NFSの設定

ONTAP 9

NetApp
January 23, 2026

目次

NFSの設定

ONTAP CLI を使用した NFS 構成について学習します

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 アクセスを設定することができます。

ここで説明する手順は、ボリュームまたはqtreeへのアクセスを設定する場合に使用します。想定している状況は次のとおりです。

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

  System Manager を使用して NAS マルチプロトコルアクセスを構成するには、"NFSとSMBの両方を使用したWindowsおよびLinux用のNASストレージのプロビジョニング"を参照してください。

- 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、"ONTAPコマンド リファレンス"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保有している。

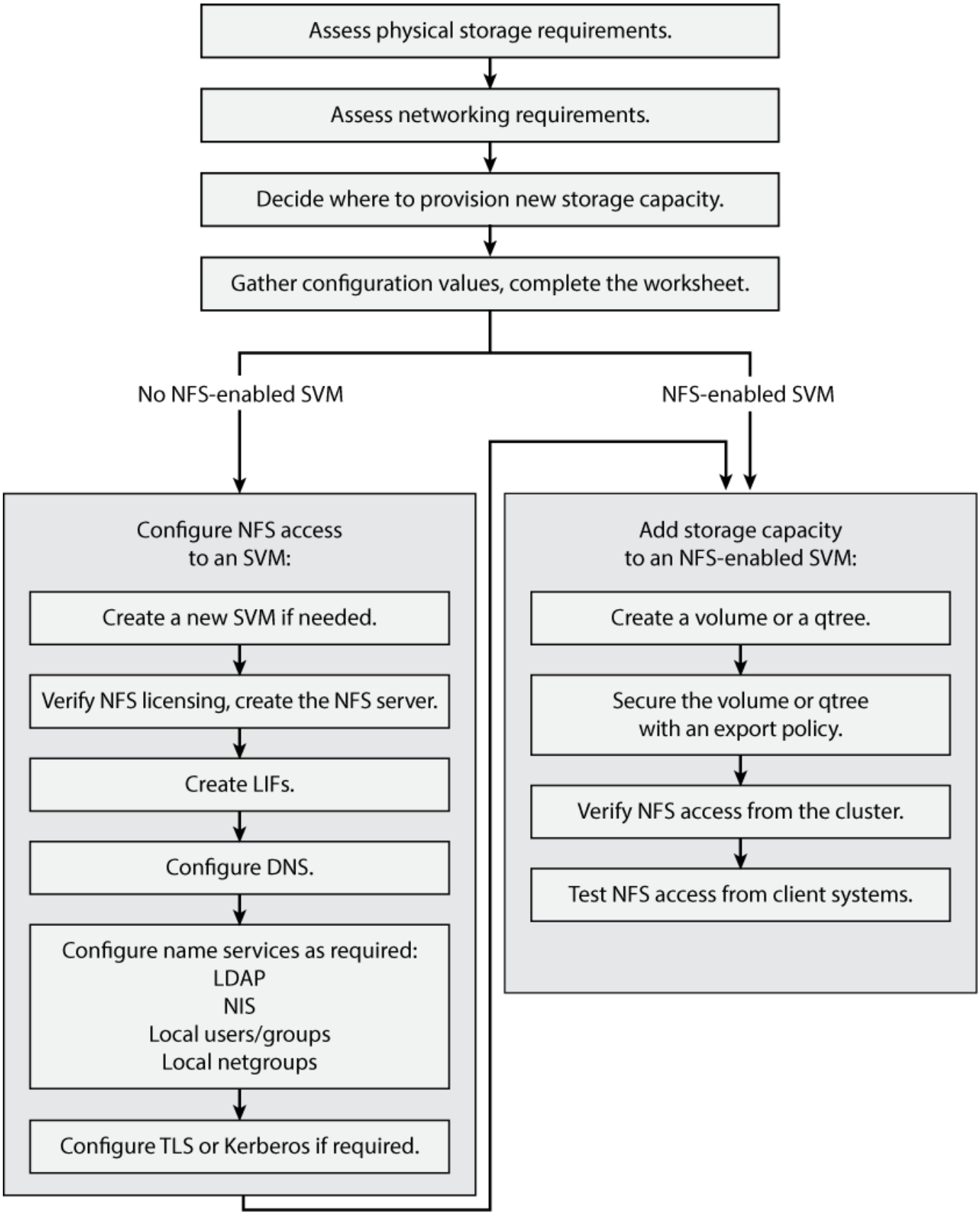
ONTAP NFS プロトコルの機能範囲の詳細については、"NFSプロトコルのONTAPファイルアクセスについて学ぶ"を参照してください。

ONTAPでこの処理を行うその他の方法

タスクを実行するツール	参照先
新しいSystem Manager（ONTAP 9.7以降で使用可能）	"NFSを使用したLinuxサーバ用のNASストレージのプロビジョニング"
System Manager Classic（ONTAP 9.7以前）	"NFS 構成の概要"

ONTAP NFSの設定ワークフローについて

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

ONTAP NFS物理ストレージ要件を評価する

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

関連情報

- "ローカル階層（アグリゲート）へのディスクの追加"
- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP NFSネットワーク構成要件を評価する

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

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. 利用可能な物理ポートおよび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。
   - `network port show`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

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予定の場合は、サブネットが存在し、十分なアドレスが使用可能であることを確認します：+

   ```
   network subnet show
   ```

   `network subnet show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-show.html["ONTAPコマンド リファレンス"^]を参照してください。

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

   `network subnet create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-create.html["ONTAPコマンド リファレンス"^]を参照してください。

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。

`network ipspace show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-ipspace-show.html["ONTAPコマンド リファレンス"^]をご覧ください。

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、 `network options ipv6 modify` コマンドを使用して IPv6 を有効にすることができます。

   `network options ipv6 show`および `network options ipv6 modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+options+ipv6["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP NFSストレージ容量のプロビジョニングについて学ぶ

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

オプション

- 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アクセスの設定

  NFS対応SVMへのNFSストレージの追加

  次のいずれかに該当する場合は、新しいSVMを作成します。

  - クラスタで初めてNFSを有効にします。
  - NFSサポートを有効にしたくないクラスタ内に既存のSVMがあります。
  - クラスタ内にNFS対応SVMが1つ以上あり、分離されたネームスペースに別のNFSサーバを配置する必要がある場合（マルチテナンシーシナリオ）。NFSが有効になっているが未設定の既存のSVMに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。SANアクセス用にSVMを作成した場合や、SVMの作成時にプロトコルが有効になっていなかった場合に、この状況が発生する可能性があります。

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

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

ONTAP NFS構成ワークシート

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応じて、以下に記載するセクションのワークシートのどちらかまたは両方を記入する必要があります。

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

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

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

- NFS対応SVMへのストレージ容量の追加

SVMへのNFSアクセスの設定

SVMを作成するためのパラメータ

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

フィールド	概要	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）が存在する個別の IP アドレス空間です。	

NFSサーバの作成用パラメータ

新しいNFSサーバを作成し、サポートされているNFSバージョンを指定するときに、 `vserver nfs create`コマンドでこれらの値を指定します。

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	概要	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。 v4.2は、 `v4.1`が有効になっている場合、ONTAP 9.8以降でもサポートされます。	
`-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）を指定します。	

LIFを作成するためのパラメータ

これらの値は、LIFを作成する際に `network interface create`コマンドで指定します。"ONTAPコマンド リファレンス"の `network interface create`の詳細を確認してください。

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	概要	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	`network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノード。 `network interface revert`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-revert.html["ONTAPコマンド リファレンス"^]を参照してください。	
-home-port	`network interface revert`コマンドがLIFで実行されたときにLIFが戻るポートまたはインターフェイスグループ。	
-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。 `-address`と`-netmask`の代わりに使用され、アドレスとネットマスクを自動的に割り当てます。	
-firewall-policy	このワークフローではデフォルトのデータ ファイアウォール ポリシーを使用します。	data

DNSホスト名解決のパラメータ

DNSを構成するときに、 `vserver services name-service dns create`コマンドでこれらの値を指定します。

フィールド	概要	あなたの価値

-domains	最大5つのDNSドメイン名を指定します。	
-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

ローカルユーザを作成するためのパラメータ

`vserver services name-service unix-user create`コマンドを使用してローカルユーザを作成する場合は、これらの値を指定します。Uniform Resource Identifier（URI）からUNIXユーザを含むファイルを読み込んで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。

