



# NFSでのKerberos使用によるセキュリティ強化

## ONTAP 9

NetApp  
December 20, 2024

# 目次

NFSでのKerberos使用によるセキュリティ強化	1
ONTAPでのKerberosのサポート	1
NFSでKerberosを設定するための要件	1
NFSv4のユーザIDドメインの指定	5

# NFSでのKerberos使用によるセキュリティ強化

## ONTAPでのKerberosのサポート

Kerberosは、クライアント/サーバアプリケーションに強力な安全な認証を提供します。認証は、サーバに対するユーザIDとプロセスIDの検証を提供します。ONTAP環境では、KerberosでStorage Virtual Machine (SVM) とNFSクライアント間の認証を実行できます。

ONTAP 9では、次のKerberos機能がサポートされます。

- 整合性チェック機能を備えたKerberos 5認証 (krb5i)

krb5iは、チェックサムを使用して、クライアントとサーバ間で転送される各NFSメッセージの整合性を検証します。これは、セキュリティ上の理由（データが改ざんされていないことの確認など）とデータ整合性上の理由（信頼性の低いネットワークでNFSを使用する場合のデータ破損の防止など）の両方で役立ちます。

- プライバシーチェックを使用したKerberos 5認証 (krb5p)

krb5pはチェックサムを使用して、クライアントとサーバ間のすべてのトラフィックを暗号化します。これはより安全であり、より多くの負荷が発生します。

- 128ビットおよび256ビットのAES暗号化

Advanced Encryption Standard (AES) は、電子データを保護するための暗号化アルゴリズムです。ONTAPでは、セキュリティを強化するために、128ビットキーによるAES (AES-128) と256ビットキーによるAES (AES-256) がKerberosでサポートされます。

- SVMレベルのKerberos Realm設定

SVM管理者は、Kerberos Realm設定をSVMレベルで作成できるようになりました。つまり、SVM管理者はKerberos Realmの設定に関してクラスタ管理者に頼る必要がなくなり、個々のKerberos Realm設定をマルチテナンシー環境で作成できます。

## NFSでKerberosを設定するための要件

NFSでKerberosを使用するようにシステムで設定する前に、ネットワークおよびストレージの環境内の特定の項目が適切に設定されていることを確認する必要があります。



環境を設定する手順は、使用しているクライアントオペレーティングシステム、ドメインコントローラ、Kerberos、DNSなどのバージョンとタイプによって異なります。これらすべての変数を文書化することは、このドキュメントの範囲外です。詳細については、各コンポーネントのそれぞれのドキュメントを参照してください。

Windows Server 2008 R2のActive DirectoryおよびLinuxホストを使用する環境でのNFSv3およびNFSv4でのONTAPおよびKerberos 5のセットアップ方法の詳細な例については、テクニカルレポート4073を参照してください。

最初に次の項目を設定する必要があります。

## ネットワーク環境の要件

- Kerberos

Windows Active DirectoryベースのKerberosやMIT Kerberosなど、Key Distribution Center (KDC; キー配布センター) を使用してKerberosを設定しておく必要があります。

NFSサーバは、マシンプリンシパルのプライマリコンポーネントとしてを使用する必要があります `nfs`。

- ディレクトリサービス

Active DirectoryやOpenLDAPなど、SSL/TLS経由のLDAPを使用するように設定されたセキュアなディレクトリサービスを環境で使用する必要があります。

- 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。

- ユーザアカウント

各クライアントには、Kerberos Realmのユーザアカウントが必要です。NFS サーバでは 'マシン・プリンシパルの主要コンポーネントとして NFS' を使用する必要があります

