザを作成します `vserver services unix-user create` コマンドを実行します

> ユーザをマッピングするには、 Windows ユーザ名のマッピング先となる UNIX ユーザ名があらかじめ存在している必要があります。

9. 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、このマッピング手順を実行する必要はありません。

   Windows ユーザ名は対応する UNIX ユーザ名にマッピングされます。Windows ユーザは、ホームディレクトリ共有に接続すると、 Windows ユーザ名に対応する共有名を使用して動的に作成されたホームディレクトリに接続することになります。その際、ディレクトリ名が UNIX ユーザ名に対応していることはユーザにはわかりません。

10. ユーザにホームディレクトリがある場合は、ホームディレクトリを含むように指定した qtree またはボリュームに対応するディレクトリを作成します。

   たとえば、パスがのqtreeを作成したとします `/vol/vol1/users` ディレクトリを作成するユーザのマッピングされたUNIXユーザ名が「unixuser1」である場合は、次のパスでディレクトリを作成します。 `/vol/vol1/users/unixuser1`。

   にマウントされた「home1」という名前のボリュームを作成した場合 `/home1`では、次のパスでディレクトリを作成します。 `/home1/unixuser1`。

11. ドライブをマッピングするか、 UNC パスを使用して、ユーザがホームディレクトリ共有に正常に接続できることを確認します。

   たとえば、UNIXユーザunixuser1にマッピングされるユーザmydomain\user1が、SVM vs1上にあるディレクトリ（手順10で作成）に接続する場合は、UNCパスを使用して接続します `\\vs1\user1`。

例

次の例のコマンドでは、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ために使用される検索パス `/home1`、は、UNIXセキュリティ形式で設定されたボリュームです。
- 設定は SVM vs1 上に作成されます。

ユーザが Windows ホストから、または Windows ホストと UNIX ホストからホームディレクトリにアクセスし、ファイルシステム管理者が UNIX ベースのユーザおよびグループを使用してファイルシステムへのアクセスを制御する場合には、このようなホームディレクトリ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の設定

追加のホームディレクトリの設定

を使用して、追加のホームディレクトリ設定を作成できます `%w`、 `%d`および `%u` 変数。必要に応じてホームディレクトリの設定をカスタマイズできます。

共有名と検索パスで変数と静的文字列の組み合わせを使用して、多数のホームディレクトリの設定を作成できます。次の表に、さまざまなホームディレクトリ設定を作成する例を示します。

で作成されるパス `/vol1/user` ホームディレクトリを含む...	**share** コマンド
をクリックして共有パスを作成します `\\vs1\~win_username` これにより、ユーザがに誘導されます `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
をクリックして共有パスを作成します `\\vs1\win_username` これにより、ユーザがに誘導されます `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
をクリックして共有パスを作成します `\\vs1\win_username` これにより、ユーザがに誘導されます `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
をクリックして共有パスを作成します `\\vs1\unix_username` これにより、ユーザがに誘導されます `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

検索パスを管理するコマンド

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、検索パスに関する情報を追加、削除、表示するためのコマンドがあります。また、検索パスの順序を変更するためのコマンドもあります。

状況	使用するコマンド
検索パスを追加します	`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します	`vserver cifs home-directory search-path reorder`
検索パスを削除します	`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。これは、複数の CIFS ホームディレクトリパスが設定されている場合に、ユーザのホームディレクトリが含まれるパスを確認するときに役立ちます。

ステップ

1. 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` コマンドを実行します

   ```
   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はそのユーザしかアクセスできません。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。

作業を開始する前に

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。共有の命名要件は次のとおりです。

ホームディレクトリの共有名	共有に接続するコマンドの例
｛チルダ｝ %d ｛チルダ｝ %w	`net use * \\IPaddress\~domain~user/u:credentials`

ホームディレクトリの共有名	共有に接続するコマンドの例
｛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+ `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を表示する

UNIX シンボリックリンクへの **SMB** クライアントアクセスを設定する

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、相対および絶対シンボリックリンクをサポートしています。

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、を使用して共有ごとに設定できます `-symlink -properties` のオプション `vserver cifs share create` 次のいずれかの設定を指定してコマンドを実行します。

- 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。widelink を作成するときは、そのクライアントが参照するための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のリパースジャンクションポイントを検出するための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）を削除しようとした場合、シンボリックリンクのみが削除され、ターゲットファイルまたはターゲットディレクトリは削除されません。それに対して、クライアントがワイドリンクを削除しようとした場合には、ワイドリンクが参照する実際のターゲットファイルやターゲットディレクトリが削除されることがあります。クライアントは SVM 外のターゲットファイルまたはディレクトリを明示的に開いて削除できるため、 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。リパースポイントは、 SMB クライアントが NTFS 形式のボリュームで作業する際に、拡張ファイルシステムサービスを受け取る機能を提供します。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、クライアントがさらに処理するために SMB クライアントが取得できるリパースポイントのコンテンツで構成されます。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中で、 ONTAP 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を実装しています。リパースポイントの内容を認識できない SMB クライアントは、単に無視し、リパースポイントで有効になる可能性が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、ファイルが格納されている別の場所（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）を参照できる、ファイルシステムディレクトリ構造内の場所です。ONTAP SMB サーバでは、ディレクトリの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し、ディレクトリのジャンクションポイントがトラバースされたときに対応したクライアントが ONTAP からリパースポイントのコンテンツを取得できるようにします。その結果、異なるパスやストレージデバイスを、同じファイルシステムに属しているかのように移動して接続することができます。

- * 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 *

  。 `-is-use-junctions-as-reparse-points-enabled` ONTAP 9では、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、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可能であり、サポート対象とサポー

ト対象外の両方の SMB クライアントに対応できるようにします。ONTAP 9.2以降のリリースでは、オプションを有効にする必要があります `-widelink-as-reparse-point-versions` ワイドリンクを使用して共有にアクセスする各クライアントプロトコル（デフォルトはSMB1）。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レポートされ、 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際には、一定の制限事項を理解しておく必要があります。

制限（ **Limit** ）	説明
4時45分	CIFS サーバ名の FQDN を使用して指定できる CIFS サーバ名の最大文字数。 代わりに、 CIFS サーバ名を NetBIOS 名として指定できますが、その場合は 15 文字に制限されます。
80	共有名の最大文字数。
256	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 文字の制限に含まれます。
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 文字の制限に含まれます。

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

CIFS サーバオプションを使用して、 **ONTAP** で **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 UNIX シンボリックリンクサポートを設定する

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によって、 SMB 共有で UNIX シンボリックリンクのサポートを設定できます。UNIX シンボリックリンクのサポートはデフォルトで有効になっています。UNIX シンボリックリンクのサポートを共有で無効にすることもできます。

このタスクについて

SMB 共有で UNIX シンボリックリンクのサポートを設定する場合は、次の設定のいずれかを選択できます。

設定	説明
`enable` （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。
`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。ワイドリンクアクセスは常に読み取り / 書き込みです。

設定	説明
`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します。
`no-strict-security`	クライアントに共有の範囲を越えるシンボリックリンクの参照を許可します。
`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オプションが設定されていても、DFS通知は生成されません `is-advertise-dfs-enabled` がに設定されます `true`。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有効にします。DFS通知は、CIFSオプションが指定されている場合でも、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ます `is-advertise-dfs-enabled` がに設定されます `false`。
`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オプションが設定されていても、DFS通知は生成されません `is-advertise-dfs-enabled` がに設定されます `true`。
`""` （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化します。

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
""	-
symlinks	symlinks-and-widelinks

条件	入力するコマンド
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共有を作成します `enable`：

```
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します

SMB 共有に対する UNIX シンボリックリンクのマッピングを作成できます。親フォルダに対して相対的なファイルまたはフォルダを参照する相対シンボリックリンクを作成することも、絶対パスを使用してファイルまたはフォルダを参照する絶対シンボリックリンクを作成することもできます。

このタスクについて

SMB 2.x を使用している場合、 Mac OS X クライアントからワイドリンクにアクセスすることはできませんMac OS X クライアントからワイドリンクを使用して共有に接続しようとすると、接続に失敗します。ただし、 SMB 1 を使用している場合は、 Mac OS X クライアントでワイドリンクを使用できます。

手順

1. SMB共有のシンボリックリンクマッピングを作成するには： `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 (`/`）と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 (`/`）と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 名として指定できます。NetBIOS名は、を使用して確認できます `vserver cifs show` コマンドを実行しますこのオプションパラメータを指定しない場合、デフォルト値のローカル CIFS サーバの NetBIOS 名が使用されます。

   `-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、このパラメータをに設定する必要があります `true` ターゲットの共有がホームディレクトリとして設定されている場合。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。UNIXパスが設定されている `/src/`、SMB共有名「ソース」、CIFSパス `/mycompany/source/` およびCIFSサーバのIPアドレス123.123.123.123。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を管理するコマンド

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。

利点

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。

作業を開始する前に

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の概要で **SMB** 共有のコンテンツをキャッシュする

BranchCache は、要求元のクライアントのローカルコンピュータにコンテンツをキャッシュできるようにするために Microsoft が開発した機能です。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することができます。

BranchCache を設定すると、 Windows BranchCache クライアントはまず SVM のコンテンツを取得し、次に取得したコンテンツをブランチオフィスのコンピュータにキャッシュします。ブランチオフィスの別の BranchCache 対応クライアントが同じコンテンツを要求すると、 SVM は最初に要求元ユーザの認証と許可を実行します。次に SVM は、キャッシュされたコンテンツが最新のものであるかどうかを確認し、最新のものである場合はそのコンテンツに関するメタデータをクライアントに送信します。クライアントは、そのメタデータを使用して、ローカルのキャッシュから直接コンテンツを取得します。

関連情報

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 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 SMB2.1 のみサポートするクライアント、 SMB3.0 をサポートするクライアントが混在する場合は、 BranchCache 1 と BranchCache 2 の両方のキャッシングをサポートする CIFS サーバに BranchCache 構成を実装することができます。

> 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。また、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があります。

BranchCache 1 は、次の ONTAP バージョンと Windows ホストでサポートされています。

- コンテンツサーバ： 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。
- 有効なハッシュが適用されたファイルがを使用してリストアされた場合 `snap restore` コマンドを実行します
- BranchCache対応のSMB共有を含むボリュームがを使用してリストアされた場合 `snap restore` コマンドを実行します

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 アップデートが許可されるボリューム上に配置する必要があります。

  ハッシュストアでは、ハッシュファイルへのアクセス時間を使用して、アクセス頻度の高いファイルを管理します。atime アップデートが無効になっている場合、作成時間がこの目的に使用されます。使用頻度の高いファイルを追跡するために atime を使用することを推奨します。

- SnapMirror デスティネーションや SnapLock ボリュームなどの読み取り専用のファイルシステムにはハッシュを格納できません。
- ハッシュストアが最大サイズに達すると、新しいハッシュを格納するスペースを確保するために古いハッシュがフラッシュされます。

ハッシュストアの最大サイズを増やすと、キャッシュからフラッシュされるハッシュの量を減らすことができます。

- ハッシュを格納するボリュームが使用できないか、いっぱいである場合、またはクラスタ内通信に BranchCache サービスがハッシュ情報を取得できない問題がある場合、 BranchCache サービスは使用できません。

  ボリュームは、オフラインであるため、またはストレージ管理者がハッシュストアの新しい場所を指定したために、使用できないことがあります。

  これは、ファイルアクセスに関する原因の問題ではありません。ハッシュストアに正常にアクセスできない場合は、 ONTAP からクライアントに Microsoft 定義のエラーが返され、クライアントは通常の SMB 読み取り要求を使用してファイルを要求します。

関連情報

SMBサーバでのBranchCacheの設定

BranchCache の設定を変更します

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によって再利用されるファイルコンテンツ、または単一のリモートユーザが繰り返しアクセスするファイルコンテンツを含む共有の場合に役立ちます。
- Snapshot コピーのデータや SnapMirror デスティネーションのデータなどの読み取り専用コンテンツのキャッシュを有効にすることを検討してください。