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

ローカルグループを作成するためのパラメータ

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

	グループ名(-name)	グループID (-id)
例	Engineering	100
1		

2		
3		
…		
n		

NISのパラメータ

これらの値は `vserver services name-service nis-domain create`コマンドで指定します。

> `-nis-servers`フィールドは `-servers`フィールドを置き換えます。 `-nis-servers`フィールドを使用して、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	概要	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`
`-nis-servers`	ドメイン設定で使用する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

これらの値は `vserver services name-service ldap client create`コマンドで指定します。

自己署名ルートCA証明書 `.pem`ファイルも必要になります。

フィールド	概要	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を指定します。	
`-ldap-servers`	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。	

フィールド	概要	あなたの価値
`-query-timeout`	このワークフローではデフォルトの `3`秒を使用します。	`3`
`-min-bind-level`	最小のバインド認証レベル。デフォルトは `anonymous`です。署名と封印が設定されている場合は `sasl`に設定する必要があります。	
`-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 テンプレートを指定します。デフォルトまたはカスタムのスキーマを使用できます。	
`-port`	このワークフローにはデフォルトのLDAPサーバポート `389`を使用します。	`389`
`-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 `""`（root）です。	
`-base-scope`	このワークフローのデフォルトの基本検索範囲 `subnet`を使用します。	`subnet`
`-session-security`	LDAP署名または署名とシーリングを有効にします。デフォルトは `none`です。	
`-use-start-tls`	LDAP over TLSを有効にします。デフォルトは `false`です。	

Kerberos認証のパラメータ

これらの値は `vserver nfs kerberos realm create`コマンドで指定します。一部の値は、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 などの UNIX KDC サーバを使用するかによって異なります。

フィールド	概要	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の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。	
-adserver-ip	Microsoft KDC のみ：AD サーバ IP アドレス。	
-adminserver-ip	UNIX KDC のみ：管理サーバの IP アドレス。	
-adminserver-port	UNIX KDC のみ：管理サーバのポート番号。	
-passwordserver-ip	UNIX KDCのみ：パスワードサーバのIPアドレス。	
-passwordserver-port	UNIX KDCのみ：パスワードサーバポート。	
-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。

これらの値は `vserver nfs kerberos interface enable`コマンドで指定します。

フィールド	概要	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`	NFS 経由の Kerberos に許可される暗号化タイプ。クライアントの機能に応じて `aes-256`が推奨されます。	
`-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。パスワードが必要です。	
`-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とルールを作成するためのパラメータ

これらの値は `vserver export-policy create`コマンドで指定します。

フィールド	概要	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。	

`vserver export-policy rule create`コマンドを使用して、各ルールにこれらの値を指定します。

フィールド	概要	あなたの価値

`-clientmatch`	クライアント照合を指定します。	
`-ruleindex`	ルール リスト内のエクスポート ルールの位置を指定します。	
`-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	any	krb5	sys	65534
1					
2					
3					
…					
n					

ボリュームを作成するためのパラメータ

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

フィールド	概要	あなたの価値
`-vserver`	新しいボリュームをホストする新規または既存のSVMの名前を指定します。	

-volume	新しいボリュームに対して、一意のわかりやすい名前を指定します。	
-aggregate	新しいNFSボリュームに対応できる十分なスペースを持つクラスタ内のアグリゲートの名前を指定します。	
-size	新しいボリュームのサイズとして任意の整数を指定します。	
-user	ボリュームのルートの所有者に設定するユーザの名前またはIDを指定します。	
-group	ボリュームのルートの所有者に設定するグループの名前またはIDを指定します。	
--security-style	このワークフローにはUNIXセキュリティ形式を使用します。	unix
-junction-path	新しいボリュームのマウント先とする、ルート（/）の下の場所を指定します。	
-export-policy	既存のエクスポート ポリシーを使用する場合は、ボリュームの作成時に名前を入力できます。	

qtreeを作成するためのパラメータ

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

フィールド	概要	あなたの価値
-vserver	qtreeを格納するボリュームが配置されているSVMの名前を指定します。	
-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`	ボリュームとqtreeを別々の引数として指定する代わりに、`/vol/*volume_name/qtree_name*\>`の形式でqtreeパス引数を指定できます。	
`-unix-permissions`	オプション：qtreeのUNIXパーミッション。	
`-export-policy`	既存のエクスポート ポリシーを使用する場合は、qtreeの作成時に名前を入力できます。	

関連情報

- "ONTAPコマンド リファレンス"

SVMへのNFSアクセスの設定

NFSデータアクセス用のONTAP SVMを作成する

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

開始する前に

- ONTAP 9.13.1以降では、ストレージVMの最大容量を設定できます。また、SVMの容量がしきい値に近づいた場合にアラートを設定することもできます。詳細については、SVMの容量の管理を参照してください。

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
   ```

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

2. 新しく作成したSVMの設定および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。このリストは後で編集できます。

`Vserver Operational State`フィールドには
`running`状態が表示される必要があります。
`initializing`状態が表示される場合、ルート
ボリュームの作成などの中間操作が失敗したことを意味し、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を持つSVMが作成され、自動的に起動されて `running`状態になっていることを示しています。ルートボリュームにはルールが含まれていないデフォルトのエクスポート ポリシーが適用されているため、作成時にルートボリュームは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を適用できます。このポリシーは、SVMを作成した後にのみ適用できます。このプロセスの詳細については、アダプティブ ポリシー グループ テンプレートの設定を参照してください。

ONTAP SVMでNFSプロトコルの有効化を確認する

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

タスク概要

これは通常、SVM のセットアップ中に実行されますが、セットアップ中にプロトコルを有効にしなかった場合は、後で `vserver add-protocols`コマンドを使用して有効にできます。

LIF を作成した後は、プロトコルを追加したり削除したりすることはできません。

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

手順

1. SVM に対して現在有効になっているプロトコルと無効になっているプロトコルを確認します：

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

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

2. 必要に応じて、プロトコルを有効または無効にします：
   - NFSプロトコルを有効にするには：+ `vserver add-protocols -vserver vserver_name -protocols nfs`
   - プロトコルを無効にするには：+ `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,…]`
3. 有効化されたプロトコルと無効化された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 という名前の SVM で現在有効になっているプロトコルと無効になっているプロトコル（許可されているプロトコルと許可されていないプロトコル）を表示します：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

次のコマンドは、vs1という名前のSVM上の有効なプロトコルのリストに`nfs`を追加することで、NFS経由のアクセスを許可します：

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

ONTAP SVM上のNFSクライアント アクセスを開く

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

タスク概要

新しいSVMが作成されると、SVMのルート ボリュームに対してデフォルトのエクスポート ポリシー（default）が自動的に作成されます。クライアントがSVM上のデータに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 ポリシーにルールを1つ以上作成する必要があります。

デフォルトのエクスポート ポリシーですべてのNFSクライアントにアクセスを許可したうえで、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 ポリシーをチェックします。

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

   コマンド出力は次のようになります：

   ```
   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ルールが存在する場合、このタスクは完了です。存在しない場合は、次のステップに進みます。

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
   ```

   SVM に Kerberos で保護されたボリュームのみが含まれる場合は、ルート ボリュームのエクスポート ルール オプション `-rorule`、 `-rwrule`、 `-superuser`を `krb5`または `krb5i`に設定できます。次に例を示します：

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

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

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、NFSクライアントからアクセスできるようになりました。

ONTAP NFSサーバを作成する

クラスタ上でNFSのライセンスが付与されていることを確認したら、 `vserver nfs create`コマンドを使用してSVM上にNFSサーバを作成し、サポートするNFSバージョンを指定できます。

タスク概要

SVMは、1つ以上のNFS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：

- 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 クライアント上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環境でのネーム サービスにはLDAPを使用する必要があります。

開始する前に

SVMでNFS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。

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
   ```

   有効でない場合は、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バージョンの任意の組み合わせを有効にできます。pNFSをサポートする場合は、 `-v4.1`と `-v4.1-pnfs`の両方のオプションを有効にする必要があります。

   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、ユーザ名とグループ名のドメイン部分をNFSv4プロトコルで定義されている値に指定します。デフォルトでは、NISドメインが設定されている場合は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の所有者属性で数字IDのサポートを有効にするかどうかを指定します。デフォルト設定が有効になっていますが、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。

