



SVMへのSMBアクセスの設定

ONTAP 9

NetApp
April 24, 2024

目次

SVMへのSMBアクセスの設定	1
SVMへのSMBアクセスの設定	1
SVM を作成します。	1
SVMでSMBプロトコルが有効になっていることを確認する	3
SVM ルートボリュームのエクスポートポリシーを開きます	4
LIF を作成	5
ホスト名解決に使用する DNS を有効にします	8
Active Directory ドメイン内に SMB サーバをセットアップする	10
ワークグループ内に SMB サーバをセットアップする	15
有効な SMB のバージョンを確認	21
DNS サーバでの SMB サーバのマッピング	23

SVMへのSMBアクセスの設定

SVMへのSMBアクセスの設定

SMB クライアントアクセス用に SVM を設定していない場合は、新しい SVM を作成して設定するか、既存の SVM を設定する必要があります。SMB を設定する場合は、SVM ルートボリュームへのアクセスを許可し、SMB サーバを作成し、LIF を作成し、ホスト名解決を有効にし、ネームサービスを設定し、必要に応じて Kerberos セキュリティの有効化。

SVM を作成します。

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

作業を開始する前に

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

手順

1. SVM を作成します。 `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
 - のNTFS設定を使用します。 `-rootvolume-security-style` オプション
 - デフォルトのC.UTF-8を使用します `-language` オプション
 - `ipspace` 設定はオプションです。
2. 新しく作成した SVM の設定とステータスを確認します。 `vserver show -vserver vserver_name`
 - Allowed Protocols フィールドにはCIFSを含める必要があります。このリストはあとで編集できます。
 - Vserver Operational State フィールドにはを表示する必要があります running 状態。が表示された場合 initializing 状態にすると、ルートボリュームの作成などの中間処理が失敗したため、SVM を削除して再作成する必要があります。

例

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

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -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追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含まないデフォルトのエクスポートポリシーがあるため、ルートボリュームは作成時にエクスポートされません。

```
cluster1::> 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: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



ONTAP 9.13.1以降では、アダプティブQoSポリシーグループテンプレートを設定して、SVM内のボリュームにスループットの下限と上限の制限を適用できます。このポリシーはSVMの作成後にのみ適用できます。このプロセスの詳細については、[を参照してください アダプティブポリシーグループテンプレートを設定します。](#)

SVMでSMBプロトコルが有効になっていることを確認する

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

このタスクについて

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



作成したプロトコルは、LIF から追加または削除することはできません。

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

手順

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

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

2. 必要に応じて、プロトコルを有効または無効にします。

- SMBプロトコルを有効にする手順は次のとおりです。 `vserver add-protocols -vserver vserver_name -protocols cifs`
- プロトコルを無効にするには： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. 有効 / 無効なプロトコルが正しく更新されたことを確認します。 `vserver show -vserver vserver_name -protocols`

例

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

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

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

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

SVM ルートボリュームのエクスポートポリシーを開きます

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

このタスクについて

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

デフォルトのエクスポートポリシーですべての SMB アクセスが許可されていることを確認してから、ボリュームまたは qtrees ごとにカスタムのエクスポートポリシーを作成して各ボリュームへのアクセスを制限します。

手順

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

次のようなコマンド出力が表示されます。

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

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

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

2. SVM ルートボリュームのエクスポートルールを作成します。 `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. を使用してルールの作成を確認します `vserver export-policy rule show` コマンドを実行します

結果

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

LIF を作成

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

作業を開始する前に

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

サブネットには、同じレイヤ 3 サブネットに属する IP アドレスのプールが含まれています。これらはを使用して作成されます `network subnet create` コマンドを実行します

- LIF で処理するトラフィックのタイプを指定するメカニズムが変更されました。ONTAP 9.5 以前では、LIF はロールを使用して処理するトラフィックのタイプを指定していました。ONTAP 9.6 以降では、サービスポリシーを使用して、処理するトラフィックのタイプを指定します。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内の LIF の数が多い場合は、を使用して、クラスタでサポートされる LIF の容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされる LIF の容量を確認します `network interface capacity details show` コマンド（advanced 権限レベル）。
- ONTAP 9.7 以降では、同じサブネット内に SVM 用の他の LIF がすでに存在する場合、LIF のホームポートを指定する必要はありません。ONTAP は、同じサブネットにすでに設定されている他の LIF と同じブロードキャストドメインにある指定したホームノード上のランダムなポートを自動的に選択します。

手順

1. LIF を作成します。

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

* ONTAP 9.5 以前 *

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

* ONTAP 9.6 以降 *

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home
-node node_name -home-port port_name {-address IP_address -netmask IP_address
-subnet-name subnet_name} -firewall-policy data -auto-revert {true
false}`
```

