CLIを使用したNFSの設定

ONTAP 9

NetApp
December 20, 2024

目次

CLIを使用したNFSの設定

CLIを使用したNFSの設定 - 概要

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

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

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

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

- すべての選択肢について検討するのではなく、ベストプラクティスに従う。

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

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

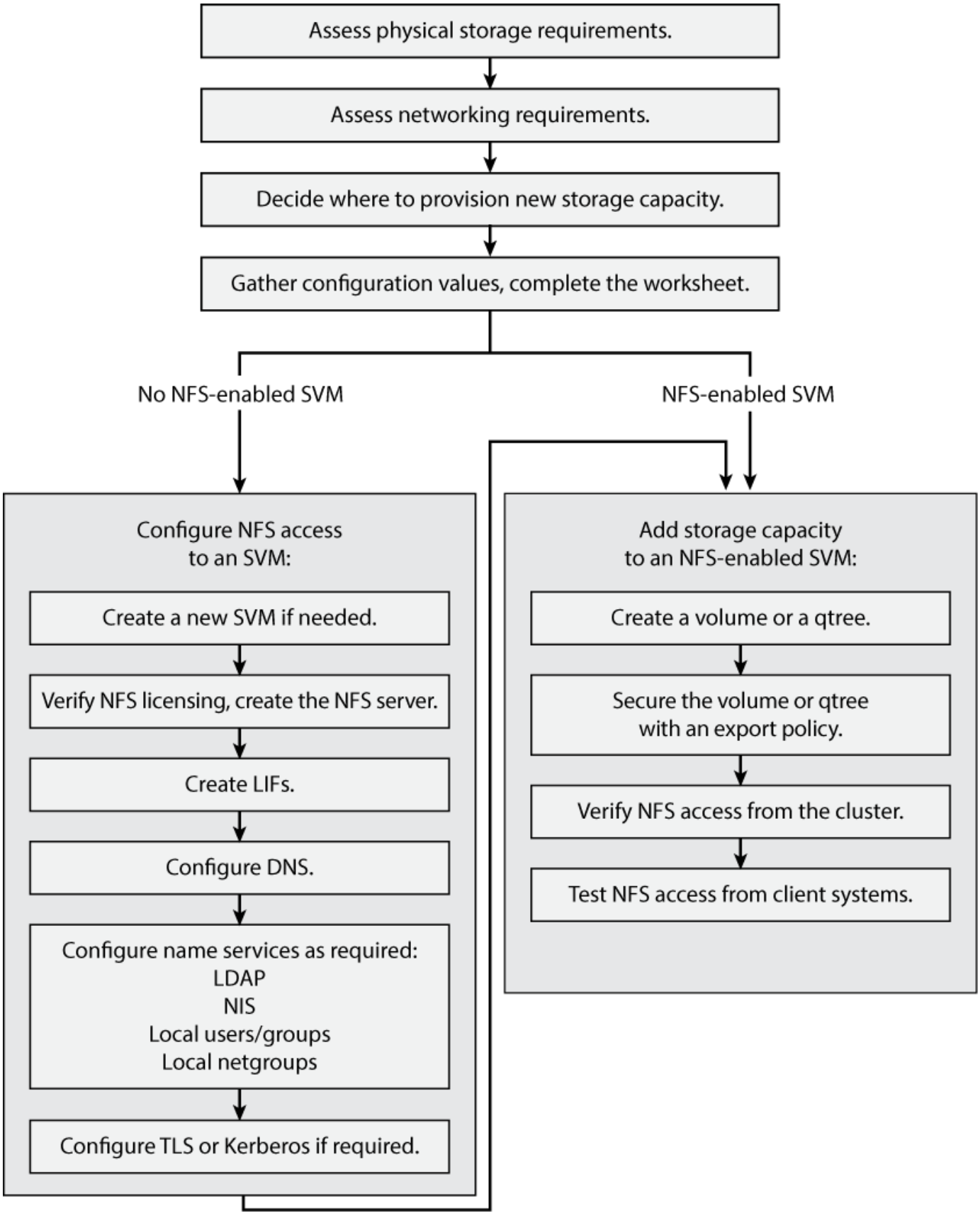
ONTAP NFSプロトコルの機能の範囲の詳細については、を参照して"NFSリファレンスの概要"ください。