BranchCache を設定します

BranchCache の概要を設定

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 を設定するための要件

BranchCache のセットアップを開始する前に、いくつかの前提条件を満たす必要があります。

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ます。 "ONTAP One"。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。

このタスクについて

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 ごとに設定します。BranchCache サービスを設定する CIFS 対応の SVM を指定する必要があります。

必須パラメータ	説明
ハッシュストアへのパス _	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。他のデータが格納されているボリュームにハッシュデータを格納するか、ハッシュデータを格納するための別のボリュームを作成することができます。 SVM が SVM ディザスタリカバリソースである場合、ハッシュパスをルートボリューム上に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、ファイル名に使用できる文字と空白を含めることができます。

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 がサポートされています。バージョン 1 、バージョン 2 、または両方のバージョンを有効にできます。デフォルトでは、両方のバージョンが有効になります。
_ 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、新しいハッシュを格納する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。ハッシュが過剰に破棄されない方が、 BranchCache のパフォーマンスは向上します。ハッシュストアがいっぱいになるのが原因でハッシュが頻繁に破棄されていると判断した場合は、 BranchCache の設定を変更して、ハッシュストアのサイズを大きくすることができます。

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 サービスによって使用されるサーバキーを指定できます。指定しない場合、サーバキーは BranchCache の設定の作成時にランダムに生成されます。サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。サーバキーにスペースを含める場合は、サーバキーを引用符で囲む必要があります。
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`

      このコマンドを実行すると、 SMB 2.0 と SMB 2.1 の両方が有効になります。

   d. 必要に応じて、SMB 3.0を有効にします。 `vserver cifs options modify -vserver 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するときに、サーバキーは表示されません。

3. BranchCacheの設定が正しいことを確認します。 `vserver cifs branchcache show -vserver vserver_name`

例

次のコマンドを実行すると、 SMB 2.1 と 3.0 の両方が有効になっていることが確認され、 SVM vs1 上のすべての SMB 共有でキャッシュを自動的に有効にするように BranchCache が設定されます。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

次のコマンドを実行すると、 SMB 2.1 と 3.0 の両方が有効になっていることが確認され、 SVM vs1 上の共有ごとにキャッシュを有効にするように BranchCache が設定されて、 BranchCache の設定が確認されます。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> 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を指定します

BranchCache が有効な SMB 共有を作成

既存の SMB 共有で BranchCache を有効にします

BranchCache の設定を変更します

SMB 共有で BranchCache を無効にする手順の概要

SVM の BranchCache 設定を削除します

リモートオフィスでの **BranchCache** の設定に関する情報の参照先を指定します

SMB サーバで BranchCache を設定したら、クライアントコンピュータに BranchCache をインストールして設定する必要があります。また、必要に応じて、リモートオフィスのキャッシュサーバにも 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 から説明が提供されています。

ブランチオフィスのクライアントを設定する手順、および必要に応じて BranchCache を使用するキャッシュサーバを Microsoft BranchCache の Web サイトで設定する手順について説明します。

"Microsoft BranchCache のドキュメント：「 What's New"

BranchCache が有効な **SMB** 共有を設定

BranchCache が有効な **SMB** 共有の概要を設定

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 共有で有効にするか、共有ごとに有効にすることができます。

- BranchCache を共有ごとに有効にする場合、 BranchCache は共有の作成時に有効にするか、既存の共有を変更して有効にすることができます。

  既存の SMB 共有でキャッシュを有効にすると、その共有で BranchCache を有効にした時点で、 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 が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容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

SMB共有の作成時にを設定して、共有でBranchCacheを有効にすることができます `branchcache` 共有プロパティ。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  これは、共有を作成するときのデフォルト設定です。

- BranchCache が有効な共有を作成するときに、オプションの共有パラメータを追加で指定することもできます。

- を設定できます `branchcache` 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も含む共有のプロパティ。

  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。

- を使用するときに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です `-share-properties` パラメータを指定する場合は、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指定する必要があります `branchcache` プロパティを共有するには、カンマで区切って指定します。
- 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 `vserver cifs share create` コマンドを実行します

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. 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` コマンドを実行します

例

次のコマンドでは、「data」という名前のBranchCacheが有効なSMB共有をパスに作成します `/data` SVM vs1上。デフォルトでは、オフラインファイルの設定はに設定されています `manual`：

```
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** を有効にします

既存のSMB共有でBranchCacheを有効にするには、を追加します `branchcache` 共有プロパティを既存の共有プロパティリストに追加します。

このタスクについて

- SMB 共有で BranchCache を有効にする場合は、共有のオフラインファイル設定を手動キャッシュに設定する必要があります。

  既存の共有のオフラインファイル設定が手動キャッシュに設定されていない場合は、共有を変更して設定する必要があります。

- を設定できます `branchcache` 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も含む共有のプロパティ。

  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。

- を追加したとき `branchcache` 共有プロパティ共有に対する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。を使用する方法の詳細については、を参照してください `vserver cifs share properties add` コマンドについては、マニュアルページを参照してください。

手順

1. 必要に応じて、オフラインファイルの共有設定を手動キャッシュに設定します。
   a. 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` コマンドを実行します
   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、「data2」という名前の既存のSMB共有（パス）でBranchCacheを有効にします `/data2` SVM vs1：

```
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 の設定を管理および監視する

BranchCache 設定を変更

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 BranchCachet 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める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を変更する	`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めるボリュームのサイズを増やします	`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。 の詳細を確認してください "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を変更します

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リソースである場合、ハッシュパスをルートボリューム上に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、ファイル名に使用できる文字と空白を含めることができます。  ハッシュパスを変更する場合は、 `-flush-hashes` は、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必須パラメータです。には次の値を設定できます `-flush-hashes` パラメータ：  を指定する場合 `**true**`**ONTAP** では、元の場所にあるハッシュが削除され、**BranchCache**対応クライアントから新しい要求が行われると、新しい場所に新しいハッシュが作成されます。 を指定する場合 `false`を指定すると、ハッシュはフラッシュされません。 + この場合、後でハッシュストアパスを元の場所に戻して、既存のハッシュを再利用することができます。
動作モードを変更します	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` 動作モードを変更するときは、次の点に注意してください。 **SMB**セッションのセットアップ時に、**ONTAP** によって、**BranchCache**の共有のサポートが通知されます。 BranchCache が有効なときにすでにセッションを確立していたクライアントは、キャッシュされている内容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 バージョンを変更します	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. を使用して、設定の変更を確認します `vserver cifs branchcache show` コマンドを実行します

BranchCache 設定に関する情報を表示します

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 サーバキーを変更します

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。

このタスクについて

サーバキーを特定の値に設定すると、複数のサーバが同じファイルの BranchCache データを提供している場合に、クライアントがその同じサーバキーを使用してサーバのハッシュを使用できるようになります。

サーバキーを変更する場合は、ハッシュキャッシュをフラッシュすることも必要になります。ハッシュのフラッシュ後、 BranchCache 対応クライアントによって新しい要求が行われると、 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、も指定する必要があります `-flush-hashes` に設定します `true`。

2. を使用して、BranchCacheの設定が正しいことを確認します `vserver cifs branchcache show` コマ

ンドを実行します

例

次の例は、 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します

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の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 対応の共有にあるデータのハッシュをピーク以外の時間帯に計算するのに役立ちます。

このタスクについて

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、を使用する必要があります `statistics start` およびオプションです `statistics stop` コマンド

- ハッシュを事前に計算する対象の Storage Virtual Machine （ SVM ）とパスを指定する必要があります。
- また、ハッシュを再帰的に計算するかどうかも指定する必要があります。
- ハッシュを再帰的に計算する場合、 BranchCache サービスでは、指定されたパスの下のディレクトリツリー全体を参照し、対象となる各オブジェクトのハッシュを計算します。

手順

1. 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を再帰的に処理します	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. を使用して、ハッシュが計算されていることを確認します `statistics` コマンドを実行します
   a. の統計を表示します `hashd` 目的のSVMインスタンスのオブジェクト。 `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

次の例は、パスにハッシュを作成します `/data` 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で、次のコマンドを実行します。

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                                11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

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します

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。

このタスクについて

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、さまざまな目的の中でも、キャッシュが適切に機能しているかどうかの確認、キャッシュコンテンツをクライアントに提供しているかどうかの確認、新しいハッシュデータのスペースを確保するためにハッシュファイルが削除されたかどうかの確認に特に役立ちます。

このタスクについて

。 `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 権限レベルで収集して表示できます。

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`

   ```
   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. を使用して、BranchCache関連のカウンタを表示します `statistics catalog counter show` コマンドを実行します

   統計カウンタの詳細については、このコマンドのマニュアルページを参照してください。

   ```
   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. を使用して、BranchCache関連の統計を収集します `statistics start` および `statistics stop` コマンド

```
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. を使用して、収集したBranchCache統計を表示します `statistics show` コマンドを実行します

```
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

統計情報を表示します

"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がサポートされます

ONTAP BranchCache では、 BranchCache のグループポリシーオブジェクト（ GPO ）

をサポートしており、特定の BranchCache の設定パラメータを一元的に管理できます。BranchCache の GPO には、 BranchCache のハッシュの発行 GPO と BranchCache のハッシュバージョンサポート GPO の 2 つがあります。

- * BranchCache のハッシュの発行 GPO *

  BranchCacheのハッシュの発行GPOはに対応します `-operating-mode` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位（ OU ）に含まれる Storage Virtual Machine （ SVM ）オブジェクトにこの値が適用されます。

- * BranchCache のハッシュバージョンサポート *

  BranchCacheのハッシュバージョンサポートGPOはに対応します `-versions` パラメータGPO の更新が行われると、グループポリシーが適用される組織単位に含まれる SVM オブジェクトにこの値が適用されます。

関連情報

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します

CIFS サーバの Group Policy Object （ GPO ；グループポリシーオブジェクト）設定に関する情報を表示して、 CIFS サーバが属しているドメインで BranchCache GPO が定義されているかどうか、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も確認できます。

このタスクについて

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かぎりません。適用される GPO 設定は、 CIFS 対応の SVM に適用されているすべての定義済み GPO の一部です。GPO を介して適用された BranchCache 設定は、 CLI を介して適用された設定よりも優先さ

手順

1. 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` コマンドを実行します

   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. 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` コマンドを実行します`

> 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 サーバ上で GPO サポートを有効または無効にします

SMB 共有で BranchCache を無効にします

SMB 共有で BranchCache を無効にする手順の概要

特定の SMB 共有で BranchCache キャッシュサービスを提供する必要がなくなったが、あとでそれらの共有でキャッシュサービスが必要になる可能性がある場合は、共有ごとに BranchCache を無効にすることができます。すべての共有でキャッシュを提供するように BranchCache を設定しているが、一時的にすべてのキャッシュサービスを無効にする必要がある場合は、 BranchCache 設定を変更してすべての共有で自動キャッシュを停止することができます。

SMB 共有で有効になっていた BranchCache をあとから無効にすると、 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 が有効な SMB 共有の設定

単一の **SMB** 共有で **BranchCache** を無効にします

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** 共有での自動キャッシュを停止します

Storage Virtual Machine （ SVM ）のすべての SMB 共有に対して BranchCache キャッシュを自動的に有効にするように設定している場合、 BranchCache の設定を変更することで、すべての SMB 共有に対するコンテンツの自動キャッシュを停止することができます。

このタスクについて

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

次のコマンドは、 Storage Virtual Machine （ SVM 、旧 Vserver） vs1 の BranchCache 設定を変更して、すべての SMB 共有に対する自動キャッシュを停止します。

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

SVM で **BranchCache** を有効または無効にします

CIFS サーバで **BranchCache** を無効または再度有効にしたときの動作

BranchCache を設定したあとに、ブランチオフィスのクライアントがキャッシュされたコンテンツを使用できないようにするには、 CIFS サーバでキャッシュを無効にします。BranchCache を無効にするときは、それを実行した場合の動作について理解しておく必要があります

BranchCache を無効にすると、 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 を有効または無効にします