- 。 -role サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。
- 。 -data-protocol サービスポリシーを使用してLIFを作成する場合はパラメータは必要ありません（ONTAP 9.6以降）。ONTAP 9.5以前を使用している場合 -data-protocol パラメータはLIFの作成時に指定する必要があります。あとで変更するには、データLIFを削除して再作成する必要があります。
- 。 -home-node は、の実行時にLIFが戻るノードです network interface revert LIFに対してコマンドを実行します。

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

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

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



ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシーに置き換えられました。詳細については、を参照してください "[LIF のファイアウォールポリシーを設定します](#)"。

- 。 -auto-revert 起動時、管理データベースのステータスが変化したとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルト設定はです false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。

2. LIF が正常に作成されたことを確認します。

```
network interface show
```

3. 設定した IP アドレスに到達できることを確認します。

対象	使用
IPv4 アドレス	network ping
IPv6アドレス	network ping6

例

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

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

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

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

次のコマンドは、cluster-1 内のすべての LIF を表示します。datalif1 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、datalif4 には IPv6 アドレスを設定しています。

```
network interface show
```

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

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

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

ホスト名解決に使用する **DNS** を有効にします

を使用できます vsriver services name-service dns コマンドを使用してSVM

でDNSを有効にし、ホスト名解決にDNSを使用するように設定します。ホスト名は外部DNSサーバを使用して解決されます。

作業を開始する前に

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

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

このタスクについて

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

手順

1. SVMでDNSを有効にします。`vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

次のコマンドは、SVM vs1 で外部DNSサーバを有効にします。

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



ONTAP 9.2以降では、`vserver services name-service dns create` コマンドは設定の自動検証を実行し、ONTAP がネームサーバに接続できない場合はエラーメッセージを報告します。

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

次のコマンドは、クラスタ内のすべてのSVMのDNS設定を表示します。

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

次のコマンドは、SVM vs1 のDNS設定の詳細を表示します。

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

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

。 `vserver services name-service dns check` コマンドはONTAP 9.2以降で使用できます。

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

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

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

タイムサービスを設定

Active Directory ドメインコントローラで SMB サーバを作成する前に、クラスタ時間と SMB サーバが所属するドメインのドメインコントローラの時間のずれが 5 分以内であることを確認する必要があります。

このタスクについて

Active Directory ドメインと同じ NTP サーバを使用して時刻を同期するようにクラスタ NTP サービスを設定する必要があります。

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

手順

1. を使用してタイムサービスを設定します `cluster time-service ntp server create` コマンドを実行します
 - 。 対称認証を使用せずにタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address`
 - 。 対称認証を使用してタイムサービスを設定するには、次のコマンドを入力します。 `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster`

```
time-service ntp server create -server 10.10.10.1 cluster time-service ntp
server create -server 10.10.10.2
```

2. を使用して、タイムサービスが正しく設定されていることを確認します cluster time-service ntp server show コマンドを実行します


```
cluster time-service ntp server show
```