`vserver nfs modify`コマンドを使用して、後で追加のNFS機能を有効にすることができます。

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が有効になっている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
...
```

ONTAP NFS LIFを作成する

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ので、引き続きネットワークと通信できます。

開始する前に

- 基盤となる物理または論理ネットワーク ポートが管理 `up`ステータスに設定されている必要があります。"ONTAPコマンド リファレンス"の `up`の詳細を確認してください。
- 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ている必要があります。

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

  > `network subnet create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-create.html["ONTAPコマンド リファレンス"^]を参照してください。

- LIFが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以前ではロールで指定していました。ONTAP 9.6以降ではサービス ポリシーで指定します。

タスク概要

- 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。
- クラスタ内に多数のLIFがある場合は、 `network interface capacity show`コマンドを使用してクラスタでサポートされているLIF容量を確認し、 `network interface capacity details show`コマンド（高度な権限レベル）を使用して各ノードでサポートされているLIF容量を確認できます。

  > `network interface capacity show`および `network interface capacity details show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface+capacity+show["ONTAPコマンド リファレンス"^]をご覧ください。

- ONTAP 9.7以降では、同じサブネットにSVM用の他のLIFがすでに存在していれば、LIFのホーム ポートを指定する必要はありません。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 ドメインにあるホーム ノードから任意のポートが自動的に選択されます。

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}
   ```

   `network interface create`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html["ONTAPコマンド リファレンス"^]を参照してください。

オプション	概要
• 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}`

- サービス ポリシーを使用してLIFを作成する場合、 `-role`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、データLIFを破棄して再作成しない限り、後で変更することはできません。

  サービス ポリシーを使用してLIFを作成する場合、 `-data-protocol`パラメータは必要ありません（ONTAP 9.6以降）。

- `-home-node`は、 `network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノードです。

  `-auto-revert`オプションを使用して、
  LIFが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も指定できます。

  `network interface revert`
  の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-revert.html["ONTAPコマンド リファレンス"^]を参照してください。

- `-home-port`は、LIF上で `network interface revert`コマンドが実行されたときにLIFが戻る物理ポートまたは論理ポートです。
- `-address`および `-netmask`オプションを使用してIPアドレスを指定することも、 `-subnet_name`オプションを使用してサブネットからの割り当てを有効にすることもできます。
- サブネットを使用してIPアドレスとネットワーク マスクを指定した場合、サブネットにゲートウェイが定義されていると、そのサブネットを使用してLIFを作成するときにゲートウェイへのデフォルト ルートがSVMに自動的に追加されます。
- IPアドレスを手動で割り当てる場合（サブネットを使用せず）、クライアントまたはドメインコントローラが異なるIPサブネット上にある場合は、ゲートウェイへのデフォルトルートを設定する必要がある場合があります。 `network route create`およびSVM内での静的ルートの作成方法の詳細については、"ONTAP コマンド リファレンス"を参照してください。
- `-firewall-policy`オプションには、LIFロールと同じデフォルトの `data`を使用します。

  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、ファイアウォールポリシーは廃止され、LIFサービスポリシーに完全に置き換えられました。詳細については、"LIFのファイアウォール ポリシーの設定"を参照してください。

- `-auto-revert`では、起動時、管理データベースのステータス変更時、ネットワーク接続時などの状況において、データLIFをホームノードに自動的にリバートするかどうかを指定できます。デフォルト設定は `false`ですが、環境のネットワーク管理ポリシーに応じて `false`に設定できます。

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

  b. 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	方法
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

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

     これらの各LIFでKerberosを個別に有効にする必要があります。

例

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

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

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

```
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。データLIFのdatalif1とdatalif3にはIPv4アドレスが、datalif4にはIPv6アドレスが設定されています。

```
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、 `default-data-files`サービス ポリシーが割り当てられたNASデータLIFを作成する方法を示しています：

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

関連情報

- "network ping"
- "ネットワーク インターフェイス"

ONTAP NFS SVMホスト名解決のためにDNSを有効にする

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

開始する前に

ホスト名を検索するために、サイト規模のDNSサーバが使用できなければなりません。

単一障害点を回避するため、複数のDNSサーバーを設定する必要があります。 `vserver services name-service dns create`コマンドは、DNSサーバー名を1つだけ入力した場合に警告を発します。

タスク概要

"SVM でのダイナミック DNS の設定"についての詳細をご覧ください。

手順

1. SVMでDNSを有効にします。

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

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

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

   > この `vserver services name-service dns create`コマンドは自動構成検証を実行し、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. `vserver services name-service dns show`コマンドを使用してDNSドメイン構成を表示します。

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

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

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

ネーム サービスを設定する

ONTAP NFSネーム サービスについて学ぶ

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

クライアント認証時の名前検索を容易にするために、NISやLDAPなどのネーム サービスを使用する必要があります。特にNFSv4以降を導入する場合は、セキュリティを強化するために、可能な限りLDAPを使用することをお勧めします。また、外部ネーム サーバが利用できない場合に備えて、ローカル ユーザとグループを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された状態に保つ必要があります。

ONTAP NFSネーム サービス スイッチ テーブルを設定する

ONTAPがローカルまたは外部のネーム サービスを参照して、ホスト、ユーザ、グループ、ネットグループ、または名前のマッピング情報を取得できるようにするには、ネーム サービス スイッチ テーブルを正しく設定する必要があります。

開始する前に

環境に応じて、ホスト、ユーザー、グループ、ネットグループ、または名前のマッピングに使用するネーム サービスを決定する必要があります。

ネットグループを使用する場合は、ネットグループで指定されたすべてのIPv6アドレスをRFC 5952で指定されているとおりに短縮および圧縮する必要があります。

タスク概要

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、 `-sources nis`オプションを指定しないでください。

手順

1. ネーム サービス スイッチ テーブルに必要なエントリを追加します。

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

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

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

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

例

次の例では、SVM vs1 のネーム サービス スイッチ テーブルに新しいエントリを作成し、ローカル ネットグループ ファイルと外部 NIS サーバを使用して、その順序でネットグループ情報を検索します：

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

終了後の操作

- データ アクセスを提供するには、SVM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の名前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 サービスを削除できなかった場合、ストレージ システムへのクライアント アクセスが期待どおりに機能しない可能性があります。

ローカルUNIXユーザおよびグループの設定

ONTAP NFS SVMのローカルUNIXユーザーとグループについて学習します

SVM上のローカルUNIXユーザとグループを、認証と名前マッピングに使用できます。UNIXユーザと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ユーザー グループとグループ メンバーの合計数は、デフォルトで32,768個に制限されています。クラスタ管理者はこの制限を変更できます。

ONTAP NFS SVMにローカルUNIXユーザーを作成する

`vserver services name-service unix-user create`
コマンドを使用して、ローカルUNIXユーザを作成できます。ローカルUNIXユーザとは、ネームマッピングの処理で使用するUNIXネームサービスオプションとしてSVM上に作成するUNIXユーザです。

手順

1. ローカルUNIXユーザを作成します：

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

   `-user *user_name*`ユーザー名を指定します。ユーザー名の長さは64文字以下である必要があります。

   `-id *integer*`割り当てるユーザー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、ユーザはプライマリ グループに追加されます。ユーザの作成後、必要に応じて任意の追加グループに手動でユーザを追加できます。