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`

状況	入力するコマンド
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 設定を削除します

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、既存のハッシュを削除します	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
BranchCache 設定を削除するが、既存のハッシュは保持する	`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
```

リバートした場合の **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ときは、それを実行した場合の動作について理解しておくことが重要です。

- 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手動で BranchCache の設定をリバートする必要があります。

  このコマンドは、 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 設定を削除します

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概要を改善します

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のどちらについても、 CIFS サーバと LUN の両方に対応しています。

ODX 以外のファイル転送では、ソースからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーションに転送します。つまり、クライアントコンピュータ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、データはソースからデスティネーションに直接コピーされます。

ODX オフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量（ CPU 、メモリ）の削減、ネットワーク I/O 帯域幅の使用量の削減などが挙げられます。

SMB 環境では、この機能は、クライアントとストレージサーバの両方で SMB 3.0 および ODX 機能がサポートされている場合にのみ使用できます。SAN 環境では、この機能は、クライアントとストレージサーバの両方で ODX 機能がサポートされている場合にのみ使用できます。ODX がサポートされていて有効になっているクライアントコンピュータでは、ファイルの移動やコピーを行う際に、オフロードファイル転送が自動的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 で SMB 自動ノードリファーラルを提供することで、クライアントの応答時間を改善します

"Microsoft Hyper-V および SQL Server 向けの SMB の設定"

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。

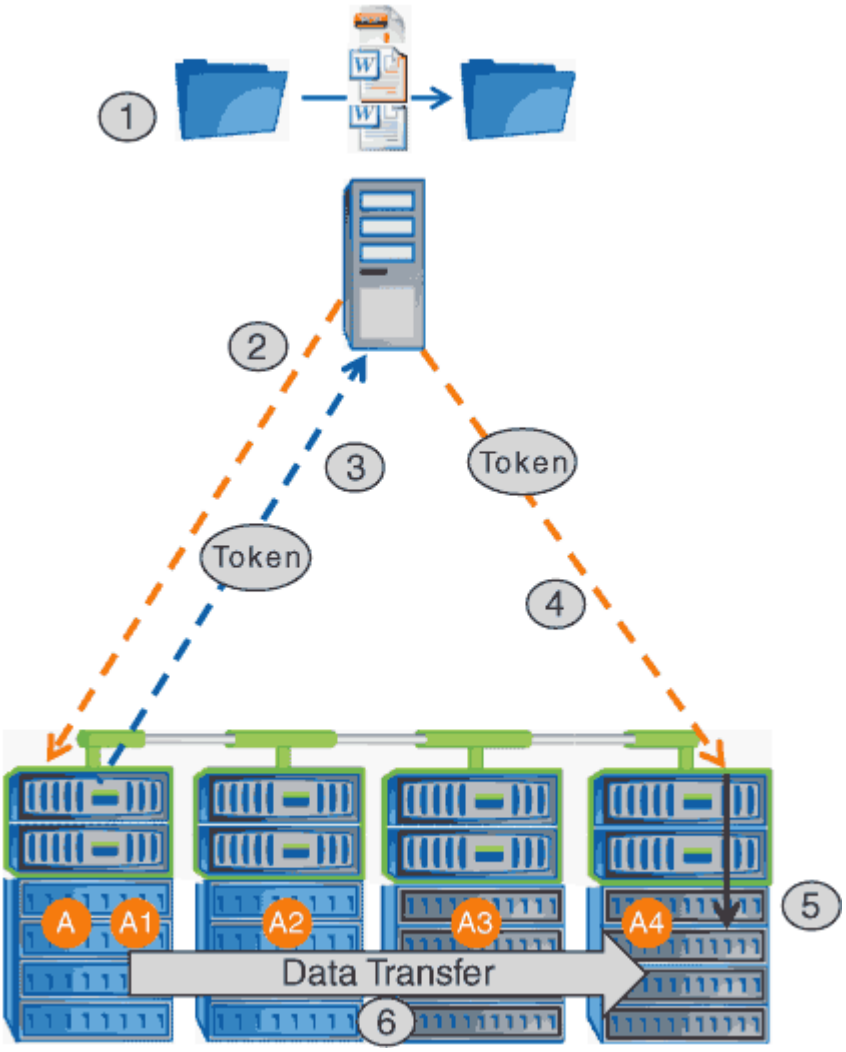
ODX クライアントは、 CIFS サーバが ODX 対応であると認識すると、ソースファイルを開いて CIFS サーバのトークンを要求します。デスティネーションファイルを開いたあと、クライアントはトークンを使用して、データをソースからデスティネーションに直接コピーするようにサーバに指示します。

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 を使用するための要件

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 の各リリースで 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 Interoperability Matrix を参照してください"サポートされているWindowsクライアントに関する最新情報が含まれています。

ボリューム要件：

- ソースボリュームは 1.25GB 以上でなければなりません。
- 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 を使用する場合は、一定のガイドラインについて理解しておく必要があります。たとえば、 ODX を使用できるボリュームのタイプや、クラスタ内およびクラスタ間の ODX に関する考慮事項を把握しておく必要があります。

ボリュームガイドライン

- 次のようなボリューム設定では、コピーオフロードに ODX を使用できません。
  - ソースボリュームサイズが 1.25GB 未満である必要があります

    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 デスティネーションボリューム、または SnapVault デスティネーションボリュームに存在するファイルやフォルダには ODX を使用できません。

  - ソースボリュームが重複排除されていない場合
- ODX コピーはクラスタ内のコピーにのみ対応しています。

  ODX を使用して、ファイルまたはフォルダを別のクラスタ内のボリュームにコピーすることはできません。

その他のガイドライン

- SMB 環境では、コピーオフロードに ODX を使用するには、 256KB 以上のファイルである必要があります。

  サイズの小さいファイルは、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環として重複排除が実行されます。

  データのコピーまたは移動時に SVM のボリュームで重複排除が発生しないようにする場合は、その SVM で ODX コピーオフロードを無効にする必要があります。

- データ転送を実行するアプリケーションは、 ODX をサポートするように記述する必要があります。

  ODX がサポートされるアプリケーション処理は次のとおりです。

  - Virtual Hard Disk （ VHD ；仮想ハードディスク）の作成および変換、 Snapshot コピーの管理、仮想マシン間でのファイルのコピーなど、 Hyper-V の管理処理
  - 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上でアプリケーションを実行する必要があります。

+
Windows サーバおよびクライアントでサポートされる 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際に、デフォルトでコピーオフロードが使用されます。Windows サーバ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任意の時点で失敗した場合は、コピーまたは移動処理が従来の読み取りと書き込みの処理を使用して実行されます。

ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。

- ボリューム内

  ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと SVM は同じです

  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 は同じです

  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、ノードは同じです

  ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

  ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- クラスタ間

  ソース LUN とデスティネーション LUN は、異なるクラスタの異なるノード上の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、いくつかの特殊なユースケースがあります。

- ONTAP の ODX の実装で ODX を使用すると、 SMB 共有と FC / iSCSI で接続された仮想ドライブとの間でファイルをコピーできます。

  SMB 共有と LUN が同じクラスタにある場合は、 Windows エクスプローラ、 Windows CLI または 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を使用して、 SMB 共有と接続された LUN 間の ODX コピーオフロードを使用してファイルをシームレスにコピーまたは移動できます。

- Hyper-V では、さらに次のようなユースケースでも ODX コピーオフロードが使用されます。

  - Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（ VHD ）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。

    これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

  - 容量固定 VHD を作成する際に、 ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
  - ソースとデスティネーションのストレージが同じクラスタにある場合に、 ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。

> Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、 ODX をサポートするストレージ（ SMB または SAN ）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、 ODX のパススルーはサポートされません。

ODXの有効化または無効化

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は ODX コピーオフロードのサポートも有効になります。

作業を開始する前に

SMB 3.0 が有効になっている必要があります。

このタスクについて

SMB 3.0 を無効にすると、 ONTAP でも SMB ODX が無効になります。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	`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 で SMB 自動ノードリファーラルを提供することで、クライアントの応答時間を短縮します

Auto Location の概要を示す SMB 自動ノードリファーラルを提供することで、クライアントの応答時間を改善します

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します。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改善できます。

SMB クライアントが SVM 上でホストされている SMB 共有に接続するときに、要求されたデータを所有していないノード上の LIF を使用して接続することがあります。クライアントが接続しているノードは、クラスタネットワークを使用して別のノードが所有しているデータにアクセスします。SMB 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

- 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 1 つあることを特定した場合です。

- 自動ノードリファーラルでは、 IPv4 と IPv6 の LIF の IP アドレスがサポートされます。
- リファーラルは、クライアントの接続に使用されてい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を参照する場合、共有内のデータは複数のノードに分散されます。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 では、これらのローカルでないボリュームに含まれるデータを取得する際にクラスタネットワークを使用する必要があります。 このタイプのネームスペースアーキテクチャでは、自動ノードリファーラルによる大幅なパフォーマンス向上は望めない場合があります。

データをホストするノードに使用可能な LIF がない場合、 ONTAP は、クライアントが選択した LIF を使用して接続を確立します。ファイルが SMB クライアントによって開かれると、クライアントは参照された同じ接続を介してファイルへのアクセスを継続します。

何らかの理由で CIFS サーバがリファーラルを作成できない場合でも、 SMB サービスが中断されることはありません。自動ノードリファーラルが有効でない場合と同様に SMB 接続が確立されます。

関連情報

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。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 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ます。 "ONTAP One"。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 ONTAP 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 で確認できます"

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 プロトコルのどちらかが有効になっていない場合は機能しないことがあります。

この要件が満たされない場合でも、データアクセスには影響しません。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 サーバを含むドメインと自動ノードリファーラルを使用するクライアントを含むドメインで、 NTLM 認証が許可されている必要があります。

リファー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には NTLM 認証が使用されるため、参照された接続に対しては Kerberos 認証は実行されません。

これは、WindowsクライアントがKerberosで使用されるサービスプリンシパル名（の形式）を作成できないためです `service/NetBIOS name` および `service/FQDN`）。これは、クライアントがサービスにKerberosチケットを要求できないことを意味します。

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を次に示します

ホームディレクトリ共有プロパティを有効にして共有を設定した場合、ホームディレクトリの設定で 1 つ以上のホームディレクトリ検索パスを設定できます。この検索パスで、 SVM のボリュームを含む各ノードに格納されているボリュームを指定できます。クライアントはリファーラルを受け取り、使用できるアクティブなローカルデータ LIF があれば、ホームユーザのホームディレクトリに対してローカルな、参照された LIF を介して接続します。

SMB 1.0 クライアントで自動ノードリファー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 サーバに対してユーザの名前が指定されていない段階で自動ノードリファーラルが必要になるからです。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が正常に機能するのは、次の条件に該当する場合です。

- 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は、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を次に示します

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しているため、オプションを無効にしたあとも、参照接続用にクライアントにキャッシュされている DFS リファー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、クライアントのキャッシュから DFS リファーラルがタイムアウトするまで、引き続きリファーラルを使用します。

オートロケーションは、 SMB 自動ノードリファーラルを使用してクライアントに SVM のデータボリュームを所有しているノード上の LIF を参照させることで、 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 接続が要求されたデータを含むノード上にある LIF を使用している場合、クライアントへの応答時間が短縮されます。

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されてい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を次に示します

Mac OS では Microsoft の Distributed File System （ DFS ；分散ファイルシステム）がサポートされていますが、 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。これにより、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 で動的ホームディレクトリを有効にする方法

"Network Management の略"

"NetApp Interoperability Matrix Tool で確認できます"

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を有効または無効にします

SMB 自動ノードリファーラルを有効にして、 SMB クライアントアクセスのパフォーマンスを向上させることができます。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。

作業を開始する前に

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。

このタスクについて

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	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

このオプション設定は、新しい SMB セッションで有効になります。既存の接続を使用しているクライアントは、その既存のキャッシュがタイムアウトになった場合にのみノードリファーラルを利用できます

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します

参照されるSMB接続の数を確認するには、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ます `statistics` コマンドを実行し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に対して接続が割り当てられている範囲を把握し、データ LIF を再配分して CIFS サーバの共有へのローカルアクセスを向上させるべきかどうかを判断することができます。

このタスクについて

。 `cifs` オブジェクトには、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、ローカルアクセスを使用するとパフォーマンスが最適化され

- `node_referral_not_possible`

  共有のルートとは別のノードでホストされる LIF を使用して接続したクライアントのうち、共有のルート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。これは、共有のルートのノードに対するアクティブなデータ LIF が見つからないためです。

- `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使用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により、 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、サンプルが固定された状態になります。データ収集を停止しないと、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。

> から収集した情報を評価および使用するため `statistics` コマンドを使用する場合は、環境内でのクライアントの分散状況について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. 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` コマンドを実行します

   次に、一定のサンプリング時間におけるデータを収集して表示することにより、自動ノードリファ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

いように、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だけを示しています。

3. admin 権限レベルに戻ります。 `set -privilege admin`

関連情報

統計情報を表示します

"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します

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を使用します `dfsutil.exe` ユーティリティ。

Windows 7以降のクライアントで使用できるRemote Server Administration Tools（RSAT）キットには、が含まれています `dfsutil.exe` ユーティリティ。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できるほか、クライアントで現在使用されている各リファーラルに関する情報を表示できます。また、このユーティリティを使用して、クライアントのリファー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を使用して共有のフォルダのセキュリティを確保します

アクセスベースの列挙の概要を使用して、共有のフォルダのセキュリティを提供します

Access-Based Enumeration が SMB 共有で有効になっていると、共有内のフォルダまたはファイルに（個人またはグループの権限制限により）アクセスする権限がないユーザの環境には、その共有リソースは表示されませんが、共有自体は表示されたままです。

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権限を持つユーザ（個人またはグループ）を指定できます。ただし、権限のないユーザに対して共有内のフォルダやファイルを表示可能とするかどうかを制御することはできません。この状態だと、共有内のこれらのフォルダ名またはファイル名に、顧客名や開発中の製品などの重要な情報が記述されている場合に問題になることがあります。

ABE では、共有プロパティが強化され、共有内のファイルやフォルダの列挙表示も対象になりました。このため、 ABE を使用して、ユーザのアクセス権に基づいて共有内のファイルとフォルダの表示をフィルタリングすることができます。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したり非表示にしたりすることができます。職場の機密情報を保護するだけでなく、 ABE を使用すると大きなディレクトリ構造の表示を簡略化できるため、あらゆる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があります。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することができます。

詳細はこちら "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を有効または無効にします

SMB 共有で Access-Based Enumeration を有効または無効にすると、ユーザがアクセス権のない共有リソースを表示することを許可または禁止できます。

このタスクについて

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 を有効にします	`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、のマニュアルページを参照してください `vserver cifs share create` コマンドを実行します
既存の共有で ABE を有効にします	`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 を無効にします	`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リストから削除されます。

2. を使用して、共有設定が正しいことを確認します `vserver cifs share show` コマンドを実行します

例

次の例は、「sales」という名前のABE SMB共有をパスに作成します `/sales` SVM vs1上。共有はを使用して作成されます `access-based-enumeration` 共有プロパティとして：