ONTAPで実行するその他の方法

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

NFSの設定ワークフロー

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


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

準備

物理ストレージ要件の評価

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

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

   ```
   storage aggregate show
   ```

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

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

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

ネットワーク要件の評価

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

必要なもの

次のクラスタネットワークオブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャストドメイン

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

手順

1. 使用可能な物理ポートと仮想ポートを表示します。

   ```
   network port show
   ```

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

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

   ```
   network subnet show
   ```

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

3. 使用可能なIPspaceを表示します。

   ```
   network ipspace show
   ```

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

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

   ```
   network options ipv6 show
   ```

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

新しい**NFS**ストレージ容量のプロビジョニング先の検討

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

選択肢

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

  SVMへのNFSアクセスの設定

  NFS対応SVMへのNFSストレージの追加

次のいずれかに該当する場合は、新しいSVMを作成します。

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

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

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

  NFS対応SVMへのストレージ容量の追加

NFS設定情報を収集するためのワークシート

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

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

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

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

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

- NFS対応SVMへのストレージ容量の追加

SVMへの**NFS**アクセスの設定

- SVM を作成するためのパラメータ *

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

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

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

* NFS サーバ作成用のパラメータ *

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

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

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

* NFS接続のTLS暗号化を有効にするパラメータ*

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

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

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

- LIF 作成用のパラメータ *

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

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

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

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

- DNS ホスト名解決のパラメータ *

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

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

ネームサービス情報

- ローカルユーザー作成用のパラメータ *

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

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

• ローカルグループを作成するためのパラメータ *

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

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

• NISのパラメータ*

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

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

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

• LDAPのパラメータ*

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

また、自己署名ルートCA証明書ファイルも必要 `.pem`です。

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

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

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

- Kerberos 認証のパラメータ *

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

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

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

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

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

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 *

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

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

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

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

エクスポート ポリシーごとにルールを1つ以上作成する必要があります。

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

2					
3					
…					
n					

* ボリュームを作成するためのパラメータ *

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

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

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

- qtree を作成するためのパラメータ *

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

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

関連情報

- "ONTAPコマンド リファレンス"

SVMへのNFSアクセスの設定

SVMの作成

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

開始する前に

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

管理。

手順

1. SVMを作成します。

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

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

2. 新しく作成したSVMの設定とステータスを確認します。

   ```
   vserver show -vserver vserver_name
   ```

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

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

例

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

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

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

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されて状態になっていることを示しています running。ルートボリュームには、ルールが含まれていないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

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

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

SVMでNFSプロトコルが有効になっていることの確認

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

タスクの内容

この作業は通常、SVMのセットアップ時に実行します。ただし、セットアップ時にプロトコルを有効にしなかった場合でも、コマンドを使用してあとから有効にすることができます `vserver add-protocols`。

作成したプロトコルは、 LIF から追加または削除することはできません。

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

手順

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

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

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

2. 必要に応じて、プロトコルを有効または無効にします。
   - NFSプロトコルを有効にするには+ `vserver add-protocols -vserver vserver_name -protocols nfs`
   - プロトコルを無効にするには：+ `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,…]`
3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。

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

例

次のコマンドは、 vs1 という SVM で現在有効 / 無効（許可 / 不許可）になっているプロトコルを表示します。

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

次のコマンドは、vs1というSVMで有効になっているプロトコルのリストにを追加することで、NFS経由のアクセスを許可し `nfs`ます。

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

SVMルートボリュームのエクスポートポリシーを開く

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

タスクの内容

新しいSVMが作成されると、デフォルトのエクスポートポリシー（default）がSVMのルートボリュームに対して自動的に作成されます。SVM上のデータにクライアントからアクセスできるようにするには、デフォルトのエクスポートポリシーのルールを1つ以上作成する必要があります。

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

手順

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

   `vserver export-policy rule show`

   次のようなコマンド出力が表示されます。

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

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

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

2. SVM ルートボリュームのエクスポートルールを作成します。

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

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

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

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

結果

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

NFSサーバを作成する

クラスタでNFSのライセンスが有効であることを確認したら、コマンドを使用してSVMにNFSサーバを作成し、サポートするNFSのバージョンを指定できます `vserver nfs`

