



SMB サーバのサポート ONTAP 9

NetApp
April 24, 2024

目次

SMB サーバのサポート	1
SMB サーバのサポートの概要	1
サポートされる SMB のバージョンと機能	1
サポートされない Windows の機能	4
SVM に NIS または LDAP ネームサービスを設定します	4
ONTAP のネームサービススイッチ設定の仕組み	7

SMB サーバのサポート

SMB サーバのサポートの概要

Storage Virtual Machine（SVM）上で SMB サーバを有効にして設定し、SMB クライアントがクラスタ上のファイルにアクセスできるようにすることができます。

- クラスタ内のデータ SVM は、それぞれ 1 つの Active Directory ドメインにバインドできます。
- データ SVM は、必ずしも同じドメインにバインドする必要はありません。
- 複数の SVM を同じドメインにバインドできます。

SMB サーバを作成する前に、データの提供に使用する SVM と LIF を設定しておく必要があります。データネットワークがフラットでない場合は、IPspace、ブロードキャストドメイン、およびサブネットの設定も必要になることがあります。詳細については、『ネットワーク管理ガイド』を参照してください。

関連情報

["Network Management の略"](#)

[SMB サーバを変更](#)

["システム管理"](#)

サポートされる SMB のバージョンと機能

Server Message Block（SMB；サーバメッセージブロック）は、Microsoft Windows クライアントおよびサーバで使用されるリモートファイル共有プロトコルです。ONTAP 9 ではすべての SMB のバージョンがサポートされますが、デフォルトである SMB 1.0 がサポートされるかどうかは ONTAP のバージョンによって異なります。ONTAP SMB サーバが、ご使用の環境で必要なクライアントと機能をサポートしていることを確認する必要があります。

ONTAP がサポートする SMB クライアントおよびドメインコントローラの最新情報については、Interoperability Matrix Tool を参照してください。

SMB 2.0 以降のバージョンは ONTAP 9 の SMB サーバではデフォルトで有効になっており、必要に応じて有効または無効を切り替えることができます。次の表に、SMB 1.0 のサポートとデフォルト設定を示します。

SMB 1.0 の機能：	ONTAP 9 のリリース：			
	9.0	9.1	9.2.	9.3以降
はデフォルトで有効になっています	はい。	はい。	はい。	いいえ

SMB 1.0 の機能：	ONTAP 9 のリリース：			
有効または無効にすることができます	いいえ	はい * 9.1 P8 以降が必要です。	はい。	はい。



SMB 1.0 および 2.0 のドメインコントローラへの接続に関するデフォルト設定も ONTAP のバージョンによって異なります。詳細については、[vserver cifs security modify](#) のマニュアルページ。既存の CIFS サーバで SMB 1.0 を実行している環境では、できるだけ早く最新の SMB バージョンに移行して、セキュリティとコンプライアンスを強化する必要があります。詳細については、ネットアップの担当者にお問い合わせください。

次の表に、SMB でサポートされる機能と対応するバージョンを示します。SMB の機能には、デフォルトで有効になるものと追加の設定が必要なものがあります。

* この機能：	* 有効化が必要： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
		1.0	"2.0"	2.1	3.0	3.1.1
従来の SMB 1.0 の機能		X	X	X	X	X
永続性ハンドル			X	X	X	X
複合操作			X	X	X	X
非同期操作			X	X	X	X
読み取り / 書き込みバッファのサイズが増加します			X	X	X	X
拡張性の向上			X	X	X	X
SMB 署名	X	X	X	X	X	X
代替データストリーム (ADS) ファイル形式	X	X	X	X	X	X

* この機能： *	* 有効化が必要 ： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
Large MTU (ONTAP 9.7 以降ではデフォルトで有効)	X			X	X	X
oplock リース				X	X	X
共有の継続的な可用性	X				X	X
永続的ハンドル					X	X
監視					X	X
SMB 暗号化： AES-128-CCM	X				X	X
スケールアウト (CA 共有で必要)					X	X
透過的なフェイルオーバー					X	X
SMB マルチチャネル (ONTAP 9.4 以降)	X				X	X
事前認証の整合性						X
クラスタ・クライアント・フェイルオーバー v.2 (CCFv2)						X