```
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、を追加します `access-based-enumeration` 「data2」という名前のSMB共有への共有プロパティ：

```
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します

SMB 共有での Access-Based Enumeration の有効化と無効化は Windows クライアントから実行できるため、この共有設定は CIFS サーバに接続することなく編集できます。

。 `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ました。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}`

   詳細については、を参照してください `abecmd` コマンドについては、Windowsクライアントのマニュアルを参照してください。

NFS と SMB のファイルとディレクトリの命名規則

NFS と **SMB** のファイルとディレクトリの命名規則について概要を示します

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のプロトコルによって、次の要素が決定します。

- ファイル名に使用できる文字
- ファイル名での大文字と小文字の区別

ONTAP では、 ONTAP のリリースに応じて、ファイル、ディレクトリ、 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。この違いがマルチプロトコル環境に及ぼす影響と、 SMB 共有の作成時にパスを指定するときや、共有内のデータにアクセスするときにどのような対処が必要になるかを理解しておく必要があります。

SMBクライアントがという名前のディレクトリを作成する場合 `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した場合`TESTDIR`を指定することはできません。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ます。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場合 `TESTDIR` では、NFSクライアントとSMBクライアントで表示されるディレクトリ名は次のように異なります。

- NFSクライアントでは、両方のディレクトリ名が作成したとおりに表示されます（例：） `testdir` および `TESTDIR`ディレクトリ名では大文字と小文字が区別されるためです。
- SMB クライアントでは、 2 つのディレクトリを区別するために 8.3 形式の名前が使用されます。1 つのディレクトリには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、が表示されます `testdir` および `TESTDI~1`。
  - ONTAP によってが作成されます `TESTDI~1` 2つのディレクトリを区別するディレクトリ名。

    この場合、 Storage Virtual Machine （ SVM ）での共有の作成時または変更時に共有パスを指定するときは、 8.3 形式の名前を使用する必要があります。

ファイルについても、SMBクライアントでが作成された場合と同様です `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した場合 `Test.txt`を指定することはできません。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ます。NFSユーザがあとでという名前のファイルを作成した場合 `Test.txt`では、NFSクライアントとSMBクライアントで表示されるファイル名は次のように異なります。

- NFSクライアントでは、両方のファイル名が作成されたとおりに表示され、 `test.txt` および `Test.txt` ファイル名では大文字と小文字が区別されるためです。
- SMB クライアントでは、 2 つのファイルを区別するために 8.3 形式の名前が使用されます。1 つのファイルにはベースファイル名が付けられます。追加のファイルには 8.3 形式のファイル名が割り当てられます。
  - SMBクライアントでは、が表示されます `test.txt` および `TEST~1.TXT`。
  - ONTAP によってが作成されます `TEST~1.TXT` 2つのファイルを区別するためのファイル名。

> SVM 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、大文字と小文字は区別されない Windows ルックアップは大文字と小文字が区別されます。

ONTAP による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とします `specifications.html`ONTAP で作成される8.3形式のファイル名はです `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名前の別のファイルを作成したとします `specifications_new.html`、8.3形式の `specifications_new.html` はです `specif~2.htm`。

マルチバイトを含むファイル名、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 エンコード形式の名前がサポートされるようになり、 Basic Multilingual Plane （ BMP ；基本多言語面）以外の Unicode 補助文字を含むファイル、ディレクトリ、ツリーの名前を作成および表示できるようになりました。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には、でnew_utf8mb4_言語コードを使用できます `vserver` および `volume` コマンド・ファミリー。

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。

- ボリュームを設定しています `-language` 明示的なオプション： `volume create -language utf8mb4 {…}`
- ボリュームを継承しています `-language` オプションを指定して作成または変更したSVMから、次のオプションを選択します。 `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。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。

  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、 `[-language <Language code>]` ボリュームの言語を*。utf-8からutf8mb4に変更するためのパラメータ。ボリュームの言語を変更するには、 "ネットアップサポート"。

> 現在のところ、 4 バイトの UTF-8 文字を含む LUN 名はサポートされていません。

- 一般に、 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 ）、 NFS ファイルシステムでは 8-bit Unicode Transformation Format （ UTF-8 ）を使用して表現されます。

  ONTAP 9.5 よりも前のリリースでは、 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 UTF-16 に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作成したファイル名に有効な追加文字が含まれている場合や無効な追加文字が含まれている場合、 ONTAP はそれらのファイル名を拒否し、ファイル名が無効であることを示すエラーを返します。

  この問題を回避するには、ファイル名に BMP 文字のみを使用して補助文字は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。

- どちらかを使用できます `volume qtree` 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を使用します。
- 日本語や中国語などの Unicode 形式のマルチバイト文字を qtree 名に含めることができます。
- ONTAP 9.5 よりも前のリリースでは、 BMP 文字（つまり 3 バイトで表現可能な文字）のみがサポートされます。

> ONTAP 9.5 よりも前のリリースでは、 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 名や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、 qtree が utf8mb4 に対応したボリュームに含まれていれば、 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を設定します

NFS クライアントは、 SMB クライアントと特定の Windows アプリケーションでは無効な文字を含むファイル名を作成できます。ボリュームにおけるファイル名の変換のための文字マッピングを設定できます。これにより、そのままでは無効な NFS 名を持つファイルに SMB クライアントからアクセスできます。

このタスクについて

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 はファイル名を調べます。ファイル名が有効な SMB ファイル名でない場合は（たとえば、コロン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、長いファイル名に重要な情報を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を使用するクライアント間でファイルを共有する場合は、両方のオペレーティングシステムで有効な文字をファイル名に使用する必要があります。

ただし、 SMB クライアントで有効でない文字を含む NFS クライアントが作成したファイル名がある場合は、無効な NFS の文字を、 SMB と特定の Windows アプリケーションの両方で有効な Unicode 文字に変換するマッピングを定義できます。たとえば、この機能は CATIAR MCAD および Mathematica アプリケーションをサポートしていますが、同じ要件を持つほかのアプリケーションでも使用できます。

文字マッピングはボリューム単位で設定できます。

ボリュームで文字マッピングを設定する場合は、次の点に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をまたいで適用されません。

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。

- 無効な文字を表す Unicode 文字が、通常はファイル名に使用されないようにする必要があります。これらの文字が使用されていた場合、不要なマッピングが発生します。

  たとえば ' コロン (:) をハイフン (-) にマッ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てもまだマッピングに無効な Windows 文字が含まれている場合、 ONTAP は Windows 8.3 ファイル名にフォールバックします。
- FPolicy 通知、 NAS 監査ログ、セキュリティトレースメッセージでは、マッピングされたファイル名が表示されます。
- タイプが DP である SnapMirror 関係が作成されても、ソースボリュームの文字マッピングはデスティネーション DP ボリュームにレプリケートされません。
- 大文字と小文字の区別：マッピングされた Windows 名は NFS 名に変換されるため、名前の検索は NFS のセマンティクスに従います。NFS ルックアップでは大文字と小文字が区別されるという事実も含まれます。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ません。ただし、 8.3 形式の名前は大文字と小文字が区別されません。
- 部分マッピングまたは無効なマッピング：ディレクトリ列挙（「 dir 」）を実行しているクライアントに返すように名前をマッピングしたあと、結果の Unicode 名について Windows の有効性がチェックされます。その名前にまだ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（「 . 」または空白で終わる場合など）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 進数値で入力された Unicode 文字です。例： 3C ： E03C[+]

それぞれの最初の値 `mapping_text` コロンで区切られたペアは、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。マッピングのペアは一意である必要があります（ 1 対 1 のマッピングが存在する必要があります）。

- ソースマッピング +

次の表に、ソースマッピングで許可されている Unicode 文字セットを示します。

[+]

Unicode 文字	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

Unicode 文字	印刷された文字	説明
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	>	が次の値より大きい
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 ネームスペース内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を管理するコマンド

FlexVol での SMB ファイル名の変換に使用する情報を作成、変更、表示したり、ファイル文字マッピングを削除したりすることで、文字マッピングを管理できます。

状況	使用するコマンド
新しいファイル文字マッピングを作成します	`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します	`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を設定する

NASデータへのS3クライアントアクセスを提供

S3マルチプロトコルの概要

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プロトコルおよびSMBプロトコルを使用するクライアントに提供されているデータに再フォーマットせずにアクセスできるようにすることができます。この機能により、NASデータは引き続きNASクライアントに提供され、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が提供されます。

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

   既存のデータが従来のNASクライアント（NFSまたはSMB）を使用して作成され、NASボリューム（FlexVol またはFlexGroup ボリューム）にある場合、S3クライアント上の分析ツールを使用してこのデータにアクセスできるようになりました。

2. NASとS3の両方のプロトコルを使用したI/O処理に対応できる、最新のクライアント用のバックエンドストレージです

   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仕組み

ONTAP マルチプロトコルを使用すると、同じデータセットをファイル階層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の作成、読み取り、削除、および列挙をS3クライアントに許可する「S3 NASバケット」を作成します。このマッピングは、NASセキュリティ設定に準拠しており、ファイルおよび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、マップされたディレクトリから下の位置に相対的な名前を持つS3オブジェクトとして表され、ディレクトリ境界はスラッシュ文字（/）で表されます。

ONTAPで定義された通常のS3ユーザは、このストレージにアクセスできます。このストレージは、NASディレクトリにマッピングされるバケットに定義されたバケットポリシーで管理されます。これを可能にするには、S3ユーザとSMB / NFSユーザ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クライアントが作成すると、ファイルはすぐにディレクトリに配置され、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クライアントはセマンティクスが異なることを要求します。セマンティクスでは、新しいオブジェクトはすべてのデータが書き込まれるまで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は外部には表示されません。

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、S3監査を設定してアクセスを監査することはできません。の詳細を確認してください "S3監査"。

ただし、S3 NASバケットにマッピングされているNASファイルとディレクトリは、従来のONTAP 監査手順を使用してアクセスイベントを監査できます。したがって、S3処理ではNAS監査イベントがトリガーされますが、次の例外があります。

- S3ポリシーの設定（グループまたはバケットポリシー）によってS3クライアントアクセスが拒否された場合、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個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の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 "SVMでNASイベントを監査する"。

S3および**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点を除いて、NASとS3の標準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 NASバケットでは現在、**S3**機能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、現在のリリースのオブジェクトデータと一緒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（つまり、「tagging」クエリー文字列を持つPUT、GET、Deleteの各要求）でタグを更新する要求は、エラーで拒否されます。

バージョン管理

バージョン管理をバケットのマッピング設定で指定することはできません。

- バージョンがnullでない仕様（versionId=xyzクエリ文字列）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に影響する要求は拒否され、エラーが発生します。

マルチパート処理

次の操作はサポートされません。

- AbortMultipartUpload の略
- CompleteMultipartUpload
- CreateMultipartUpload を実行します
- ListMultipartUpload の略

NASデータの**S3**クライアントアクセス要件

NASファイルとディレクトリをS3アクセス用にマッピングする場合は、互換性が確保されていない問題がいくつかあることに注意してください。NASファイル階層は、S3 NASバケットを使用して階層を提供する前に調整しなければならない場合があります。

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みなされます。オブジェクト名は、S3バケットの設定で指定されたディレクトリに相対的な、ファイルのスラッシュで区切られたパス名です。

このマッピングは、S3 NASバケットを使用してファイルとディレクトリにサービスを提供する際にいくつかの要件を適用します。

- S3の名前は1024バイトに制限されているため、長いパス名を持つファイルに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、オブジェクト名には、連続する255文字以外の文字（「/」）を使用できません
- バックスラッシュ（「\」）で区切られたSMBパス名は、s3にはスラッシュ（「/」）ではなく、オブジェクト名として表示されます。
- 有効なS3オブジェクト名のペアの一部は、マッピングされたNASディレクトリツリーに共存できません。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。「part1/part2」は、最初の名前に含まれるファイルで、もう一方の名前に含まれるディレクトリです。
  - 「part1/part2」が既存のファイルの場合、「part1/part2/part3」のS3作成は失敗します。
  - "part1/part2/part3"が既存のファイルの場合、"part1/part2"のS3作成または削除が失敗します。
  - 既存のオブジェクトの名前と一致するS3オブジェクトの作成によって、（バージョン管理されていないバケット内の）既存のオブジェクトが置き換えられます。これはNASを保持するが、完全に一致する必要があります。上記の例では、名前が競合している間は原因 によって既存のオブジェクトが削除されないため、これらのオブジェクトは削除されません。

オブジェクトストアは非常に多く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、非常に多数の名前が1つのディレクトリに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、名前にスラッシュ（/）文字が含まれていない場合、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される方が適切です。

NASデータへのS3プロトコルアクセスを有効にします

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を満たしていることを確認する（オブジェクトストアサーバの追加、ネットワークと認証の要件の確認を含む）ことが必要です。

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、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構成"
- "SMBの設定"

作業を開始する前に

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。
- SVMが目的のNASプロトコル用に設定されている。
- NFSサーバと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こと。
- NASデータをクライアントシステムにエクスポートまたは共有しています。

このタスクについて

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つのソースのCA証明書を使用できます。

- 新しいONTAP 自己署名証明書をSVMに作成します。
- 既存のONTAP 自己署名証明書がSVMに存在している。
- サードパーティの証明書。