Server	Version
10.10.10.1	auto
10.10.10.2	auto

NTP サーバの対称認証を管理するコマンドです

ONTAP 9.5 以降では、ネットワークタイムプロトコル（NTP）バージョン 3 がサポートされます。NTPv3 には SHA-1 鍵を使用した対称認証機能が含まれ、ネットワークセキュリティが強化されます。

作業	使用するコマンド
対称認証を使用せずに NTP サーバを設定する	cluster time-service ntp server create -server server_name
対称認証を使用して NTP サーバを設定する	cluster time-service ntp server create -server server_ip_address -key-id key_id
既存の NTP サーバに対して対称認証を有効にする必要なキー ID を追加することで、既存の NTP サーバを変更して認証を有効にすることができます	cluster time-service ntp server modify -server server_name -key-id key_id
共有 NTP キーを設定する	cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value <div>  <p>共有キーは ID で参照されます。ID、そのタイプ、および値が、ノードと NTP サーバで同じである必要があります</p> </div>
不明なキー ID で NTP サーバを設定する	cluster time-service ntp server create -server server_name -key-id key_id

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

Active Directory ドメイン内に SMB サーバを作成します

を使用できます `vserver cifs create` コマンドを使用してSVM上にSMBサーバを作成し、所属先のActive Directory (AD) ドメインを指定します。

作業を開始する前に

データ処理に使用している SVM および LIF が、SMB プロトコルを許可するように設定されている必要があります。LIF は、SVM 上で設定されている DNS サーバ、および SMB サーバの追加先ドメインの AD ドメインコントローラに接続できる必要があります。

SMB サーバの追加先となる AD ドメイン内のマシンアカウントの作成を許可されているユーザなら誰でも、SVM 上に SMB サーバを作成できます。これには、他のドメインのユーザを含めることができます。

ONTAP 9.7 以降では、権限がある Windows アカウントの名前とパスワードの代わりに、keytab ファイルの URI を AD 管理者から提供される場合があります。URIを受け取ったら、に含めます `-keytab-uri` パラメータと `vserver cifs` コマンド

このタスクについて

Activity Directory ドメインで SMB サーバを作成する場合の条件は次のとおりです。

- ドメインを指定するときは Fully Qualified Domain Name (FQDN ; 完全修飾ドメイン名) を使用する必要があります。
- デフォルト設定では、SMB サーバマシンアカウントは Active Directory CN=Computer オブジェクトに追加されます。
- を使用して、SMBサーバを別の組織単位 (OU) に追加することもできます `-ou` オプション
- 必要に応じて、SMB サーバの 1 つ以上の NetBIOS エイリアス (最大 200 個) をカンマで区切って追加できます。

SMB サーバの NetBIOS エイリアスを設定すると、他のファイルサーバのデータを SMB サーバに統合して、SMB サーバが元のファイルサーバの名前に応答するようにする場合に役立ちます。

。 `vserver cifs` マニュアルページには、追加のオプションパラメータと命名要件が記載されています。



ONTAP 9.1 以降では、SMB バージョン 2.0 からドメインコントローラ（DC）への接続を有効にすることができます。これは、ドメインコントローラで SMB 1.0 を無効にしている場合は必須です。ONTAP 9.2 以降では、SMB 2.0 がデフォルトで有効になります。

ONTAP 9.8 以降では、ドメインコントローラへの接続を暗号化するように指定できます。ONTAP では、ドメインコントローラの通信に暗号化が必要です `-encryption-required-for-dc-connection` オプションはに設定されています `true`; デフォルトは `false`。このオプションを設定すると、SMB3 でのみ暗号化がサポートされるため、SMB3 プロトコルのみが使用されます。。

"SMBの管理" SMB サーバ設定オプションの詳細については、を参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

SMBライセンスには含まれています。 **"ONTAP One"**。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB サーバを認証のみに使用する場合は、CIFS ライセンスは必要ありません。

2. ADドメインにSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

ドメインに参加する場合、このコマンドの実行には数分かかることがあります。

次のコマンドは、ドメイン「`example.com`"`」に SMB サーバ「`'smb_server01'`」を作成します

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

次のコマンドは、ドメイン「`mydomain.com`"`」に SMB サーバ「`'smb_server02'`」を作成し、keytab ファイルを使用して ONTAP 管理者を認証します。

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. を使用してSMBサーバの設定を確認します `vserver cifs show` コマンドを実行します

この例では、「`'s MB_SERVER01'`」という名前の SMB サーバが SVM `vs1.example.com` 上に作成され、「`example.com`"` ドメイン」に追加されたことがコマンド出力に示されています。

```
cluster1::> vsriver cifs show -vsriver vs1
```

```

Vsvriver: vs1.example.com
CIFS Svriver NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Svriver Administrative Status: up
CIFS Svriver Description: -
List of NetBIOS Aliases: -
```

4. 必要に応じて、ドメインコントローラとの暗号化通信を有効にします（ONTAP 9.8以降）。`vsriver cifs security modify -vsriver svm_name -encryption-required-for-dc-connection true`

例

次のコマンドは、SVM `vs2.example.com` の「`example.com`」ドメインに「`MB_Server02`」という名前の SMB サーバを作成します。マシン・アカウントは「`OU=eng`、`OU=corp`、`DC=example`、`DC=com`」コンテナに作成されますSMB サーバには NetBIOS エイリアスが割り当てられます。

```
cluster1::> vsriver cifs create -vsriver vs2.example.com -cifs-svriver
smb_svriver02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_svriver01
```

```
cluster1::> vsriver cifs show -vsriver vs1
Vsvriver: vs2.example.com
CIFS Svriver NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Svriver Administrative Status: up
CIFS Svriver Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

次のコマンドは、別のドメインのユーザ（ここでは信頼できるドメインの管理者）が、SVM `vs3.example.com` 上に「`smb_svriver03`」という名前の SMB サーバを作成できるようにします。。
-domain optionは、SMBサーバを作成するホームドメイン（DNSの設定で指定）の名前を指定します。。
username オプションは、信頼できるドメインの管理者を指定します。

- ホームドメイン： `example.com`
- 信頼できるドメイン： `trust.lab.com`
- 信頼できるドメインのユーザ名： `Administrator1`


```
cluster1::> vsync cifs create -vsync vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

Username: Administrator1@trust.lab.com

Password: . . .

SMB 認証用の keytab ファイルを作成します

ONTAP 9.7 以降 ONTAP では、keytab ファイルを使用した Active Directory（AD）サーバとの SVM 認証がサポートされます。AD 管理者は keytab ファイルを生成し、Uniform Resource Identifier（URI; ユニフォームリソース識別子）として ONTAP 管理者が使用できるようにします。このファイルは、に指定します `vsync cifs` コマンドを実行するには、AD ドメインとの Kerberos 認証が必要です。

AD 管理者は、標準の Windows Server を使用して keytab ファイルを作成できます `ktpass` コマンドを実行しますこのコマンドは、認証が必要なプライマリドメインで実行する必要があります。。 `ktpass` コマンドを使用して keytab ファイルを生成できるのはプライマリドメインユーザのみです。信頼できるドメインユーザを使用して生成されたキーはサポートされていません。

keytab ファイルは、特定の ONTAP 管理者ユーザ用に生成されます。管理者ユーザのパスワードが変更されないかぎり、特定の暗号化タイプとドメインに対して生成されたキーは変更されません。したがって、管理者ユーザのパスワードを変更した場合は、そのたびに新しい keytab ファイルが必要になります。

次の暗号化タイプがサポートされています。

- AES256-SHA1
- des-cbc-md5



ONTAP では、DES-CBC-CRC 暗号化タイプはサポートされていません。

- RC4-HMAC

最も高度な暗号化タイプは AES256 です。ONTAP システムで有効な場合は AES256 を使用してください。

keytab ファイルは、管理パスワードを指定して生成するか、ランダムに生成されたパスワードを使用して生成できます。ただし、keytab ファイル内のキーを復号化するために AD サーバ側で管理者ユーザに固有な秘密鍵が必要になるため、ある時点で使用できるパスワードオプションはどちらか 1 つだけです。特定の管理者の秘密鍵を変更すると、keytab ファイルは無効になります。

