NFSでのKerberos使用によるセキュリティ強化

ONTAP 9

NetApp
February 12, 2026

目次

NFSでのKerberos使用によるセキュリティ強化 . . . 1
ONTAP の Kerberos に対する NFS サポート . . . 1
ONTAP NFSでKerberosを設定するための要件 . . . 1
ネットワーク環境の要件 . . . 2
NFSクライアントの要件 . . . 2
ストレージ システムの要件 . . . 3
NFSv4のONTAPユーザーIDドメインを指定します . . . 6

NFSでのKerberos使用によるセキュリティ強化

ONTAP の Kerberos に対する NFS サポート

Kerberosは、クライアント / サーバ アプリケーションに対して強力でセキュアな認証を提供し、サーバに対してユーザおよびプロセスのIDの検証機能を提供します。ONTAP環境では、Storage Virtual Machine（SVM）とNFSクライアント間の認証をKerberosで実行できます。

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では、チェックサムを使用して、クライアントとサーバとの間で転送される各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保証など）とデータ整合性に関する理由（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）の両方で有用です。

- プライバシー チェック機能を備えたKerberos 5認証（krb5p）

  krb5pでは、クライアントとサーバ間のすべてのトラフィックがチェックサムで暗号化されます。これによって安全性は高まりますが、負荷も高くなります。

- 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、セキュリティ強化のために、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でサポートされています。

- 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設定に関してクラスタ管理者に頼る必要がなくなり、個別のKerberos Realm設定をマルチテナンシー環境で作成することができます。

ONTAP NFSでKerberosを設定するための要件

NFSでKerberosを使用するための設定をシステムで行う前に、ネットワークおよびストレージの環境のいくつかの項目について、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、クライアントで使用しているオペレーティング システム、ドメイン コントローラ、Kerberos、DNSなどのバージョンや種類によって異なります。このドキュメントでは、それらのすべてについては説明していません。詳細については、それぞれのコンポーネントの対応する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ONTAPとKerberos 5およびNFSv3 / NFSv4の設定方法に関する詳しい例については、テクニカル レポート4073を参照してください。

次の項目について事前に設定しておく必要があります。

ネットワーク環境の要件

- Kerberos

  KerberosをKey Distribution Center（KDC;キー配布センター）で設定しておく必要があります（たとえば、Windows Active DirectoryベースのKerberosまたはMIT Kerberos）。

  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 `nfs`を使用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する必要があります。

- NTP

  タイム サーバでNTPを実行している必要があります。これは、時刻のずれによるKerberos認証の失敗を回避するために必要です。

- ドメイン名解決（DNS）

  それぞれのUNIXクライアントおよびSVM LIFについて、KDCの前方参照ゾーンと逆引き参照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。すべてのコンポーネントは、DNSで正しく解決できる必要があります。

- ユーザ アカウント

  各クライアントは Kerberos レルム内にユーザーアカウントを持っている必要があります。NFSサーバーは、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 “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。

  クライアントでRFC1964およびRFC2203がサポートされ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になっています。

  非常にセキュリティ性の高いAES-256。

- TGT 通信に最も安全な暗号化タイプが有効になっています。
- Kerberos 領域とドメインが正しく設定されています。
- GSSが有効。

  マシンのクレデンシャルを使用する場合：

- `gssd`を `-n`パラメータを付けて実行しないでください。
- `kinit`をrootユーザーとして実行しないでください。

- 各クライアントは、最新かつ更新済みバージョンのオペレーティング システムを使用している必要があります。

  これにより、KerberosでのAES暗号化の互換性と信頼性が最大限確保されます。

- DNS

  DNSを使用して名前が正しく解決され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サーバと同期されている必要があります。

- ホストとドメインの情報

  各クライアントの `/etc/hosts`および `/etc/resolv.conf`ファイルには、それぞれ正しいホスト名とDNS情報が含まれている必要があります。

- keytabファイル

  各クライアントについて、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。最高レベルのセキュリティを得るために、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設定します。

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環境で、Windowsクレデンシャルのチェックを行う場合にのみ必要になります。純粋な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得るために、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。

Name	設定
セキュリティ形式	UNIX
UID	rootまたはID 0
GID	root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 ボリュームのセキュリティ形式は任意に設定してかまいません。

- 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
daemon	1
root	0
pcuser	65534（SVMを作成すると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	ユーザー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 ユーザの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とCIFSのマルチプロトコルで必要 SVMの作成時に、ONTAPによって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

  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 ポリシーとエクスポート ルール

  ルートボリューム、データボリューム、およびqtreeに必要なエクスポート ルールを含むエクスポート ポリシー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がKerberos経由でアクセスされる場合は、ルートボリュームのエクスポート ルール オプション `-rorule`、 `-rwrule`、および `-superuser` を `krb5`、 `krb5i`、または `krb5p`に設定できます。

- Kerberos-UNIXネーム マッピング

  NFSクライアント ユーザのSPNによって識別されたユーザにroot権限を持たせる場合は、rootに対するネーム 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ONTAPユーザーIDドメインを指定します

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

タスク概要

デフォルトでは、ONTAPはNISドメインが設定されている場合、NFSv4ユーザIDマッピングにNISドメインを使用します。NIS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。例えば、複数のユーザIDドメインがある場合は、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する必要があります。NFSv3では必要ありません。

手順

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

商標に関する情報