NASデータの提供に使用するS3 / NASバケットにも同じデータLIFを使用できます。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 を作成します。"。S3データトラフィックをLIFで有効にするには、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を変更して、S3を含めることができます。

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完全修飾ドメイン名（FQDN）としてS3サーバ名を入力できるように準備しておく必要があります。S3サーバのFQDNの先頭をバケット名にすることはできません。

System Manager の略

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と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。
   c. ネットワークインターフェイスを入力してください。
2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書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。
   - シークレットキーは今後表示されません。
   - 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 の使用

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 にインストールします"。
3. サービスデータポリシーを更新します
   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、を追加し `data-core` `data-s3-server` `services` 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]`

S3 サーバの作成時またはあとからいつでも追加のオプションを指定できます。

- HTTPS は、ポート 443 で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 はデフォルトではディセーブルです。イネーブルにすると、サーバはポート 80 をリッスンします。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 が有効な場合は、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が必要に応じて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バケットを作成する

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ネームスペースのすべての部分にS3アクセスを提供できます。

作業を開始する前に

- 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ます "S3クライアントアクセスの要件"。

このタスクについて

S3 NASバケットは、SVMのルートディレクトリ内のすべてのファイルとディレクトリのセットを指定するように設定できます。

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処理を実行する権限を制限するグループが別々に必要になることがあります。

S3 NAS「バケット」はマッピングであり、S3バケットではないため、標準S3バケットの次のプロパティは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Snapshotテクノロジが用意されています。ただし、バージョン管理は現在S3 NASバケットでは使用できません。
- * logical-used\ object-count *+
  NASボリュームについては、volumeコマンドを使用して同等の統計情報を使用できます。

System Manager の略

NAS対応Storage VMに新しいS3 NASバケットを追加

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設定に関連しないオプションは非表示になります。
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 の使用

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します

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、バケットサービスポリシーを使用してNASデータへのアクセス権を付与する必要があります。

作業を開始する前に

クライアントアクセス用のユーザ名（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。

このタスクについて

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ファイルに対する許可チェックがS3クライアントからアクセスされたときに実施されます。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、を使用して変更できます `vserver object-store-server modify` コマンドを実行します

ローカルのネームマッピング構成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すると、ユーザにアクセスを許可するリソース（ディレクトリとファイル）と、ユーザがアクセスを許可された操作、または許可されなかった操作を指定する権限を付与できます。

System Manager の略

1. UNIXまたはWindowsクライアント（あるいはその両方）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 の使用

1. UNIXまたはWindowsクライアント（あるいはその両方）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` -マッピング評価の優先順位番号。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}` -ユーザがアクション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。
- `-principal <Objectstore Principal>, …` -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す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は、グループ名にプレフィックスグループ/を追加することによって指定します。
  - `-principal -`（ハイフン文字）は、すべてのユーザにアクセスを許可します。
- `-resource <text>, …` -許可または拒否の権限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ステートメントのオプションのテキストコメントを指定します。

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 および SQL Server 向けの SMB の設定

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。

SMB のノンストップオペレーションを実装する場合は、次の手順を使用する必要があります。

- 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 仮想マシンファイル
  - 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に関する追加情報については、次のテクニカルレポート（TR）を参照してください。

"ネットアップ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** ソリューション用に **ONTAP** を設定する

継続的な可用性が確保された SMB 3.0 以降の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 SQL Server システムデータベースとユーザデータベースを SVM 内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間のノンストップオペレーション（ NDO ）を実現できます。

SMB を介した **Microsoft Hyper-V**

Hyper-V over SMB 解決策を作成するには、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継続的な可用性が確保された SMB 3.0 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 サーバの構成については、スタンドアロンの構成とクラスタ化された構成の両方がサポートされます。

- Microsoft クラスタおよび Hyper-V サーバの作成については、 Microsoft の Web サイトを参照してください。
- SnapManager for Hyper-V は、 Snapshot コピーベースの高速バックアップサービスを容易に実現できるホストベースのアプリケーションで、 Hyper-V over SMB 構成と統合できるように設計されています。

  Hyper-V over SMB 構成での SnapManager の使用については、 SnapManager for Hyper-V 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 解決策を作成するには、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。さらに、 Microsoft クラスタも設定する必要があります（クラスタ構成を使用する場合）。その後、 Windows サーバに SQL Server をインストールして設定し、 CIFS サーバにホストされている共有への継続的可用性を備えた SMB 3.0 接続を作成します。SVM ボリュームに格納されているデータベースファイルを保護するオプションで、バックアップサービスを設定することもできます。

> SQL Server は、 Windows Server 2012 以降にインストールし、設定する必要があります。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できるホストベースのアプリケーションで、SQL Server over SMB構成と統合できるように設計されています。

SnapCenter Plug-in for Microsoft SQL Serverの使用方法については、を参照してください "SnapCenter Plug-in for Microsoft SQL Server" 文書化

Hyper-V および SQL Server over SMB でのノンストップオペレーション

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、さまざまな管理作業の間も、アプリケーションサーバおよびそれに格納された仮想マシンやデータベースをオンラインのまま維持して、継続的な可用性を実現できる機能の組み合わせのことです。これには、ストレージインフラの計画的停止と計画外停止の両方が含まれます。

SMB を介したアプリケーションサーバのノンストップオペレーションでは、次のような操作がサポートされます。

- 計画的なテイクオーバーとギブバック
- 計画外のテイクオーバー
- アップグレード
- 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 を介したノンストップオペレーションを可能にするプロトコル

SMB 3.0 のリリースに伴い、 Microsoft から、 Hyper-V および SQL Server over SMB のノンストップオペレーションのサポートに必要な機能を備えた新しいプロトコルがリリースされました。

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 および SQL Server over SMB のノンストップオペレーションの主要な概念

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。これにはが含まれます `continuously-available` 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。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 ）のデータ LIF のいずれかを使用して、同じ LIF または別の LIF を介して再接続できます。

アグリゲートの再配置、テイクオーバー、およびギブバックはすべて、 SFO ペア間で行われます。永続的ハンドルを持つファイルを使用したセッションの切断と再接続をシームレスに管理するために、パートナーノードでは、すべての永続的ハンドルのロック情報のコピーが保持されます。イベントが計画的か計画外かに関係なく、 SFO パートナーは、永続的ハンドルの再接続を無停止で管理できます。この新機能を使用すると、従来では業務が停止する状況となるイベントでも、 CIFS サーバへの SMB 3.0 接続を、 SVM に割り当てられた別のデータ LIF に透過的に無停止でフェイルオーバーできます。

永続的ハンドルを使用すると、 CIFS サーバで SMB 3.0 接続を透過的にフェイルオーバーできるようになりますが、障害が発生したために Hyper-V アプリケーションが Windows Server クラスタ内の別のノードにフェイルオーバーされる場合、クライアントは切断されたハンドルのファイルハンドルを再要求できません。このシナリオでは、切断された状態のファイルハンドルによって、別のノードで再起動した Hyper-V アプリケーションのアクセスがブロックされる可能性があります。「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のノードの SFO パートナーに、少なくとも 1 つ以上、アプリケーションサーバのデータをホスティングする Storage Virtual Machine （ SVM ）に割り当てられた運用中のデータ LIF がある。

> 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。

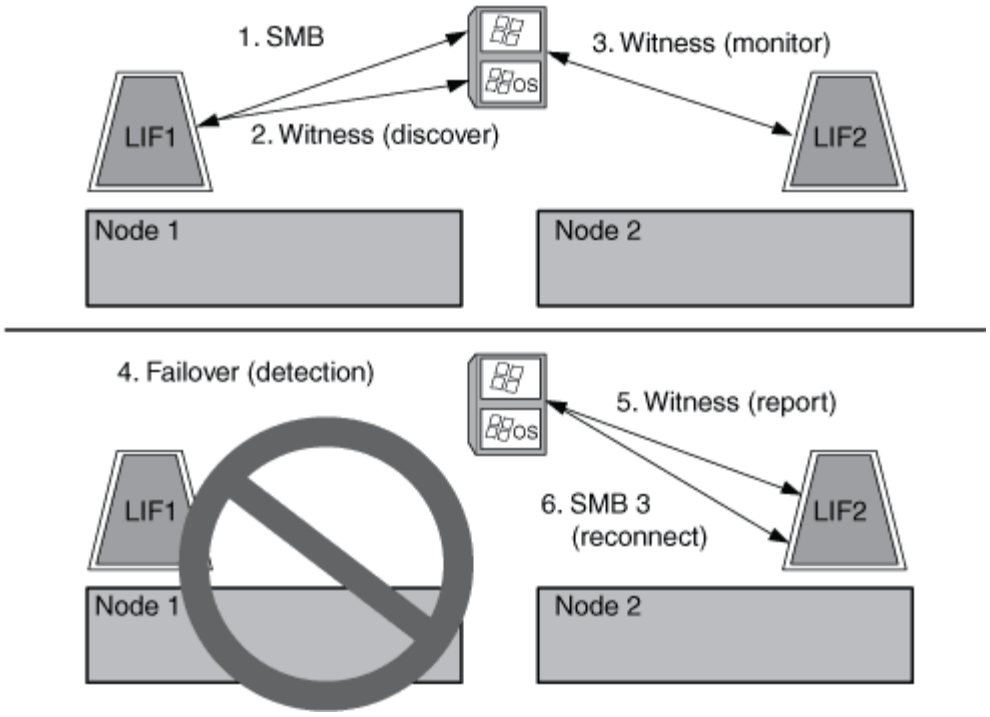
- アプリケーションサーバは、個々の LIF IP アドレスではなく、 DNS に格納されている CIFS サーバ名を使用して CIFS サーバに接続する必要があります。

監視プロトコルの仕組み

ONTAP では、ノードの SFO パートナーを監視役として使用して、監視プロトコルが実装されます。障害が発生すると、パートナーが障害を迅速に検出し、 SMB クライアントに通知します。

監視プロトコルでは、次のプロセスを使用してフェイルオーバーが強化されます。

1. アプリケーションサーバがノード 1 への継続的な可用性が確保された SMB 接続を確立すると、 CIFS サーバからアプリケーションサーバに監視が利用可能であることが通知されます。
2. アプリケーションサーバは、ノード 1 に監視サーバの IP アドレスを要求し、 Storage Virtual Machine （ SVM ）に割り当てられたノード 2 （ SFO パートナー）のデータ LIF の IP アドレスリストを受け取ります。
3. アプリケーションサーバは、いずれかの IP アドレスを選択し、ノード 2 への監視接続を作成して、ノード 1 の継続的な可用性が確保された接続を移行する必要がある場合に通知されるように登録します。
4. ノード 1 でフェイルオーバーが発生した場合、監視によってフェイルオーバーが容易になりますが、ギブバックには影響しません。
5. 監視によってフェイルオーバーイベントが検出され、監視接続を介してアプリケーションサーバに、 SMB 接続をノード 2 に移行する必要があることが通知されます。
6. アプリケーションサーバは、 SMB セッションをノード 2 に移行し、クライアントアクセスを中断することなく接続をリカバリします。



リモート **VSS** による共有ベースのバックアップ

リモート **VSS** による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 サーバに格納された Hyper-V 仮想マシンファイルの共有ベースのバックアップを実行できます。

Microsoft 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にも対応するように VSS インフラが拡張され、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）の概念について説明します。リモート VSS が Hyper-V over SMB 構成でバックアップサービスによってどのように使用されるかを理解するには、これらの概念を理解しておく必要があります。

- * VSS （ボリューム・シャドウ・コピー・サービス） *

  特定の時点で特定のボリュームのバックアップコピーまたはデータの Snapshot を作成するために使用される 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、およびストレージ管理ソフトウェアを調整して、整合性のあるバックアップの作成と管理をサポートします。

- * リモート VSS （リモートボリュームシャドウコピーサービス） *

  SMB 3.0 共有を介してデータにアクセスした特定の時点における整合性が取れた共有ベースのバックアップコピーを作成する Microsoft のテクノロジです。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。シャドウコピーを使用すると、システムやアプリケーションによる元のボリュームのデータ更新を継続したまま、整合性が取れたポイントインタイムバックアップを作成できます。

- * シャドウ・コピー・セット *

  1 つ以上のシャドウコピーの集合です。各シャドウコピーが 1 つの共有に対応します。シャドウコピーセット内のシャドウコピーに対応する共有は、すべて同じ処理でバックアップする必要があります。セットに含めるシャドウコピーは、 VSS に対応したアプリケーションの VSS クライアントで識別されます。

- * シャドウ・コピー・セットの自動リカバリ *

  リモート VSS に対応したバックアップアプリケーションのバックアッププロセスの一環として実行される、シャドウコピーを格納するレプリカディレクトリの整合性が取れたポイントインタイムコピーを作成する処理です。バックアップの開始時に、アプリケーションの VSS クライアントで、バックアップ対象としてスケジュールされたデータ（ Hyper-V の場合は仮想マシンファイル）にソフトウェアチェックポイントを設定する処理が開始されます。これにより、 VSS クライアントでアプリケーションの続行が許可されます。シャドウコピーセットが作成されると、リモート VSS によってシャドウコピーセットが書き込み可能にされ、書き込み可能なコピーがアプリケーションに公開されます。アプリケーションでは、シャドウコピーセットをバックアップする準備として、前の処理で作成されたソフトウェアチェックポイントを使用して自動リカバリを実行します。自動リカバリでは、チェックポイントの作成後にファイルやディレクトリに対して行われた変更を元に戻すことで、シャドウコピーを整合性のある状態にします。自動リカバリは、 VSS に対応したバックアップのオプションの手順です。

- * シャドウ・コピー ID *

  シャドウコピーを一意に識別する GUID です。

- * シャドウ・コピー・セット ID *

  同じサーバに対する一連のシャドウコピー ID を一意に識別する GUID です。

- * SnapManager for Hyper-V *

  Microsoft Windows Server 2012 Hyper-V のバックアップとリストアの処理を自動化して簡単に実行できるようにするソフトウェアですSnapManager for Hyper-V では、リモート VSS と自動リカバリを使用して、 SMB 共有を介して Hyper-V ファイルをバックアップします。

関連情報

Hyper-V および SQL Server over SMB のノンストップオペレーションの主要な概念

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しく作成できるように、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。

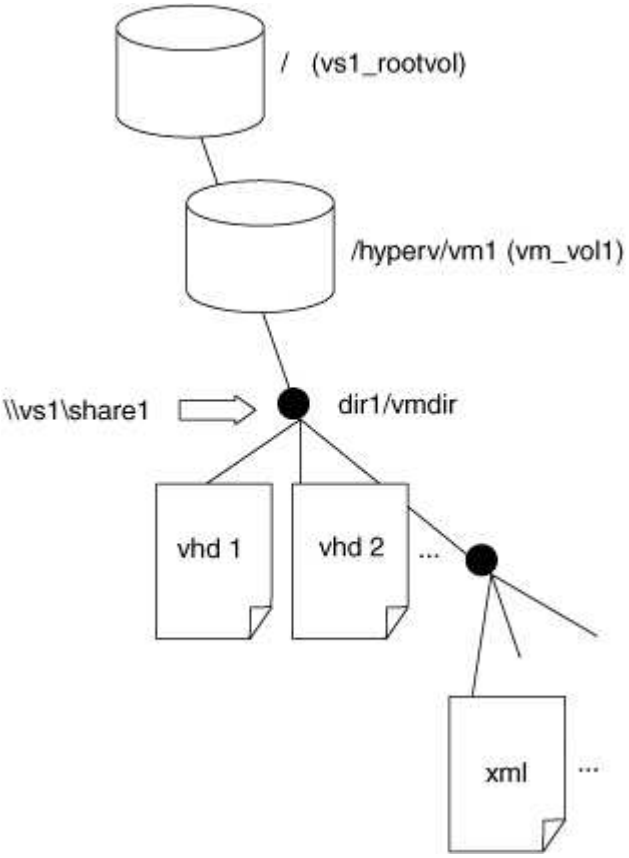
シャドウコピーを正常に作成するためにサポートされるディレクトリ構造は、次の要件を満たしています。

- 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、通常以外のファイルは含まれません。

- 仮想マシンのファイルはすべて単一の共有内に存在します。
- 仮想マシンファイルの格納に使用されるディレクトリ構造は、設定されたシャドウコピーディレクトリの階層より深くなりません。
- 共有のルートディレクトリには、仮想マシンファイルまたはディレクトリのみが含まれます。

次の図では、ジャンクションポイントがであるvm_vol1という名前のボリュームが作成されています `/hyperv/vm1` Storage Virtual Machine（SVM）vs1上。ジャンクションポイントの下には、仮想マシンファイルを格納するサブディレクトリが作成されます。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内（設定されたシャドウコピーのディレクトリ階層まで）に格納されたすべての仮想マシンファイルのシャドウコピーが作成されます。



SnapManager for Hyper-V による **Hyper-V over SMB** のリモート **VSS** ベースのバックアップの管理方法

SnapManager for Hyper-V を使用して、リモート VSS ベースのバックアップサービスを管理できます。スペース効率に優れたバックアップセットを作成するには、SnapManager for Hyper-V で管理されているバックアップサービスを使用すると効果的です。

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 環境経由のコピー処理を実行する際のパフォーマンスが向上します。

ODX 以外のファイル転送では、ソース CIFS サーバからデータが読み取られ、ネットワーク経由でクライアントコンピュータに転送されます。クライアントコンピュータは、データをネットワーク経由でデスティネーション CIFS サーバに転送します。つまり、クライアントコンピュータ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、データはソースからデスティネーションに直接コピーされます。

ODX オフロードコピーはソースストレージとデスティネーションストレージの間で直接実行されるため、パフォーマンスが大幅に向上します。実現するパフォーマンスの向上には、ソースとデスティネーションの間のコピー時間の短縮、クライアントでのリソース使用量（ CPU 、メモリ）の削減、ネットワーク I/O 帯域幅の使用量の削減などが挙げられます。

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
ODX コピーおよび移動の使用は、以下のユースケースでサポートされます。
```

