テクニカル レポート

NFS Kerberos in ONTAP

NetApp
Justin Parisi
2021年6月| TR-4616

概要

このドキュメントでは、NetApp® ONTAP® ソフトウェアでのNFS Kerberosのサポートと、Active DirectoryおよびRed Hat Enterprise Linux（RHEL）クライアントでの設定手順について説明します。

目次

表一覧

図一覧

概要

ドキュメントの範囲

このドキュメントでは、NetApp ONTAPでのKerberos設定について説明します。構成の範囲は、次のコンポーネントを含む環境に限定されます。

- Microsoft Windows 2016 Active Directoryキー配布センター（KDC）
- RHELバージョン6.7以降
- AES-256暗号化方式
- ONTAP 9.5以降

  注： RHELの設定はCentOSクライアントに簡単に適用できます。

多くの場合、この概念は、コマンドさえも、他のクライアントやKDCに適用できます。Windows以外のKDCについては、このドキュメントに「Windows以外のKDCを使用する」という短いセクションがあります。

上記の環境（以前のバージョンのONTAPや異なるLinuxクライアントを使用している場合など）から逸脱する必要があり、このドキュメントで目的の結果が得られない場合は、該当するクライアントOSのドキュメントおよびWindowsのドキュメントを参照してください。

TL；DR-基本的な手順を教えてください

NFS Kerberosに付随する情報を必要とせず、基本的な手順の短いリストを希望する場合は、このセクションを参照してください。また、このリストを手順のチェックリストとして使用し、「一般的な問題」セクションに従ってトラブルシューティングを行うこともできます。このリストの詳細なバージョンは、「詳細な設定手順」セクションにも記載されています。短いリストで立ち往生している場合は、より詳細な設定手順に進むことをお勧めします。

必要なコンポーネントの概要：必要なもの

次のコンポーネントは、ONTAPのKerberos設定でネゴシエートできません。

- 一般的なDNS設定。
- クライアントおよびサーバのフォワードおよびリバースDNSエントリ。
- SPN（NFSマウントに使用される共通名）とDNS名の一致。
- 共通のKDCサーバとレルム情報。
- クライアント、サーバ、およびKDCで5分以内の時間。
- クライアントにインストールされているKerberosユーティリティ。
- キータブ（ドメイン参加プロセス中に作成）。
- krb - UNIXネームマッピングルール
- Kerberosを許可するエクスポートポリシールール
- 受信Kerberos UPNと同じクライアントとサーバで一致するUNIXユーザ名。
- クライアントでKerberosが許可/実行されています。

これらの項目は推奨されますが、オプションであり、必須ではありません。

- NFSv4.xの場合、クライアントとサーバのIDドメインが一致する。
- LDAP / SSSD（ネームサービス/ UNIX ID用）。

NFSクライアントセツテイ

NFS Kerberosクライアントごとに、次の手順を実行する必要があります。

- ホスト名をFully Qualified Domain Name（FQDN；完全修飾ドメイン名）に設定します。
- KDCのDNSにDNSを設定します。
- クライアントとKDCの時間が5分以内であることを確認します（異なるタイムゾーンに合わせてノーマライズ）。
- 必要なKerberosユーティリティをインストールします。
  - CentOS / RHEL 6.x以前の場合は、samba、samba-winbind、samba-winbind-clients、ntp、authconfig -gtk *。
  - CentOS/RHEL 7.x以降では、krb5-workstation（kinit/klistコマンド用）をインストールします。
  - その他のNFSクライアントオペレーティングシステムについては、ベンダーの製品ドキュメントを参照してください。
- NFSクライアントをActive Directoryドメインに追加します。
- `/etc/krb5.conf` Kerberos Realm情報を含むファイルを設定します。
- NFSクライアントのホスト名/IPアドレスをA/AAAAレコード（CNAME）としてDNSに追加し、IPアドレスをPTR（ホスト名とSPNが一致している必要があります）として追加し、を使用してホスト名が解決されることを確認します。`nslookup`
- 必要に応じて、Active DirectoryをLDAPサーバとして使用するようにSSSDを設定します（詳細については TR-4835を参照）。
- Kerberosサービスが開始されていること、NFSクライアント設定でセキュアなNFSが許可されていること（クライアントのオペレーティングシステムのバージョンによって異なります）を確認します。
- 目的の暗号化タイプを使用するようにNFSクライアントマシンアカウントを変更します（NFS KerberosのONTAPではRC4-HMACがサポートされていないため）。
  - または、`/etc/krb5.conf` ファイルを変更して、許可されている暗号化タイプからRC4-HMACを除外します。
- KDCからのKerberosチケットの取得をテストします（kinitとユーザ名/パスワードを使用）。

NFSサーバの設定

この場合、NFSサーバはNetApp ONTAP Storage Virtual Machine（SVM）上のデータLIFの設定を指します。この設定は、無効化や削除が行われないかぎり、一度だけ実行する必要があります。

- SVMにKerberos Realmを作成します。
- SVMのDNS情報をNFSクライアントと同じ情報に設定します。
- NFSサーバオプション `permitted-enc-types` を目的の値に設定します。
- クラスタの日時がKDCおよびNFSクライアントの日時から5分以内であることを確認します（タイムゾーンを考慮）。
- Kerberosで使用するNFSデータLIFのホスト名/ IPアドレスをDNSにA/AAAAレコード（CNAME）として、IPアドレスをPTRとして追加し、を使用して解決されることを確認します。 `nslookup`
- 使用するSPNを指定して、Kerberosに使用するデータLIFを設定します。これは、クライアントがNFSサーバにアクセスする際に使用するDNSホスト名と一致している必要があります（例：nfs/name.domain.com = DNSのA/AAAAレコードname.domain.com）。
  - この手順でデータLIFをドメイン（CIFS / SMBサーバに似ています）に追加しますが、CIFS / SMBに使用されているマシンアカウントとは別のマシンアカウントを使用します。
- NFSサーバのマシンアカウントを調べて、目的の暗号化タイプだけが設定されていることを確認します。
- ボリュームのエクスポートポリシールールでkrb5認証が許可されていることを確認します。
  - `export-policy check-access` krb5がエクスポートへのアクセスを許可されているかどうかを確認するために使用します。
- NFSクライアント用のkrb-UNIXネームマッピングルールを作成します。詳細については、「マシンアカウントのSPNからUNIXへのネームマッピング」を参照してください。
- root以外のUNIXユーザにKerberosマウントへのアクセスを許可する場合は、ONTAPがUNIXユーザ名をUIDに、UIDをユーザ名に解決できることを確認します。（詳細については、TR-4835および『User SPN to UNIX name mapping』を参照してください）。

  - または、デフォルトで同じユーザ名を使用してローカルUNIXユーザおよびグループを設定し、着信UPNをマッピングします。
- NFSv4.xを使用する場合は、NFSサーバオプションのNFSv4ドメインID文字列をNFSクライアントの設定と一致するように設定します（詳細についてはTR-4067を参照）。
- 設定したNFSクライアントからkrb5を使用してNFSマウントをテストします。失敗した場合は、「一般的な問題」セクションを参照してください。

Kerberosの用語

このセクションでは、Kerberosプロセスについて説明する際に使用する主な用語を定義します。このセクションは、ストレージ管理者にとって馴染みのない用語を明確にすることを目的としています。

キー配布センター

KDCは、チケット付与サービス（TGS）と認証サービス（AS）を含む認証サーバです。KDC、AS、およびTGSという用語は同じ意味で使用されます。Microsoft環境では、Active Directoryドメインコントローラは KDCです。

Realm（またはKerberos Realm）

レルム（またはKerberosレルム）には任意のASCII文字列を使用できます。標準では、ドメイン名を大文字で使用します。たとえば、 `domain.com` はレルムになります `DOMAIN.COM`。

管理上、それぞれが `principal@REALM` 一意です。単一点障害（Single Point of Failure）を回避するために、各レルムには、同じデータベース（プリンシパルとそのパスワード）を共有し、同じKDCマスターキーを持つ多数のKDCを含めることができます。Microsoft Windows Active Directoryは、Active Directoryレプリケーションを使用してネイティブにこれを行います。このレプリケーションは、デフォルトで15分ごとに実行されます。

プリンシパル

プリンシパルという用語は'Kerberosデータベース内のすべてのエンティティを指しますクライアント上で実行されるユーザー、コンピュータ、およびサービスはすべてプリンシパルです。すべてのプリンシパルはKerberosデータベース内で一意であり、識別名によって定義されます。プリンシパルには、ユーザプリンシパル名（UPN）またはサービスプリンシパル名（SPN）を使用できます。

主体名は次の3つの部分で構成されます。

- **プライマリ。**プライマリ部分は、ユーザまたは「NFS」サービスなどのサービスです。また、このサービスプリンシパルがFTP、RSH、NFSなどのさまざまなネットワークサービスを提供するように設定されていることを示す特別なサービス「host」にすることもできます。
- **インスタンス。**ユーザーの場合、この部分はオプションです。ユーザは複数のプリンシパルを持つことができます。たとえば、Fredには日常的に使用するプリンシパルと、sysadminアカウントなどの特権的な使用を許可するプリンシパルがあります。インスタンスはサービスプリンシパルに必要であり、サービスを提供するホストのFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を指定します。
- **レルム。**Kerberos Realmは、Kerberosサーバ内に登録された一連のKerberosプリンシパルです。通常、レルム名はDNS名と同じですが、大文字に変換されます。大文字は必須ではありませんが、DNS名とレルム名を簡単に区別できます。

次のプリンシパルの例を参照してください。

```
user@DOMAIN.COM
user/admin@DOMAIN.COM
host/host.domain.com@DOMAIN.COM
root/host.domain.com@DOMAIN.COM
nfs/host.domain.com@DOMAIN.COM
```

チケット

チケットは、サービスのプリンシパルのIDを確認し、セッションキーを含む一時的な資格情報のセットです。チケットには、サービス、アプリケーションチケット、またはチケット交付チケット（TGT）があります。

シークレットキー

Kerberosでは、対称キーシステムを使用します。このシステムでは、秘密キーが暗号化と復号化の両方に使用されます。秘密鍵は、一方向ハッシュ関数を使用してプリンシパルのKerberosパスワードから生成されます。KDCは各プリンシパルのパスワードを保存するため、プリンシパルの秘密鍵を生成できます。Kerberosサービスを要求するユーザの場合、シークレットキーは通常、 `kinit` プログラムに提示されたパスワードから取得されます。通常、サービスプリンシパルとデーモンプリンシパルはパスワードを使用しません。代わりに、一方向ハッシュ関数の結果がkeytabに格納されます。

keytab

keytabには'プリンシパルとその秘密キーのリストが含まれていますkeytabのシークレットキーは、ランダムなパスワードを使用して作成されることが多く、主にサービスプリンシパルまたはデーモンプリンシパルに使用されます。

サポートされる暗号化タイプ

NetApp ONTAPテクノロジでは、動作モードと使用するバージョンに応じて、特定の暗号化タイプでNFS Kerberosがサポートされます。

クライアントが確実に適切な暗号化タイプを使用するには、 `krb5.conf` 可能であれば、オブジェクトプリンシパル（マシンアカウントなど）またはファイルではなくkeytabファイルで有効な暗号化タイプを制限します。このアプローチは、大規模なエンタープライズ環境ではるかに拡張性が高く、自動化が容易であり、サポートされている場合はクライアントがより強力な暗号化タイプを使用できることを確認します。

表1 に、ONTAPのバージョンと動作モードに基づいてサポートされる暗号化タイプを示します。これらのタイプはNFS Kerberos専用であり、CIFS Kerberosのサポートは含まれていません。

表1）ONTAPでサポートされる暗号化タイプ

ONTAPのバージョンとモード	サポートされる暗号化タイプ
Data ONTAP 7-Mode 7.x以降	DESおよびDES3のみ **注**：（RC4-HMACは機能しますが、公式サポートはありません）
Data ONTAP 8.2.x以前（clustered）	DESおよびDES3
Data ONTAP 8.3.x	AES（128ビットおよび256ビット）、DES、およびDES3
ONTAP 9.x	AES（128ビットおよび256ビット）、DES、およびDES3

サポートされるKerberosセキュリティモード

暗号化タイプの概念に加えて、Kerberosにはセキュリティレベルと整合性チェック機能もあり、NFSトラフィックにエンドツーエンドの暗号化を提供することで中間者攻撃を防ぐことができます。表2 に、ONTAPのさまざまなバージョンでサポートされているKerberosセキュリティモードのレベルを示します。Kerberosのセキュリティモードは、クライアントとKDCで設定されます。その後、特定のセキュリティモードを許可するようにエクスポートポリシールールを設定できます。

表2）ONTAPでサポートされるKerberosセキュリティモード

ONTAPのバージョンとモード	サポートされるKerberosセキュリティモード
Data ONTAP 7-Mode 7.x以降	krb5、krb5i、krb5p
Data ONTAP 8.2.x以前（clustered）	krb5
Data ONTAP 8.3.x	krb5、krb5i

ONTAPのバージョンとモード	サポートされるKerberosセキュリティモード
ONTAP 9.x	krb5、krb5i、krb5p

ONTAPでのNFSでのKerberos認証の動作

Kerberosは、秘密キーを使用してプリンシパルのIDを検証する認証プロトコルです。

Windows Active DirectoryなどのKDCでは、プリンシパルとそのKerberosパスワードのデータベースが維持されます。秘密鍵は、暗号鍵形式に変換されたプリンシパルのパスワードにすぎません。NFSサーバおよびクライアントの場合、シークレットキーはランダムなパスワードを使用して生成でき、NFSサーバまたはクライアントのkeytabに格納されます。

Kerberosでは、秘密鍵は一意のIDの証明と見なされます。そのため、KDCは、マウント時にNFSサーバのSPNに対してNFSクライアントのSPNを認証するなど、他のすべてのプリンシパルの認証を信頼できます。NFSマウントポイントへのユーザアクセス用に、NFSサーバSPNに対するユーザプリンシパルを認証することも信頼できます。Kerberosでは、認証用にクリアテキストのパスワードはネットワーク経由で送信されません。

NFSマウントプロセス時のKerberos

NFSクライアントがKerberosを使用してマウントすると、次のプロセスが実行されます。

- DNSにホスト名/IPルックアップが照会されます。DNS名は、NFS SPN要求の作成に使用されます。
- NFSクライアントSPNは、KDCから認証サービス要求（AS-REQ）を実行するために使用されます。
- NFSクライアントSPNがKDCに存在し、パスワード/ keytab認証が成功すると、NFS SPNのクライアントからTicket Granting Service要求（TGS-REQ）が開始されます。
- NFSクライアントのSPNは、ONTAPでのkrb-unixネームマッピング処理で使用されます。Kerberos SPNを有効なUNIXユーザにマッピングできる場合は、マウント要求が許可されます。有効なネームマッピングがない場合、アクセスは拒否されます。（詳細については、「マシンアカウントSPNからUNIXへのネームマッピング」を参照してください）。
- NFSサーバのエクスポートポリシールールによって、クライアントアクセスが許可されているかどうかがチェックされます。NFS Kerberosを使用したクライアントへのアクセスが許可されていれば、マウントは成功します。エクスポートポリシールールにクライアントが含まれていない場合、またはルールでKerberosが許可されていない場合、アクセスは拒否されます。詳細については、「エクスポートポリシーのトラブルシューティング」を参照してください。