## NFSクライアントの要件

- NFS

NFSv3またはNFSv4を使用してネットワーク経由で通信するように各クライアントが適切に設定されている必要があります。

クライアントがRFC1964およびRFC2203をサポートしている必要があります。

- Kerberos

Kerberos認証を使用するように各クライアントが適切に設定されている必要があります。詳細は次のとおりです。

- TGS 通信の暗号化が有効です。

最も強力なセキュリティを実現するAES-256。

- TGT 通信に対する最も安全な暗号化タイプが有効です。

- Kerberos Realm とドメインを正しく設定します。

- GSSはイネーブルです。

マシンのクレデンシャルを使用する場合：

- パラメータを指定し `n` を実行しないで `gssd` ください。
- をrootユーザとして実行しない `kinit` ください。
- 各クライアントは、最新の更新されたオペレーティングシステムバージョンを使用する必要があります。  
これにより、Kerberosを使用したAES暗号化に最高の互換性と信頼性が提供されます。
- DNS  
正しい名前解決のためにDNSを使用するように各クライアントが適切に設定されている必要があります。
- NTP  
各クライアントがNTPサーバと同期している必要があります。
- ホストおよびドメインの情報  
各クライアントの `/etc/hosts` ファイルと `/etc/resolv.conf` ファイルに正しいホスト名とDNS情報が格納されている必要があります。
- keytabファイル  
各クライアントには、KDCのkeytabファイルが必要です。Realmは大文字で指定する必要があります。セキュリティを最大限に高めるには、暗号化タイプをAES-256にする必要があります。
- オプション：パフォーマンスを最大限に高めるには、ローカルエリアネットワークとの通信用とストレージネットワークとの通信用に少なくとも2つのネットワークインターフェイスを用意する必要があります。

## ストレージシステムの要件

- NFSライセンス  
ストレージシステムに有効なNFSライセンスがインストールされている必要があります。
- CIFSライセンス  
CIFSライセンスはオプションです。マルチプロトコルのネームマッピングを使用する場合にWindowsクレデンシャルを確認するためにのみ必要です。厳密なUNIXのみの環境では必要ありません。
- SVM  
システムでSVMを少なくとも1つ設定しておく必要があります。
- SVMでのDNS  
各SVMでDNSを設定しておく必要があります。
- NFSサーバ

SVMでNFSを設定しておく必要があります。

- AES暗号化

最高レベルのセキュリティを確保するには、KerberosでAES-256暗号化のみを許可するようにNFSサーバを設定する必要があります。

- SMB サーバ

マルチプロトコル環境の場合は、SVMでSMBを設定しておく必要があります。SMBサーバはマルチプロトコルのネームマッピングに必要です。

- ボリューム

SVMで使用するルートボリュームと少なくとも1つのデータボリュームを設定しておく必要があります。

- ルートボリューム

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
セキュリティ形式	UNIX
UID	ルートまたはID 0
GID	ルートまたはID 0
UNIX権限	777

ルートボリュームとは異なり、データボリュームにはどちらのセキュリティ形式も使用できます。

- UNIXグループ

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
pcuser	65534 (SVMを作成するとONTAPによって自動的に作成されます)

- UNIXユーザ

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。
pcuser	65534	65534	NFSトCIFSノマルチプロトコルノシヨウニヒツヨウ  SVMを作成すると、ONTAPで自動的に作成されてpcuserグループに追加されます。
root	0	0	マウントに必要な

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。

- エクスポートポリシーおよびルール

ルートボリューム、データボリューム、およびqtreeに対するエクスポートポリシーと必要なエクスポートルールを設定しておく必要があります。SVMのすべてのボリュームへのアクセスにKerberosを使用する場合は、ルートボリュームのエクスポートルールオプション、`-rwrule`、`-superuser`、を、``krb5i``または``krb5p``に``krb5``設定でき``-rorule``ます。

- Kerberos-UNIXネームマッピング

NFSクライアントユーザSPNによって識別されたユーザにroot権限を付与する場合は、rootへのネームマッピングを作成する必要があります。

#### 関連情報

["NetAppテクニカルレポート4073：『Secure Unified Authentication』"](#)

["NetApp Interoperability Matrix Tool"](#)

["システム管理"](#)

["論理ストレージ管理"](#)

## NFSv4のユーザIDドメインの指定

ユーザIDドメインを指定するには、オプションを設定し``-v4-id-domain``ます。

#### タスクの内容

NFSv4 ユーザ ID のマッピングにデフォルトで使用されるドメインは、NIS ドメインが設定されている場合は NIS ドメインになります。ONTAPNISドメインが設定されていない場合は、DNSドメインが使用されます。たとえば、複数のユーザIDドメインがある場合などに、ユーザIDドメインの設定が必要になることがあります。ドメイン名は、ドメインコントローラのドメイン設定と一致している必要があります。NFSv3の場合は必要ありません。

#### ステップ

1. 次のコマンドを入力します。

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```



## 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。