- ボリューム内

  ソースとデスティネーションのファイルまたは LUN は、同じボリューム内にあります。

- ボリュームが異なり、ノードと 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 は同じです

  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、ノードは同じです

  ソースとデスティネーションのファイルまたは LUN は、同じノード上の異なるボリュームにあります。データは異なる SVM に所有されます。

- SVM とノードが異なります

  ソースとデスティネーションのファイルまたは LUN は、異なるノード上の異なるボリュームにありま

す。データは異なる SVM に所有されます。

Hyper-V ソリューションでの ODX コピーオフロードの具体的な用途には、次のようなものがあります。

- Hyper-V で ODX コピーオフロードのパススルーを使用して、仮想ハードディスク（ VHD ）ファイル内および VHD ファイル間でのデータのコピー、または同じクラスタ内のマッピングされた SMB 共有と接続された iSCSI LUN の間でのデータのコピーを実行できます。

  これにより、ゲストオペレーティングシステムからのコピーを基盤となるストレージに渡すことができます。

- 容量固定 VHD を作成する際に、 ODX を使用して、既知の初期化済みトークンによってディスクを初期化します。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、 ODX コピーオフロードを使用して、仮想マシンのストレージを移行します。

> Hyper-V での ODX コピーオフロードのパススルーの用途を活用するには、ゲストオペレーティングシステムで ODX がサポートされている必要があります。また、ゲストオペレーティングシステムのディスクが、 ODX をサポートするストレージ（ SMB または SAN ）から作成された SCSI ディスクである必要があります。ゲストオペレーティングシステムのディスクが IDE ディスクの場合、 ODX のパススルーはサポートされません。