図1 に、NFS Kerberosマウント要求のAS-REQカンバセーションのパケットキャプチャを示します。

図1）マウント時のKerberos AS-REQカンバセーション-パケットキャプチャ

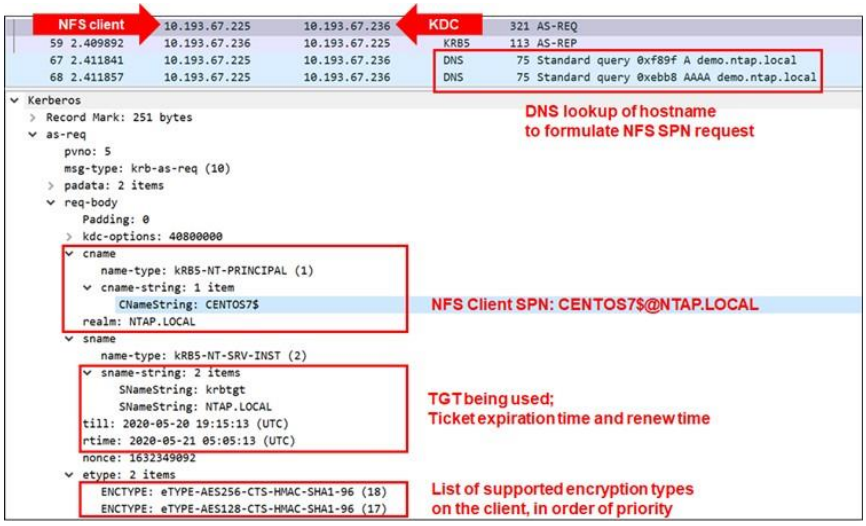
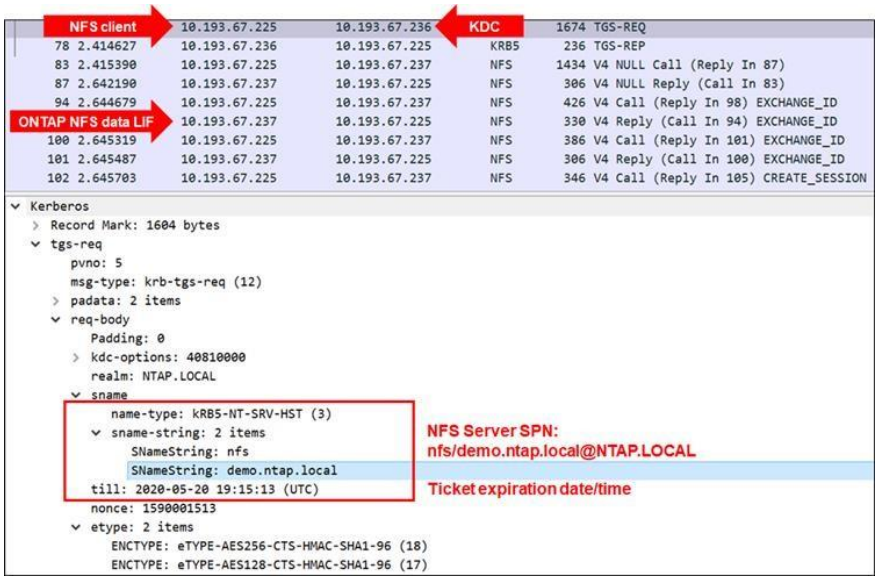


図2 に、NFSマウントプロセス中のTGS-REQカンバセーションを示します。

図2）マウント時のKerberos TGS-REQカンバセーション-パケットキャプチャ



Kerberos SPN形式

Kerberos SPNには、Kerberosのマウントおよびアクセスプロセスで送信される形式がいくつかあります。

- `root/host.domain.com` NFSクライアントがマウント要求に使用します。
- `nfs/server.domain.com` は、NFSサーバによって使用されます（例：`nfs/cluster.domain.com`）。
- `host/host.domain.com` は、NFSクライアント（通常はSSSDなどのサードパーティアプリケーション用）で使用されます。
- `CLIENT$` NFSクライアントがマウント要求に使用しますが、この形式は通常Windows KDCでのみ使用されます。

上記のいずれかのタイプを使用してActive Directoryでプリンシパルを作成できますが、必要なプリンシパルは1つだけです。図1 の例では `CLIENT$ SPN`、という形式が使用されて `realm join`います。これは、を使用してNFSクライアントがドメインに参加する場合のデフォルトです。

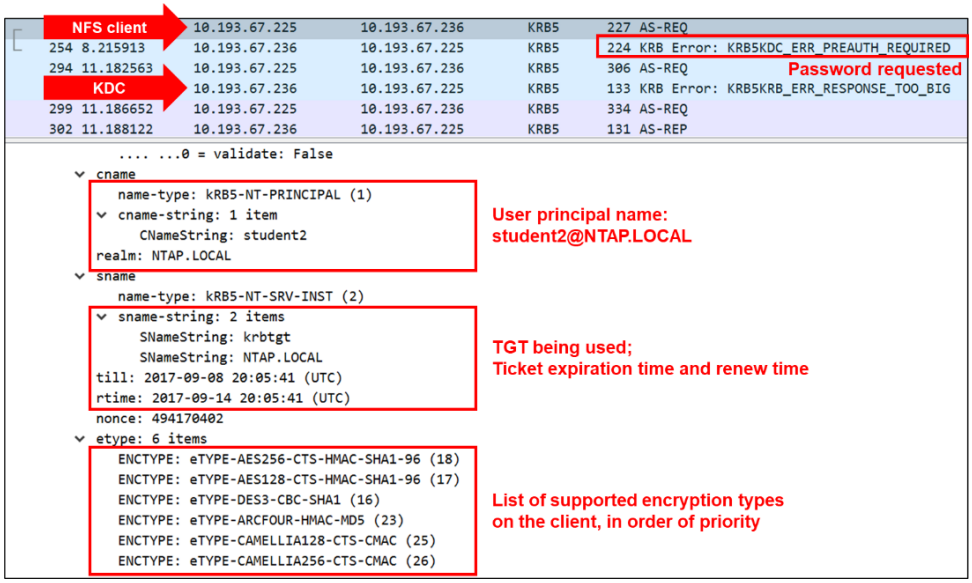
NFSマウントアクセス時のKerberos

ユーザやサービスなどのKerberosプリンシパルがを使用してKerberos Realmにログインする `kinit`と、プリンシパルは、パスワードやシークレットキーではなく、プリンシパル名を含むTGT要求を `krb5kdc` デーモンに送信します。これはAS-REQと呼ばれます。

この要求を受信すると、KDCはKDCデータベースのプリンシパルを検索し、データベースから関連付けられたパスワードを使用してTGT応答を暗号化します。

プリンシパルが存在する場合、暗号化されたTGTがKDCから要求者に送信されます。プリンシパルは、パスワードまたはkeytabから取得した秘密鍵を使用して、TGT応答を復号化します。この会話を図3に示します。

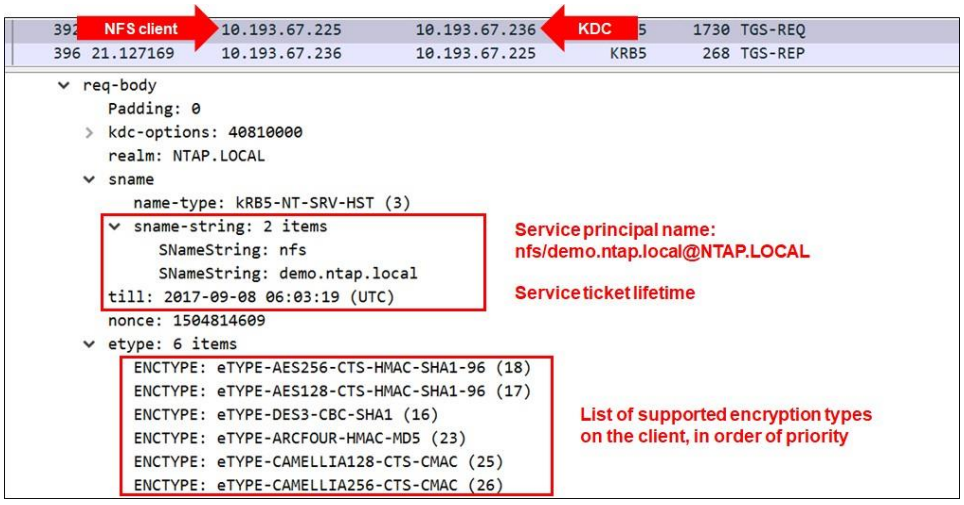
図3）kinit時のKerberos AS-REQカンバセーション（パケットキャプチャ）



次に、プリンシパルはNFSサーバプリンシパルと暗号化されたTGTをチケット付与サーバ（TGS）に提示することで、NFSサーバ（この場合はONTAP）に認証を要求します。これは、ユーザがNFSエクスポート（TGS-REQ）にアクセスしようとしたときに発生します。

その後、TGSはNFSサーバのチケットを発行します。このチケットは、プリンシパルがマウントできるようにするための認証（NFSクライアントSPNの場合）、またはNetAppクラスタからNFS経由でマウントされた特定のファイルシステムを使用できるようにするための認証（ユーザプリンシパルの場合）を提供します。このTGS-REQカンバセーションを図4に示します。

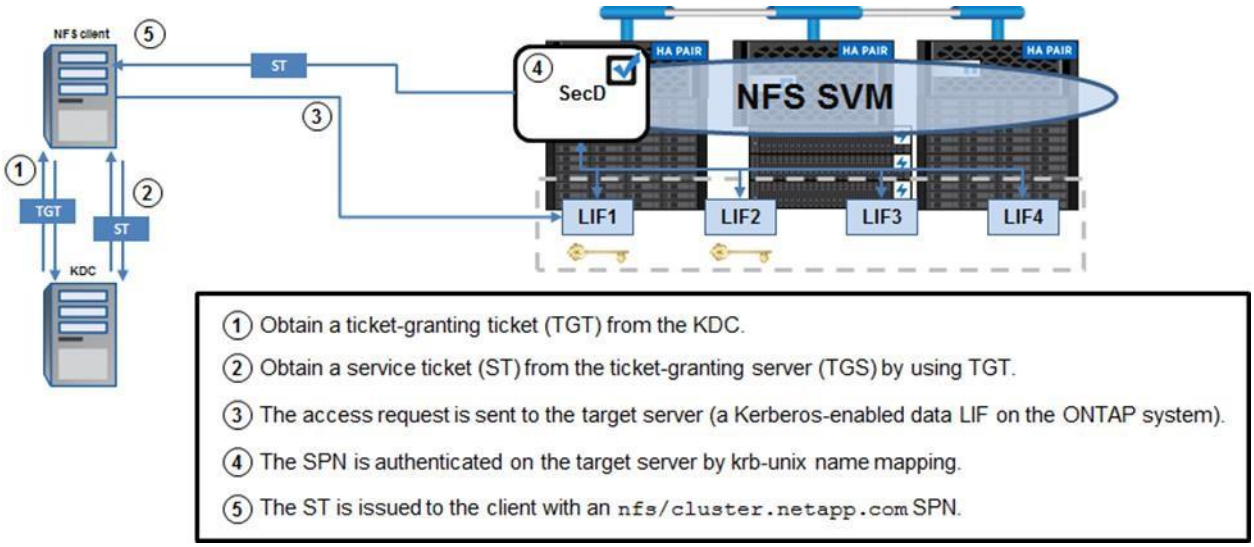
図4）kinit時のKerberos TGS-REQカンバセーション（パケットキャプチャ）



NFSサーバはkeytabエントリを使用してTGSの一部を復号化するため、ONTAP NFSサーバとKDCの間でKerberos通信は行われません。図5 は、クライアント、KDC、NFSサーバ間のKerberosワークフローを示しています。

ONTAPでは、キャッシュがクリアされるか（タイムアウトまたは手動コマンドによって）ノードがリブートされるまで、Kerberosチケットがキャッシュされます。詳細については、「Kerberosキャッシュ」を参照してください。

図5）クライアント、KDC、NetAppストレージ上のNFSサーバ間のKerberosワークフロー



krb - UNIXネームマッピングの動作

ONTAPには、`krb-unix` NFS Kerberos認証のためにKerberos SPNをONTAPにマッピングする方法を制御するネームマッピングルールがあります。Kerberos SPNをONTAPにマッピングすると、NFSエクスポートでユーザをどのように表示するかが制御されます。つまり、権限はユーザが誰として認証したかによって異なります。NFS Kerberosマウントでは、3つの `krb-spn` マッピングが実行されます。

マシンアカウントのSPNからUNIXへのネームマッピング

ONTAPへの最初のKerberosマウント要求では、マシンアカウントSPNが認証に使用されます。ONTAPは、通常のユーザ名と同じルールを使用して、有効なUNIXユーザにSPNをマッピングしようとします。

- 1：1のネームマッピング（name== name）
- `krb-unix` ネームマッピングルール（明示的なネームマッピング定義）

マシンアカウントSPNは、クライアントのKerberos keytabファイル（`/etc/krb5.keytab`）によって定義され、クライアント管理者がクライアントをKerberos用に設定した方法によって異なります。`Samba/realm/net ads` を使用してActive Directoryドメインに参加する場合、keytabファイルには次の形式のSPNが含まれます。

```
root/fqdn.domain.com@DOMAIN.COM
host/fqdn.domain.com@DOMAIN.COM
SHORTNAME$@DOMAIN.COM
```

上記の例では、1：1のネームマッピングが次のUNIXユーザにマッピングされます。

```
root
host
SHORTNAME$
```

これらの名前のUNIXユーザが存在しない場合、ONTAPはネームマッピングルールを検索して初期マウントアクセスを決定します。krb-UNIXネームマッピングに有効なUNIXユーザが存在しない場合、マウントは「permission denied」で失敗し、EMSメッセージがONTAPに記録されます。

有効なUNIXユーザが存在する場合（エクスポートポリシールールで許可されている場合）、NFS Kerberosのマウントは成功します。この認証プロセスは、 `root` Kerberosマウントでのユーザの処理方法を制御します。

例：

- ONTAPにマッピングされるSPNがの場合、 root/fqdn.domain.com@DOMAIN.COMroot はです root。root ユーザには root、常に取得されるのと同じ権限が付与されます。
- ONTAPにマッピングされているSPNがである場合は host/fqdn.domain.com@DOMAIN.COM、が root host ユーザになります。の権限/ファイル所有権 root は、に許可されるアクセスによって決まり hostます。
- ONTAPにマッピングされるSPNがである場合 SHORTNAME$@DOMAIN.COM、は root マシンアカウントがマッピングされるユーザになります。 SHORTNAME$ ユーザが存在する場合は、が root ユーザになり SHORTNAME$ます。すべてのコンピュータ名に対してネームマッピングルールが存在する場合（「NFSクライアントプリンシパルをマッピングするUNIXユーザまたはネームマッピングルールの作成」を参照）、その後、SHORTNAME$ SPNがルール内のマッピングされたユーザになります。の権限/ファイル所有権 root はマッピングされたUNIXユーザによって決まります。

  注： NFSクライアントからONTAPへのマッピング方法は root、ユーザアクセスを管理することで、セキュリティを強化するレイヤとして使用できます。

ユーザSPNからUNIXへのネームマッピング

ユーザがを使用して、 kinit NFSサービスチケット（ST）によってNFS Kerberosマウントにアクセスするために使用されるKerberos TGTを取得する場合、認証目的でそのユーザをONTAPに提示する方法も制御します。

たとえば、というUNIXユーザ student1 がという kinit ユーザにを使用している場合、 student2@NTAP.LOCAL そのユーザは krb-unix というネームマッピングを使用してONTAPにマッピングされ student2@NTAP.LOCALます。マシンアカウントSPNと同じネームマッピングロジックを使用して、次のプロセスが適用されます。

- 1：1のネームマッピング（name== name）
- krb-unix ネームマッピングルール（明示的なネームマッピング定義）

つまり、UNIXユーザ student1 （uidNumber 1301）がマウントにアクセスしていても、は kinit student2 SPN（uidNumber 1302）を使用して実行されたため、student1 student2 アクセス用になります。

ユーザが kinit（UNIXユーザIDを持たない）KDC内の有効なユーザを使用してにアクセスしようとすると、マウントへのアクセスは失敗します。次の例は、2つのシナリオを示しています。

例1：有効なUNIXユーザ名を持つユーザからKerberos TGTを取得するユーザ

次の例で student1 は、が student2 ログインクレデンシャルを使用しています。おそらくこの場合、 student2 student1 Homedirに書き込みをしようとしていますが、 student2 ログイン情報しかありません。

```
# id student1
uid=1301(student1) gid=1101(group1) groups=1101(group1),1203(group3),1220(sharedgroup)
# id student2
uid=1302(student2) gid=1101(group1)
groups=1101(group1),1203(group3),1220(sharedgroup),10000(Domain Users),1202(group2)
```

student1 student2 自身のhomedirへの書き込みアクセス権を持つユーザは、次のとおりです。

```
# ls -la | grep student
drwxr-xr-x   2 student1              group1                4096 Apr 24 13:42 student1
drwxr-xr-x   2 student2              group1                4096 Apr 24 13:42 student2
```

になります student1が、 student2次のようにkinit/loginできます。

```
# su student1
sh-4.2$ kinit student2
Password for student2@NTAP.LOCAL:
sh-4.2$ klist -e
Ticket cache: KEYRING:persistent:1301:1301
Default principal: student2@NTAP.LOCAL

Valid starting       Expires              Service principal
```

```
04/24/2020 13:27:44 04/24/2020 23:27:44 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/01/2020 13:27:44, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

これを行うと、 student2 期待される結果であるhomdirへの書き込みアクセスのみが可能になります。

