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で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`てを実行しないで `gssd`ください。

◦ をrootユーザとして実行しない `kinit`でください。

- 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ノマルチフ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

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

商標に関する情報