



CLI で NFS を設定

ONTAP 9

NetApp
April 24, 2024

目次

CLI で NFS を設定	1
CLI を使用した NFS の設定の概要	1
NFS の設定ワークフロー	1
準備	2
SVM への NFS アクセスを設定	14
NFS 対応 SVM にストレージ容量を追加	51
追加情報の参照先	65
ONTAP エクスポートと 7-Mode エクスポートの違い	66

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。

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

関連情報

["ONTAP の概念"](#)

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。 <div>  <p>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。</p> </div>	
-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）。	

• 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
<code>-lif</code>	新しい LIF の名前を指定します。	
<code>-role</code>	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
<code>-data-protocol</code>	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
<code>-home-node</code>	でLIFが戻るノードを指定します <code>network interface revert</code> LIFに対してコマンドを実行します。	
<code>-home-port</code>	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 <code>network interface revert</code> LIFに対して コマンドを実行します。	
<code>-address</code>	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。	
<code>-netmask</code>	LIF のネットワークマスクとゲートウェイを指定します。	
<code>-subnet</code>	IP アドレスのプール。の代わりに使用されます <code>-address</code> および <code>-netmask</code> アドレスとネットワークを自動的に割り当てます。	
<code>-firewall-policy</code>	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
<code>-domain</code>	SVM で名前検索に使用される NIS ドメインを指定します。	
<code>-active</code>	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
<code>-servers</code>	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。	
<code>-nis-servers</code>	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
<code>-vserver</code>	LDAP クライアント設定を作成する SVM の名前を指定します。	
<code>-client-config</code>	新しい LDAP クライアント設定に割り当てる名前。	

フィールド	説明	あなたの価値
-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
-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。	

フィールド	説明	あなたの価値
-use-start-tls	LDAP over TLS を有効にします。 デフォルトは 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
<code>-vserver</code>	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。	
<code>-volume</code>	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。	
<code>-aggregate</code>	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ー内のアグリゲートの名前を指定します。	
<code>-size</code>	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。	
<code>-user</code>	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。	
<code>-group</code>	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。	
<code>--security-style</code>	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
<code>-junction-path</code>	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。	
<code>-export-policy</code>	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

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 vservice_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 *	<code>network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>

-subnet-name <i>subnet_name</i> } -firewall-policy data -auto-revert {true	false}`
• ONTAP 9.6 以降 *	`network interface create -vserver <i>vserver_name</i> -lif <i>lif_name</i> -role data -data-protocol nfs -home-node <i>node_name</i> -home-port <i>port_name</i> {-address <i>IP_address</i> -netmask <i>IP_address</i>
-subnet-name <i>subnet_name</i> } -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のル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化したとき、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	<code>network ping</code>
IPv6アドレス	<code>network ping6</code>

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 elc -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 elc -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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	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
node-2					
true	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
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c
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 vsriver 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
```

Vserver	State	Domains	Name 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るホスト、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

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|https|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`。

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|https|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`。このパラメータを指定した場合 `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、外部名前サーバ（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 vs1 -source
{ftp|http|https|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 チャン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 接続でチャンネルバインドを試行します。ネームサーバとの LDAP チャン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 チャン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 リファラー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 リファラー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 vservice_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、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`。

- 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
- 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|sas1}` 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 `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 **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 `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。

- `-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 リファラール追跡を有効にした場合など)。デフォルト値は `""` (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 `subtree`。

- `-referral-enabled {true|false}` LDAPリファー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 vs1 -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::> vservice 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::> vservice 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::> vservice 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::> vservice 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 vservice 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: cl |  
| 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
```

Vserver	Database	Source
-----	-----	-----
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	<code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>
グループ情報	<code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>
ネットグループ情報	<code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code>