```
sh-4.2$ cd student1
sh-4.2$ touch newfile-student1-student2
touch: cannot touch 'newfile-student1-student2': Permission denied

sh-4.2$ cd student2
sh-4.2$ touch newfile-student1-student2
sh-4.2$ ls -la | grep newfile-student1-student2
-rw-r--r--  1 student2 group1    0 Apr 24 13:28 newfile-student1-student2
```

student1 本当になることができる唯一の方法 student2 は、 student1 が student2s パスワードを持っている場合です。NFS Kerberosを使用すると、共有にアクセスするユーザが実際のユーザであることを確認できます。

例2：あるユーザが、有効なUNIXユーザ名*がない*ユーザからKerberos TGTを取得する

この例では、kinit KDC内の有効なユーザ（Windowsサービスアカウントなど）に対してが実行されますが、そのユーザには有効なUNIX IDがありません。この場合、ユーザはLDAP認証に使用されるバインドユーザです（ユーザ名は）bind。ONTAPでLDAPを設定する方法については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

ユーザがNFSクライアント上にUNIXユーザとして存在するかどうか、およびONTAPが有効なUNIXユーザを見つけることができるかどうかを確認します。

```
# id bind
id: bind: no such user

cluster::*> getxxbyyy getpwbyname -node cluster-01 -vserver DEMO -username bind
  (vserver services name-service getxxbyyy getpwbyname)

Error: command failed: Failed to resolve bind. Reason: Entry not found for "bind: bind".
```

この場合、は student2 まだ持っていないアクセス権を取得しようとしています。今回は、LDAP bind ユーザを使用してKerberosアクセスを取得しようとします。

```
# su student2
sh-4.2$ kinit bind
Password for bind@NTAP.LOCAL:
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1302:1302
Default principal: bind@NTAP.LOCAL

Valid starting       Expires              Service principal
04/24/2020 13:48:22 04/24/2020 23:48:22 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/01/2020 13:48:22
```

バインドユーザには有効なUNIX IDがないため、有効なNFSサービスチケットが発行されていても、マウントアクセスは失敗します。これは、権限を決定するには有効なUNIXユーザが必要であるためです。ユーザなし=アクセスなし。

```
sh-4.2$ cd /kerberos/
sh: cd: /kerberos/: Permission denied


sh-4.2$ klist
Ticket cache: KEYRING:persistent:1302:1302
Default principal: bind@NTAP.LOCAL

Valid starting       Expires              Service principal
04/24/2020 13:49:27  04/24/2020 23:48:22  nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/01/2020 13:48:22
04/24/2020 13:48:22  04/24/2020 23:48:22  krbtgt/NTAP.LOCAL@NTAP.LOCAL
```

```
        renew until 05/01/2020 13:48:22
```

クラスタイベントログには、`event log show`次のエラーログが記録されています。

```
ERROR         secd.nfsAuth.problem: vserver (DEMO) General NFS authorization problem. Error: RPC
accept GSS token procedure failed
  [ 0 ms] Using the NFS service credential for logical interface 1034
(SPN='nfs/demo.ntap.local@NTAP.LOCAL') from cache.
  [     0] GSS_S_COMPLETE: client = 'bind@NTAP.LOCAL'
  [     1] Trying to map SPN 'bind@NTAP.LOCAL' to UNIX user 'bind' using implicit mapping
  [     1] Unix User Name found in Name Service Negative Cache
  [     1] Unable to map SPN 'bind@NTAP.LOCAL'
**[     1] FAILURE: Unable to map Kerberos NFS user 'bind@NTAP.LOCAL' to appropriate UNIX user
  [     1] Failed to accept the context: The routine completed successfully (minor: Unknown
error). Result = 6916
```

これは、有効なKerberosチケットにアクセスするだけでは、ONTAP内のKerberos NFSマウントへのアクセスは保証されないことを示しています。ユーザSPN/UPNも、有効なUNIXユーザ名に解決できる必要があります。

ユーザSPNマッピング用のローカルUNIXユーザの作成

LDAPなどのネームサービス（Cloud Volumes ONTAPなど）にアクセスできない場合もあります。また、Kerberosのニーズが限られている場合もあります。アクセスが必要なのは少数のユーザのみです。これは、LDAPサーバ全体をID用に設定することを正当化するものではありません。ほとんどの場合、Apacheや NetApp NIPAMモジュールなどのアプリケーションに必要なユーザは1人だけです。そのため、このようなユースケースでは、単純にローカルUNIXユーザを作成した方が簡単な場合があります。

ONTAPでローカルUNIXユーザを作成するには、次のコマンドを実行して、ユーザ名と数値IDがクライアントのものと一致すること、およびUNIXグループも作成されることを確認します。

```
cluster::> unix-group create
cluster::> unix-user create
```

ユーザとグループが作成されると、そのユーザ名（user@REALM.COM）のKerberos SPNが自動的にユーザにマッピングされ、ONTAPへの適切な認証が行われます。

ユーザSPNの明示的なネームマッピングルールの作成

ユーザSPNを別のUNIXユーザにマッピングする場合や、すべてのユーザSPNを同じUNIXユーザにマッピングする場合は、ネームマッピングルールを使用できます。ただし、このオプションを使用すると、受信KerberosユーザSPNのID検証の目的が失われるため、ほとんどの場合、このオプションは推奨されません。ただし、一部のユースケース（単一のUNIXユーザのみを使用するアプリケーションなど）では、この方法が推奨される場合があります。

`krb-unix` ネームマッピングルールを作成するには、次のコマンドを実行します。

```
cluster::> vserver name-mapping create -vserver NFS -direction krb-unix ?
   [-position] {1..2147483647}          Position
   [-pattern] <text (size 1..256)>      Pattern
   [-replacement] <text (size 1..256)>  Replacement
  { [[-address] <IP Address/Mask>]      IP Address with Subnet Mask
  | [ -hostname <text> ] }              Hostname
```

グローバルユーザSPN/UPNネームマッピングを作成する（たとえば、すべてのマシンアカウントSPNまたはユーザSPNを「apache」ユーザにマッピングする）には、次の例を参照してください。

```
Vserver:   DEMO
Direction: krb-unix
Position Hostname            IP Address/Mask
-------- ------------------- --------------------

1        -                   -                       Pattern: (.+)\$@NTAP.LOCAL << MACHINE$ SPN
                                                  Replacement: apache
2        -                   -                       Pattern: host/(.+)@NTAP.LOCAL << host/ SPN
                                                  Replacement: apache
```

```
3       -                -                    Pattern: (.+)@ntap.local << user SPN
                                          Replacement: apache
```

NFSサービスのSPNからUNIXへのネームマッピング

ユーザがログインしてKDCで有効なユーザになり、を使用してTGTを取得すると `kinit`、NFSサービスのSPNが有効なUNIXユーザにマッピングされていれば、そのユーザはKerberos NFSマウントにアクセスできます。このプロセスで失敗すると、Kerberosエクスポートへの変更時に「permission denied」または「not a directory」エラーが発生します。

NFSサービスSPNは、ONTAPのデータインターフェイスでKerberosを有効にすると定義されます。通常、NFSサービスSPNは次の形式を使用します。

```
nfs/nfsservername.domain.com@DOMAIN.COM
```

上記の例では、NFSサービスSPNは `nfs` firstという名前のUNIXユーザへのマッピングを試行します。これに失敗すると、ONTAPは明示的なネームマッピングルールを検索します。そのSPNマッピングに有効なUNIXユーザが存在しない場合、要求は失敗し、ONTAPにエラーが記録されます。

ユーザがマウントにアクセスすると、KDCでSPNが照会されます。NFSクライアントがSPNを要求する方法は、マウントで指定されたNFSサーバの名前解決によって異なります。ほとんどの場合、DNSが推奨されますが、ローカルホストファイルも使用できます。詳細については、「DNSの代わりにローカルホストファイルを使用する」を参照してください。

Kerberos対応NFSを使用する利点

Kerberosは、ユーザとホストの認証モードです。この認証は、ファイルやディレクトリのアクセス制御リスト（ACL）またはモードビットを使用してユーザのアクセスを決定する許可と混同されることがあります。許可は、ユーザまたはホストの認証後に実行されます。

- 認証はあなたが誰であるかを証明します。
- 許可を使用すると、認証後に必要な操作を行うことができます。

たとえば、地下鉄の切符を購入すると、ターンスタイル(認証)を通過できます。ただし、乗車券にアクセス(許可)が明記されていない場合は、駅内に入ってから目的地までの移動が許可されない場合があります。

ONTAPでNFS Kerberosを使用するメリットは次のとおりです。

- プレーンテキストのパスワードがネットワーク経由で渡されないようにする
- AES-256およびAES-128によるエンドツーエンドのエンタープライズクラス暗号化
- `krb-unix` ネームマッピングルールによるSPNからユーザマッピングへの制御
- 標準のAUTH_SYS（最大16）と比較して、グループメンバーシップの制限が引き上げられました（最大32）。

  注： ONTAP 8.3以降では、AUTH_SYSとAUTH_GSSの両方で、AUTH_SYSとAUTH_GSSの制限を1、024に上げることができます。ONTAPでNFSの補助グループの制限を拡張する方法の詳細については、TR-4067：『NFS Best Practice and Implementation Guide』を参照してください。

ONTAP構成

このセクションでは、NFS Kerberosを設定するためにNetApp ONTAPを設定する方法について説明します。ここでは、ONTAPでNFS Kerberosを設定する場合の手順を順番に説明しています。

このセクションでは、次のトピックについて説明します。

- NFSサーバの設定

- ONTAPでのDNS設定の構成
- Kerberos Realmの作成
- データLIFでKerberosを有効にする
- エクスポートポリシールールを変更してKerberosを許可する
- UNIXユーザまたはネームマッピングルールを作成してNFSサービスプリンシパルをマッピングする
- UNIXユーザまたはネームマッピングルールを作成してNFSクライアントプリンシパルをマッピング
- AESのみを許可するようにNFSサーバマシンアカウントを変更する

NFSサーバの設定

NFSサーバの場合は、オプションを有効にして設定し、クライアントに必要な機能を提供する必要があります。NFS Kerberosを設定する前に、使用するNFSのバージョン、選択するオプションなどを決定しておく必要があります。NFS構成を決定する際に役立つ情報については、TR-4067を参照してください。NFS Kerberosの場合は、次の点も考慮してください。

- **NFSv3ではすべてをKerberosに対応できません。**NFSv3には、マウント、ポートマッパー、NLMなどの補助プロトコルがあります。ONTAPのKerberosは、プロトコルバージョンのNFSの部分のみに対応しています。NFSv4.xではスタック全体が標準に従って結合されるため、スタック全体をKerberos対応にできます。

  注： ONTAP 8.2P5以前でNFSv3にKerberosを使用する場合は、エクスポートポリシールールで `sys` と `krb5*`（バグ756081に従って）が許可されていることを確認してください。（バグリンクを表示するには、NetAppサポートへのログインが必要になる場合があります）。

- **NFSv3ではkrb5iとkrb5pを使用できます。**NFSv3を使用する場合はNFSパケットを暗号化できますが、前述のように、NFSv3の補助プロトコルではKerberosは使用されません。
- **NFS Kerberosを使用すると、パフォーマンスが低下します。**Kerberosを使用するとパフォーマンスが低下します。詳細については、「NFS Kerberos Performance Testing」を参照してください。
- **安全性の低い暗号化タイプの削除を検討してください。**ONTAPのNFSサーバでは、作成時に次の暗号化タイプ（enctypes）がデフォルトで許可されます。

```
des,des3,aes-128,aes-256
```

DESとDES3は、安全性の低いエンコーディングタイプです。実際、最新のWindows KDCでは、DESはデフォルトで無効になっています。DESまたはDES3が不要な場合は、リストから削除します。ONTAP SVMでKerberosを有効にしたあとにエンタイプを削除するにはダウンタイムが必要です。ONTAPでNFS Kerberosを有効にする前に、エンタイプを削除することを推奨します。

ONTAP SVMでDESとDES3を無効にするには、次の手順を実行します。

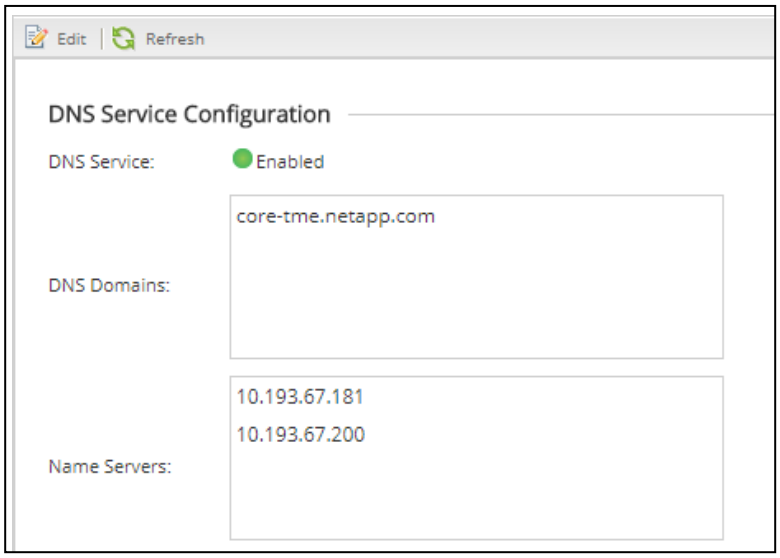
```
cluster::> nfs modify -vserver [vserver] -permitted-enc-types aes-*
```

注：現在、ONTAP System Managerを使用して、許可されている暗号化タイプを変更することはできません。

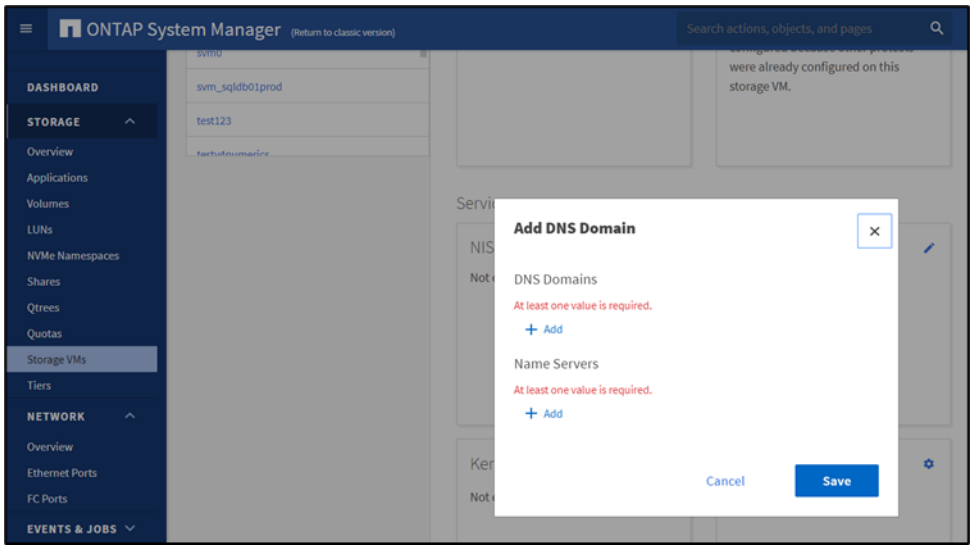
ONTAPでのDNS設定の構成

Active Directory接続およびONTAPでのKerberos機能のためにDNSルックアップが適切に機能するためには、DNSをデータSVMレベルで設定する必要があります。DNSは、ONTAPシステムマネージャまたはコマンドラインを使用して設定できます。DNSサーバは、/AAAAレコードまたはDNS転送/委譲を使用して、クラスタのデータLIFとクライアントのホスト名を解決できる必要があります。

ONTAP 9.7より前のSystem ManagerでDNSを設定するには、[SVM]>[SVM設定]>[DNS / DDNS]に移動します。



ONTAP System Manager 9.7以降でDNSを設定するには、[サービス]セクションで[ストレージ]>[Storage VM]>[DNS]に移動し、歯車の記号をクリックします。



CLIでDNSを設定するには、次のコマンドを実行します。