ワークグループ内に SMB サーバをセットアップする

ワークグループの概要で SMB サーバをセットアップする

ワークグループ内のメンバーとして SMB サーバをセットアップするには、SMB サーバを作成してから、ローカルユーザとローカルグループを作成します。

Microsoft Active Directory ドメインインフラを使用できない場合は、ワークグループに SMB サーバを設定で

きます。

ワークグループモードの SMB サーバでは NTLM 認証のみがサポートされ、Kerberos 認証はサポートされません。

ワークグループ内に **SMB** サーバを作成

を使用できます `vserver cifs create` コマンドを使用してSVM上にSMBサーバを作成し、所属先のワークグループを指定します。

作業を開始する前に

データ処理に使用している SVM および LIF が、SMB プロトコルを許可するように設定されている必要があります。LIF は、SVM で設定されている DNS サーバに接続できる必要があります。

このタスクについて

ワークグループモードの SMB サーバでは、次の SMB 機能はサポートされません。

- SMB3 監視プロトコル
- SMB3 CA 共有
- SQL over SMB
- フォルダリダイレクト
- 移動プロファイル
- グループポリシーオブジェクト（GPO）
- ボリューム Snapshot サービス（VSS）

。 `vserver cifs` その他のオプションの設定パラメータと命名要件については、マニュアルページを参照してください。

手順

1. クラスタでSMBのライセンスが有効になっていることを確認します。 `system license show -package cifs`

SMBライセンスには含まれています。 ["ONTAP One"](#)。ONTAP Oneをお持ちでなく、ライセンスがインストールされていない場合は、営業担当者にお問い合わせください。

SMB サーバを認証のみに使用する場合は、CIFS ライセンスは必要ありません。

2. ワークグループ内にSMBサーバを作成します。 `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

次のコマンドは 'ワークグループ "workgroup01" 内に SMB サーバ "smb_server01" を作成します

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
SMB_SERVER01 -workgroup workgroup01
```

3. を使用してSMBサーバの設定を確認します `vserver cifs show` コマンドを実行します

次の例では、コマンド出力は、ワークグループ「workgroup01」内の SVM vs1.example.com 上に「smb_server01」という名前の SMB サーバが作成されたことを示しています。

```
cluster1::> vsserver cifs show -vsriver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

完了後

ワークグループ内の CIFS サーバについては、SVM 上でローカルユーザ、およびオプションでローカルグループを作成する必要があります。

関連情報

["SMBの管理"](#)

ローカルユーザアカウントを作成します

SVM に格納されたデータへの SMB 接続によるアクセスの許可に使用できるローカルユーザアカウントを作成できます。ローカルユーザアカウントは、SMB セッションを作成する際の認証にも使用できます。

このタスクについて

ローカルユーザの機能は、SVM の作成時にデフォルトで有効になります。

ローカルユーザアカウントを作成するときは、ユーザ名を指定する必要があり、アカウントを関連付ける SVM を指定する必要があります。

。vsriver cifs users-and-groups local-user マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

手順

1. ローカルユーザを作成します。vsriver cifs users-and-groups local-user create -vsriver vsriver_name -user-name user_name optional_parameters

次のオプションのパラメータが役に立つ場合があります。

- ° -full-name

ユーザのフルネーム。

◦ -description

ローカルユーザの概要。

◦ -is-account-disabled {true|false}

ユーザアカウントが有効になっているか無効になっているかを示します。このパラメータを指定しない場合、ユーザアカウントはデフォルトで有効になります。

ローカルユーザのパスワードを入力するように求められます。

2. ローカルユーザのパスワードを入力し、確認のためにもう一度入力します。

3. ユーザが正常に作成されたことを確認します。 `vserver cifs users-and-groups local-user show -vserver vserver_name`