create。

タスクの内容

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

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

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

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

開始する前に

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

手順

1. クラスタ上でNFSのライセンスが有効であることを確認します。

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

   サポートされていない場合は、営業担当者にお問い合わせください。

2. NFSサーバを作成します。

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

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

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

   - `-v4-id-domain`

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

   - `-v4-numeric-ids`

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

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

3. NFSが実行されていることを確認します。

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

4. NFSが必要に応じて設定されていることを確認します。

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

例
次のコマンドは、 NFSv3 と NFSv4.0 が有効な vs1 という名前の SVM 上に NFS サーバを作成します。

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

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

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

vs1::> vserver nfs show -vserver vs1

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

LIFの作成

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

必要なもの

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

がすでに存在している必要があります。

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

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

タスクの内容

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

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

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

手順

1. LIFを作成します。

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

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

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

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

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

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

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

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

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

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

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

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

3. 設定したIPアドレスに到達できることを確認します。

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

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

   これらの各LIFでKerberosを個別に有効にする必要があります。

例

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

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

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

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

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

```
network interface show

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

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

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

ホスト名解決のための**DNS**の有効化

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

解決されます。

必要なもの

ホスト名検索にサイト規模のDNSサーバが使用できる必要があります。

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

タスクの内容

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

手順

1. SVMでDNSを有効にします。

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

   次のコマンドは、vs1というSVMで外部DNSサーバを有効にします。

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

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

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

   次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

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

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

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

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

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

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

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

ネームサービスを設定する

ネームサービスの設定の概要

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

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

ネームサービス情報は、すべてのソースで同期を維持する必要があります。

ネームサービススイッチテーブルを設定する

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

必要なもの

ホスト、ユーザ、グループ、ネットグループ、またはネームマッピングで現在の環境に該当するように使用するネームサービスを決定しておく必要があります。

ネットグループの使用を計画する場合、ネットグループ内に指定されているすべての IPv6 アドレスは、 RFC 5952 での指定どおりに短縮および圧縮されている必要があります。

タスクの内容

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

手順

1. ネームサービススイッチテーブルに必要なエントリを追加します。

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

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

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

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

例

次の例は、 SVM vs1 がローカルネットグループファイルを使用し、外部 NIS サーバがネットグループ情報をこの順序で検索するように、ネームサービススイッチテーブルに新しいエントリを作成します。

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

終了後

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

  ネームサービススイッチテーブルからネームサービスを削除しないと、ストレージシステムへのクライアントアクセスが想定どおりに機能しない場合があります。

ローカル**UNIX**ユーザおよびグループの設定

ローカル**UNIX**ユーザおよびグループの設定の概要

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

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

ローカル**UNIX**ユーザを作成する

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

ステップ

1. ローカル UNIX ユーザを作成します。

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

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

   `-id *integer*`割り当てるユーザIDを指定します。

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

例

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

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

URIからローカル**UNIX**ユーザをロードします。

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

手順

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

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

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

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

サポートされる最大ファイルサイズは 2.5MB です。

2. リストに重複した情報が含まれていないことを確認します。

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

3. ファイルをサーバにコピーします。

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

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

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

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

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

例

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

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

ローカル**UNIX**グループを作成する

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

ステップ

1. ローカル UNIX グループを作成します。

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

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

   `-id *integer*`割り当てるグループIDを指定します。

例

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

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

ローカル**UNIX**グループにユーザを追加する

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

ステップ

1. ローカル UNIX グループにユーザを追加します。

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

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

例

次のコマンドは、 vs1 という SVM の eng というローカル UNIX グループに、 max という名前のユーザを追加します。

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

URIからローカル**UNIX**グループをロードする

個 々 のローカルUNIXグループを手動で作成する別の方法として、コマンドを使用して、ローカルUNIXグループのリストをUniform Resource Identifier（URI）からSVMにロードすることができます `vserver services name-service unix-group load-from-uri`。

手順

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

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

   `group_name: password: group_ID: comma_separated_list_of_users`

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

   サポートされる最大ファイルサイズは 1MB です。

グループファイルの 1 行の最大長は、 32 、 768 文字です。

2. リストに重複した情報が含まれていないことを確認します。

   重複するエントリがリストに含まれていてはいけません。含まれていると、リストのロードに失敗します。SVMにすでにエントリがある場合は、パラメータをに `true`設定して既存のエントリをすべて新しいファイルで上書きするか、新しいファイルに既存のエントリと重複するエントリが一切含まれないようにする必要があります `-overwrite`。

3. ファイルをサーバにコピーします。

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

4. ファイルの URI を確認します。

   この URI は、ファイルの場所を示すためにストレージシステムに指定するアドレスです。

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

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

   `-overwrite true false}` は、エントリを上書きするかどうかを指定します。デフォルトはです `false`。このパラメータをに指定する `true`と、ONTAPは、指定したSVMの既存のローカルUNIXグループデータベース全体を、ロードするファイルのエントリで置き換えます。

例

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

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

ネットグループの使用

ネットグループの使用の概要

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

必要なもの

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

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

  さらに、クライアントのIPアドレスに複数のPTRレコードがある場合、それらのホスト名はすべてネットグループのメンバーであり、対応するAレコードを持っている必要があります。

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

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

タスクの内容

ネットグループについては次の処理を実行できます。

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

  検索を実行するための基盤となるサービスは、設定されているネームサービススイッチの順序に基づいて選択されます。

ネットグループを**SVM**にロードする

エクスポートポリシールールでクライアントの照合に使用できる方法の 1 つは、ネットグループにリストされているホストを使用することです。ネットグループは、外部ネームサーバに格納されているネットグループを使用する代わりに、Uniform Resource Identifier（URI）を使用(`vserver services name-service netgroup load`してSVMにロードできます。

必要なもの

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

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

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

- ネットグループファイル内のホスト名に含まれる英文字は、すべて小文字にする必要があります。
- サポートされる最大ファイルサイズは 5MB です。

- ネットグループでサポートされる最大ネストレベルは 1000 です。
- ネットグループファイルでホスト名を定義する際に使用できるのは、プライマリ DNS ホスト名のみです。

  エクスポートへのアクセスに関する問題を回避するために、ホスト名の定義には DNS CNAME やラウンドロビンレコードを使用しないでください。

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

  ホスト / IP の部分のみがサポートされます。

タスクの内容

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

ステップ

1. URI から SVM にネットグループをロードします。

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

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

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

例

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

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

ネットグループの定義のステータスを確認する

SVMにネットグループをロードしたら、コマンドを使用してネットグループの定義のステータスを確認できます `vserver services name-service netgroup status`。これにより、ネットグループの定義が SVM の基盤となるすべてのノードで一貫した状態になっているかどうかを確認することができます。

手順

1. 権限レベルをadvancedに設定します。

   `set -privilege advanced`

2. ネットグループの定義のステータスを確認します。

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

   追加情報をより詳細なビューで表示できます。

3. admin権限レベルに戻ります。

   ```
   set -privilege admin
   ```

例

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

