



# SVMへのNFSアクセスの設定

## ONTAP 9

NetApp  
December 20, 2024

# 目次

SVMへのNFSアクセスの設定 .....	1
SVMの作成 .....	1
SVMでNFSプロトコルが有効になっていることの確認 .....	3
SVMルートボリュームのエクスポートポリシーを開く .....	4
NFSサーバを作成する .....	5
LIFの作成 .....	7
ホスト名解決のためのDNSの有効化 .....	11
ネームサービスを設定する .....	13
NFSでKerberosを使用してセキュリティを強化 .....	31
NFSでTLSを使用したセキュリティ強化 .....	38

# 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ます  
`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::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspaces 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::> vservers show -vservers 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에만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ルートボリ्यूムのエクスポートポリシーを開く

SVMルートボリ्यू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とそのボリ्यू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のルートボリ्यू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、個々のボリ्यू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リ्यू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リ्यू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 ルートボリ्यू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 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 *	`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}`
• ONTAP 9.6 以降 *	`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}`

- `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 ``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	<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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
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
```

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。

## 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 `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ます `/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 `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 `false`。このパラメータを `true` と指定すると、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、`vs1``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、チャンネルバインドが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接続でチャンネルバインディングを試行します。ネームサーバとのLDAPチャン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チャン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リファラー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管理者にお問い合わせください。

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、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、`-default-site` を指定する必要があります。
- 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せん `-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|sas}`` 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::> vservice 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::> vservice 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::> vservice 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 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 `vservice 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: 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

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	<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

### NFSでのKerberos使用によるセキュリティ強化の概要

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

環境が次のガイドラインを満たしている必要があります。

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

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

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

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

- ディレクトリサービス

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

- NTP

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

- ドメイン名解決 (DNS)

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

## Kerberos設定の権限の確認

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

手順

1. SVM ルートボリュームについて、関連する権限を表示します。

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

SVMのルートボリュームを次のように設定しておく必要があります。

名前	設定
UID	ルートまたはID 0
GID	ルートまたはID 0

名前	設定
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` で更新します。

## 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ます `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、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	<p>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。<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で許可されてい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	<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` で結果を表示します。

```
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
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
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` で結果を表示します。

```
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
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
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
```

Vserver Name	Logical Interface	Address	TLS Status	TLS Certificate
vs1	data1	10.0.1.1	disabled	-
vs2	data2	10.0.1.2	enabled	new_cert

2 entries were displayed.

## 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。