* この機能： *	* 有効化が必要 ： *	* ONTAP 9 では、以下のバージョンの SMB がサポートされています。 *				
SMB 暗号化： AES-128- GCM （ ONTAP 9.1 以 降）	X					X

関連情報

[SMB 署名を使用したネットワークセキュリティの強化](#)

[SMBサーバの最小認証セキュリティレベルの設定](#)

[SMB を介したデータ転送での SMB サーバの SMB 暗号化要求の設定](#)

["ネットアップテクニカルレポート 4543：『SMB Protocol Best Practices』"](#)

["ネットアップの相互運用性"](#)

サポートされない Windows の機能

ネットワークで CIFS を使用する場合は、一部の Windows の機能が ONTAP ではサポートされないことに注意する必要があります。

ONTAP では、次の Windows 機能はサポートされません。

- Encrypted File System （EFS；暗号化ファイルシステム）
- 変更ジャーナルでの NT File System （NTFS）イベントのロギング
- Microsoft File Replication Service （FRS；ファイルレプリケーションサービス）
- Microsoft Windows インデックスサービス
- Hierarchical Storage Management （HSM；階層型ストレージ管理）経由のリモートストレージ
- Windows クライアントからのクォータ管理
- Windows のクォータのセマンティクス
- LMHOSTS ファイル
- NTFS のネイティブ圧縮機能です

SVM に NIS または LDAP ネームサービスを設定します

SMB アクセスでは、NTFS セキュリティ形式のボリューム内のデータにアクセスする場合でも、UNIX ユーザへのユーザマッピングが常に実行されます。NIS または LDAP ディレクトリストアにその情報が格納されている UNIX ユーザに Windows ユーザをマッピングする場合や、ネームマッピングに LDAP を使用する場合は、SMB のセットアップ

時にこのネームサービスを設定する必要があります。

作業を開始する前に

ネームサービスデータベース設定をネームサービスインフラに合わせてカスタマイズしておく必要があります。

このタスクについて

SVM は、ネームサービス ns-switch データベースを使用して、指定されたネームサービスデータベースを検索するソースの順番を決定します。ns-switch ソースには、「files」、「nis」、または「ldap」を任意に組み合わせて使用できます。グループデータベースの場合、ONTAP は設定されたすべてのソースからグループメンバーシップを取得し、統合されたグループメンバーシップ情報をアクセスチェックに使用します。UNIX グループ情報の取得時にこれらのいずれかのソースを使用できないと、ONTAP は完全な UNIX クレデンシャルを取得できず、アクセスチェックが失敗することがあります。そのため、ns-switch 設定にグループデータベースのすべての ns-switch ソースが設定されていることを必ず確認する必要があります。

デフォルトでは、SMBサーバは、すべてのWindowsユーザをローカルに格納されているデフォルトのUNIXユーザにマッピングします passwd データベース：デフォルトの設定を使用する場合、SMB アクセスに対する、NIS または LDAP UNIX ユーザおよびグループのネームサービスまたは LDAP ユーザマッピングの設定は省略可能です。

手順

1. UNIX ユーザ、グループ、ネットグループ情報が NIS ネームサービスによって管理されている場合、NIS ネームサービスを次のように設定します。

- a. を使用して、ネームサービスの現在の順序を確認します `vserver services name-service ns-switch show` コマンドを実行します

この例では、3つのデータベースを示します (group、passwd および netgroup を使用できます `nis` ネームサービスソースがのみを使用している files 情報源として

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

を追加する必要があります nis を参照してください group および passwd データベース、およびオプションでにアクセスできます netgroup データベース：

- b. を使用して、ネームサービスns-switchデータベースを必要な順序で調整します `vserver services name-service ns-switch modify` コマンドを実行します