```
cluster::> dns modify -vserver [SVM] -domains [domain1,domain2..] -name-servers [IP1, IP2..]
```

SVMデータLIFのDNSレコードを追加または組み込みのDNSを設定する

NFS Kerberosに参加するSVMのデータLIFをDNSに追加する必要があります。LIFは、/AAAAレコードおよびPTRレコードを使用して追加するか、組み込みのDNSを利用して追加できます。このタスクは、DNS管理者に依頼して実行してください。内蔵DNSの設定やDNSへのレコードの追加については、TR-4523を参照してください。

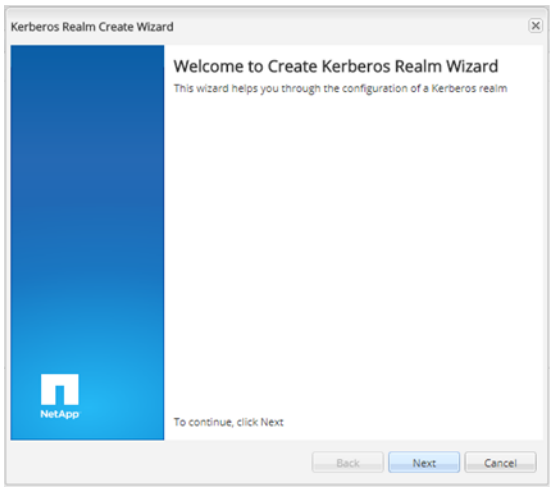
Kerberos Realmの作成

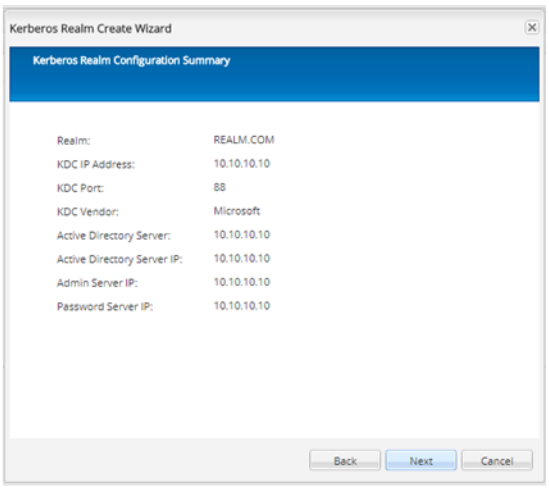
Kerberos Realmは、Kerberosチケット要求を適切にフォーマットする方法をクラスタが認識できるようにする必要があります。ONTAPでのRealmの作成は、 `/etc/krb5.conf` NFSクライアントでの設定に似ています。Kerberos realmコマンドで指定されたIPアドレスは、マシンアカウントオブジェクトまたはSPNの作成時にのみ使用されます。Kerberosを有効にした後は、これらのIPアドレスは実際のKerberos対応NFSトラフィックには使

用されません。そのため、これらのコマンドでフェイルオーバーやDNSエイリアスのKDCを指定する必要はありません。Kerberosトラフィックの KDCフェールオーバーは、DNS SRVレコードを使用して処理されます。

Kerberos Realmは、ONTAP System ManagerまたはCLIを使用して作成できます。ONTAP 9.7より前のバージョンのSystem ManagerでKerberos Realmを作成するには、次の手順を実行します。

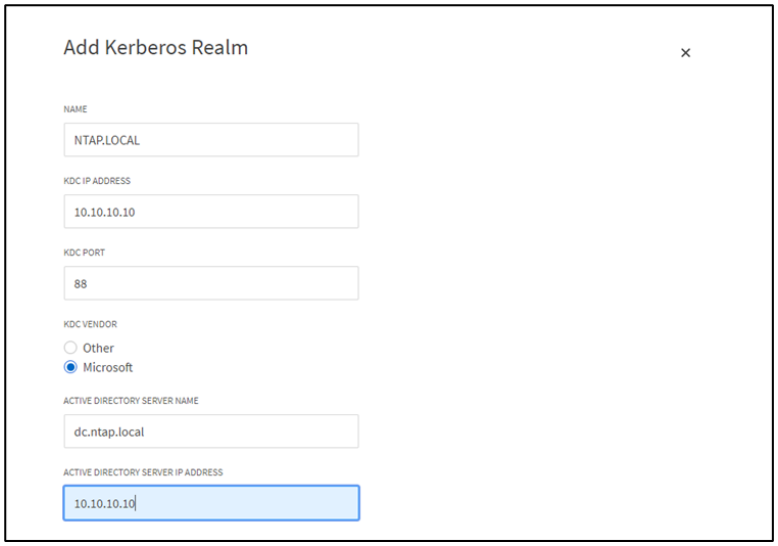
1. [SVMs]>[SVM設定]>[サービス]>[Kerberos Realm]の順に選択します。
2. レルム設定がウィザードとして表示されます。各画面で値を入力し、[Next]をクリックします。





ONTAP 9.7以降のSystem ManagerでKerberos Realmを作成するには、次の手順を実行します。

1. [サービス]セクションで、[ストレージ]>[Storage VM]>[Kerberos]を選択します。
2. [Add]をクリックし、フィールドに値を入力します。



CLIでKerberos Realmを作成するには、次のコマンドを使用します。

```
cluster::> kerberos-realm create -configname REALM -realm DOMAIN.NETAPP.COM -kdc-vendor Microsoft
-kdc-ip 10.63.98.101 -kdc-port 88 -clock-skew 5 -adminserver-ip 10.63.98.101 -adminserver-port
749 -passwordserver-ip 10.63.98.101 -passwordserver-port 464 -adserver-name WIN2K8-DC -adserver-
ip 10.63.98.101
```

データLIFでKerberosを有効にする

NFSにKerberosを使用するには、SVM内のデータLIFでKerberosを有効にする必要があります。Kerberosを有効にすると、SPNが定義され、Kerberos Realm設定で指定したKDCにプリンシパルが作成されます。デフォルトでは、このマシンアカウントは、NFS SPNの最初の15文字（の `nfs/` 部分を含む）のみを使用します。そのため、Kerberos対応のデータLIFを複数使用する場合は、最初の15文字以内で一意の名前を使用します。後でマシンオブジェクト名の重複による問題を回避するために、 `-machine-account` コマンドでオプションを指定するか、事後にマシンアカウントオブジェクトの名前を変更します。マシンアカウントの名前を変更する方法の詳細については、「Active DirectoryでのNFS Kerberosマシンアカウントの名前変更」を参照してください。

ONTAPでKerberosが有効になっている場合、KDCに接続してクレデンシャルが交換されます。入力したクレデンシャルには、Active Directoryのコンピュータの組織単位（OU）にオブジェクトを作成する権限が必要です。このユーザは、ドメイン管理者、またはそのOUの管理を委任された権限を持つユーザです。Windows以外のKDCの場合は、SPNを作成および変更できる必要もあります。

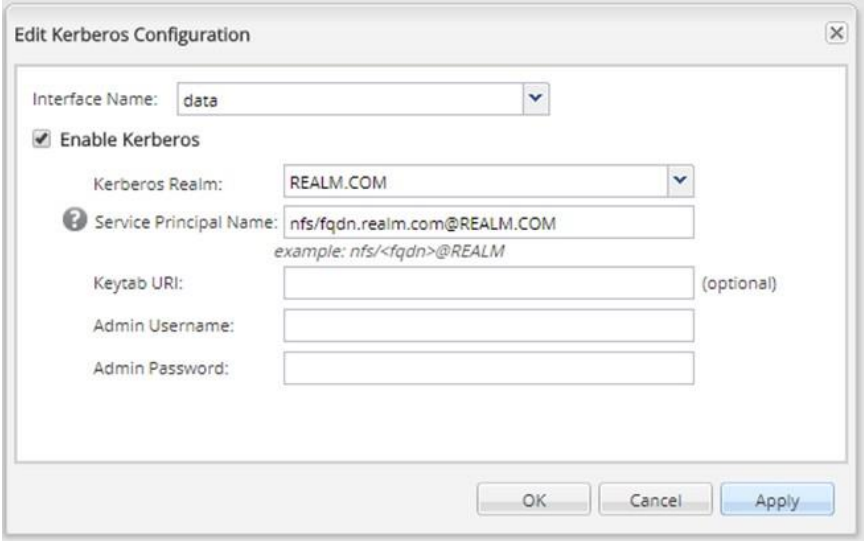
SPNでは、の例の形式を使用する必要があります `primary/instance@REALM`。 `REALM` は常にすべて大文字です。この形式を使用しないと、コマンドは失敗します。この例およびその他の考えられるエラーについては、「ONTAPでKerberosインターフェイスの有効化、変更、または作成時のエラー」を参照してください。

考慮すべきその他の要素には、次のようなものがあります。

- このプロセスは、一度に1つのデータLIFで実行されます。
- データLIFでKerberosを有効にすると、以降のデータLIFで同じSPNを使用する場合、クレデンシャル交換は必要ありません。
- 複数のLIFに同じSPNを使用することも、データLIFごとに異なるSPNを使用することもできます。
- 新しいSPNを指定するたびに、新しいマシンアカウントがActive Directoryにデフォルト名 `NFS-SPN-NAME`（最大15文字）で作成されます。この動作を無効にするには、`-machine- account` オプションを使用します。
- 同じSPNのデータLIFに対しては、マシンアカウントが1つだけ作成されます。
- 指定したドメインOUにオブジェクトを作成する権限を持つドメインユーザが必要です。デフォルトのOUはです `DC=DOMAIN, DC=COM`。
- OUを指定する場合は含めない `DC=DOMAIN, DC=COM`でください。ベースDNは暗黙的に使用されます。
- SPNはとして作成され `nfs/[desired DNS name for access]@REALM_IN_CAPS.COM`ます。
- keytabを手動で作成し、`keytab-uri` commandオプションを使用する場合、kerberos interfaceコマンドのSPNでは大文字と小文字が区別されます。つまり、KDCでSPNをと指定し `NFS/name`、`nfs/name` ONTAPコマンドでSPNとしてを使用しようとすると、コマンドは失敗します。

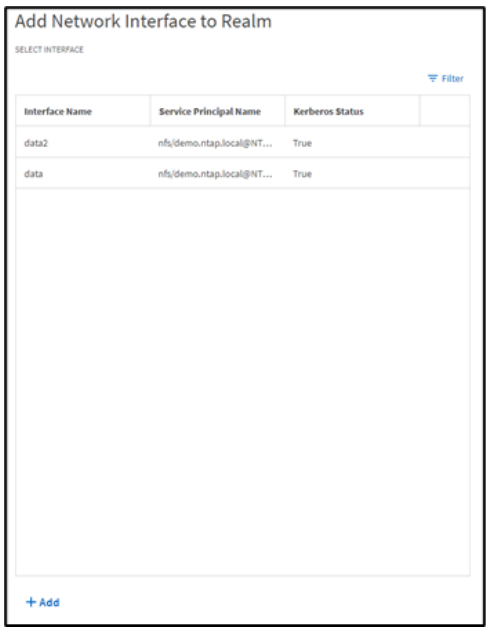
ONTAP 9.7より前のONTAP System Managerでユーザとグループを作成するには、図6に示すように、[SVM]>[SVM設定]に移動し、[サービス]>[Kerberosインターフェイス]に移動します。

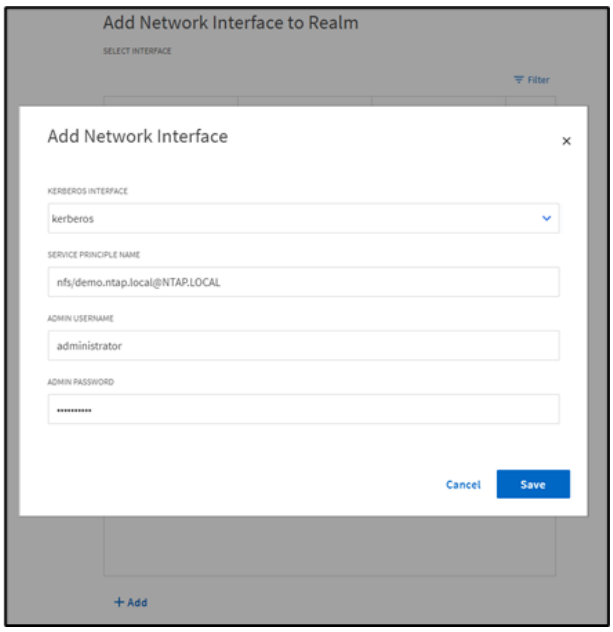
図6）Kerberosインターフェイスの設定-ONTAP 9.7より前のSystem Manager



ONTAP System Manager 9.7以降でユーザとグループを作成するには、次の手順を実行します。

1. [サービス]セクションで、[ストレージ]>[Storage VM]>[Kerberos]に移動します。
2. [既存のKerberos設定の追加または編集]をクリックします。
3. [Add Network Interface to Realm]セクションまで下にスクロールします。
4. 追加をクリックします。





CLIでユーザとグループを作成するには、次のコマンドを実行します。

```
kerberos interface enable -vserver [SVM] -lif data1 -spn [nfs/fqdn.domain.com@REALM.COM] -ou
[CN=Servers] -machine-account[machineaccountname]
```

エクスポートポリシールールを変更してKerberosを許可する

ONTAPのエクスポートポリシーは、エクスポートポリシールールのコンテナです。エクスポートポリシールールは、NFSエクスポートに適用される共有レベルの権限です。アクセスは、IPアドレス、ホスト名、ネットグループ、Kerberos認証などのホストIDに基づいて提供または拒否されます。

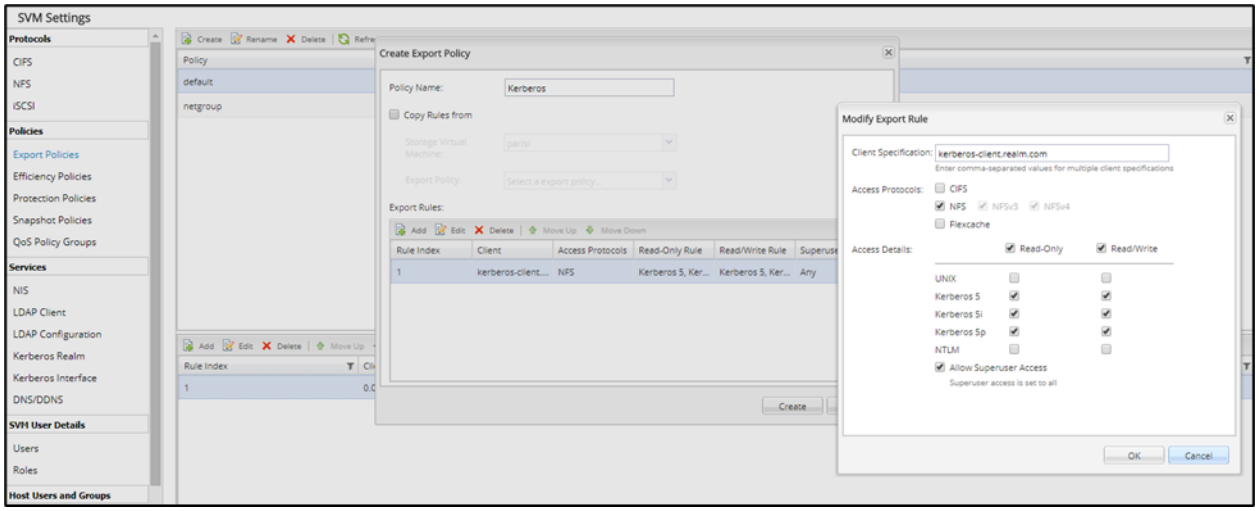
Kerberosマウントを許可するには、`rorule`、`rwrule`、`superuser` 許可するアクセスのレベルに応じて、エクスポートポリシールールの、および/またはフィールドでKerberosセキュリティを指定する必要があります。ONTAP 9以降では、さまざまなバージョンのKerberosセキュリティを使用できます。

- **krb5**ローカルUNIXユーザID（UID）とグループID（GID）ではなく、Kerberos V5の名前文字列とユーザプリンシパル名を使用してユーザを認証します。
- **krb5i**Kerberos v5を使用してユーザ認証を行い、セキュアなチェックサムを使用してNFS処理の整合性チェックを実行し、データの改ざんや中間者攻撃を防止します。
- **krb5p**Kerberos v5を使用してユーザ認証と整合性チェックを行い、すべてのNFSトラフィックを暗号化してパケットスニッフィングを防止します。この設定は最も安全ですが、パフォーマンスオーバーヘッドも最大になります。

Kerberosセキュリティオプションは、クライアントとKDCの間でネゴシエートされます。ONTAPのエクスポートポリシーとルールは、特定のセキュリティオプションを許可（場合によっては必須）する方法を提供するだけです。エクスポートポリシールールでkrb5セキュリティオプションが指定されていない場合、NFS Kerberosエクスポートのマウントは失敗し、アクセスが拒否されたり、権限の問題が発生したりします。エクスポートポリシールールへのアクセスは、CLIを使用して確認できます。詳細については、「エクスポートポリシーのトラブルシューティング」を参照してください。

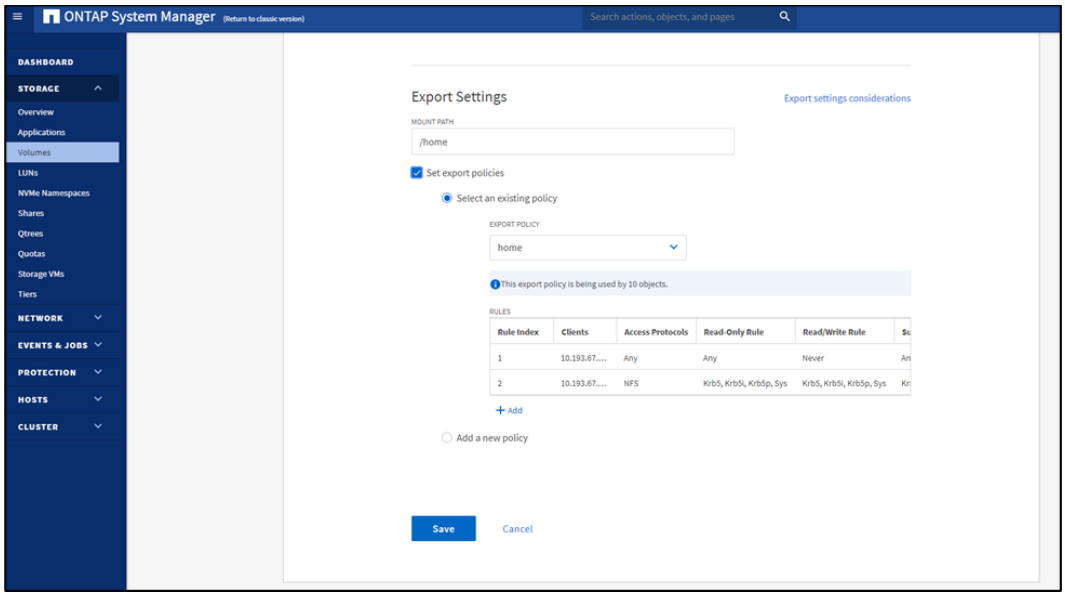
注： ONTAP 9.2より前のバージョンでは、NetAppでkrb5iまたはkrb5pの使用は推奨されていません。

ONTAP 9.7より前のバージョンのONTAP System Managerでエクスポートポリシーとルールを作成または変更するには、[SVM]>[SVM設定]の[ポリシー]>[エクスポートポリシー]に移動します。



ONTAP System Manager 9.7以降でユーザとグループを作成するには、次の手順を実行します。

1. [Storage] > [Volumes]に移動します。
2. エクスポートポリシーおよびルールを設定するボリュームを選択します。
3. [編集]をクリックします。
4. [Export Settings]まで下にスクロールし、[Set export policies]を選択します。
5. 既存のポリシーを選択してルールを編集するか、新しいポリシーとルールを作成します。



CLIでkrb5を許可するエクスポートポリシールールを変更するには、次のコマンドを実行します。