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	<p>a. SVMのNFS Kerberosで許可される暗号化タイプを設定します。[+] <code>vserver nfs modify -vserver vserver_name -permitted -enc-types encryption_types</code></p> <p>暗号化タイプが複数ある場合はカンマで区切ります。</p> <p>b. 変更が成功したことを確認します。[+] <code>vserver nfs show -vserver vserver_name -fields permitted-enc-types</code></p>
AES-128またはAES-256	<p>a. Kerberosが有効になっているSVMとLIFを特定します。[+] <code>vserver nfs kerberos interface show</code></p> <p>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。[+] <code>vserver nfs kerberos interface disable -lif lif_name</code></p> <p>c. SVMのNFS Kerberosで許可される暗号化タイプを設定します。[+] <code>vserver nfs modify -vserver vserver_name -permitted -enc-types encryption_types</code></p> <p>暗号化タイプが複数ある場合はカンマで区切ります。</p> <p>d. 変更が成功したことを確認します。[+] <code>vserver nfs show -vserver vserver_name -fields permitted-enc-types</code></p> <p>e. SVM上のすべてのLIFでKerberosを再度有効にします。[+] <code>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</code></p> <p>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。[+] <code>vserver nfs kerberos interface show</code></p>

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

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	<code>-admin-username kdc_admin_username</code>
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	<code>-keytab-uri {ftp</code>

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 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。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 of 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	<code>.example.com</code> または <code>.example.com, .example.net, ...</code>
ホスト名	<code>host1</code> または <code>host1, host2, ...</code>
IPv4 アドレス	<code>10.1.12.24</code> または <code>10.1.12.24, 10.1.12.25, ...</code>
サブネットマスクをビット数で表した IPv4 アドレス	<code>10.1.12.10/4</code> または <code>10.1.12.10/4, 10.1.12.11/4, ...</code>
IPv4 アドレスとネットワークマスク	<code>10.1.16.0/255.255.255.0</code> または <code>10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0, ...</code>
ピリオド区切りの形式の IPv6 アドレス	<code>::1.2.3.4</code> または <code>::1.2.3.4, ::1.2.3.5, ...</code>
サブネットマスクをビット数で表した IPv6 アドレス	<code>ff::00/32</code> または <code>ff::00/32, ff::01/32, ...</code>
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	<code>@netgroup1</code> または <code>@netgroup1, @netgroup2, ...</code>

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
<code>any</code>	受信セキュリティタイプに関係なく、常に実行されます。
<code>none</code>	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せん。
<code>never</code>	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。
<code>krb5</code>	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。
<code>krb5i</code>	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。
<code>krb5p</code>	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。
<code>ntlm</code>	CIFS NTLM によって認証されます。

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
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	<p>a. ポリシー内の既存のルールを表示します。[+] <code>vserver export-policy rule show -instance -policyname <i>your_policy</i></code></p> <p>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。</p>

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せん。

```
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 Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	exp1	1	nfs	eng.company.com, @netgroup1	sys

```
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。この規則のインデックス番号は21です。この規則は、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::> vsserver 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::> vsserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs2	expol2	21	nfs	@dev_netgroup_main	sys

```
vs2::> vsserver 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
```

Vserver	Volume	Active	Junction Path	Junction 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
```

Vserver	Volume	Active	Junction Path	Junction 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 vs1.example.com { -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 vs1.example.com { -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 -vserver 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 -vserver 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
```

Path	Policy	Policy Owner	Policy Owner Type	Rule 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

ーネッ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。

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	<ul style="list-style-type: none"> 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。 	<ul style="list-style-type: none"> 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。	<p>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。</p> <div>  <p>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。</p> </div>
------------	--	--

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)

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

1. exp_vol1 というエクスポートポリシーを作成します。

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

2. 基本コマンドに対して、次のパラメータを指定して 3 つのルールを作成します。

- 基本コマンド： `[+] vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
- ルールパラメータ： `[] -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none` [] -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys [+] -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`

3. ボリューム vol1 にポリシーを割り当てます。

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

7-Mode エクスポートの統合の例

次の例は、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。

- vservers export-policy create -vservers NewSVM -policyname exp_vol1q1
- vservers export-policy create -vservers NewSVM -policyname exp_vol1q2

2. 各ポリシーのルールを作成します。

- vservers export-policy rule create -vservers NewSVM -policyname exp_vol1q1
-clientmatch host1519s -rwrule sys -superuser sys
- vservers export-policy rule create -vservers 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 -vservers NewSVM -qtree-path /vol/vol1/q_1472 -export
-policy exp_vol1q1
- [続く 4 つの qtree ...]
- volume qtree modify -vservers 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。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。