例

次の例では、SVM `vs1.example.com` に関連付けられた「SMB_SERVER1\Sue」という完全な名前のローカルユーザ「Sue Chang」を作成します。

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

Enter the password:

Confirm the password:

```
cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                               Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator                   Built-in administrator
account
vs1      SMB_SERVER01\sue                             Sue Chang
```

ローカルグループを作成します

SVM に関連付けられたデータへの SMB 接続によるアクセスの許可に使用できるローカルグループを作成できます。また、グループのメンバーに付与するユーザ権限と機能を定義した権限を割り当てることもできます。

このタスクについて

ローカルグループの機能は、SVM の作成時にデフォルトで有効になります。

ローカルグループを作成するときは、グループの名前を指定する必要があります。グループに関連付ける SVM を指定する必要があります。グループ名を指定する際、ローカルドメイン名は指定してもしなくても構いません。また、オプションで、ローカルグループの概要を指定することもできます。別のローカルグループにローカルグループを追加することはできません。

。vserver cifs users-and-groups local-group マニュアルページには、オプションのパラメータと命名要件の詳細が記載されています。

手順

1. ローカルグループを作成します。vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name

次のオプションのパラメータが役に立つ場合があります。

- -description

ローカルグループの概要。

2. グループが正常に作成されたことを確認します。vserver cifs users-and-groups local-group show -vserver vserver_name

例

次の例では、SVM vs1 に関連付けられるローカルグループ「s MB_SERVER01\engineering」を作成します。

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
```

Vserver	Group Name	Description
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

完了後

新しいグループにメンバーを追加する必要があります。

ローカルグループメンバーシップを管理します

ローカルグループメンバーシップの管理では、ローカルユーザやドメインユーザの追加と削除、ドメイングループの追加と削除ができます。この機能は、特定のグループに対するアクセス制御に基づいてデータへのアクセスを制御したり、グループに関連した権限をユーザに付与したりする上で役に立ちます。

このタスクについて

特定のグループのメンバーシップに基づいてローカルユーザ、ドメインユーザ、またはドメイングループに付与されたアクセス権や権限を取り消す場合に、メンバーをグループから削除できます。

メンバーをローカルグループに追加する場合は、次の点に注意する必要があります。

- 特殊なグループ `_Everyone` にユーザを追加することはできません。
- 別のローカルグループにローカルグループを追加することはできません。
- ローカルグループにドメインユーザまたはグループを追加するには、ONTAP で名前を SID に解決できる必要があります。

メンバーをローカルグループから削除する場合は、次の点に注意する必要があります。

- 特殊なグループ `_Everyone` からメンバーを削除することはできません。
- ローカルグループからメンバーを削除するには、ONTAP で名前を SID に解決できる必要があります。

手順

1. メンバーをグループに追加するか、グループから削除します。

- メンバーを追加します。 `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループに追加します。

- メンバーを削除します。 `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

カンマ区切りのリストに記載されたローカルユーザ、ドメインユーザ、ドメイングループを指定し、特定のローカルグループから削除します。

例

次の例では、SVM `vs1.example.com` 上のローカルグループ「`s MB_SERVER01\engineering`」にローカルユーザ「`""s MB_SERVER01\engineering`」を追加します。

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

次の例では、SVM `vs1.example.com` 上のローカルグループ「`s MB_SERVER1\engineering`」からローカルユーザ「`s MB_SERVER01\Sue`」および「`S MB_SERVER01\engineering`」を削除します。

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

有効な SMB のバージョンを確認

ONTAP 9 のリリースによって、クライアントおよびドメインコントローラとの接続に対してデフォルトで有効になっている SMB のバージョンが決まります。ご使用の環境で必要なクライアントと機能を、SMB サーバがサポートしていることを確認する必要があります。

このタスクについて

クライアントとドメインコントローラの両方と接続するために、可能な限り SMB 2.0 以降を有効にする必要があります。セキュリティ上の理由から、SMB 1.0 の使用は避け、お使いの環境で不要であることを確認した場合は無効にする必要があります。

ONTAP 9 では、SMB バージョン 2.0 以降がクライアント接続用にデフォルトで有効になっていますが、デフォルトで有効になっている SMB 1.0 のバージョンは ONTAP リリースによって異なります。

- ONTAP 9.1 P8 以降では、SVM で SMB 1.0 を無効にすることができます。
 - 。 -smb1-enabled オプションをに設定します `vserver cifs options modify` コマンドは、SMB 1.0 を有効または無効にします。
- ONTAP 9.3 以降では、新しい SVM でデフォルトで無効になっています。

SMB サーバが Active Directory (AD) ドメイン内にある場合、ONTAP 9.1 以降では、ドメインコントローラ (DC) に接続するために SMB 2.0 を有効にすることができます。DC 上で SMB 1.0 を無効にしている場合は、この処理は必須です。ONTAP 9.2 以降では、SMB 2.0 が DC 接続用にデフォルトで有効になります。



状況 -smb1-enabled-for-dc-connections がに設定されます false 間 -smb1-enabled がに設定されます true`ONTAP では、クライアントとしての SMB 1.0 の接続は拒否されますが、サーバとしての SMB 1.0 のインバウンド接続は引き続き受け入れます。

"SMBの管理" サポートされる SMB のバージョンと機能に関する詳細が記載されています。

手順

1. 権限レベルを advanced に設定します。