```
cluster::> export-policy rule modify
```

エクスポートポリシーおよびルールの詳細については、TR-4067を参照してください。

UNIXユーザまたはネームマッピングルールを作成してNFSサービスプリンシパルをマッピングする

クライアントがNFS Kerberosを使用してマウントにアクセスしようとすると、Kerberos設定で定義されているSPNを使用してサービスチケットが要求されます。このSPNは `krb-unix` 、SPNの最初の部分をデフォルトのUNIXユーザ名として使用して、ネームマッピングを使用してONTAPにマッピングしようとします。Kerberosが有効なインターフェイスの場合、この名前はです `nfs/fqdn.realm.com@REALM.COM`。

ネームマッピングまたは有効なUNIXユーザ（NFSなど）が存在しない場合、Kerberosアクセスの試行は失敗し、クライアントから「access denied / permission denied」と報告されます。ONTAPは、ネームマッピングエラーの形式でイベント管理システム（EMS）に障害を記録します。

ログに記録されたEMSイベントを確認するには、次のコマンドを使用します。

```
cluster::> event log show -messagename secd*
```

このタスクには、次の2つの方法のいずれかを使用できます。

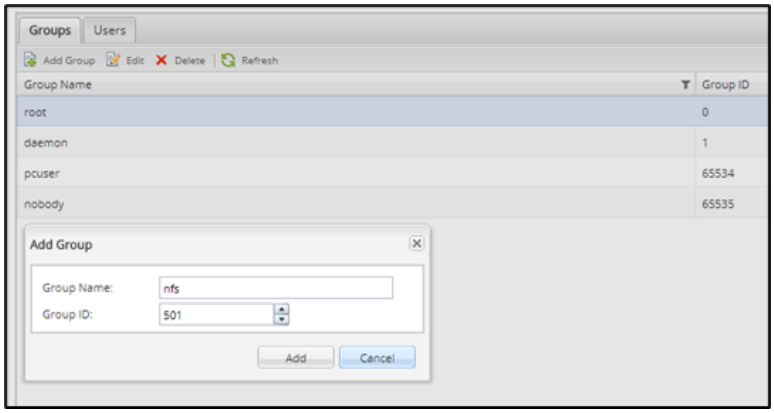
- `nfs` 暗黙的なネームマッピングのためにという名前のUNIXユーザをローカルまたはLDAP（LDAPを使用している場合）に作成します。
- SPNの明示的なSVMネームマッピングルールを作成して、既存の有効なUNIXユーザにマッピングします。

KerberosからUNIXへのネームマッピングの詳細については、「KRB - UNIXネームマッピングの動作」を参照してください。

オプション1：UNIXユーザおよびグループを作成する

ONTAPでUNIXユーザを作成するには、ONTAPシステムマネージャまたはコマンドラインを使用して、任意のUIDとGIDを持つ「nfs」という名前のユーザとグループを作成します。一般に、サービスアカウントではUIDとGIDに1～1,024の範囲を使用します。数値UIDまたはGIDを定義する前に、環境内の他の場所で使用されていないことを確認してください。

ONTAP System Managerでユーザとグループを作成するには、[SVM]>[SVM設定]の[ホストユーザとグループ]に移動します。



注： 現時点では、ONTAP 9.7以降の新しいONTAPシステムマネージャビューでローカルUNIXユーザおよびグループを作成する方法はありません。

CLIでユーザとグループを作成するには、次のコマンドを実行します。

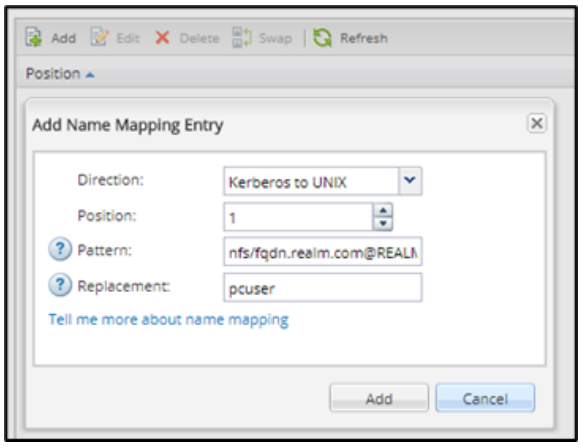
```
unix-user create -vserver [SVM] -user nfs -id [500] -primary-gid [500] -full-name "NFS Kerberos"

unix-group create -vserver [SVM] -name nfs -id [500]
```

UNIXユーザおよびグループを作成することは、`krb-unix` クラスタ内でNFS Kerberos SPN認証を処理する最も簡単な方法です。また、環境内にLDAPがある場合は、LDAPで「nfs」という名前のユーザを作成することもできます。

オプション2：krb-UNIXネームマッピングルールを作成する

UNIXユーザおよびグループを作成しない場合は、NFS Kerberos SPN認証を処理するネームマッピングルールを作成できます。このアプローチでは `nfs/fqdn.realm.com@REALM.COM`、（Kerberosインターフェイスコマンドで定義された）SPNが、選択したUNIXユーザにマッピングされます。次の例では、SPNを「pcuser」にマッピングします。

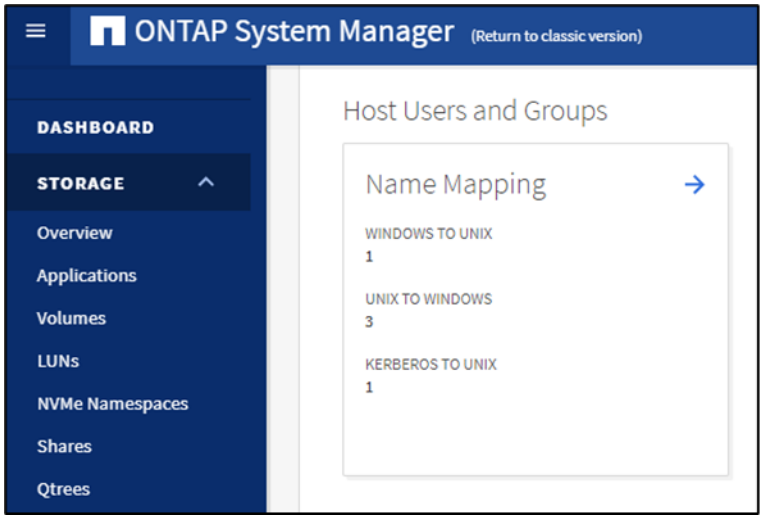
ONTAP 9.7より前のONTAP System Managerでネームマッピングを作成するには、[SVM]>[SVM設定]の[ホストユーザとグループ]に移動します。



ONTAP System Manager 9.7以降でユーザとグループを作成するには、次の手順を実行します。

1. [ストレージ]>[Storage VM]の順に選択し、目的のSVMを選択します。
2. [Settings]タブを下にスクロールして、[Host Users and Groups]セクションを表示します。

3. 矢印をクリックします。
4. [KerberosからUNIXへのルール]で[追加]をクリックするか、編集する既存のネームマッピングルールをクリックします。



CLIでネームマッピングを作成するには、次のコマンドを実行します。

```
vserver name-mapping create -vserver [SVM] -direction krb-unix -position 1 -pattern
nfs/fqdn.realm.com@REALM.COM -replacement pcuser
```

UNIXユーザまたはネームマッピングルールを作成してNFSクライアントプリンシパルをマッピング

NFSクライアントがKerberosを使用してONTAPでNFSエクスポートをマウントしようとすると、クライアントのプリンシパルが認証のためにONTAPに渡されます。クライアントが認証に使用するプリンシパルは、そのNFSクライアントでKerberosがどのように設定されているかによって異なります。を使用すると、クライアントのkeytabからどのプリンシパルが使用される可能性があるかを表示できます `klist -kte`。

`realmd` またはを使用してドメインに参加する場合、 `net ads`通常、プリンシパルは `MACHINENAME$@REALM.COM` デフォルトで送信されます。RHELで `nfs/hostname` `root/hostname` SPNとして（RHEL 6.xより前のバージョン）または（通常は手動でkeytabを作成）が使用される場合があります。

`mount` コマンドが実行されると、そのプリンシパルがNFSクライアントからに送信され、ONTAPは `krb-unix` ネームマッピングの実行を試みます。ドメインに参加しているクライアントのデフォルトの動作では、ONTAPはという名前のUNIXユーザを検索し `MACHINEACCOUNT$`ます。これは、NFSクライアントSPNの1：1マッピングです `MACHINEACCOUNT$@REALM.COM`。SVM用に設定されたローカルファイルまたはネームサービスにそのユーザが存在しない場合、ONTAPは明示的なネームマッピングルールを検索します。明示的なネームマッピングルールが存在しない場合、NFS Kerberosのマウントは権限またはアクセス問題で失敗します。ONTAPでは `secd`、エラーとしてEMSに記録されます。

ログに記録されたEMSイベントを確認するには、次のコマンドを使用します。

```
cluster::> event log show -messagename secd*
```

このタスクは、次の2つの方法のいずれかで実行できます。

- SPN/UPN用の明示的なネームマッピングルールを作成して、既存の有効なUNIXユーザにマッピングします。
- `MACHINEACCOUNT$` 暗黙的なネームマッピングのためにという名前のUNIXユーザをローカルまたはLDAP内に作成します（LDAPが設定されている場合）。

KerberosからUNIXへのネームマッピングの詳細については、「KRB - UNIXネームマッピングの動作」を参照してください。

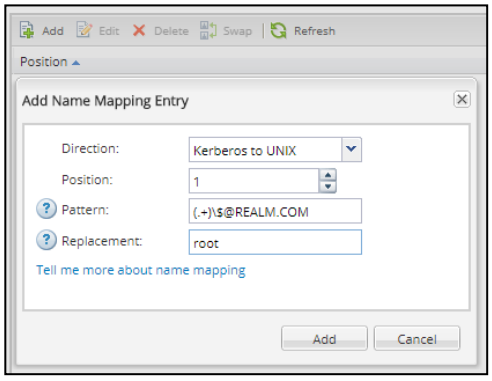
注： `nfs/hostname root/hostname` SPNとしてまたはを使用する場合は、「nfs」または「root」という名前のUNIXユーザを作成する必要があります。 ONTAPでは常にrootがデフォルトユーザであるため、この場合の対処は不要です。

オプション1：ネームマッピングルールを作成する（推奨）

RHELクライアント用に複数のUNIXユーザを作成するのではなく、 `MACHINEACCOUNT$@REALM.COM` rootに対して認証を試行するすべてのLinuxクライアントをマッピングするグローバルネームマッピングルールを作成することを推奨します。アカウントをrootにマッピングしても、rootユーザ以外にrootアクセスは許可されません。マウントにアクセスする他のユーザプリンシパルは、ユーザ名とパスワードを使用して自身を認証する必要があります。このグローバルネームマッピングルールは、ONTAP System ManagerまたはCLIを使用して作成できます。

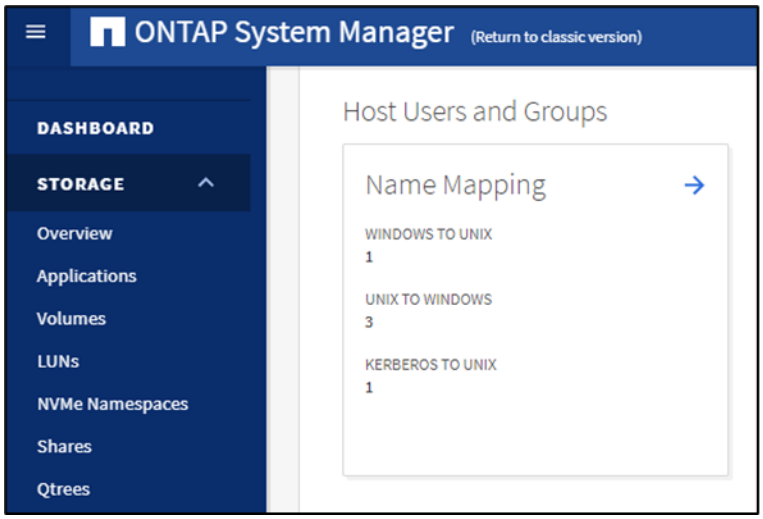
次の例では、の正規表現を使用して、Kerberosアクセスをrootに試行するすべてのコンピュータアカウント名をマッピングするルールを作成し `(.+)\$`ます。このネームマッピングルールでは、ユーザプリンシパルはrootにマッピングされません。マシンアカウントのみがマッピングされます（ユーザの名前が指定されていない場合 `mailto:user$@REALM.COM`）。

ONTAP 9.7より前のONTAP System Managerでネームマッピングを作成するには、[SVM]>[SVM設定]の[ホストユーザとグループ]に移動します。



ONTAP System Manager 9.7以降でユーザとグループを作成するには、次の手順を実行します。

1. [ストレージ]>[Storage VM]の順に選択し、目的のSVMを選択します。
2. [Settings]タブを下にスクロールして、[Host Users and Groups]セクションを表示します。
3. 矢印をクリックします。
4. [KerberosからUNIXへのルール]で[追加]をクリックするか、編集する既存のネームマッピングルールをクリックします。



CLIでネームマッピングを作成するには、次のコマンドを実行します。

```
vserver name-mapping create -vserver [SVM] -direction krb-unix -position 1 -pattern
(.+)\$@REALM.COM -replacement root
```

ここで「root」ユーザを使用すると、クライアントのrootユーザは「root」として動作します。 ルートアクセスを引き下げたい場合は、受信するSPNを別のUNIXユーザにマッピングできます。

注： 受信するNFSクライアントプリンシパルは、クライアントのLinuxバージョンとKerberosの設定方法に大きく依存します。`ktlist -kte`ネームマッピングの作成方法を決定するときは、受信SPNを確認します（パケットのキャプチャまたは表示を使用）。たとえば、一部のクライアントは `host/name.realm.com` Kerberosプリンシパルとしてを使用できます。`Event log show` ONTAP CLIでは、障害が発生したときにどのプリンシパルが認証しようとしているかに関する詳細も配信できます。

ネームマッピングをテストするには、次のコマンドを実行します。