```
vs1::> set -privilege advanced

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

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

NISドメイン設定を作成する

環境でNetwork Information Service（NIS；ネットワーク情報サービス）がネームサービスに使用されている場合は、コマンドを使用して、SVMのNISドメイン設定を作成する必要があります `vserver services name-service nis-domain create`。

開始する前に

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

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

タスクの内容

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

ホスト名解決にNISを使用することはサポートされていません。

手順

1. NISドメイン設定を作成します。

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

   最大10台のNISサーバを指定できます。

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

2. ドメインが作成されたことを確認します。

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

例

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

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

LDAPを使用

LDAPノシヨウホウホウノカイヨウ

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

10.1以降では、チャネルバインドが**ONTAP 9**接続とネームサービス**LDAP**接続の両方でデフォルトでサポートされます。**ONTAP**は、**Start-TLS**または**LDAPS**が有効で、セッションセキュリティが署名または封印のいずれかに設定されている場合にのみ、**LDAP**接続でチャネルバインディングを試行します。ネームサーバと**LDAP**チャネルバインドを無効または再度有効にするには、コマンドでパラメータを **`ldap client modify`**使用し **`-try-channel-binding`**ます。

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

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

    次のセッションセキュリティオプションを使用できます。

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

次の設定はLDAPリファーラル追跡ではサポートされていません。

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

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

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

- ホスト名解決にLDAPを使用することはサポートされていません。

詳細情報

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

新しい**LDAP**クライアントスキーマを作成する

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

タスクの内容

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

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

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

ONTAPが提供するデフォルトのLDAPスキーマは変更できません。新しいスキーマを作成するには、コピーを作成し、それに応じてコピーを変更します。

手順

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

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

2. 権限レベルをadvancedに設定します。

```
set -privilege advanced
```

3. 既存のLDAPクライアントスキーマのコピーを作成します。

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

4. 新しいスキーマを変更し、環境に合わせてカスタマイズします。

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

5. admin権限レベルに戻ります。

```
set -privilege admin
```

LDAPクライアント設定を作成する

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

必要なもの

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

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

手順

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

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

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

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

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

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

b. デフォルトまたはカスタムのLDAPスキーマを指定します。

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

デフォルトのスキーマ：

- MS-AD-BIS

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

- AD-IDMU

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

- AD-SFU

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

- RFC-2307

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

c. バインド値を選択します。

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

  デフォルト値はです **anonymous**。

- `-bind-dn *LDAP_DN*`バインドユーザを指定します。

  Active Directoryサーバの場合は、アカウント（domain\user）またはプリンシパル（user@domain.com）の形式でユーザを指定する必要があります。それ以外の場合は、識別名（CN=user、DC=domain、DC=com）の形式でユーザを指定する必要があります。