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"
```

ONTAP NFS SVMにローカルUNIXユーザーリストをロードする

SVM で個々のローカル UNIX ユーザーを手動で作成する代わりに、Uniform Resource Identifier（URI(`vserver services name-service unix-user load-from-uri`）からローカル UNIX ユーザーのリストを SVM にロードすることで、タスクを簡素化できます。

手順

1. ロードするローカル UNIX ユーザーのリストを含むファイルを作成します。

   ファイルには、UNIX `/etc/passwd` 形式のユーザー情報が含まれている必要があります：

   `user_name: password: user_ID: group_ID: full_name`

   このコマンドは、 *`password`* フィールドの値と、 *`full_name`* フィールドの後のフィールドの値（ (*`home_directory`* および *`shell`*）を破棄します。

   サポートされるファイルの最大サイズは2.5MBです。

2. リストに重複する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、リストの読み込みは失敗し、エラーメッセージが表示されます。

3. ファイルをサーバーにコピーします。

   サーバーは、HTTP、HTTPS、FTP、または FTPS 経由でストレージ システムからアクセスできる必要があります。

4. ファイルの URI を確認します。

   URI は、ファイルが配置されている場所を示すためにストレージシステムに提供するアドレスです。

5. ローカル UNIX ユーザーのリストを含むファイルを 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 `false`です。

例

次のコマンドは、URI `ftp://ftp.example.com/passwd`からローカルUNIXユーザーのリストをvs1という名前のSVMにロードします。SVM上の既存のユーザーは、URIの情報によって上書きされません。

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

ONTAP NFS SVMにローカルUNIXグループを作成する

`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グループを作成できます。ローカルUNIXグループは、ローカルUNIXユーザと共に使用されます。

手順

1. ローカルUNIXグループを作成します：

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

`-name *group_name*`グループ名を指定します。グループ名の長さは64文字以下である必要があります。

`-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。このグループのIDは101です。

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

ONTAP NFS SVM上のローカルUNIXグループにユーザーを追加する

`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補足UNIXグループにユーザーを追加できます。

手順

1. ローカル UNIX グループにユーザーを追加します：

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

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

例

次のコマンドは、vs1 という名前の SVM 上の eng という名前のローカル UNIX グループに max という名前のユーザーを追加します：

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

ONTAP NFS SVM上のURIからローカルUNIXグループをロードする

個々のローカル UNIX グループを手動で作成する代わりに、`vserver services name-service unix-group load-from-uri`コマンドを使用して、Uniform Resource Identifier（URI）からローカル UNIX グループのリストを SVM にロードできます。

手順

1. ロードするローカル UNIX グループのリストを含むファイルを作成します。

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

group_name: password: group_ID: comma_separated_list_of_users

コマンドは `*password*` フィールドの値を破棄します。

サポートされるファイルの最大サイズは 1 MB です。

グループ ファイル内の各行の最大長は 32,768 文字です。

2. リストに重複する情報が含まれていないことを確認します。

   リストには重複するエントリが含まれていてはなりません。重複するとリストのロードに失敗します。SVMに既にエントリが存在する場合は、 `-overwrite`パラメータを `true`に設定して既存のエントリをすべて新しいファイルで上書きするか、新しいファイルに既存のエントリと重複するエントリが含まれていないことを確認する必要があります。

3. ファイルをサーバーにコピーします。

   サーバーは、HTTP、HTTPS、FTP、または FTPS 経由でストレージ システムからアクセスできる必要があります。

4. ファイルの URI を確認します。

   URI は、ファイルが配置されている場所を示すためにストレージシステムに提供するアドレスです。

5. ローカル UNIX グループのリストを含むファイルを 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 `false`です。このパラメータを `true`に指定すると、ONTAPは指定されたSVMの既存のローカルUNIXグループデータベース全体を、ロードするファイルのエントリに置き換えます。

例

次のコマンドは、URI `ftp://ftp.example.com/group`からローカルUNIXグループのリストをvs1という名前のSVMにロードします。SVM上の既存のグループは、URIの情報によって上書きされません。

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

ネットグループの使用

ONTAP NFS SVMのネットグループについて学ぶ

ネットグループはユーザ認証やエクスポート ルールにおけるクライアントの照合に使用できます。外部ネームサーバ（LDAPまたはNIS）からネットグループへのアクセスを提供したり、 `vserver services name-service netgroup load`コマンドを使用してURI

（Uniform Resource Identifier）からSVMにネットグループをロードしたりできます。

開始する前に

ネットグループを操作する前に、次の条件が満たされ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には、ソース（NIS、LDAP、またはローカル ファイル）にかかわらず、一貫したフォワード（正引き）およびリバース（逆引き）DNSルックアップ結果を提供するために、フォワード（A）およびリバース（PTR）の両方のDNSレコードが必要です。

  また、クライアントのあるIPアドレスに複数のPTRレコードがある場合は、それらすべてのホスト名がネットグループのメンバーであり、対応するAレコードがあることが必要です。

- 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、正しいスペルで大文字 / 小文字が区別され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で大文字 / 小文字の表記が統一されていないと、予期しない動作（エクスポート チェックの失敗など）が発生することがあります。
- ネットグループに指定されているすべてのIPv6アドレスは、RFC 5952の規定に従って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。

タスク概要

ネットグループを操作する場合、次の操作を実行できます：

- `vserver export-policy netgroup check-membership`コマンドを使用すると、クライアント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判断できます。
- `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できます。

  ルックアップの基盤となるサービスは、設定されているネーム サービス スイッチの順番に基づいて選択されます。

ONTAP NFS SVM上のURIからネットグループをロードする

エクスポートポリシールールでクライアントをマッチングする方法の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。外部ネームサーバに保存されているネットグループを使用する代わりに、URI（Uniform Resource Identifier）からSVMにネットグループをロードすることもできます(`vserver services name-service netgroup load`。

開始する前に

ネットグループ ファイルは、SVM にロードされる前に次の要件を満たしている必要があります：

- ファイルでは、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、ネットグループのテキストファイルをロードする前にフォーマットをチェックします。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、ファイルに必要な修正内容を示すメッセージが表示されます。エラーを修正したら、指定したSVMにネットグループファイルをリロードできます。

- ネットグループ ファイル内のホスト名のアルファベット文字はすべて小文字にする必要があります。
- サポートされるファイルの最大サイズは 5 MB です。
- ネストされたネットグループでサポートされる最大レベルは 1000 です。
- ネットグループ ファイルでホスト名を定義するときは、プライマリDNSホスト名のみを使用できます。

  エクスポートアクセスの問題を回避するには、DNS CNAME またはラウンドロビンレコードを使用してホスト名を定義しないでください。

- ネットグループ ファイル内のトリプルのユーザーとドメインの部分は ONTAP でサポートされていないため、空のままにしておく必要があります。

  ホスト/IP 部分のみがサポートされます。

タスク概要

ONTAPは、ローカルネットグループファイルに対するホストごとのネットグループ検索をサポートしています。ネットグループファイルをロードすると、ONTAPは自動的にnetgroup.byhostマップを作成し、ホストごとのネットグループ検索を有効にします。これにより、クライアントアクセスを評価するエクスポートポリシールールの処理時に、ローカルネットグループ検索が大幅に高速化されます。

手順

1. URI からネットグループを SVM にロードします：

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

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

   ネットグループを更新する場合は、ファイルを編集し、更新されたネットグループファイルを SVM にロードできます。

例

次のコマンドは、HTTP URL `http://intranet/downloads/corp-netgroup`から vs1 という名前の SVM にネットグループ定義をロードします：

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

ONTAP NFS SVMネットグループ定義を確認する

ネットグループをSVMにロードした後、 `vserver services name-service netgroup status`コマンドを使用してネットグループ定義のステータスを確認できます。これにより、SVMをサポートするすべてのノードでネットグループ定義が一貫しているかどうかを確認できます。

手順

1. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

2. ネットグループ定義のステータスを確認します。

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

   より詳細なビューで追加情報を表示できます。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

権限レベルが設定されると、次のコマンドはすべてのSVMのネットグループのステータスを表示します：

```
vs1::> set -privilege advanced

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

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

ONTAP NFS SVMのNISドメイン構成を作成する

環境内でネーム サービスにNetwork Information Service（NIS）が使用されている場合は、`vserver services name-service nis-domain create`コマンドを使用してSVMのNISドメイン構成を作成する必要があります。

開始する前に

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。

ディレクトリ検索にNISを使用する場合、NISサーバのマップではエントリごとに1,024文字を超えることはできません。この制限を満たしていないNISサーバを指定しないでください。そうしないと、NISエントリに依存するクライアント アクセスが失敗する可能性があります。

タスク概要

NISデータベースに `netgroup.byhost`マップが含まれている場合、ONTAPはそれを使用して検索を高速化できます。 `netgroup.byhost`と `netgroup`のマップは、クライアントアクセスの問題を回避するために、ディレクトリ内で常に同期しておく必要があります。ONTAP 9.7以降では、NIS `netgroup.byhost`エントリを`vserver services name-service nis-domain netgroup-database`コマンドを使用してキャッシュできます。