SQL Server ソリューションでの ODX コピーオフロードの具体的な用途には、次のようなものがあります。

- ODX コピーオフロードを使用して、マッピングされた SMB 共有間、または同じクラスタ内の SMB 共有と接続された iSCSI LUN の間で SQL Server データベースのエクスポートとインポートを行うことができます。
- ソースとデスティネーションのストレージが同じクラスタにある場合に、 ODX コピーオフロードを使用して、データベースのエクスポートとインポートを行います。

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 で確認できます"

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のライセンスは、 "ONTAP One"。ONTAP Oneをお持ちでない場合は、 "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"、および必要に応じて、 "インストールする"。

ネットワークとデータ **LIF** の要件

ノンストップオペレーション用に SQL Server または Hyper-V over SMB 構成を作成する場合、一定のネットワークとデータ LIF 要件について理解しておく必要があります。

ネットワークプロトコルの要件

- IPv4 および IPv6 のネットワークがサポートされています。
- SMB 3.0 以降が必要です。

  SMB 3.0 には、ノンストップオペレーションを実現するために必要となる継続的可用性を備えた SMB 接続の確立に欠かせない機能が備わっています。

- DNS サーバには、 CIFS サーバ名を Storage Virtual Machine （ SVM ）上のデータ LIF に割り当てられた IP アドレスにマッピングするエントリが格納されている必要があります。

  通常、 Hyper-V または SQL Server アプリケーションサーバは、仮想マシンまたはデータベースファイルへのアクセス時に複数のデータ LIF を介して複数の接続を確立します。正常に機能するには、アプリケーションサーバは、複数の一意の IP アドレスへの複数の接続を確立するのではなく、 CIFS サーバ名を使用してこのような複数の SMB 接続を確立する必要があります。

  監視でも、個々の LIF の 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 構成と 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 を複数導入しておく必要があります。

データ **LIF** の要件

- SMB 解決策経由のアプリケーションサーバをホストする 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、クラスタ内のどのノードも監視ノードになる可能性があります。

- データ LIF は、自動リバートするように設定されていない必要があります。

  テイクオーバーまたはギブバックの発生後は、データ LIF をホームポートに手動でリバートする必要があります。

- データ LIF のすべての IP アドレスが DNS 内にエントリを保持する必要があり、すべてのエントリが CIFS サーバ名に解決される必要があります。

  アプリケーションサーバは、 CIFS サーバ名を使用して SMB 共有に接続する必要があります。LIF IP アドレスを使用して接続を確立するようにアプリケーションサーバを設定しないでください。

- CIFS サーバ名が SVM 名と異なる場合は、 DNS エントリが CIFS サーバ名に解決される必要があります。

Hyper-V over SMB 用の **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では、 SMB 接続を確立する際にマシンアカウントが使用されます。すべての SMB アクセスで、 Windows ユーザが任意の UNIX ユーザアカウントまたはデフォルトの UNIX ユーザアカウントに正常にマッピングされる必要があるため、 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ります）。

  Hyper-V マシンファイル以外のデータにアクセスするために自動ノードリファーラルを使用する場合は、そのデータ用に別の SVM を作成する必要があります。

- 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 ではリモート VSS に対して Kerberos サービスがアドバタイズされないため、ドメインが NTLM を許可するように設定されている必要があります。

- シャドウコピー機能を有効にする必要があります。

  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。

ボリューム要件：

- 仮想マシンファイルを格納するためのボリュームは、 NTFS セキュリティ形式のボリュームとして作成されている必要があります。

  継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバの NDO を実現するには、共有を含むボリュームが NTFS ボリュームである必要があります。さらに、そのボリュームが常に 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 共有を介して直接 NDO に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 共有を介して NDO に使用する場合は、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- 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ている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

関連情報

"Microsoft TechNet ライブラリ： technet.microsoft.com/en-us/library/"

SQL Server 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 SQL Server over SMB 構成を作成する場合、 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では、 SMB 接続を確立する際にマシンアカウントが使用されます。すべての SMB アクセスで、 Windows ユーザが任意の UNIX ユーザアカウントまたはデフォルトの UNIX ユーザアカウントに正常にマッピングされる必要があるため、 ONTAP は、アプリケーションサーバのマシンアカウントをデフォルトの UNIX ユーザアカウントにマッピングできる必要があります。

さらに、 SQL Server はドメインユーザを SQL Server サービスアカウントとして使用します。サービスアカウントは、デフォルトの 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ります）。

  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、そのデータ用の SVM を個別に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 BUILTIN\Administrators グループに割り当てられます。

ボリューム要件：

- 仮想マシンファイルを格納するためのボリュームは、 NTFS セキュリティ形式のボリュームとして作成されている必要があります。

  継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバの NDO を実現するには、共有を含むボリュームが NTFS ボリュームである必要があります。さらに、そのボリュームが常に 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 共有を介して直接 NDO に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 共有を介して NDO に使用する場合は、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- データベースファイルが格納されたボリュームにジャンクションを含めることはできますが、 SQL Server はデータベースディレクトリ構造の作成時にジャンクションを横断しません。
- SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理が成功するためには、ボリュームに十分な利用可能スペースが必要です。

  SQL Server データベースファイルを格納するボリュームには、共有内にあるデータベースディレクトリ構造と、格納されているすべてのファイルを格納できる十分な容量が必要です。

関連情報

"Microsoft TechNet ライブラリ： technet.microsoft.com/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注意する必要があります。

共有の要件

- アプリケーションサーバが使用する共有には、継続的可用性が設定されている必要があります。

  継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的

ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとに SMB 共有に無停止で再接続し、ファイルロックを再取得することができます。

- リモート VSS に対応したバックアップサービスを使用する場合は、ジャンクションを含む共有に Hyper-V ファイルを配置することはできません。

  自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、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。

- リモート VSS に対応したバックアップサービスと自動リカバリを使用する場合は、以下を含む共有に Hyper-V ファイルを配置することはできません。
  - シンボリックリンク、ハードリンク、またはワイドリンク
  - 通常以外のファイル

    シャドウコピーを実行する共有にリンクまたは通常以外のファイルが含まれている場合は、シャドウコピーの作成に失敗します。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

  - 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ている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。この要件は、自動リカバリを使用する環境シャドウコピーのみです。

- アプリケーションサーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 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 の構成では、次の機能はサポートされません。
  - 監査
  - FPolicy の
- を使用したSMB共有ではウィルススキャンは実行されません `continuously-availability` パラメータをに設定します `Yes`。

SQL Server over SMB での継続的可用性を備えた共有の要件と考慮事項

ノンストップオペレーションをサポートする SQL Server over SMB 構成で継続的可用性を備えた共有を設定する場合は、一定の要件と考慮事項に注意する必要があります。

共有の要件

- 仮想マシンファイルを格納するためのボリュームは、 NTFS セキュリティ形式のボリュームとして作成されている必要があります。

  継続的な可用性が確保された SMB 接続を使用してアプリケーションサーバの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、そのボリュームが常に 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、ボリュームの一番上に ACL を手動で配置し、格納されているすべてのファイルおよびフォルダにその ACL を適用する必要があります。そうしないと、ソースボリュームまたはデスティネーションボリュームが最初は mixed セキュリティ形式または UNIX セキュリティ形式のボリュームとして作成され、あとで NTFS セキュリティ形式に変更された場合は、ファイルを別のボリュームに移動する仮想マシンの移行またはデータベースファイルのエクスポートとインポートに失敗する可能性があります。

- アプリケーションサーバが使用する共有には、継続的可用性が設定されている必要があります。

  継続的可用性を備えた共有に接続するアプリケーションサーバは永続的ハンドルを受け取ります。永続的ハンドルを使用すると、テイクオーバー、ギブバック、アグリゲートの再配置などの停止イベントのあとに SMB 共有に無停止で再接続し、ファイルロックを再取得することができます。

- データベースファイルが格納されたボリュームにジャンクションを含めることはできますが、 SQL Server はデータベースディレクトリ構造の作成時にジャンクションを横断しません。
- SnapCenter Plug-in for Microsoft SQL Serverの処理が成功するためには、ボリュームに十分な利用可能スペースが必要です。

  SQL Server データベースファイルを格納するボリュームには、共有内にあるデータベースディレクトリ構造と、格納されているすべてのファイルを格納できる十分な容量が必要です。

- アプリケーションサーバが使用する継続的可用性を備えた共有では、次の共有プロパティを設定しないでください。
  - ホームディレクトリ
  - 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 の
- を使用したSMB共有ではウィルススキャンは実行されません `continuously-availability` 共有プロパティが設定されました。

Hyper-V over SMB 構成用のリモート VSS に関する考慮事項

Hyper-V over SMB 構成用のリモート VSS に対応したバックアップソリューションを使用する場合は、一定の考慮事項について理解しておく必要があります。

一般的なリモート 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。

  シャドウコピー処理は、同じ CIFS サーバ上で別のシャドウコピー処理が進行中である場合には失敗します。これは Microsoft の要件です。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、ジャンクションは許可されません。
  - 自動リカバリの場合、共有のトラバース時にジャンクションが見つかると、シャドウコピーの作成は失敗します。
  - 自動リカバリではない場合、シャドウコピーの作成は失敗しませんが、ジャンクションは何も参照しません。

自動リカバリを行うシャドウコピーのみに適用されるリモート VSS の考慮事項

一部の制限は、自動リカバリを行うシャドウコピー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ている共有内のすべてのファイル、ディレクトリ、およびサブディレクトリによって使用される合計スペースと同サイズ以上である必要があります。

- リモート VSS によってシャドウコピーが作成されるディレクトリ構造内では、リンク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** 用の **ODX** コピーオフロード要件

アプリケーションサーバ経由で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 以上でなければなりません。
- コピーオフロードに使用するボリュームで重複排除を有効にする必要があります。
- 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ようにします。
- 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際にゲスト内 iSCSI ドライブを使用します。共有 `.VHDX` ONTAP SMB共有のHyper-V over SMBではファイルがサポートされません。

Hyper-V または SQL Server over SMB 構成を計画

ボリューム設定ワークシートに記入

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、次のパスにアプリケーションサーバの共有を作成できます。 `/data1/vol1`、 `/data1/vol2`、 `/data2/vol3`および `/data2/vol4`。

```
                      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
Volume 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

このワークシートを使用して、 SQL Server および Hyper-V over SMB 構成用に継続的可用性を備えた 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 共有のプロパティおよび設定に関する情報

共有ごとに、次の情報を指定する必要があります。

- Storage Virtual Machine （ SVM ）名

  SVM 名はすべての共有で同じです

- 共有名
- パス
- 共有プロパティ

  次の 2 つの共有プロパティを設定する必要があります。

  - `oplocks`
  - `continuously-available`

次の共有プロパティは設定しないでください。

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - シンボリックリンクが無効になっている必要があります（の値） `-symlink-properties` パラメータは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」に格納する場合は、アプリケーションサーバの共有を次のパスに作成する必要があります。 `/data1/vol1`、 `/data1/vol2`、 `/data2/vol3`および `/data2/vol4`。