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

d. 必要に応じて、セッションセキュリティオプションを選択します。

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

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

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

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

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

  に設定し、LDAPサーバでサポートされている場合、 **`true`**`LDAP`クライアントはサーバへの暗号化された`TLS`接続を使用します。デフォルト値はです **`false`**。このオプションを使用するには、LDAPサーバの自己署名ルートCA証明書をインストールする必要があります。

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

e. ポート、クエリ、およびベースの値を選択します。

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

- `-port *port*`LDAPサーバポートを指定します。

  デフォルト値はです `389`。

Start TLSを使用してLDAP接続を保護する場合は、デフォルトのポート389を使用する必要があります。Start TLSはLDAPのデフォルトポート389経由でプレーンテキスト接続として開始され、その後TLS接続にアップグレードされます。ポートを変更すると、Start TLSが失敗します。

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

  指定できる範囲は1～10秒です。デフォルト値は秒です `3`。

- `-base-dn *LDAP_DN*`ベースDNを指定します。

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

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

  デフォルト値はです `subtree`。

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

す。

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

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

2. Storage VMにLDAPクライアント設定を作成します。

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

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

3. LDAPクライアント設定が正常に作成されたことを確認します。

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

例

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

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

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

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

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

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

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

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

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

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

LDAPクライアント設定を**SVM**に関連付ける

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

必要なもの

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

手順

1. SVMでLDAPを有効にします。

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

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

   次のコマンドは、「vs1」SVMでLDAPを有効にし、「ldap1」LDAPクライアント設定を使用するように

設定します。

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

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

次のコマンドは、SVM vs1のLDAPサーバを検証します。

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

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

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

ネームサービススイッチテーブルで**LDAP**ソースを確認

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

手順

1. 現在のネームサービススイッチテーブルの内容を表示します。

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

次のコマンドは、 SVM My_SVM の結果を表示します。

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

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

2. 必要に応じてエントリを更新し `ns-switch`ます。

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

NFSでKerberosを使用してセキュリティを強化

NFSでKerberos使用によるセキュリティ強化の概要

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

環境が次のガイドラインを満たしている必要があります。

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

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

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

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

- ディレクトリサービス

  Active Directory や OpenLDAP などのセキュアなディレクトリサービスを環境に導入し、 SSL / TLS 経由の LDAP を使用するように設定してください。NIS を使用すると、要求がクリアテキストで送信されセキュアではないため、 NIS は使用しないでください。

- NTP

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

- ドメイン名解決（DNS）

  各UNIXクライアントおよび各SVM LIFについて、KDCのフォワードルックアップゾーンとリバースルックアップゾーンに適切なサービスレコード（SRV）が登録されている必要があります。すべての参加者は、DNSを介して適切に解決できる必要があります。

Kerberos設定の権限の確認

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

手順

1. SVM ルートボリュームについて、関連する権限を表示します。

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

   SVMのルートボリュームを次のように設定しておく必要があります。

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

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

2. ローカル UNIX ユーザを表示します。

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

   SVMで次のUNIXユーザを設定しておく必要があります。

ユーザ名	ユーザID	プライマリグループID	コメント
NFS	500	0	GSS INIT フェーズで必要。 NFSクライアントユーザSPNの最初のコンポーネントがユーザとして使用されます。 NFSクライアントユーザのSPNに対するKerberos-UNIXネームマッピングがある場合は、nfsユーザは必要ありません。
root	0	0	マウントに必要。

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

3. ローカル UNIX グループを表示します。

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

   SVMで次のUNIXグループを設定しておく必要があります。

グループ名	グループID
デーモン	1
root	0

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

NFS Kerberos Realmの設定を作成します。

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

必要なもの

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

手順

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

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

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

   ```
   vserver nfs kerberos realm show
   ```

例

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

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

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

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

NFS Kerberosで許可される暗号化タイプの設定

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

タスクの内容

クライアントの互換性を最大限に高めるために、ONTAPはデフォルトで弱いDES暗号化と強いAES暗号化の両方をサポートしています。つまり、たとえば、セキュリティを強化する必要があり、環境でサポートされている場合は、この手順を使用してDESと3DESを無効にし、クライアントにAES暗号化のみの使用を要求できます。