NIS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。

手順

1. NISドメイン設定を作成します。

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

   最大10台のNISサーバを指定できます。

   > ℹ `-nis-servers`フィールドは `-servers`フィールドを置き換えます。 `-nis-servers`フィールドを使用して、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、 `vs1`という名前のSVM上で、 `nisdomain`と呼ばれるNISドメインのNISドメイン設定を、IPアドレス `192.0.2.180`のNISサーバを使用して作成します：

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

LDAPの使用

ONTAP NFS SVMでのLDAPネームサービスの使用について学習します

LDAPがネーム サービスに使用されている環境では、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、Active Directoryとネーム サービスの LDAP接続の両方で、LDAPチャネル バインディング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signまたはsealに設定されている場合にのみ、LDAP接続でチャネル バインディングを試行します。ネー

ム サーバとのLDAPチャネル バインディングを無効化または再有効化するには、 `ldap client modify`コマンドで `-try-channel-binding`パラメータを使用します。

詳細については、"Windows の 2020 年 LDAP チャネル バインディングおよび LDAP 署名要件"を参照してください。

- LDAPをONTAP用に設定する前に、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する必要があります。
  - LDAPサーバでサポートされるLDAPユーザのパスワード ハッシュ タイプに、ONTAPでサポートされる次の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。

    以下のセッション 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（TLSまたはSSL経由のLDAP）
  - 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。
  - START TLSまたはLDAPSを有効にする場合、次の点を考慮する必要があります。
    - NetAppでは、LDAPSではなくStart TLSの使用を推奨しています。
    - ONTAP 9.5以降でLDAPSを使用する場合は、TLS用またはSSL用にLDAPサーバ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が設定されている必要があります。
      - 双方向
      - 一方向（プライマリ ドメインがリファーラル ドメインを信頼）
      - 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が設定されている必要があります。

- --bind-as-cifs-server が true に設定されている場合、認証にはドメイン パスワードが同じである必要があります。

次の設定はLDAPリファーラル追跡でサポートされていません。

- すべてのONTAPバージョン：
  - 管理SVM上のLDAPクライアント
- ONTAP 9.8以前の場合（9.9.1以降でサポートされます）：
  - LDAP署名とシーリング（ `-session-security`オプション）
  - 暗号化されたTLS接続（ `-use-start-tls` オプション）
  - LDAPSポート636経由の通信（ `-use-ldaps-for-ad-ldap` オプション）

- SVMでLDAPクライアントを設定する際は、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で問題ありません。ただし、環境のLDAPスキーマがデフォルトのスキーマと異なる場合は、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。

詳細情報

- "NetAppテクニカルレポート4835：ONTAPでLDAPを設定する方法"
- "ONTAP SMB SVMに自己署名ルートCA証明書をインストールする"

ONTAP NFS SVM用の新しい**LDAP**クライアント スキーマを作成する

環境で使用するLDAPスキーマがONTAPのデフォルトと異なる場合は、LDAPクライアント設定を作成する前に、ONTAP用の新しいLDAPクライアント スキーマを作成する必要があります。

タスク概要

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（Windows Server 2012以降のほとんどのADサーバで優先されるスキーマ）
- 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しておく必要があります。新しいスキーマを作成する前に、LDAP管理者にお問い合わせください。

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、そのコピーを必要に応じて変更します。

手順

1. 既存のLDAPクライアント スキーマの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
   ```

ONTAP NFSアクセス用の**LDAP**クライアント構成を作成する

環境でONTAPから外部のLDAPやActive Directoryのサービスにアクセスする場合は、まずストレージ システム上でLDAPクライアントを設定する必要があります。

開始する前に

Active Directoryドメイン解決リストの最初の3台のサーバのうち1台が起動していて、データを提供している必要があります。そうでない場合、このタスクは失敗します。

複数のサーバがあり、どの時点でもそのうち3台以上のサーバがダウンしている状態です。

手順

1. LDAP管理者に相談して、 `vserver services name-service ldap client create`コマンドの適切な構成値を決定してください：

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

   `-ad-domain`オプションと `-servers`オプションは相互に排他的です。

   - Active Directoryドメインで LDAPサーバ検出を有効にするには、 `-ad-domain`オプションを使用します。
     - `-restrict-discovery-to-site`オプションを使用すると、LDAPサーバ検出を指定したドメインのCIFSデフォルト サイトに制限できます。このオプションを使用する場合は、 `-default-site`でCIFSデフォルト サイトも指定する必要があります。
   - `-preferred-ad-servers`オプションを使用すると、1つ以上の優先Active DirectoryサーバをIPアドレスでカンマ区切りのリストで指定できます。クライアントの作成後、 `vserver services name-

service ldap client modify`コマンドを使用してこのリストを変更できます。

- `-servers`オプションを使用して、カンマ区切りのリストでIPアドレス別に1つ以上のLDAPサーバー（Active DirectoryまたはUNIX）を指定します。

> この `-servers`オプションは非推奨です。 `-ldap-servers`フィールドは `-servers`フィールドに置き換えられます。このフィールドには、LDAPサーバのホスト名またはIPアドレスのいずれかを指定できます。

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によって提供されているデフォルトの読み取り専用スキーマを使用できます。他のスキーマを使用する必要がある場合を除き、デフォルトのスキーマを使用することを推奨します。他のスキーマを使用する場合は、デフォルトのスキーマ（読み取り専用）をコピーし、コピーを変更することによって、独自のスキーマを作成できます。

デフォルトのスキーマ：

- MS-AD-BIS

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

- `AD-IDMU`

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

- `RFC-2307`

  RFC-2307（*An Approach for Using LDAP as a Network Information Service*）に基づくこのスキーマは、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}`最小のバインド認証レベルを指定します。

  デフォルト値は `**anonymous**`です。

- `-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署名と封印（暗号化）、またはLDAP over TLS（LDAPサーバで必要な場合）を有効にできます。

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

  署名(`sign`（データ整合性）、署名とシーリング(`seal`（データ整合性と暗号化）、またはどちらも有効にしない `none`（署名もシーリングも有効にしない）ことができます。デフォルト値は `none`です。

  署名とシーリングのバインドが失敗した場合に **`anonymous`**`または **`simple`**`にバインド認証をフォールバックさせたくない場合は、 `-min-bind-level {`sasl`も設定する必要があります。

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

  > `*true*`に設定され、`LDAP`サーバがサポートしている場合、`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 `*false*`です。このオプションを使用するには、`LDAP`サーバの自己署名ルート`CA`証明書をインストールする必要があります。

  > ストレージVMのドメインにSMBサーバが追加されており、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、 `vserver cifs security modify`コマンドを使用して `-session-security-for-ad-ldap`オプションを変更できます。

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 `389`です。

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

- `-query-timeout *integer*`クエリの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 `3`秒です。

- `-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（例：LDAP参照追跡が有効になっている場合）。デフォルト値は `""`（root）です。

- `-base-scope {base|onelevel|subtree}`は基本検索範囲を指定します。

  デフォルト値は `subtree`です。

- `-referral-enabled {true|false}`は、LDAP参照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、プライマリLDAPサーバから目的のレコードが参照先のLDAPサーバに存在することを示すLDAP参照応答が返された場合、ONTAP LDAPクライアントは検索要求を他のLDAPサーバに参照できるようになります。デフォルト値は `**false**`です。

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でLDAPクライアント設定を作成します。

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

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

3. LDAPクライアント設定が正常に作成されたことを確認します。

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

例

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

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

次のコマンドでは、署名と封印が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1でldap1という名前の新しいLDAPクライアント設定を作成します。また、LDAPサーバ検出は指定したドメインの特定サイトに制限されます。

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

次のコマンドでは、LDAPリファーラル追跡が必要なLDAPのActive Directoryサーバと連携するために、Storage VM vs1にldap1という名前の新しいLDAPクライアント設定を作成します。

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

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

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

次のコマンドでは、リファーラル追跡を有効にすることで、Storage VM vs1のldap1という名前のLDAPクライアント設定を変更します。

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

LDAPクライアント設定を**ONTAP NFS SVM**に関連付ける

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

開始する前に

- 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
   ```

   > ℹ `vserver services name-service ldap create`コマンドは自動構成検証を実行し、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」という名前のLDAPクライアント設定を使用するように設定します。