```
set diag; diag secd name-mapping show -node [node] -vserver [SVM] -direction krb-unix -name
[MACHINEACCOUNTNAME$@DOMAIN.COM]
```

オプション2：UNIXユーザおよびグループを作成する（非推奨）

に指定されたONTAP for NFSクライアントプリンシパルでUNIXユーザを作成するには `MACHINEACCOUNTNAME$@REALM.COM`、ONTAPシステムマネージャまたはコマンドラインを使用して、`MACHINEACCOUNTNAME$`任意のUIDとGIDを持つという名前のユーザとグループを作成します。一般に、サービスアカウントではUIDとGIDに1～1,024の範囲を使用します。数値UIDまたはGIDを定義する前に、環境内の他の場所で使用されていないことを確認してください。LDAP属性を変更して作成された既存のマシンアカウントオブジェクトを使用して、LDAPでこのタスクを実行することもできます。

この処理を実行すると、NFS Kerberosマウントではrootユーザが「root」として表示されなくなり、作成したユーザに割り当てられているUIDでファイルの読み取りと書き込みが行われることに注意してください。

たとえば、という名前のローカルUNIXユーザを `CENTOS7$` UID 599で作成すると、SPN `CENTOS7$@NTAP.LOCAL` がそのユーザにマッピングされます。

```
cluster::*> access-check name-mapping show -vserver DEMO -direction krb-unix -name
CENTOS7$@NTAP.LOCAL
'CENTOS7$@NTAP.LOCAL' maps to 'CENTOS7$'
cluster::*> unix-user show -vserver DEMO -user CENTOS7$

         Vserver: DEMO
       User Name: CENTOS7$
         User ID: 599
Primary Group ID: 1
User's Full Name:
```

NFS Kerberosを使用してマウントすると、 `nobody` SPNがONTAPにマッピングされるため、「root」によるファイルへの書き込みがファイル所有者にと表示されます。

```
# id
uid=0(root) gid=0(root) groups=0(root)
# touch rootfile2
# ls -la | grep rootfile2
-rw-r--r--   1 nobody   daemon    0 May 21 13:53 rootfile2
```

次の例は、ONTAPがファイル所有者として認識するUID 599を示しています。

```
cluster::*> vserver security file-directory show -vserver DEMO -path /home/rootfile2

               Vserver: DEMO
             File Path: /home/rootfile2
     File Inode Number: 27980
        Security Style: unix
       Effective Style: unix
```

```
         DOS Attributes: 20
 DOS Attributes in Text: ---A----
Expanded Dos Attributes: -
           UNIX User Id: 599
          UNIX Group Id: 1
         UNIX Mode Bits: 644
 UNIX Mode Bits in Text: rw-r--r--
                   ACLs: -
```

注： 環境にはKerberosを使用するNFSクライアントが数百も存在する可能性がNetAppあるため、拡張性の妨げになる可能性があるため、この方法の使用は推奨されません。

AESのみを許可するようにNFSサーバマシンアカウントを変更する

NFSサーバのマシンアカウントをAESのみを許可するように変更すると、NFSクライアントはONTAP NFSマウントで弱い暗号化タイプ（DESなど）やサポートされない暗号化タイプ（RC4-HMACなど）を試行できなくなります。ONTAPでKerberosを有効にすると、Active DirectoryにNFS固有のマシンアカウントが作成されます（既存のCIFS / SMBサーバマシンアカウントとは別）。ONTAP 9.9.1以降では、ONTAPはこのフィールドにNFSサーバオプションpermitted-enc-typesで指定された値を自動的に入力するため、マシンアカウントの変更は不要になりました（ 詳細についてはバグ1316456を参照してください）。

注： ONTAP 9.9.1RC1には、この修正が適用された問題があります。この場合、NFSサーバの設定に関係なく、マシンアカウントでサポートされていない暗号化タイプ（DESおよびRC4-HMAC）が使用されます。そのリリースでは、次の手順に従って暗号化タイプ属性を変更する必要があります。この問題を回避するには、必ず最新のONTAP 9.9.1パッチリリースを使用してください。

NFSサーバのマシンアカウントを変更する最も簡単な方法は、Windows PowerShellを使用することです。

```
PS C:\> Set-ADComputer NFS-KRB-NAME$ -KerberosEncryptionType AES256,AES128
```

PowerShellが選択できない場合は、[Active Directoryユーザーとコンピュータ]を使用して `msDs-SupportedEncryptiontypes` フィールドを目的の暗号化タイプに変更することもできます。これに使用できる値については、「付録B：マシンアカウント属性」を参照してください。

Active Directoryマシンアカウントを変更できない場合は `/etc/krb5.conf`、次の行を追加または変更することで、クライアントのファイルを変更してAESのみを許可することができます。

```
permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96
default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96
default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96
```

Red Hat Enterprise Linuxクライアントの設定

最新のNFSクライアントがシンプルなコマンドを使用してドメインに参加する方法を追加する前は、Active Directory KDCでNFS Kerberosを設定するのは手動のプロセスであり、複数のチームの操作が必要でした。Active Directoryのクライアントプリンシパルは KDCから手動で作成する必要があり、keytabファイルは手動でクライアントに移動する必要がありました。その後、を使用してメインのkeytabファイルに手動で追加する必要が `kutil` ありました。

メモ： クライアントの手動設定手順についてさらにサポートが必要な場合は、OSベンダーのドキュメントを参照してください。

新しいRHELクライアントには、Windowsと同等の動作をするユーティリティが用意されています。ユーティリティを使用すると、クライアントはActive Directoryドメインに参加することでKerberos設定プロセスを自動化できます。ドメインがに参加すると `realmd`、KDCでのプリンシパルの作成、クライアントのKerberos設定、およびkeytabの転送が自動的に実行されます。KDCに触れる必要はありません。クライアントをActive Directoryドメインに追加する際に推奨されるRHELパッケージは次のとおりです。

- RHEL 6.x：Winbind / Samba（ネット広告を使用）
- RHEL 7.x以降：Realmd

さらに、Active Directoryドメインに参加すると、LDAPクライアントSSSDがUNIX ID管理用にActive Directory環境を自動的に使用するように設定されます。ただし、SSSDが適切なLDAP検索を実行していることを確認するために、一部の設定が必要になる場合があります。

LDAPおよびSSSDの考慮事項の設定の詳細については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

この設定セクションには、RHELクライアントに関する次の前提条件があります。

- RHELクライアントのDNSには、フォワード（A/AAAA）レコードとリバース（PTR）レコードがあります。
- AES暗号化が使用されます。
- RHELクライアントには、次のパッケージがインストールされています（オプションのパッケージは*で示されます）。
  - nfs-utils、realmd、samba、samba-client、samba-winbind、 autofs *、ntp、bind-utils、tcpdump *、ssd（またはその他のLDAPクライアント）*、krb5-workstation、krb5-libs、auth-config-gtk

ネットワークタイムプロトコルサービスの設定

RHELクライアントでタイムサービスを設定すると、Kerberosのタイムスキューに関する問題を回避できます。ネットワークタイムプロトコル（NTP）サービスを設定するには、次のコマンドを実行します。

```
ntpdate [pool.ntp.org]
systemctl start ntpd.service
systemctl enable ntpd.service
```

DNSの確認

この検証により、クライアントがDNSに存在することを確認できます。Kerberosが適切に機能するには、DNSフォワードレコードとリバースレコードが必要です。DNSを確認するには、次のコマンドを実行します。

```
# nslookup [hostname/FQDN of SVM data LIFs]
# nslookup [IP address of SVM data LIFs]
# nslookup [hostname/FQDN of NFS client(s)]
# nslookup [IP address of NFS client(s)]
```

クライアントがDNSにない場合は、DNS管理者に依頼してクライアントを追加するか、RHELの動的DNS機能を使用します。

ドメインへの参加

この手順では、NFSクライアントのサービスプリンシパル/マシンアカウントがKDCに自動的に作成され、keytabファイルとSSSDが設定され `/etc/nsswitch.conf`、クライアントの `/etc/krb5.conf` ファイルでKerberosが設定されます。ドメインに参加するには、指定されたActive Directoryコンテナにオブジェクトを作成するためのアクセス権を持つユーザアカウントが必要です。デフォルトのコンテナはです `OU=Computers`が、使用するコマンドで指定できます。

- RHEL 6.xの場合 `net ads`は `realmd`、が古いクライアントには存在しないため、を使用します。
  「NET ADS JoinでKerberosを使用するようにNFSクライアントを設定する」を参照してください。
- RHEL 7.x以降の場合は、を使用し `realmd`ます。
  「KerberosとRealm Joinを使用するようにNFSクライアントを設定する」を参照してください。

マシンアカウントプリンシパルの変更

ほとんどのクライアントとKDCのやり取りはドメインに参加すると自動的に行われますが、KerberosがNetApp ONTAPで適切に機能することを確認するために、マシンアカウントプリンシパルを手動で設定する必要があります。

クライアントマシンアカウントでサポートされているエンタイプの変更

この手順は、クライアントがNFSに対してRC4-HMAC Kerberosを試行しないようにするために推奨されますが、ONTAPではサポートされていません。この手順では、PowerShellを使用して `msDs-SupportedEncryptionTypes` 値を変更し、AES-256およびAES-128のみを使用します。この手順については、「AESのみを許可するようにNFSサーバマシンアカウントを変更する」を参照してください。

RC4-HMACを使用している場合の障害の例を次に示します。

```
6/29/2016 16:09:56 node03
WARNING       secd.nfsAuth.problem: vserver (parisi) General NFS authorization problem. Error:
RPC accept GSS token procedure failed
  [ 0 ms] Using the NFS service credential for logical interface 1035 (SPN='nfs/parisi-nfs.core-
tme.netapp.com@CORE-TME.NETAPP.COM') from cache.
**[     1] FAILURE: Failed to accept the context: Unspecified GSS failure. Minor code may
provide more information (minor: Encryption type ArcFour with HMAC/md5 not permitted).
```

オプション：マシンアカウントのサービスプリンシパルを**userPrincipalName**フィールドに追加します。

この手順では、が `kinit -k` クライアントだけでなく、Kerberosのマシンアカウントサービスプリンシパルを使用する必要があるアプリケーション（SSSDなど）でも動作することを確認します。

次のPowerShellコマンド例を参照してください。

```
PS C:\> Set-ADComputer CENTOS7$ -KerberosEncryptionType AES256,AES128 -UserPrincipalName
HOST/centos7.ntap.local@NTAP.LOCAL
```

オプション：**krb5.conf**ファイルをカスタマイズして**DNS**の正規化をバイパスする

クライアントでDNSを使用してNFSサービスプリンシパルを作成しないようにする（つまり、ONTAP SVMに複数のAレコードがある）場合は[`libdefaults`]、のに次のオプションを追加します `/etc/krb5.conf`。

```
dns_canonicalize_hostname = false
```

ベストプラクティス

次に、NetApp ONTAPでNFS Kerberosを使用する場合のベストプラクティスを示します。これらはベストプラクティスであり、要件ではありません。これらのベストプラクティスに従うことで最適な結果を得ることができますが、Kerberosが正常に動作するためにすべての手順が必要となるわけではありません。

このリストは包括的ではありません。このリストにベストプラクティスが記載されている問題を発見した場合、または追加提案をご希望の場合は、「お問い合わせ」セクションの手順に従ってコメントをお送りください。

ONTAPのベストプラクティス

- NFS Kerberosに参加するデータLIFを、フォワードレコードとリバース（PTR）レコードを使用してDNSに追加します。
- NFS Kerberosデータアクセス用にSVMごとに複数のデータLIFを設定します（データLIFはSVMのノードごとに1つを推奨）。このベストプラクティスは、パフォーマンスと耐障害性に関する考慮事項です。NASデータLIFのベストプラクティスの詳細については、TR-4067を参照してください。
- 複数のデータLIFを使用している場合は、負荷分散機能を提供するために、同じFQDNの/AAAAレコードをDNSに作成することを検討してください。
- クライアントアクセスにDNSエイリアスを使用する場合は、正規名（CNAME）を使用します。
- SVM内のデータLIFのDNSレコードは、（Kerberosインターフェイスコマンドを使用して）データLIFのNFS Kerberos設定で使用されるNFSサービスプリンシパルに設定された名前と一致している必要があります。

- NFS Kerberosを設定する前に、`permitted- enc-types` AES暗号化のみを使用する場合は、NFSサーバのオプションからDESおよびDES3暗号化タイプを削除してください。プリンシパルの作成後にDESとDES3を無効にするには、マシンアカウントを再作成して新しいキータブを生成する必要があるため、停止が必要です。
- NFS Kerberosで組み込みのDNSロードバランシングまたは外部のDNSロードバランシングを使用する場合は、DNSロードバランシングゾーンに属するすべてのデータLIFでNFS Kerberosを有効にします。
- 「nfs」という名前のローカルUNIXユーザまたはLDAPユーザを作成して、`krb-unix` NFSサービスプリンシパルに暗黙的なネームマッピングを許可します。
- `krb-unix` 受信NFSクライアントマシンアカウントをマッピングするためのグローバルネームマッピングルールを作成します。マシンアカウントプリンシパルはONTAPへのマッピングを試行し、マッピング先の有効なUNIXユーザを持つ必要があります。詳細については 、このドキュメントのセクション0を参照してください。
- 可能であれば、マシンアカウント名の長さは15文字未満にしてください。マシンアカウント名は、`kerberos interface enable` コマンドで指定したSPNを使用して作成され、`-machine-account` オプションで上書きできます。マシンアカウントが15文字を超えて一意でない場合、Active Directoryではマシンアカウント名の重複が許可されないため、マシンアカウントの作成は失敗します。マシンアカウントの作成後に名前を変更することもできます。
- ID管理の一貫性のためにNFSクライアントと同じLDAPサーバを使用するようにONTAPを設定します。LDAPの設定については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。
- SVMルートボリューム（/）に、少なくともクライアントへの読み取りアクセスを許可するエクスポートポリシールールが設定されていることを確認します。クライアントがネームスペースの最上位レベルをトラバースできるようにするには、読み取りアクセスが必要です。詳細については、TR-4067を参照してください。

NFSクライアントのベストプラクティス

- NTPを使用して、NFSクライアントとKDCおよびクラスタの時刻の同期を維持します。NFS Kerberosで原因が停止する可能性があるため、5分以内にタイムスキューが発生する可能性があります。
- Kerberosを使用するNFSクライアントのDNSにフォワードおよびリバース（PTR）レコードを追加します。DNS Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）は、Kerberos Realmのクライアントプリンシパルおよびkerberos設定の内容と一致している必要があります。
- `klist kinit` キータブを表示してKerberos機能をテストするには、コマンドとコマンドを使用します。NFS Kerberosマウントにアクセスするroot以外のユーザは `kinit` 、マウントにアクセスするチケットを要求する前に、KDCに（ログインして）アクセスできる必要があります。
- NFS Kerberosのマウント時にタイムアウトの問題が発生したクライアントのrpcgssdのタイムアウト値を-T 60に設定します。この値の設定方法の詳細については、NFSクライアントのOSガイドを参照してください。
- `tcpdump/var/log/messages`ほとんどのKerberosの問題をトラブルシューティングするには、rpcgssdとmountにパケットトレース（）、およびデバッグレベルを使用することをお勧めします。多くの場合、KDCとONTAPクラスタへのアクセスも必要になります。
- KDCで、NFSクライアントマシンアカウントで適切な暗号化タイプが有効になっていることを確認します。クライアントで使用できる 暗号化タイプと使用できない暗号化タイプの詳細については、「サポートされる暗号化タイプ」を参照してください。
- NFS Kerberosスタックのバグを回避するには、クライアントのカーネルの最新バージョンを使用します。
- Kerberos用にNFSクライアントを設定するには、Kerberosを手動で設定するのではなく、ドメイン参加を使用します。
- Kerberosを設定またはトラブルシューティングするときは、Kerberosキャッシュとチケットの有効期間を必ず考慮してください。問題が発生した場合、キャッシュがKerberosの動作に影響を与える可能性があります。詳細については、「Kerberosキャッシュ」を参照してください。

Windows KDCのベストプラクティス

- `setspn /q` 重複したSPNをKDCで検索する場合に使用します。SPNの原因アクセスに関する問題が重複しているため、追跡が困難です。

- Kerberosの問題をトラブルシューティングするときは、パケットトレースを十分に活用してください。
- タイムスキューの問題を回避するには、KDCの時間を最新の状態に保ち、ONTAPクラスタとNFSクライアントから5分以内にする必要があります。
- マシンアカウントを変更する簡単な方法としてPowerShellを使用します。
- トラブルシューティング時に、ドメインコントローラのイベントビューアでKerberosエラーとセキュリティエラーを確認します。
- Windows 2008以降のバージョンでは、DES暗号化はデフォルトで無効になっています。必要な場合にのみDESを使用してください。代わりにAESを使用します。AESはWindows KDCでデフォルトで有効になっています。
- Windows Active Directoryでは現在、Kerberosの暗号化タイプとしてRC4-HMACがデフォルトで設定されています。ONTAPではNFS Kerberos用のRC4-HMACがサポートされないため、NetAppでは、NFS KerberosクライアントおよびONTAPサーバ用のオプションとしてRC4-HMACを削除することを推奨しています。セクション 0 では、NFSクライアントマシンアカウントを変更する方法について説明します。セクション 0 では、NFSサーバアカウントを変更する方法について説明します。

コウセイレイ

ここでは、NFS Kerberosの設定例を示します。

NetApp ONTAP

Kerberos Realm

