



SMBサーバのサポート

ONTAP 9

NetApp
December 20, 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上のNISまたはLDAPネームサービスの設定	4
ONTAPネームサービススイッチ設定の仕組み	6

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) 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を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を設定する必要があります。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。

関連情報

["ネットワーク管理"](#)

[SMBサーバの変更](#)

["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の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バージョンがサポートされますが、デフォルトでサポートされるSMB 1.0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 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にすることができます。次の表に、SMB 1.0のサポートとデフォルトの設定を示します。

SMB 1.0の機能：	ONTAP 9 のリリース：			
	9.0	9.1	9.2	9.3以降
デフォルトで有効	○	○	○	いいえ
有効/無効を切り替えることができます。	いいえ	はい * 9.1 P8 以降が必要です。	○	○



ドメインコントローラへのSMB 1.0および2.0接続のデフォルト設定も、ONTAPのバージョンによって異なります。詳細については、のマニュアルページを参照し `vserver cifs security modify` てください。既存のCIFSサーバでSMB 1.0を実行している環境では、できるだけ早く新しいバージョンのSMB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、NetApp担当者にお問い合わせください。

次の表に、SMBの各バージョンでサポートされるSMBの機能を示します。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 サイズの増加			X	X	X	X
拡張性の向上			X	X	X	X
SMBシヨメイ	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
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
継続的可用性 を備えた共有	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。 *				
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マルチチャンネル (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
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経由のデータ転送でのSMBサーバでのSMB暗号化要求の設定](#)

["NetApp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上のNISまたはLDAPネームサービスの設定

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れらのネームサービスを設定する必要があります。

開始する前に

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

タスクの内容

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序を決定します。ns-switchソースには、nis、またはldap`を任意に組み合わせて指定できます`files。グループデータベースの場合、ONTAPは設定されているすべてのソースからグループメンバーシップを取得しようとし、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ソースのいずれかが使用できないと、ONTAPは完全なUNIXクレデンシャルを取得できず、以降の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設定で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常に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ユーザをローカルデータベース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`passwd`ます。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オプションです。

手順

1. UNIXユーザ、グループ、および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

は、NISネームサービスを次のように設定します。

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

この例では、ネームサービスソースとして使用できる3つのデータベース(`group`、`passwd` および `netgroup`) `nis` がソースとしてのみを使用しています `files`。

```
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

ソースを `group` データベースと `passwd` データベースに追加する必要があります。必要に応じてデータベースにも `netgroup` 追加できます `nis`。

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

パフォーマンスを最大限に高めるには、SVMで設定する予定でないネームサービスデータベースに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は、変更する各ネームサービスデータベースに対して個別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` がデータベースおよび `passwd` のソースとしてこの順序で設定されています `group` ます。残り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. コマンドを使用して、ネームサービスの順序が正しいことを確認し `vserver services name-service ns-switch show` ます。

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

Vserver	Database	Enabled	Source
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>,...

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



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。

- e. NISネームサービスが適切に設定され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	Server
vs1	example.com	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、場所にある情報を使用してLDAPネームサービスを設定します"[NFSの管理](#)".

ONTAPネームサービススイッチ設定の仕組み

ONTAPでは、UNIXシステムのファイル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。このテーブルを環境に合わせて適切に設定できるように、このテーブルの機能とONTAPでの使用方法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序で参照するかを決定します。ネームサービススイッチテーブルは、SVMごとにONTAPで管理されます。

データベースタイプ

このテーブルには、次のデータベースタイプごとに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	ホスト名から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の検索	ファイル、NIS、LDAP
パスワード	ユーザ情報の検索	ファイル、NIS、LDAP
ネットグループ	ネットグループ情報の検索	ファイル、NIS、LDAP
namemap	ユーザ名のマッピング	ファイル、LDAP

ソースタイプ

ソースによって、適切な情報の取得に使用するネームサービスソースが指定されます。

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を使用する場合でも、NISまたはLDAP認証が失敗した場合に備えて、ローカルユーザをフォールバックとして含めて設定しておく必要があります files。

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にアクセスするために、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
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

ユーザーまたはグループ情報を検索するために、ONTAPはローカルソースファイルのみを参照します。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を検索するために、ONTAPは最初に外部NISサーバを参照します。クエリから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チェックされます。

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ありません。したがって、ONTAPはデフォルトでローカルソースファイルのみを参照します。

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権を有し、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権については、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。