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

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

   次のコマンドは、SVM vs1のLDAPサーバを検証します。

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

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

ONTAP NFS SVMのLDAPソースを確認する

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 テーブルに正しく登録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`名前マッピング情報を検索するソースとその順序を指定します。UNIXのみの環境では、このエントリは不要です。名前マッピングは、UNIXとWindowsが混在する環境でのみ必要です。

2. `ns-switch`エントリを必要に応じて更新します：

ネーム サービス スイッチ エントリを更新する場合...	コマンドを入力してください...
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でのKerberos使用によるセキュリティ強化

セキュリティ認証のためにONTAP NFSでKerberosを使用する方法について学習します

Kerberosを使用して強力な認証が実装されている環境では、Kerberos管理者と協力して要件および適切なストレージ システム構成を決定したうえで、SVMをKerberosクライアントとして有効にする必要があります。

次のガイドラインに従う必要があります。

- ONTAP の Kerberos を設定する前に、サイト展開は Kerberos サーバーとクライアント設定のベストプラクティスに従う必要があります。
- 可能であれば、Kerberos 認証が必要な場合は NFSv4 以降を使用してください。

  NFSv3はKerberosと併用できます。ただし、Kerberosのセキュリティ上の利点を完全に享受できるのは、ONTAPでNFSv4以降を導入している環境でのみです。

- 冗長サーバ アクセスを促進するには、同じ SPN を使用してクラスタ内の複数のノード上の複数のデータ LIF で Kerberos を有効にする必要があります。
- SVM で Kerberos が有効になっている場合、NFS クライアント設定に応じて、ボリュームまたは qtree のエクスポートルールに次のいずれかのセキュリティメソッドを指定する必要があります。
  - `krb5`（Kerberos v5 プロトコル）
  - `krb5i`（チェックサムを使用した整合性チェックを備えた Kerberos v5 プロトコル）
  - `krb5p`（プライバシーサービスを備えた Kerberos v5 プロトコル）

Kerberos サーバとクライアントに加えて、 ONTAP が Kerberos をサポートするには、次の外部サービスを設定する必要があります。

- ディレクトリ サービス

  お使いの環境では、Active DirectoryやOpenLDAPなど、SSL/TLS経由でLDAPを使用するように構成され

た安全なディレクトリサービスを使用する必要があります。NISはリクエストがクリアテキストで送信されるため安全ではないので、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は、DNSで正しく解決できる必要があります。

ONTAP SVM上の**NFS Kerberos**構成の**UNIX**権限を確認する

Kerberos では、SVM ルート ボリュームおよびローカル ユーザとグループに対して特定の UNIX 権限を設定する必要があります。

手順

1. SVM ルート ボリュームの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
UNIX権限	755

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

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	ユーザーID	プライマリ グループID	コメント
nfs	500	0	GSS INIT フェーズに必要です。 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。
root	0	0	マウントに必要です。

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

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
daemon	1
root	0

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

ONTAP SVMでNFS Kerberosレルム構成を作成する

ONTAPで環境内の外部Kerberosサーバにアクセスする場合は、まず既存のKerberosレルムを使用するように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てから、 `vserver nfs kerberos realm create`コマンドを使用してSVM上にKerberosレルム設定を作成する必要があります。

開始する前に

認証の問題を回避するため、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サーバにNTPを設定する必要があります。クライアントとサーバ間の時刻差（クロック スキュー）は、認証失敗の一般的な原因です。

手順

1. Kerberos管理者に相談して、 `vserver nfs kerberos realm create`コマンドに指定する適切な構成値を決定してください。
2. SVM に Kerberos レルム設定を作成します：

   ```
   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、SVM vs1のNFS Kerberosレルム設定を作成します。この設定では、Microsoft Active DirectoryサーバをKDCサーバとして使用します。Kerberosレルムは AUTH.EXAMPLE.COM です。Active Directoryサーバの名前は ad-1、IPアドレスは 10.10.8.14 です。許容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、ポート番号は 88（デフォルト）です。コメントは「Microsoft Kerberos config」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SVM vs1のNFS Kerberosレルム設定を作成します。Kerberosレルムは SECURITY.EXAMPLE.COM です。許容クロック スキューは300秒です。KDCサーバのIPアドレスは 10.10.9.1、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、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、ポート番号は464（デフォルト）です。コメントは「UNIX Kerberos config」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"
```

ONTAP SVMのNFS Kerberos許可暗号化タイプを設定する

デフォルトでは、ONTAPはNFS Kerberosの以下の暗号化タイプをサポートしています：DES、3DES、AES-128、AES-256。 `vserver nfs modify`コマンドに `-permitted-enc-types`パラメータを指定することで、各SVMで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。

タスク概要

クライアントの互換性を最大にするために、ONTAPでは弱い暗号化のDESと強い暗号化のAESの両方をデフォルトでサポートしています。たとえば、セキュリティの強化が必要な環境でAES暗号化がサポートされている場合、ここに記載する手順を使用してDESと3DESを無効にし、クライアントにAES暗号化の使用を必須にすることができます。

利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、これは AES-256 です。この暗号化レベルがお使いの環境でサポートされているかどうかは、KDC 管理者にご確認ください。

- 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操作では、元のDESプリンシパル / keytabファイルが破棄され、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ため、システムの停止を伴います。

  この変更を行う前に、NFSクライアントがSVMのAES暗号化に依存しないことを確認しておく必要があります。

- DES または 3DES を有効化または無効化する場合、LIF 上の Kerberos 設定を変更する必要はありません。

手順

1. 許可される暗号化タイプを有効または無効にします。

有効または無効にする場合は...	次の手順に従ってください。
DESまたは3DES	a. SVMのNFS Kerberos許可暗号化タイプを設定します：+ `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 複数の暗号化タイプ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場合は...	次の手順に従ってください。
AES-128またはAES-256	a. どの SVM および LIF で Kerberos が有効になっているかを特定します：+ `vserver nfs kerberos interface show` b. 変更する NFS Kerberos 許可暗号化タイプの 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許可暗号化タイプを設定します：+ `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` 複数の暗号化タイプ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`

ONTAP LIFで**NFS Kerberos**を有にする

`vserver nfs kerberos interface enable`コマンドを使用して、データLIFでKerberosを有効にすることができます。これにより、SVMはNFSのKerberosセキュリティサービスを使用できるようになります。

タスク概要

Active Directory KDCを使用している場合、使用されるSPNの最初の15文字は、レルム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構成を作成します：

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

   ONTAPでは、Kerberosインターフェイスを有効にするためにKDCからのSPNの秘密キーが必要です。

   Microsoft KDCの場合、KDCに接続し、CLIでユーザー名とパスワードの入力を求めるプロンプトが表示さ

れ、秘密鍵が取得されます。Kerberosレルム内の別のOUにSPNを作成する必要がある場合は、オプションの `-ou`パラメータを指定できます。

Microsoft 以外の KDC の場合、秘密キーは次の 2 つの方法のいずれかで取得できます：

状況	コマンドには次のパラメータも含める必要があります。
KDC から直接キーを取得するための KDC 管理者の資格情報を持っている	`-admin-username` *kdc_admin_username*
KDC管理者のクレデンシャルは持っていないが、キーを含むKDCからのキータブ ファイルを持っている	`-keytab-uri` {ftp

2. LIF上でKerberosが有効になったことを確認します。

   ```
   vserver nfs kerberos-config show
   ```

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

例

次のコマンドは、OU lab2ou内のSPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COMを使用して、論理インターフェイスves03-d1上のvs1という名前のSVMのNFS Kerberos設定を作成し、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対応SVMへのストレージ容量の追加

ONTAP NFS対応SVMにストレージ容量を追加する方法について学習します

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。

開始する前に

- NFS は SVM 上で完全に設定され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 ポリシーには、すべてのクライアントへのアクセスを許可するエクスポート ルールが含まれている必要があります。
- ネーム サービス構成の更新はすべて完了している必要があります。
- Kerberos 構成への追加または変更はすべて完了している必要があります。

ONTAP NFS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、それらを保持するためのエクスポート ポリシーを作成する必要があります。 `vserver export-policy create`コマンドを使用して、エクスポート ポリシーを作成できます。