```
set -privilege advanced
```

2. 有効になっている SMB のバージョンを確認します。

```
vserver cifs options show
```

リストを下にスクロールすると、クライアント接続用に有効になっている SMB のバージョンを表示できます。また、AD ドメイン内の SMB サーバを設定している場合は、AD ドメイン接続用に有効になっているバージョンを表示できます。

3. 必要に応じて、クライアント接続用の SMB プロトコルを有効または無効にします。

- SMBバージョンを有効にするには：

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- SMBバージョンを無効にするには：

```
vserver cifs options modify -vserver vserver_name smb_version false
```

に指定できる値 smb_version：

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

次のコマンドは、SVM vs1.example.comでSMB 3.1を有効にします。

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. SMB サーバが Active Directory ドメイン内にある場合は、必要に応じて、DC 接続用の SMB プロトコルを有効または無効にします。

- SMBバージョンを有効にするには：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- SMBバージョンを無効にするには：

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. admin 権限レベルに戻ります。

```
set -privilege admin
```


DNS サーバでの SMB サーバのマッピング

Windows ユーザがドライブを SMB サーバ名にマッピングできるように、サイトの DNS サーバに、SMB サーバ名および NetBIOS エイリアスをデータ LIF の IP アドレスにマッピングしたエントリを設定する必要があります。

作業を開始する前に

サイトの DNS サーバに対する管理アクセス権が必要です。管理アクセス権がない場合は、DNS 管理者にこのタスクの実行を依頼する必要があります。

このタスクについて

SMB サーバ名に NetBIOS エイリアスを使用する場合は、各エイリアスに DNS サーバのエントリポイントを作成することを推奨します。

手順

1. DNS サーバにログインします。
2. フォワードルックアップ（A - アドレスレコード）とリバースルックアップ（PTR - ポインタレコード）のエントリを作成して、SMB サーバ名をデータ LIF の IP アドレスにマッピングします。
3. NetBIOS エイリアスを使用する場合は、エイリアスの正規名（CNAME リソースレコード）のルックアップエントリを作成して、各エイリアスを SMB サーバのデータ LIF の IP アドレスにマッピングします。

結果

ネットワーク全体にマッピングが反映されると、Windows ユーザがドライブを SMB サーバ名またはその NetBIOS エイリアスにマッピングできるようになります。

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。