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

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

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

- DES や 3DES の有効化または無効化は、 LIF での Kerberos 設定の変更を一切必要としません。

ステップ

1. 許可されている暗号化タイプを有効または無効にします。

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

有効または無効にする対象	実行する手順
AES-128またはAES-256	a. Kerberosが有効になっているSVMとLIFを特定します。+ `vserver nfs kerberos interface show` b. 変更対象のNFS Kerberosで許可されている暗号化タイプが設定されているSVM上のすべてのLIFでKerberosを無効にします。+ `vserver nfs kerberos interface disable -lif lif_name` c. SVMのNFS Kerberosで許可されている暗号化タイプを設定します。+ `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` 暗号化タイプが複数ある場合はカンマで区切ります。 d. 変更が成功したことを確認します。+ `vserver nfs show -vserver vserver_name -fields permitted-enc-types` e. SVM上のすべてのLIFでKerberosを再度有効にします。+ `vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name` f. すべてのLIFでKerberosが有効になっていることを確認します。+ `vserver nfs kerberos interface show`

データ**LIF**で**Kerberos**を有効にする

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

タスクの内容

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

手順

1. NFS Kerberos 設定を作成します。

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

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

す。

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

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

状況	コマンドとともに含める必要のあるパラメータ
KDC からキーを直接取得するための KDC 管理者のクレデンシャルが必要です	`-admin-username` *`kdc_admin_username`*
KDC 管理者のクレデンシャルはないが、キーが含まれている、 KDC の keytab ファイルはある	`-keytab-uri {ftp`

2. LIFでKerberosが有効になったことを確認します。

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

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

例

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

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

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

NFSでTLSを使用したセキュリティ強化

NFSでのTLSを使用したセキュリティ強化の概要

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

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

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

ONTAPでは、TLS経由のNFS接続にTLS 1.3が使用されます。

要件

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

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

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

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

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

TLSを有効にする

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

開始する前に

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

手順

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

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

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

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

```
vserver nfs tls interface show
```

例

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

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

```
vserver nfs tls interface show
```

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

TLSの無効化

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

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

開始する前に

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

手順

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

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

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

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

```
vserver nfs tls interface show
```

例

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

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

```
vserver nfs tls interface show
```

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

TLS設定の編集

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

開始する前に

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

手順

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

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

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

```
vserver nfs tls interface show
```

例

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

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

```
vserver nfs tls interface show
```

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

NFS対応SVMにストレージ容量を追加する

NFS対応SVMへのストレージ容量の追加の概要

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

必要なもの

- SVMでNFSの設定が完了している必要があります。
- SVM ルートボリュームのデフォルトのエクスポートポリシーに、すべてのクライアントへのアクセスを許可するルールが含まれている必要があります。
- ネームサービス設定に対する更新が完了している必要があります。

- Kerberos 設定への追加または変更が完了している必要があります。

エクスポートポリシーを作成する

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

手順

1. エクスポートポリシーを作成します。

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

   ポリシー名の最大文字数は256文字です。

2. エクスポートポリシーが作成されたことを確認します。

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

例

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

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

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

エクスポートポリシーにルールを追加する

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

必要なもの

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

  その理由は、特定のクライアント照合形式で ONTAP がデータ SVM の DNS 設定を使用して DNS ルックアップを実行することと、エクスポートポリシールールの照合が失敗するとクライアントがデータにアク

セスできなくなる可能性があることです。

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

タスクの内容

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

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

手順

1. 新しいルールのクライアントとクライアント照合形式を特定します。

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

クライアント照合形式	例
先頭に文字が付いたドメイン名	`.example.com`または `.example.com,.example.net,...`
ホスト名	`host1`または `host1,host2, ...`
IPv4アドレス	`10.1.12.24`または `10.1.12.24,10.1.12.25, ...`
サブネット マスクをビット数で表したIPv4アドレス	`10.1.12.10/4`または `10.1.12.10/4,10.1.12.11/4,...`
IPv4アドレスとネットワークマスク	`10.1.16.0/255.255.255.0`または `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
ドット付き形式のIPv6アドレス	`::1.2.3.4`または `::1.2.3.4,::1.2.3.5,...`
サブネットマスクをビット数で表したIPv6アドレス	`ff::00/32`または `ff::00/32,ff::01/32,...`