```
                      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
```

共有は上で作成できますが `/data1` および `/data2` パス管理管理用に、これらの共有を使用してデータを格納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 共有名およびパス _	
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ための **ONTAP** 設定を作成します

Hyper-V および **SQL Server over SMB** の概要を使用して、ノンストップオペレーション用の **ONTAP** 設定を作成します

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、次の作業を完了する必要があります。

- クラスタでタイムサービスがセットアップされている必要があります。
- 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 インターフェイスを設定します。
- SVM で DNS を設定します。
- SVM に必要なネームサービスをセットアップします。
- 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 構成を計画

設定に関する要件と考慮事項

Kerberos 認証および **NTLMv2** 認証の両方が許可されていることを確認する（ **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。

このタスクについて

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. を確認します `-is-exportpolicy-enabled` CIFSサーバオプションがに設定されている `false`：

   `vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled`

c. admin 権限レベルに戻ります。

   `set -privilege admin`

2. SMB のエクスポートポリシーが無効になっていない場合は無効にします。

   `vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false`

3. ドメインで NTLMv2 認証と Kerberos 認証の両方が許可されていることを確認します。

   ドメインで許可されている認証方法を確認する方法については、 Microsoft TechNet ライブラリを参照してください。

4. ドメインで NTMLv2 認証が許可されていない場合は、 Microsoft のドキュメントに記載されたいずれかの方法で NTLMv2 認証を有効にします。

例

次に、 SVM vs1 で SMB のエクスポートポリシーが無効になっていることを確認するコマンドの例を示します。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

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

ドメインアカウントがデフォルトの **UNIX** ユーザにマッピングされていることを確認します

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。

このタスクについて

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、「pcuser」という名前のデフォルトユーザがONTAP によって自動的に作成されます（UIDはになります） `65534`）および「pcuser」という名前のグループ（GIDはです`65534`をクリックし、デフォルトユーザを"`pcuser`"グループに追加します。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 解決策を設定する場合は、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ます `65534`。

   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、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` コマンドを実行します

   このコマンドの使用の詳細については、マニュアルページを参照してください。

例

次のコマンドでは、 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 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

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。

このタスクについて

- 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、を使用してあとからセキュリティ形式を変更できます `volume modify` コマンドを実行します

手順

1. SVM のルートボリュームの現在のセキュリティ形式を確認します。

   volume show -vserver *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、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。

このタスクについて

- 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`

      次のオプションはに設定する必要があります `true`：

      - `-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 `true`次の手順を実行します。

a. に設定します `true` を使用します `vserver cifs options modify` コマンドを実行します

b. オプションがに設定されていることを確認します `true` を使用します `vserver cifs options show` コマンドを実行します

3. admin 権限レベルに戻ります。

```
set -privilege admin
```

例

次に、 SVM vs1 について、 Hyper-V over SMB 構成の必要なオプションが有効になっていることを確認するコマンドの例を示します。この例の要件では、 ODX コピーオフロードのオプションを有効にする必要があります。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

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

パフォーマンスと冗長性を高めるために **SMB** マルチチャネルを設定します

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することができます。これにより、 Hyper-V 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。

作業を開始する前に

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。

このタスクについて

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 *

  クライアントから確立される接続数は NIC ごとに 1 つで、すべての接続にセッションがバインドされます。

- * クライアントおよび ONTAP クラスタ上の 10G 以上の NIC *

  クライアントから確立される接続数は NIC ごとに最大 4 つで、すべての接続にセッションがバインドされます。クライアントは 10G 以上の複数の 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`

  各マルチチャネルセッション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、クライアントの設定に対して同等の調整を行う必要があります。これには、デフォルトの接続数は 32 です。

- `-max-lifs-per-session`

  各マルチチャネルセッションで通知されるネットワークインターフェイスの最大数。デフォルトのネットワークインターフェイス数は 256 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して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 が割り当てられた 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: -
```

NTFS データボリュームを作成

Hyper-V over SMB または SQL Server over SMB アプリケーションサーバで使用する継続的可用性を備えた共有を設定する前に、 Storage Virtual Machine （ SVM ）上に NTFS データボリュームを作成する必要があります。ボリューム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。

このタスクについて

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、を参照してください "論理ストレージ管理"。

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が正しく機能しないのは、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た場合だけです。ボリュームを削除し、 NTFS セキュリティ形式でボリュームを再作成する必要があります。 または、 Windows ホストでボリュームをマッピングし、ボリュームの最上位に ACL を適用して、ボリューム内のすべてのファイルとフォルダに ACL を適用することもできます。

手順

1. 適切なコマンドを入力して、データボリュームを作成します。

ボリュームを作成する **SVM** 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*

継続的可用性を備えた **SMB** 共有を作成

データボリュームを作成したら、アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルと SQL Server データベースファイルにアクセスするために使用する継続的可用性を備えた共有を作成できます。SMB 共有を作成する場合と同様に、共有設定ワークシートを使用する必要があります。

手順

1. 既存のデータボリュームとそのジャンクションパスに関する情報を表示します。

   volume show -vserver *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、コメントを共有設定に追加することもできます。

- デフォルトでは、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共有が作成されます `Everyone` / `Full Control`。

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. を使用して、設定が正しいことを確認します `vserver cifs share show` コマンドを実行します
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、を設定します `-symlink` パラメータの値 `""`：

```
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。

このタスクについて

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 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. “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`

   の値 `-user-or-group-name` パラメータは、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を設定する（ **Hyper-V over SMB** 共有の場合）

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。

このタスクについて

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 では、すべてのサブディレクトリに対してシャドウコピーが作成されます。

> 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

既存の共有を継続的な可用性を確保するように設定し

既存の共有を変更して、継続的な可用性が確保された共有にすることができます。この共有は、 Hyper-V および SQL Server アプリケーションサーバが Hyper-V 仮想マシンおよび構成ファイルや SQL Server データベースファイルに無停止でアクセスするために使用します。

このタスクについて

既存の共有に次のような特徴がある場合、 SMB を介したアプリケーションサーバでその共有をノンストップオペレーション用の継続的可用性を備えた共有として使用することはできません。

- 状況に応じて `homedirectory` この共有に共有プロパティが設定されます
- 共有に有効なシンボリックリンクまたはワイドリンクが含まれている場合
- 共有のルート配下にジャンクションボリュームが含まれている場合

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Eitherに設定されます `manual` （デフォルト）または `none`。
- シンボリックリンクは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、の値を設定します `-symlink` パラメータの値 `""`。
   - を設定できます `-offline-files` を指定して正しい設定に変更します `manual`。
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]
```

   状況に応じて `oplocks` 共有プロパティがまだ設定されていないため、と一緒に追加する必要があります `continuously-available` 共有プロパティ。

4. 継続的な可用性が確保された共有でサポートされていない共有プロパティを削除します。

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   共有プロパティをカンマで区切って指定して、 1 つ以上の共有プロパティを削除することができます。

5. を確認します `-symlink` および `-offline-files` パラメータが正しく設定されている。

```
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、に設定されます `manual`。
- 。 `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 バックアップで VSS シャドウコピーを有効または無効にします

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。

このタスクについて

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	**`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します

使用可能な統計オブジェクトと統計カウンタを確認します

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ときの、クラスタ内の CIFS および SMB アクセスに関連する特定の統計オブジェクトの説明が表示されます。

```
cluster1::> set -privilege advanced

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

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

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
```

次のコマンドは、の一部のカウンタに関する情報を表示します `cifs` advanced権限レベルで表示されるオブジェクト。

> この例では、で使用可能なカウンタの一部が表示されているわけではありません `cifs` オブジェクト。出力は切り捨てられます。

```
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 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


[...]
```

SMB 統計を表示します

パフォーマンスの監視と問題の診断用に、さまざまな SMB 統計を表示することができ

ます。

手順

1. を使用します `statistics start` およびオプションです `statistics stop` データサンプルを収集するコマンド。
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 と SMB 3.0	**`statistics show -object smb2`**
ノードのSMBサブシステム	**`statistics show -object nblade_cifs`**

の詳細については、を参照してください `statistics` コマンド：

- "statistics showの画面には次"
- "統計が開始されます"
- "統計が停止しました"

設定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します

ヘルスモニタを使用して、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します

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になっている場合は、考えられる原因や推奨されるリカバリアクションなど、問題の詳細を表示できます。

ヘルス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（Major）	ノード上のアグリゲート内のボリュームでホストされている 1 つ以上のファイルが、継続的可用性を備えた SMB 共有を介して開かれており、障害が発生した場合でも継続性が保証されるはずだが、パートナーとの HA 関係が設定されていないか正常でない。
NoStandbyLifCifsNdo_Alert	マイナー	Storage Virtual Machine （SVM）はノードから SMB を介してアクティブにデータを提供しており、SMB ファイルは継続的可用性を備えた共有を介して継続的に開かれているが、そのパートナーノードが SVM のアクティブなデータ LIF を公開していない。

システムヘルスの監視を使用して、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

を使用できます `system health` 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コマンド。

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**

を使用します `-instance` 詳細情報を表示するためのパラメータ。

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** 共有の設定を確認します

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。

このタスクについて

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Eitherに設定されます `manual` （デフォルト）または `none`。
- シンボリックリンクは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に設定されていることを確認します `manual` または `disabled` シンボリックリンクが無効になっています。

   `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ます `manual` シンボリックリンクは無効になっています（でハイフンで指定） `Symlink Properties` フィールド出力）：

```
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 のステータスを確認

Hyper-V および SQL Server over SMB 構成の Storage Virtual Machine （ SVM ）がクラスタ内の各ノードに LIF を配置するように設定しても、日々の業務を行っているうちに、一部の LIF が他のノードのポートに移動してしまうことがあります。LIF のステータスを確認して、必要な措置を講じる必要があります。

このタスクについて

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にない場合 up 状態にして、問題を解決して、これらのインターフェイスがアップ状態になるようにします。
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を確認します

SMB セッション情報を表示します

SMB 接続、 SMB セッション ID 、セッションを使用しているワークステーションの IP アドレスなど、確立された SMB セッションに関する情報を表示できます。セッションの SMB プロトコルバージョンや継続的可用性を備えた保護のレベルに関する情報を表示できます。この情報は、セッションでノンストップオペレーションがサポートされているかどうか確認するのに役立ちます。

このタスクについて

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。

- オプションのを使用できます `-fields` 選択したフィールドに関する出力を表示するためのパラメータ。

  入ることができます `-fields ?` 使用できるフィールドを決定します。

- を使用できます `-instance` 確立されたSMBセッションに関する詳細情報を表示するためのパラメータ。
- を使用できます `-fields` パラメータまたは `-instance` パラメータのみ、または他のオプションパラメータと組み合わせて指定します。

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を要約形式で表示します	**`vserver cifs session show -vserver vserver_name`**
指定した接続 ID のセッション	**`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 アドレスからのセッションです	**`vserver cifs session show -vserver vserver_name -address workstation_IP_address`**
指定した LIF IP アドレスのセッションを表示します	**`vserver cifs session show -vserver vserver_name -lif -address LIF_IP_address`**
指定したノード上のセッションを表示します	`*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です
`vserver cifs session show -vserver vserver_name -windows-user user_name` の形式 `user_name` はです `[domain]\user`。	を指定します

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* -auth -mechanism authentication_mechanism の値 `-auth -mechanism` 次のいずれかです。 • `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セッションです

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 の値 `-protocol-version` 次のいずれかです。 • `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利用できます。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に設定します `SMB3` 以降が必要です。	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`* の値 `-continuously-available` 次のいずれかです。 • `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。この接続はドメインアカウントを使用して確立されています。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
             Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

次のコマンドは、 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情報を表示します。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ためには、 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します

SMB 接続、 SMB セッション ID 、ホスティングボリューム、共有名、共有パスなど、開いている SMB ファイルに関する情報を表示できます。ファイルの継続的可用性を備えた保護のレベルに関する情報も表示できます。この情報は、開いているファイルがノンストップオペレーションをサポートする状態であるかどうか確認するのに役立ちます。

このタスクについて

確立された SMB セッションで開いているファイルに関する情報を表示できます。これは、 SMB セッション内の特定のファイルに関する SMB セッション情報を確認する必要がある場合に役立ちます。

たとえば、SMBセッションで、開いているファイルの一部が継続的可用性を備えた保護を使用して開いている場合と、残りのファイル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場合（の値）`-continuously-available` フィールドに入力します `vserver cifs session show` コマンド出力はです `Partial`）の場合は、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。

を使用して、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` オプションのパラメータを指定しないコマンド。

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。

- オプションのを使用できます `-fields` 選択したフィールドの出力を表示するためのパラメータ。

  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。

- を使用できます `-instance` 開いているSMBファイルに関する詳細情報を表示するためのパラメータ。

  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
をクリックします	**`vserver cifs session file show -vserver vserver_name`**
指定したノード上のセッションを表示します	`*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 セッション ID のファイル
`vserver cifs session file show -vserver vserver_name -session-id integer`	指定したホスティング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です
`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 パスのオブジェクト

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ファイル
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* の値 `-continuously-available` 次のいずれかです。 • `No` • `Yes` 継続的可用性のステータスがの場合 `No`つまり、これらの開いているファイルは、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は対応していません。また、可用性の高い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。	指定した再接続の状態のファイル

ほかにも、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
```