```
                        KDC Vendor: Microsoft
                     KDC IP Address: x.x.x.y
                           KDC Port: 88
                        Clock Skew: 5
      Active Directory Server Name: ONEWAY
Active Directory Server IP Address: x.x.x.y
                           Comment:  -
            Admin Server IP Address: x.x.x.y
                  Admin Server Port: 749
         Password Server IP Address: x.x.x.y
               Password Server Port: 464
         Permitted Encryption Types: aes-256, aes-128
```

Kerberosインターフェイス

```
cluster::*> kerberos interface show -vserver DEMO -lif data*
  (vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address          Kerberos SPN
-------------- ------------- ---------------- ------------ ----------------------------------------------------
DEMO           data          x.x.x.a   enabled nfs/demo.ntap.local@NTAP.LOCAL
DEMO           data2         x.x.x.b   enabled nfs/demo.ntap.local@NTAP.LOCAL
2 entries were displayed.
```

関連するNFSサーバ構成オプション

```
cluster::*> nfs server show -vserver DEMO -fields permitted-enc-types
vserver permitted-enc-types
---------- --------------------------
DEMO    aes-256,aes-128
```

UNIXユーザおよびグループ

```
cluster::*> unix-user show -vserver DEMO
               User            User   Group Full
Vserver        Name            ID     ID    Name
-------------- --------------- ------ ----- ----------------------------------------------------------------
DEMO           nfs             500    500
DEMO           nobody          65535 65535
```

```
DEMO            pcuser          65534 65534
DEMO            root            0      1
4 entries were displayed.

cluster::*> unix-group show -vserver DEMO
Vserver         Name                    ID
--------------- --------------------------------- ----------
DEMO            daemon                  1
DEMO            nfs                     500
DEMO            nobody                  65535
DEMO            pcuser                  65534
DEMO            root                    0
5 entries were displayed.
```

ネームマッピングルール

```
cluster::*> vserver name-mapping show -vserver DEMO

Vserver:   DEMO
Direction: krb-unix
Position Hostname          IP Address/Mask
-------- ----------------- -----------------
1        -                 -                   Pattern: (.+)\$@NTAP.LOCAL
                                           Replacement: root

Vserver:   DEMO
Direction: unix-win
Position Hostname          IP Address/Mask
-------- ----------------- -----------------
1        -                 -                   Pattern: root
                                           Replacement: DEMO\\administrator
2 entries were displayed.
```

Windows（マシンアカウントとプリンシパル）

setspn

```
PS C:\> setspn /q nfs/demo.ntap.local
Checking domain DC=NTAP,DC=local
CN=KERBEROS,CN=Computers,DC=NTAP,DC=local
        nfs/KERBEROS
        HOST/KERBEROS
        HOST/nfs-demo-ntap-l.ntap.local
        nfs/nfs-demo-ntap-l.ntap.local
        nfs/demo.ntap.local

Existing SPN found!
```

メモ： 上記の例のマシンアカウントの名前が NFS-DEMO-NTAP-L からに変更されました KERBEROS。

NFSクライアントマシンアカウント

```
PS C:\> Get-ADComputer -Properties * CENTOS7$


AccountExpirationDate                :
accountExpires                       : 9223372036854775807
AccountLockoutTime                   :
AccountNotDelegated                  : False
AllowReversiblePasswordEncryption    : False
AuthenticationPolicy                 : {}
AuthenticationPolicySilo             : {}
BadLogonCount                        : 0
badPasswordTime                      : 0
badPwdCount                          : 0
CannotChangePassword                 : False
CanonicalName                        : NTAP.local/Computers/CENTOS7
```

```
Certificates                          : {}
CN                                    : CENTOS7
codePage                              : 0
CompoundIdentitySupported             : {False}
countryCode                           : 0
Created                               : 5/15/2017 5:50:49 PM
createTimeStamp                       : 5/15/2017 5:50:49 PM
Deleted                               :
Description                           :
DisplayName                           :
DistinguishedName                     : CN=CENTOS7,CN=Computers,DC=NTAP,DC=local
DNSHostName                           : centos7.ntap.local
DoesNotRequirePreAuth                 : False
dSCorePropagationData                 : {12/31/1600 7:00:00 PM}
Enabled                               : True
HomedirRequired                       : False
HomePage                              :
instanceType                          : 4
IPv4Address                           : x.x.x.x
IPv6Address                           :
isCriticalSystemObject                : False
isDeleted                             :
KerberosEncryptionType                : {AES128, AES256}
LastBadPasswordAttempt                :
LastKnownParent                       :
lastLogoff                            : 0
lastLogon                             : 131459819334568160
LastLogonDate                         : 7/25/2017 1:40:51 PM
lastLogonTimestamp                    : 131454780514971253
localPolicyFlags                      : 0
Location                              :
LockedOut                             : False
logonCount                            : 2402
ManagedBy                             :
MemberOf                              : {}
MNSLogonAccount                       : False
Modified                              : 7/25/2017 1:40:51 PM
modifyTimeStamp                       : 7/25/2017 1:40:51 PM
msDS-SupportedEncryptionTypes         : 24
msDS-User-Account-Control-Computed    : 0
Name                                  : CENTOS7
nTSecurityDescriptor                  : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                        : CN=Computer,CN=Schema,CN=Configuration,DC=NTAP,DC=local
ObjectClass                           : computer
ObjectGUID                            : 3a50009f-2b40-46ea-9014-3418b8d70bdb
objectSid                             : S-1-5-21-3552729481-4032800560-2279794651-1140
OperatingSystem                       :
OperatingSystemHotfix                 :
OperatingSystemServicePack            :
OperatingSystemVersion                :
PasswordExpired                       : False
PasswordLastSet                       : 7/8/2017 12:06:54 AM
PasswordNeverExpires                  : True
PasswordNotRequired                   : False
PrimaryGroup                          : CN=Domain Computers,CN=Users,DC=NTAP,DC=local
primaryGroupID                        : 515
PrincipalsAllowedToDelegateToAccount  : {}
ProtectedFromAccidentalDeletion       : False
pwdLastSet                            : 131439604148147009
SamAccountName                        : CENTOS7$
sAMAccountType                        : 805306369
sDRightsEffective                     : 15
ServiceAccount                        : {}
servicePrincipalName                  : {HOST/centos7.ntap.local, HOST/CENTOS7}
ServicePrincipalNames                 : {HOST/centos7.ntap.local, HOST/CENTOS7}
SID                                   : S-1-5-21-3552729481-4032800560-2279794651-1140
SIDHistory                            : {}
TrustedForDelegation                  : False
TrustedToAuthForDelegation            : False
UseDESKeyOnly                         : False
userAccountControl                    : 69632
```

```
userCertificate                     : {}
UserPrincipalName                   : HOST/centos7.ntap.local@NTAP.LOCAL
uSNChanged                          : 95586
uSNCreated                          : 77860
whenChanged                         : 7/25/2017 1:40:51 PM
whenCreated                         : 5/15/2017 5:50:49 PM
```

NFSサーバマシンアカウント（ONTAP）

```
PS C:\> Get-ADComputer -Properties * KERBEROS


AccountExpirationDate               :
accountExpires                      : 9223372036854775807
AccountLockoutTime                  :
AccountNotDelegated                 : False
AllowReversiblePasswordEncryption   :  False
AuthenticationPolicy                : {}
AuthenticationPolicySilo            : {}
BadLogonCount                       : 0
badPasswordTime                     : 0
badPwdCount                         : 0
CannotChangePassword                : False
CanonicalName                       : NTAP.local/Computers/KERBEROS
Certificates                        : {}
CN                                  : KERBEROS
codePage                            : 0
CompoundIdentitySupported           : {False}
countryCode                         : 0
Created                             : 1/17/2017 4:24:36 PM
createTimeStamp                     : 1/17/2017 4:24:36 PM
Deleted                             :
Description                         :
DisplayName                         : KERBEROS
DistinguishedName                   : CN=KERBEROS,CN=Computers,DC=NTAP,DC=local
DNSHostName                         : DEMO.NTAP.LOCAL
DoesNotRequirePreAuth               : False
dSCorePropagationData               : {12/31/1600 7:00:00 PM}
Enabled                             : True
HomedirRequired                     : False
HomePage                            :
instanceType                        : 4
IPv4Address                         : x.x.x.b
IPv6Address                         :
isCriticalSystemObject              : False
isDeleted                           :
KerberosEncryptionType              : {AES128, AES256}
LastBadPasswordAttempt              :
LastKnownParent                     :
lastLogoff                          : 0
lastLogon                           : 0
LastLogonDate                       :
localPolicyFlags                    : 0
Location                            :
LockedOut                           : False
logonCount                          : 0
ManagedBy                           :
MemberOf                            : {}
MNSLogonAccount                     : False
Modified                            : 7/13/2017 9:55:21 AM
modifyTimeStamp                     : 7/13/2017 9:55:21 AM
msDS-SupportedEncryptionTypes       : 24
msDS-User-Account-Control-Computed  : 0
Name                                : KERBEROS
nTSecurityDescriptor                : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                      : CN=Computer,CN=Schema,CN=Configuration,DC=NTAP,DC=local
ObjectClass                         : computer
ObjectGUID                          : 2ade6c5d-1411-4cb1-ab84-e9a6228fd120
objectSid                           : S-1-5-21-3552729481-4032800560-2279794651-1116
OperatingSystem                     : NetApp Release 9.1
```

```
OperatingSystemHotfix                 :
OperatingSystemServicePack            :
OperatingSystemVersion                :
PasswordExpired                       : False
PasswordLastSet                       : 1/17/2017 4:24:36 PM
PasswordNeverExpires                  : False
PasswordNotRequired                   : False
PrimaryGroup                          : CN=Domain Computers,CN=Users,DC=NTAP,DC=local
primaryGroupID                        : 515
PrincipalsAllowedToDelegateToAccount : {}
ProtectedFromAccidentalDeletion       : False
pwdLastSet                            : 131291618765754144
SamAccountName                        : KERBEROS$
sAMAccountType                        : 805306369
sDRightsEffective                     : 15
ServiceAccount                        : {}
servicePrincipalName                  : {nfs/KERBEROS, HOST/KERBEROS, HOST/nfs-demo-ntap-
l.ntap.local, nfs/nfs-demo-ntap-l.ntap.local...}
ServicePrincipalNames                 : {nfs/KERBEROS, HOST/KERBEROS, HOST/nfs-demo-ntap-
l.ntap.local, nfs/nfs-demo-ntap-l.ntap.local...}
SID                                   : S-1-5-21-3552729481-4032800560-2279794651-1116
SIDHistory                            : {}
TrustedForDelegation                  : False
TrustedToAuthForDelegation            : False
UseDESKeyOnly                         : False
userAccountControl                    : 4096
userCertificate                       : {}
UserPrincipalName                     :
uSNChanged                            : 90841
uSNCreated                            : 13490
whenChanged                           : 7/13/2017 9:55:21 AM
whenCreated                           : 1/17/2017 4:24:36 PM
```

RHEL 7.xクライアント

DNS

```
cluster::*> dns show -vserver DEMO

                              Vserver: DEMO
                              Domains: NTAP.local
                         Name Servers: x.x.x.y
      (DEPRECATED)-Enable/Disable DNS: enabled
                      Timeout (secs): 2
                   Maximum Attempts: 1
               Is TLD Query Enabled?: true
Require Source and Reply IPs to Match: true
      Require Packet Queries to Match: true
```

krb.confファイル

```
# cat /etc/krb5.conf
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
 default =  FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_ccache_name = KEYRING:persistent:%{uid}
```

```
 default_realm = NTAP.LOCAL
[realms]

 NTAP.LOCAL = {
 }

[domain_realm]
ntap.local = NTAP.LOCAL
 .ntap.local = NTAP.LOCAL
```

keytabs（klist -kを使用）

```
# klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------------------------------
   5 host/centos7.ntap.local@NTAP.LOCAL
   5 host/centos7.ntap.local@NTAP.LOCAL
   5 host/centos7.ntap.local@NTAP.LOCAL
   5 host/centos7.ntap.local@NTAP.LOCAL
   5 host/centos7.ntap.local@NTAP.LOCAL
   5 host/CENTOS7@NTAP.LOCAL
   5 host/CENTOS7@NTAP.LOCAL
   5 host/CENTOS7@NTAP.LOCAL
   5 host/CENTOS7@NTAP.LOCAL
   5 host/CENTOS7@NTAP.LOCAL
   5 CENTOS7$@NTAP.LOCAL
   5 CENTOS7$@NTAP.LOCAL
   5 CENTOS7$@NTAP.LOCAL
   5 CENTOS7$@NTAP.LOCAL
   5 CENTOS7$@NTAP.LOCAL
   5 HOST/centos7.ntap.local@NTAP.LOCAL
   5 HOST/centos7.ntap.local@NTAP.LOCAL
   5 HOST/centos7.ntap.local@NTAP.LOCAL
   5 HOST/centos7.ntap.local@NTAP.LOCAL
   5 HOST/centos7.ntap.local@NTAP.LOCAL
```

レルム出力

```
# realm list
NTAP.local
  type: kerberos
  realm-name: NTAP.LOCAL
  domain-name: ntap.local
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@ntap.local
  login-policy: allow-realm-logins
```

Kerberos対応homedir mountの使用例

1. ユーザーになる。

```
# su prof1
sh-4.2$ pwd
/root
```

2. kinit次のアカウントで「ログイン」していないため、アクセスは拒否されます。

```
sh-4.2$ cd ~
sh: cd: /home/prof1: Permission denied
```

3. ログインしてTGTを表示します。

```
sh-4.2$ kinit
Password for prof1@NTAP.LOCAL:
sh-4.2$ klist -e
Ticket cache: KEYRING:persistent:1100:1100
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
07/31/2017 11:32:31 07/31/2017 21:32:31 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 08/07/2017 11:32:28, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

4. NFSv4.1およびKerberosを使用してONTAPに自動マウントされているhomedirに移動します。

```
sh-4.2$ cd ~
sh-4.2$ klist -e
Ticket cache: KEYRING:persistent:1100:1100
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
07/31/2017 11:32:38 07/31/2017 21:32:31 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 08/07/2017 11:32:28, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
07/31/2017 11:32:31 07/31/2017 21:32:31 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 08/07/2017 11:32:28, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
sh-4.2$ pwd
/home/prof1
sh-4.2$ mount | grep prof1
demo:/home/prof1 on /home/prof1 type nfs4
(rw,nosuid,relatime,vers=4.1,rsize=1048576,wsize=1048576,namlen=255,hard,proto=tcp,port=0,timeo=6
0,retrans=2,sec=krb5,clientaddr=x.x.x.x,local_lock=none,addr=x.x.x.b)
```

コーナーケース

次のセクションでは、メインドキュメントの範囲外で、問題に対する有効な解決策であるユースケースについて説明します。このセクションに追加する問題について提案がある場合は 、このドキュメントの「お問い合わせ」セクションの手順に従ってください。

CIFS / SMBとNFS Kerberosに同じマシンアカウントを使用する

ONTAPでCIFSサーバを作成すると、Windows Active Directoryにマシンアカウントが作成されます。このマシンアカウントには、そのCIFSサーバのSPN情報と、セキュリティ上の理由から定期的に自動的に更新されるkeytabとマシンアカウントのパスワードが格納されます。