手順

1. エクスポート ポリシーを作成します。

   ```
   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という名前のSVM上にexp1という名前のエクスポート ポリシーを作成し、その作成を確認します：

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

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

ONTAP NFSエクスポート ポリシーにルールを追加する

ルールがないと、エクスポート ポリシーはクライアントにデータへのアクセスを提供できません。新しいエクスポート ルールを作成するには、クライアントを識別し、クライアントの一致形式を選択し、アクセス タイプとセキュリティ タイプを選択し、匿名ユーザIDマッピングを指定し、ルールのインデックス番号を選択し、アクセス プロトコルを選択する必要があります。その後、 `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 ポリシーに追加できます。

開始する前に

- エクスポート ルールを追加するエクスポート ポリシーを用意しておく必要があります。
- データSVMでDNSが正しく設定され、DNSサーバにNFSクライアントの正しいエントリが必要です。

  これは、ONTAPが特定のクライアント一致形式に対してデータSVMのDNS設定を使用してDNSルックアップを実行し、エクスポート ポリシー ルールの一致に失敗するとクライアント データ アクセスができなくなる可能性があるためです。

- 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`（チェックサムを使用した整合性チェックを備えたKerberos V5プロトコル）
  - `krb5p`（プライバシー サービスを備えたKerberos V5プロトコル）

タスク概要

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を使用して認証し、SVMのすべてのボリュームがKerberos経由でアクセスされる場合は、ルート ボリュームのエクスポート ルール オプション `-rorule`、 `-rwrule`、および `-superuser`を `krb5`、`krb5i`、または `krb5p`に設定できます。

手順

1. クライアント、および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。クライアント一致値は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。一致値は、以下のいずれかの形式で指定できます：

クライアント一致形式	例
「.」で始まるドメイン名	`.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,...`

クライアント一致形式	例
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,...`
@で始まる単一のネットグループ名	`@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ときには、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 アクセスを詳細に管理する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場合、動的に（DHCPなど）または一時的に（IPv6など）割り当てられた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権を失います。

- ff::12/ff::00 などのネットワーク マスク付きのIPv6アドレス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。

   指定されたセキュリティ 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`（root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。スーパーユーザのアクセスの場合も同じです。

   ルールには、複数のセキュリティ タイプをカンマ区切りのリストで指定できます。セキュリティ タイプを `any`または `never`として指定する場合は、他のセキュリティ タイプを指定しないでください。以下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 タイプが次のように設定されている場合：	一致するクライアントは、エクスポートされたデータにアクセスできます...
`any`	受信セキュリティ タイプに関係なく、常にアクセス可能です。
`none`	単独で指定した場合、どのセキュリティ タイプのクライアントにも匿名アクセスが許可されます。他のセキュリティ タイプと一緒に指定した場合、指定したセキュリティ タイプのクライアントにアクセスが許可され、それ以外のセキュリティ タイプのクライアントには匿名アクセスが許可されます。
`never`	受信セキュリティ タイプに関係なく、アクセス不可です。
`krb5`	Kerberos 5によって認証されている場合。認証のみ：各要求と応答のヘッダーが署名されます。
`krb5i`	Kerberos 5i によって認証されている場合。認証と整合性：各リクエストとレスポンスのヘッダーと本文が署名されます。
`krb5p`	Kerberos 5p によって認証されている場合。認証、整合性、およびプライバシー：各要求と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 `sys`、またはKerberosが使用されている場合は `krb5`、 `krb5i`、または `krb5p`です。

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

3. 匿名ユーザIDマッピングを指定します。

`-anon`オプションは、ユーザIDが0（ゼロ）の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に関連付けられます。デフォルト値は `65534`です。NFSクライアントは通常、ユーザID 65534をユーザ名nobody（_root squashing_とも呼ばれます）に関連付けます。ONTAPでは、このユーザIDはユーザ名pcuserに関連付けられます。ユーザIDが0のクライアントによるアクセスを無効にするには、 `65535`を指定します。

4. ルール インデックスの順序を選択します。

`-ruleindex`オプションは、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内の順序に従って評価されます。つまり、インデックス番号が小さいルールが最初に評価されます。たとえば、インデックス番号1のルールは、インデックス番号2のルールよりも先に評価されます。

追加する場合...	操作
最初のルールをエクスポート ポリシーへ	入力 1。
追加のルールをエクスポート ポリシーへ	a. ポリシー内の既存のルールを表示します：+ `vserver export-policy rule show -instance -policyname your_policy` b. 評価する順序に応じて、新しいルールのインデックス番号を選択します。

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

`nfs`任意のバージョンに一致し、 `nfs3`および`nfs4`特定のバージョンのみに一致します。

6. エクスポート ルールを作成して既存のエクスポート ポリシーに追加します。

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

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

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

このコマンドにより、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、SVM vs1 上のエクスポート ポリシー rs1 にエクスポート ルールを作成し、その作成を確認します。このルールのインデックス番号は 1 です。このルールは、ドメイン eng.company.com およびネットグループ @netgroup1 内のすべてのクライアントに一致します。このルールは、すべての NFS アクセスを有効にします。AUTH_SYS で認証されたユーザには、読み取り専用アクセスと読み取り/書き込みアクセスが許可されます。UNIX ユーザ ID が 0（ゼロ）のクライアントは、Kerberos で認証されない限り匿名化されます。

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

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

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

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

次のコマンドは、SVM vs2 上のエクスポート ポリシー expol2 にエクスポート ルールを作成し、その作成を確認します。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 のメンバーに一致させます。このルールはすべての NFS アクセスを有効にします。AUTH_SYS で認証されたユーザには読み取り専用アクセスを許可し、読み取り/書き込みアクセスとルート アクセスには Kerberos 認証が必要です。UNIX ユーザ ID が 0（ゼロ）のクライアントは、Kerberos で認証されない限り、ルート アクセスを拒否されます。

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

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

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

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

ボリュームまたは**qtree**のストレージ コンテナの作成

ONTAP NFSボリュームを作成する

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

タスク概要

ボリュームのデータをクライアントが利用できるようにするには、ボリュームに_ジャンクション パス_が必要です。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、 `volume mount`コマンドを使用してSVMネームスペースにボリュームを_マウント_する必要があります。

開始する前に

- NFS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トラッキングを有効にした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、 `-analytics-state`または `-activity-tracking-state`を `on`に設定した `volume create`コマンドを発行します。

容量分析とアクティビティ追跡の詳細については、 "ファイルシステム分析の有効化"を参照してください。"ONTAPコマンド リファレンス"の `volume create`の詳細を確認してください。

手順

1. ジャンクション ポイントを設定してボリュームを作成します。

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

   `-junction-path`の選択肢は次のとおりです：

   - たとえばルートの直下には、 */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（例： */new_dir/new_vol*）、まず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する必要があります。次に、新しい親ボリューム（新しいディレクトリ）のジャンクションパスに新しい子ボリュームを作成します。

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

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とアグリゲートaggr1上にusers1という新しいボリュームを作成します。この新しいボリュームは `/users`で利用可能になります。ボリュームのサイズは750GBで、ボリュームギャランティはvolume（デフォルト）です。

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

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

次のコマンドは、SVM「vs1.example.com」とアグリゲート「aggr1」上に「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SVM vs1のネームスペース内に既に存在しており、新しいボリュームは `/eng/home`で利用可能になります。これは `/eng/`ネームスペースのホームディレクトリになります。ボリュームのサイズは750 GB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 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
```

ONTAP NFS qtreeを作成する

`volume qtree create`コマンドを使用して、データを格納するqtreeを作成し、そのプロパティを指定できます。

開始する前に

- 新しいqtreeを格納するSVMと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ことも、`/vol/*volume_name/_qtree_name*`の形式でqtreeパス引数を指定することもできます。

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、独自のポリシー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の作成時に指定できます。また、 `volume qtree modify`コマンドを使用して後からエクスポート ポリシーを追加することもできます。

2. 目的のジャンクション パスで qtree が作成されたことを確認します：

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

例

次の例では、ジャンクション パス `/vol/data1`を持つSVM vs1.example.comにあるqt01という名前のqtreeを作成します：

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

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

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

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポートポリシーを使用して **ONTAP NFS** アクセスを保護する方法について学習します。

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かを選択できます。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、ルール違反をエラールールリストに記録できるようになりました。`vserver export-policy config-checker`コマンドはチェッカーを起動して結果を表示し、設定を検証してポリシーからエラーのあるルールを削除するために使用できます。コマンドは、ホスト名、ネットグループ、および匿名ユーザーのエクスポート設定のみを検証します。