クライアント照合形式	例
先頭に@文字が付いた単一のネットグループ	`@netgroup1`または `@netgroup1,@netgroup2,...`

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

IPアドレスを指定する場合は、次の点に注意してください。

- 10.1.12.10-10.1.12.70などのIPアドレス範囲を入力することはできません。

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

- クライアントアクセスのきめ細かな管理のためにエクスポートルールで個々の IP アドレスを指定する際には、動的（ DHCP など）または一時的（ IPv6 など）に割り当てられている IP アドレスを指定しないでください。

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

- ff ： 12/ff ： 00 のように、 IPv6 アドレスとネットワークマスクを入力することはできません。

2. クライアント一致のアクセスタイプとセキュリティタイプを選択します。

指定したセキュリティタイプで認証するクライアントには、次のアクセスモードを1つ以上指定できます。

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

> ⓘ 特定のセキュリティタイプの読み取り/書き込みアクセスは、エクスポートルールでそのセキュリティタイプの読み取り専用アクセスも許可されている場合にのみ許可されます。読み取り専用パラメータで読み取り/書き込みパラメータよりも限定的なセキュリティタイプを指定すると、クライアントに対して読み取り/書き込みアクセスが許可されない可能性があります。スーパーユーザアクセスについても同様です。

1つのルールに対して複数のセキュリティタイプをカンマで区切って指定できます。セキュリティタイプとしてまたはを `never`指定する場合は `any`、他のセキュリティタイプは指定しないでください。次の有効なセキュリティタイプから選択します。

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

セキュリティタイプの設定	一致するクライアントからエクスポートされたデータへのアクセス
none	単独で指定した場合、どのセキュリティタイプのクライアントにも匿名アクセスが許可されます。他のセキュリティタイプと一緒に指定すると、指定したセキュリティタイプのクライアントにアクセスが許可され、それ以外のセキュリティタイプのクライアントには匿名アクセスが許可されます。
never	受信セキュリティタイプに関係なく、なし。
krb5	Kerberos 5によって認証されます。認証のみ：各要求および応答のヘッダーが署名されます。
krb5i	Kerberos 5iによって認証されます。認証および整合性：各要求および応答のヘッダーと本文が署名されます。
krb5p	Kerberos 5pによって認証されます。認証、整合性、およびプライバシー：各要求および応答のヘッダーと本文が署名され、 NFS データペイロードが暗号化されます。
ntlm	CIFS NTLMによって認証されます。
sys	NFS AUTH_SYSで認証されます。

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

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

3. 匿名ユーザIDマッピングを指定します。

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

4. ルールインデックスの順序を選択します。

オプションは `-ruleindex`、ルールのインデックス番号を指定します。ルールはインデックス番号のリスト内の順序に従って評価され、インデックス番号が小さいルールが最初に評価されます。たとえば、インデックス番号が1のルールは、インデックス番号が2のルールよりも先に評価されます。

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

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

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

6. エクスポートルールを作成して既存のエクスポートポリシーに追加します。

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

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

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

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

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

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

例

次のコマンドは、 rs1 というエクスポートポリシーで vs1 という SVM に対するエクスポートルールを作成し、作成を確認します。このルールのインデックス番号は1です。このルールは、ドメインeng.company.comおよびネットグループ@netgroup1内のすべてのクライアントに一致します。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザに対する読み取り専用アクセスと読み取り/書き込みアクセスを有効にします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberosで認証されないかぎり匿名化されます。

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

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

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

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

次のコマンドは、 expol2 というエクスポートポリシーで vs2 という SVM に対するエクスポートルールを作成し、作成を確認します。このルールのインデックス番号は21です。このルールは、クライアントをネットグループdev_netgroup_mainのメンバーと照合します。このルールは、すべてのNFSアクセスを有効にします。AUTH_SYSで認証されたユーザの読み取り専用アクセスを有効にし、読み取り/書き込みアクセスとrootアクセスにはKerberos認証を必要とします。UNIXユーザIDが0（ゼロ）のクライアントは、Kerberos以外で認証されないかぎり、ルートアクセスを拒否されます。