パフォーマンスを最大にするためには、SVM に設定する予定のないネームサービスデータベースに

はネームサービスを追加しないでください。

複数のネームサービスデータベースの設定を変更する場合、変更するそれぞれのネームサービスデータベースに対して別々にコマンドを実行する必要があります。

この例では、`nis` および `files` は、のソースとして設定されています `group` および `passwd` この順番でデータベースを作成します。その他のネームサービスデータベースは変更されません。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. を使用して、ネームサービスの順序が正しいことを確認します `vserver services name-service ns-switch show` コマンドを実行します

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. NISネームサービス設定を作成します。+ `vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,... -active true`+

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



ONTAP 9.2以降では、フィールドが表示されます `-nis-servers` フィールドを置き換えます `-servers`。この新しいフィールドには、NISサーバのホスト名またはIPアドレスを指定できます。

- e. NISネームサービスが適切に設定され、アクティブになっていることを確認します。 `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```


Vserver	Domain	Active Server	
-----	-----	-----	-----
vs1	example.com	true	10.0.0.60

2. UNIX ユーザ、グループ、ネットグループ情報またはネームマッピングが LDAP ネームサービスによって管理されている場合は、格納されている情報を使用して LDAP ネームサービスを設定します ["NFS の管理"](#)。

ONTAP のネームサービススイッチ設定の仕組み

ONTAP では、に相当するテーブルにネームサービス設定情報が格納されます `/etc/nsswitch.conf` UNIX システム上のファイル。このテーブルを環境に応じて適切に設定するためには、その機能と ONTAP でテーブルがどのように使用されるかを理解しておく必要があります。

ONTAP ネームサービススイッチテーブルは、ONTAP が特定の種類のネームサービス情報を取得する際にどのネームサービスソースをどの順番で参照するかを決定します。ONTAP では、SVM ごとに個別のネームサービススイッチテーブルが保持されます。

データベースタイプ

テーブルには、次の各データベースタイプについてネームサービスのリストが格納されます。

データベースタイプ	ネームサービスソースの用途	有効なソース
ホスト	ホスト名の IP アドレスへの変換	ファイル、DNS
グループ	ユーザグループ情報を検索しています	files、nis、ldap が表示されます
パスワード	ユーザ情報を検索しています	files、nis、ldap が表示されます
ネットグループ	ネットグループ情報の検索	files、nis、ldap が表示されます
namemap	ユーザ名のマッピング	ファイル、LDAP

ソースタイプ

ソースタイプによって、該当する情報を取得するために使用するネームサービスソースが決まります。

ソースタイプ	情報の検索先	使用するコマンド
ファイル	ローカルのソースファイル	<pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre>
NIS	SVM の NIS ドメイン設定で指定された外部の NIS サーバ	<pre>vserver services name- service nis-domain</pre>
LDAP	SVM の LDAP クライアント設定で指定された外部の LDAP サーバ	<pre>vserver services name- service ldap</pre>
DNS	SVM の DNS 設定で指定された外部の DNS サーバ	<pre>vserver services name- service dns</pre>

データアクセスとSVM管理者の両方の認証にNISまたはLDAPを使用する場合も、を追加する必要があります
files また、NISまたはLDAP認証が失敗した場合のフォールバックとしてローカルユーザを設定します。

外部ソースへのアクセスに使用するプロトコル

ONTAP では、外部ソースのサーバへのアクセスに次のプロトコルを使用します。

外部のネームサービスソース	アクセスに使用するプロトコル
NIS	UDP
DNS	UDP
LDAP	TCP

例

次の例は、SVMのネームサービススイッチ設定を表示します svm_1：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

ユーザまたはグループ情報の検索では、ONTAP はローカルのソースファイルだけを参照します。結果が返されない場合、検索は失敗します。

ネットグループ情報の検索では、ONTAP が最初に外部 NIS サーバを参照し、結果が返されない場合は、次にローカルネットグループファイルが照会されます。

SVM svm_1 のテーブルには、ネームマッピング用のネームサービスエントリは含まれていません。そのため、ONTAP はデフォルトでローカルのソースファイルだけを参照します。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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