ONTAP NFSエクスポート ルールの処理順序を管理する

`vserver export-policy rule setindex`コマンドを使用して、既存のエクスポート ルールのインデックス番号を手動で設定できます。これにより、ONTAPがクライアント要求にエクスポート ルールを適用する優先順位を指定できます。

タスク概要

新しいインデックス番号がすでに使用されている場合、コマンドは指定された場所にルールを挿入し、それに応じてリストの順序を変更します。

手順

1. 指定されたエクスポート 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上のrs1というエクスポート ポリシー内のインデックス番号3のエクスポート ルールのインデックス番号をインデックス番号2に変更します：

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

ONTAP NFSエクスポート ポリシーをボリュームに割り当てる

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

タスク概要

ボリュームの作成時、または作成後いつでも、ボリュームにエクスポート ポリシーを関連付けることができます。1つのエクスポート ポリシーをボリュームに関連付けることができますが、1つのポリシーを複数のボリュームに関連付けることもできます。

手順

1. ボリュームの作成時にエクスポート ポリシーが指定されていなかった場合は、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 SVM vs1 上のボリューム vol1 に割り当て、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
```

ONTAP NFS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、ボリューム上の特定の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 ポリシーは、新しいqtreeの作成時に割り当てることも、既存のqtreeを変更して割り当てることもできます。

開始する前に

エクスポート ポリシーが存在する必要があります。

タスク概要

デフォルトでは、qtree は作成時に特に指定しない限り、それを含むボリュームの親エクスポート ポリシーを継承します。

qtreeの作成時、またはqtreeの作成後いつでも、エクスポート ポリシーをqtreeに関連付けることができます。1つのエクスポート ポリシーをqtreeに関連付けることができますが、1つのポリシーを複数のqtreeに関連付けることもできます。

手順

1. qtreeの作成時にエクスポート ポリシーが指定されていなかった場合は、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 SVM vs1 上の qtree qt1 に割り当て、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**ONTAP NFS**クライアント アクセスを確認する

UNIX管理ホスト上でUNIXファイル権限を設定することで、特定のクライアントに共有へのアクセスを許可できます。 `vserver export-policy check-access`コマンドを使用してクライアントのアクセスを確認し、必要に応じてエクスポート ルールを調整できます。

手順

1. クラスター上で、 `vserver export-policy check-access`コマンドを使用してエクスポートへのクライアント アクセスを確認します。

   次のコマンドは、IPアドレス1.2.3.4を持つNFSv3クライアントのボリュームhome2への読み取り / 書き込みアクセスを確認します。コマンド出力には、ボリュームがエクスポート ポリシー `exp-home-dir`を使用しており、アクセスが拒否されていることが示されています。

   ```
   cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
   1.2.3.4 -volume 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. 出力を調べて、エクスポート ポリシーが意図したとおりに機能し、クライアント アクセスが期待どおりに動作するかどうかを確認します。

   具体的には、ボリュームまたはqtreeで使用されているエクスポート ポリシーと、その結果クライアントが持つアクセス 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 ルールを再構成します。

クライアント システムからのONTAP NFSアクセスをテストする

新しいストレージ オブジェクトへのNFSアクセスを確認したら、NFS管理ホストにログインし、SVMとの間でデータの読み取りと書き込みを実行して設定をテストする必要があります。その後、クライアント システム上で非rootユーザとしてこのプロセスを繰り返します。

開始する前に

- クライアント システムには、先ほど指定したエクスポート ルールで許可されているIPアドレスが必要です。
- rootユーザのログイン情報が必要です。

手順

1. クラスター上で、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`

   `network interface show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

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 フォルダーに変更します：

   `cd /mnt/`

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

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

   b. 新しいボリュームをこの新しいディレクトリにマウントします：+ `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`

      次のコマンドは、test1という名前のフォルダを作成し、test1マウント フォルダのIPアドレス192.0.2.130にvol1ボリュームをマウントし、新しいtest1ディレクトリに変更します：

```
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、それが存在することを確認して、そこに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てください：+ `ls -l filename`

c. 入力：+ `cat > filename`

   テキストを入力し、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る：+ `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必要な UNIX 所有権と権限を設定します。
7. エクスポート ルールで識別された 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承認済みユーザーの 1 人としてログインし、手順 3 ～ 5 を繰り返して、ボリュームをマウントしてファイルを作成できることを確認します。

ONTAP NFSの追加情報はどこで入手できますか

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

NFSの設定

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

- "NFSの管理"

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

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

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

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

  NFSストレージ認証用にUNIXベースのKerberosバージョン5（krb5）サーバを使用する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）を使用するための設定方法について説明しています。

- "NetApp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。

ネットワークの設定

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、次に示す情報やテクニカル レポートを参照してください。

- "NFSの管理"

  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。

- "NetAppテクニカルレポート4182：クラスタ化されたData ONTAP構成におけるイーサネットストレージ設計の考慮事項と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。

- "NetApp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 ファイルの構成を設定する方法について説明しています。

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の設定に関する情報を参照してください。各種のホスト オペレーティング システムに対応した情報が用意されています。

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NetAppのベストプラクティスです。また、SVMルート ボリュームを負荷共有ミラーから昇格させてボリュームの障害や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 が NFS エクスポートを実装する方法がよくわからない場合は、7-Mode と

ONTAP のエクスポート構成ツール、およびサンプルの 7-Mode `/etc/exports` ファイルとクラスタ化されたポリシーおよびルールを比較できます。

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

関連情報

"NFSの管理"

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

7-ModeとONTAP NFSエクスポートの比較について学ぶ

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 `/etc/exports`ファイルで定義されます。	エクスポートは、SVM内でエクスポート ポリシーを作成することによって定義されます。1つのSVMに複数のエクスポート ポリシーを含めることができます。
エクスポートの範囲	• エクスポートは指定したファイル パスまたはqtreeに適用されます。 • ファイル パスまたはqtreeごとに、 `/etc/exports`で個別のエントリを作成する必要があります。 • エクスポートは、 `/etc/exports`ファイルで定義されている場合にのみ永続的です。	• エクスポート ポリシーは、ボリューム内のすべてのファイル パスおよび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、`/etc/exports`ファイルに各クライアントとその許可されたアクセスをリストする必要があります。	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リストされます。特定のクライアントに対して別のアクセスを指定するには、アクセス権限の特定のセットごとにエクスポート ルールを作成し、該当するアクセス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際に、エクスポート名をファイルパス名と異なる名前にすることができます。 `/etc/exports`ファイル内でこのようなエクスポートを定義する場合は、 `-actual`パラメータを使用する必要があります。	エクスポートしたボリュームの名前を実際のボリューム名と異なる名前にすることもできます。これを行うには、SVMネームスペース内でカスタムジャンクションパス名を使用してボリュームをマウントする必要があります。 デフォルトでは、ボリュームは本来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、マウントを解除し、名前を変更してから、再マウントする必要があります。

ONTAPのNFSエクスポート ポリシーの例について学ぶ

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 ポリシーの動作をより深く理解できます。

7-ModeエクスポートのONTAP実装例

次の例は、 `/etc/export`ファイルに表示される7-Modeエクスポートを示しています：

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

このエクスポートをクラスター化されたエクスポート 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。

Rule	要素	Value
ルール1	-clientmatch（クライアント仕様）	@readonly_netgroup
-ruleindex(ルールリスト内のエクスポート ルールの位置)	1	-protocol
nfs	-rorule（読み取り専用アクセスを許可）	sys（AUTH_SYSで認証されたクライアント）
-rwrule（読み書きアクセスを許可）	never	-superuser（スーパーユーザ アクセスを許可）
none（rootは匿名にスカッシュされます）	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. ベース コマンドに次のパラメータを使用して 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例

次の例は、10 個の qtree ごとに 1 行が含まれる 7-Mode `/etc/export` ファイルを示しています：

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

ONTAPでは、各qtreeに2つのポリシーのいずれかが必要です： `-clientmatch host1519s`を含むルールを持つポリシー、または `-clientmatch host2057s`を含むルールを持つポリシーです。

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. qtree にポリシーを適用します。
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [次の 4 つの qtree…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [次の 4 つの qtree…]

後でこれらのホストに qtree を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。