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

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

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

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

ボリュームまたは**qtree**のストレージコンテナを作成する

ボリュームの作成

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

タスクの内容

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

開始する前に

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

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

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

手順

1. ジャンクションポイントを設定してボリュームを作成します。

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

   の選択肢は `-junction-path`次のとおりです。

   - ルートの直下。例： */new_vol*

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

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

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

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

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

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

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

例

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

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

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

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

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

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

qtreeを作成する

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

必要なもの

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

手順

1. qtree を作成します。

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

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

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

2. qtree が必要なジャンクションパスで作成されたことを確認します。

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

例

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

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

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

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

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポート ポリシーを使用した**NFS**アクセスの保護

エクスポートポリシーを使用すると、ボリュームまたはqtreeへのNFSアクセスを、特定のパラメータに一致するクライアントだけに制限できます。新しいストレージをプロビジョニングする際に、既存のポリシーとルールを使用するか、既存のポリシーにルールを追加するか、新しいポリシーとルールを作成できます。エクスポートポリシーの設定も確認できます。

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

エクスポートルールの処理順序を管理します。

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

タスクの内容

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

ステップ

1. 指定したエクスポートルールのインデックス番号を変更します。

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

例

次のコマンドは、 vs1 という SVM の rs1 というエクスポートポリシーのインデックス番号を 3 から 2 に変更します。

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

ボリュームへのエクスポートポリシーの割り当て

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

タスクの内容

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

手順

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

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

2. ポリシーがボリュームに割り当てられたことを確認します。

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

例

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

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

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

qtreeへのエクスポートポリシーの割り当て

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

必要なもの

エクスポートポリシーが存在している必要があります。

タスクの内容

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

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

手順

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

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

2. ポリシーが qtree に割り当てられたことを確認します。

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

例

次のコマンドは、エクスポートポリシー nfs_policy を vs1 という SVM 上の qtree qt1 に割り当てて、割り当てを確認します。

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

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

クラスタからの**NFS**クライアントアクセスの確認

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

手順

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

   次のコマンドは、 IP アドレスが 1.2.3.4 の NFSv3 クライアントによるボリューム home2 への読み取り / 書き込みアクセスをチェックします。コマンド出力には、ボリュームでエクスポートポリシーが使用されていること、およびアクセスが拒否されたことが示されています `exp-home-dir`。

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

   3 entries were displayed.
   ```

2. 出力を確認して、エクスポートポリシーが意図したとおりに機能してクライアントアクセスが想定どおりに動作しているかどうかを判断します。

   具体的には、ボリュームまたは qtree によって使用されたエクスポートポリシーと、結果としてクライアントが行ったアクセスのタイプを確認する必要があります。

3. 必要に応じて、エクスポートポリシールールを再設定します。

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

必要なもの

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

手順

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

   `network interface show –vserver svm_name`

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

   `cd /mnt/`

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

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

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

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

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

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

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

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

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

   c. 入力：+ `cat > filename`

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

   d. テストファイルの内容を表示します。+ `cat filename`

e. テストファイルを削除します。+ `rm filename`

f. 親ディレクトリに戻ります。+ `cd ..`

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

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

詳細情報の入手方法

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

NFSの設定

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

- "NFSの管理"

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

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

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

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

  NFSストレージ認証用にUNIXベースのKerberosバージョン5（krb5）サーバを使用し、KDCおよびLightweight Directory Access Protocol（LDAP）のアイデンティティプロバイダとしてWindows Server Active Directory（AD）を使用するようにONTAPを設定する方法について説明します。

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

  ONTAPを実行するシステムに接続されたAIX、Linux、またはSolarisクライアントにおけるコンポーネ

ントを実装する際のベストプラクティスを紹介しています。

ネットワーク構成

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

- "NFSの管理"

  ONTAPネットワークを設定および管理する方法について説明します。

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

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

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

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

SANプロトコルの設定

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

ルートボリュームの保護

SVMでプロトコルを設定したら、ルートボリュームを保護してください。

- "データ保護"

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

ONTAPエクスポートと7-Modeエクスポートの違い

ONTAPエクスポートと7-Modeエクスポートの違い

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

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

関連情報

"NFSの管理"

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

7-ModeトONTAPテノエクスホオトノヒカク

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

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

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

ONTAPエクスポートポリシーの例

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

7-Mode エクスポートの ONTAP 実装例

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

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

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

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

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

1. exp_vol1というエクスポートポリシーを作成します。

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

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

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

7-Mode エクスポートの統合の例

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

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

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

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

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

著作権に関する情報

商標に関する情報