NFS Kerberosでは、Windows Active Directoryの個別の専用マシンアカウントが使用されます。これは、マシンアカウントが同じkeytab情報をONTAPと共有できないためです。そのため、CIFSパスワードが自動的に更新されると、NFS Kerberos認証が機能しなくなります。ただし、CIFS / SMB KerberosとNFS Kerberosには同じホスト名とDNSエントリを使用できます。CIFS / SMB Kerberosでは `cifs/hostname` SPNが使用され、NFSでは `nfs/hostname` SPNが使用されます。

NFS KerberosとCIFS / SMB Kerberosは別々のマシンアカウントにすることを推奨します。

複数クライアントでのキータブの共有

CIFS / SMBおよびNFS Kerberosに同じマシンアカウントを使用するのと同じ形式で、複数のクライアントで同じkeytabファイルを使用することもできません。これはKerberosのセキュリティ機能です。クライアントは、固有のキータブを使用して適切なpadata-type：krb5-PADATA-ENC-TIMESTAMP情報を送信する必要があります。複数のホストでキータブを使用しようとすると、PAデータは送信されず、認証に失敗します。

keytabファイルを使用したkinit

場合によっては、サービスアカウントがNFS Kerberos経由でマウントにアクセスする必要があります。ただし、サービスアカウントでは、さまざまな理由で、問題のkinitログインに通常のユーザ名とパスワードを使用してKerberosチケットを取得できない場合があります。

このようなシナリオでは、認証用のKerberos keytabファイルと、認証を定期的に更新するスクリプト/ cronジョブを使用できます。keytabファイルのエントリでは `kinit - k`、クレデンシャルを更新するためにKDCに対して定期的に認証するオプションを指定してコマンドを実行できます。

KDCでのkeytabの作成は、使用するKDCによって異なります。Windows KDCの場合は、ktpassを使用します。その他のKDCについては、KDCのドキュメントを参照してください。

サービスにkeytabファイルを使用する場合は、sudoersファイルへの適切なアクセス権の追加が必要になることがあります。`kinit` keytabファイルを使用して実行するには `/etc/krb5.keytab`、を `root` 所有者として使用する権限が600に設定されているため、クライアント上で昇格された権限が必要です。

```
[root@centos7 ~]# su oracle
sh-4.2$ kinit -k root/oracle@NTAP.LOCAL
kinit: Pre-authentication failed: Permission denied while getting initial credentials
```

ユーザをsudoersに追加したら、`kinit` 作成したkeytabファイルエントリでsudo toを使用します。パスワードを必要としないようにキータブを設定できます。

```
sh-4.2$ sudo kinit -k root/oracle@NTAP.LOCAL
[sudo] password for oracle:
sh-4.2$ klist -e
Ticket cache: KEYRING:persistent:1999:krb_ccache_wii6eeV
Default principal: root/oracle@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 22:39:52 04/27/2020 23:39:52 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 22:39:52, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

keytabエントリを使用すると、サービスアカウントはNFS Kerberosマウントにアクセスできます。

```
sh-4.2$ cd /kerberos
sh-4.2$ klist -e
Ticket cache: KEYRING:persistent:1999:krb_ccache_wii6eeV
Default principal: root/oracle@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 22:47:01 04/27/2020 23:39:52 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/20/2020 22:39:52, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
04/27/2020 22:39:52 04/27/2020 23:39:52 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 22:39:52, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

DNSの代わりにローカルホストファイルを使用する

Cloud Volumes ONTAPや Azure NetApp Filesのセットアップなど、場合によっては、DNSサーバをホスト名解決ですぐに使用できないことがあります。Kerberos SPNがチケット要求のためにKDCに渡されるため、ホスト名解決はKerberos操作に不可欠です。たとえば、のFQDNにマウントを実行する場合 `SVM.domain.com`、要求されるKerberos SPNはとなります `nfs/SVM.domain.com@DOMAIN.COM`。DNSが存在しない場合 `SVM.domain.com`、は有効なIPアドレスを見つけることができません。また、リバースDNSルックアップ（IPからホスト名）では、チケットを取得するためにIPを有効なKerberos SPN名に解決できません。

DNSの代わりに、NFSクライアントとONTAP SVMでローカルホストファイルのエントリを設定できます。

このプロセスの基本的な手順は次のとおりです。

- SVM内のデータLIFでKerberosを有効にします。SVM内の少なくとも1つのデータLIFがWindows KDCにアクセスできる必要があります。
- NFS SPNマシンアカウントを変更し `servicePrincipalName` てSPNを追加し `nfs/shortname`ます。
- NFS SPNマシンアカウントの `msDs-SupportedEncryptionTypes` 値を、AESのみ（24）を使用するように変更します。
- NFSクライアントのhostsファイルに、NFS SPNの短縮名とFQDNを指定したエントリを追加します。たとえば、`nfs/svm.netapp.com svm` とのホストエントリが必要になり `svm.netapp.com`ます。

ローカルホストファイルのエントリが存在する場合、クライアントはホスト名をIPアドレスに解決し、IPアドレスをホスト名に解決することができます。これにより、KDCに対するNFS SPN要求が作成されます。

次の例を参照してください。

```
[root@centos7 ~]# mount -o sec=krb5p DEMO4:/home /kerberos
[root@centos7 ~]# umount /kerberos/
[root@centos7 ~]# mount -o sec=krb5p 10.x.x.y:/home /kerberos
[root@centos7 ~]# umount /kerberos/
[root@centos7 ~]# nslookup demo3
Server:         10.x.x.x
Address:        10.x.x.x#53

** server can't find demo3: SERVFAIL

[root@centos7 ~]# nslookup demo3.ntap.local
Server:         10.x.x.x
Address:        10.x.x.x #53

** server can't find demo3.ntap.local: NXDOMAIN
```

Windows以外のKDCの使用

FreeIPA、MIT、Heimdal、または別のKDCなど、Windows以外のKDCを使用する場合、Kerberos設定プロセスは基本的に同じです。ONTAPを使用すると、KDCと連携してNFS SPNを作成することで、Kerberosの設定を自動化できます。

KDCとの対話を自動化する代わりに、NFS SPNのキータブをKDCから手動で転送することもできます。クライアントの設定手順とDNS /ホスト名の要件は、Windowsの場合と同じです。

FreeIPA Kerberos

ONTAPは `kadmin` コマンドを使用し、FreeIPAはコマンド `ipa` セットを使用するため、ONTAPとの対話では現在自動化されたプロセスを使用してKerberosを設定しません。FreeIPAをKDCとして使用する場合は、次の手順を実行します。

1. `ipa host-add` AESエンタイプを使用して指定し、NFS Kerberos SPNを手動で追加します。

```
ipa host-add demo-ipa.centos-ldap.local
ipa service-add nfs/demo-ipa.centos-ldap.local
ipa-getkeytab -p nfs/demo-ipa.centos-ldap.local -k ./nfs.keytab -e aes256-cts-hmac-sha1-
96,aes128-cts-hmac-sha1-96
```

2. 作成したkeytabファイルをWebサーバにコピーし、 `kerberos interface enable -keytab-uri` オプションを使用してコマンドを実行します。

```
cluster::*> kerberos interface enable -vserver NFS -lif ipa-krb -spn nfs/demo-ipa.centos-
ldap.local@CENTOS-LDAP.LOCAL -keytab-uri http://web-server/files/ipakrb-ontap.keytab
```

DNSエイリアス/正規名

データLIFでKerberosを有効にする場合は、設定時にSPNが指定されます。このSPNは、Kerberosマウントへのアクセスに使用するホスト名を決定します。たとえば、のSPNを `nfs/kerberos.domain.com` 使用する場合、のFQDN `kerberos.domain.com` またはの短いホスト名を使用してマウントにアクセスできます `kerberos`。DNSエントリが必要になるのは、マウントで使用されるホスト名によって認証のためにKDCに渡すSPNが決定されるためです。DNS A/AAAAレコードを使用してなどのエイリアスを作成する `nfskrb.domain.com`と、そのホスト名がSPNとしてKDCに渡され、Kerberosマウントは「access denied」エラーで失敗します。

```
# mount -o sec=krb5 nfskrb:/unix /mnt
mount.nfs: access denied by server while mounting nfskrb:/unix
```

要求されているDNS名がSPNと一致しないため、パケットトレースまたは対応するKerberosログでは、Kerberos要求にPRINCIAL_UNKNOWNエラーが表示されます。上記の例では `krb.domain.com` `nfs/Kerberos.domain.com`、!=となっているため、アクセスは拒否されます。

DNSエイリアスを正しく作成するには、NFS SPNに関連付けられたDNS A/AAAAレコードを指すDNS CNAMEを使用します。CNAMEポイントのDNS A/AAAAレコードは、データLIF SPNで使用されている名前と同じ名前を使用する必要があります。たとえば、Kerberosインターフェイスの場合、`nfs/kerberos.domain.com` CNAMEポイントが必要なDNS A/AAAAレコードが必要です `kerberos.domain.com`。

この手順を実行すると、DNS要求が設定されたホスト名に転送され、Kerberos要求に使用されます。

次の例を参照してください。

```
DNS 113 Standard query response 0x8e5f A svmdr.ntap.local CNAME svmdr1.ntap.local A x.x.x.x
DNS 97     Standard query response 0xeea2 AAAA svmdr.ntap.local CNAME svmdr1.ntap.local
DNS 77     Standard query 0x2632 A svmdr1.ntap.local
DNS 77     Standard query 0x8021 AAAA svmdr1.ntap.local
NFS 1438 V4 NULL Call
```

```
▾ sname
    name-type: kRB5-NT-SRV-HST (3)
  ▾ sname-string: 2 items
      SNameString: nfs
      SNameString: svmdr1.ntap.local
▾ enc-part
    etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    kvno: 2
    cipher: afae0a6853a3cf0b080c1cfc5e3149d7bd3970e5fa7d37f4…
```

Cloud Volumes ONTAPテノNFSKerberos

Cloud Volumes ONTAPでは、セキュリティを重視するストレージ管理者向けに、NFS Kerberosを使用してネットワークを介したNFS通信を暗号化できます。Cloud Volumes ONTAPはクラウドで実行されるONTAPインスタンスであるため、特に設定に関する考慮事項はありません。必要に応じて、keytabを手動で作成することで、LDAPやKDCなどの外部ネームサービスに接続することなくNFS Kerberosを使用するようにCloud Volumes ONTAPインスタンスを設定できます（「手動でのkeytab設定：クライアントとONTAP」の項を参照）。

IPSec：NFSパケットを暗号化する代替手段

ONTAP 9.8では、IPSecサポートが導入されました。この機能では、NFSやiSCSIなど、あらゆる種類のイーサネット通信を暗号化できます。IPSecは、ネットワーク上での暗号化を実現するためだけにネームサービスやKDCのセットアップを必要としないというNFS Kerberosよりも明確な利点があります。これは、インフラを追加して解決策に請求可能な時間を追加できるCloud Volumes ONTAP構成で特に便利です。IPSecの詳細については、次を参照してください。

- エピソード275: ONTAP 9.8セキュリティアップデート(IPSec搭載) (音声ポッドキャスト)
- ONTAP 9.8以降でIPsec用に複数のクライアントを設定する方法
- TR-4569：『Security Hardening Guide for NetApp ONTAP 9』

NFS KerberosとStorage Virtual Machineによるディザスタリカバリ

SVMディザスタリカバリ（SVM-DR）は、SVMの設定レプリケーションとデータボリュームの通常のSnapMirrorレプリケーションを行うONTAPの機能です。環境でSVM-DRを設定するために必要な手順については、NetAppのドキュメントを参照してください。

SVM-DRは、CIFS / SMB共有、DNS、ネームサービス設定のほか、Kerberos Realmやインターフェイスもレプリケートします。SVM-DRにはレプリケーションのオプションがいくつかあります。SVM設定のレプリケーションのレベルは、ソースシステムとデスティネーションシステムでのNFS Kerberosの設定方法に直接影響します。設定に関する考慮事項は、ドキュメントに記載されているCIFS / SMBの推奨事項と同じです。

identity-preserveをtrueに設定したSVM-DR（すべての設定が同一）

identity-preserveをtrueに設定してNFS Kerberosを使用する場合（IPアドレスとKerberos Realmは同一で、ホスト名は同じ）、NFS Kerberosに関して何もする必要はありません。フェイルオーバーは通常どおり機能し、手動操作は必要ありません。

identity-preserveをtrueに設定したSVM-DR（ネットワークインターフェイスがレプリケートされない）

IPアドレスがソースからデスティネーションに変更された場合は、一意のSPNを持つソースとデスティネーションの両方のSVMでNFS Kerberosを有効にする必要があります。これにより、クライアントとKerberosのやり取りに使用できる各SVMにキータブが作成されます。KDCでマシンアカウント/ SPNを共有しようとすると、クライアントがデスティネーションシステムで適切な認証トークンを見つけることができないため、Kerberosマウントが失敗します。

一意のSPNに加えて、各SPNのDNS A/AAAAレコードを作成し、目的のSVMのホスト名を指すCNAMEレコードを作成する必要があります（詳細については、「DNSエイリアス/正規名」を参照してください）。

フェイルオーバー（計画的または計画外）が発生した場合は、もう一方のSVMのホスト名を指すようにCNAMEを変更します。DNSはホスト名検索を適切なA/AAAAレコードにリダイレクトし、Kerberos認証に使用します。

次の例を参照してください。

- SVMDR1にはIP `x.x.x.x` があり、SPNでKerberosが有効になって `nfs/svmdr1.domain.com`います。
- SVMDR2にはIP `y.y.y.y` があり、SPNでKerberosが有効になってい `nfs/svmdr2.domain.com`ます。
- `svmdr1.domain.com` およびのDNS A/AAAAレコード `svmdr2.domain.com` が作成されます。
- という名前のCNAMEレコード `svmdr.domain.com` が作成され、参照され `svmdr1.domain.com`ます。

CNAMEレコードが照会されると、次の出力が生成されます。

```
# nslookup svmdr.domain.com
Server:         x.x.x.z
Address:        x.x.x.z#53

svmdr.ntap.local        canonical name = svmdr1.ntap.local.
Name:   svmdr1.ntap.local
Address: x.x.x.x
```

CNAMEが他のSVMにリダイレクトされると、CNAMEは設定されているIPに変更されます。

```
# nslookup svmdr.domain.com
Server:         x.x.x.z
Address:        x.x.x.z#53

svmdr.ntap.local        canonical name = svmdr2.ntap.local.
Name:   svmdr2.ntap.local
Address: y.y.y.y
```

NFS Kerberosマウントでは、マウントにそれぞれ固有のSPNが使用されます。

```
$ klist
Ticket cache: KCM:1587401110
Default principal: user@DOMAIN.COM

Valid starting       Expires              Service principal
06/10/2020 11:31:48 06/10/2020 11:41:44 nfs/svmdr1.domain.com@DOMAIN.COM
        renew until 06/10/2020 21:31:44
06/10/2020 11:31:46 06/10/2020 11:41:44 krbtgt/DOMAIN.COM@DOMAIN.COM
        renew until 06/10/2020 21:31:44
06/10/2020 11:34:47 06/10/2020 11:41:44 nfs/svmdr2.domain.com@DOMAIN.COM
        renew until 06/10/2020 21:31:44
```

identity-preserveをfalseに設定したSVM-DR

identity-preserveをfalseに設定する場合は、以前の設定と同じ手順を実行する必要があります（identity-preserveをtrueに設定したSVM-DRが、ネットワークインターフェイスはtrueに設定されません）。一意のインターフェイスとNFS Kerberos SPNをDNSエントリとともに設定する必要があります。

次の例は、前のセクションの例を示しています。

- SVMDR1にはIP `x.x.x.x` があり、SPNでKerberosが有効になって `nfs/svmdr1.domain.com`います。
- SVMDR2にはIP `y.y.y.y` があり、SPNでKerberosが有効になってい `nfs/svmdr2.domain.com`ます。
- `svmdr1.domain.com` およびのDNS A/AAAAレコード `svmdr2.domain.com` が作成されます。
- という名前のCNAMEレコード `svmdr.domain.com` が作成され、参照され `svmdr1.domain.com`ます。

keytabの手動設定：クライアントおよびONTAP

場合によっては、realm joinやnet adsなど、自動化されたクライアント側コマンドを使用してKerberosのkeytabを作成できないことがあります。

次のような原因が考えられます。

- Linuxクライアントでの Sambaパッケージの使用に関するセキュリティ制限
- エアギャップネームサービス（クライアントのみがKDCとDNSにアクセスできる）
- 到達できないCloud Volumes ONTAPとオンプレミスのKDC / DNS

このような場合は、keytabを手動で作成し、必要なクライアントまたはONTAP SVMにインポートする必要があります。

- Microsoft Active Directoryでkeytabを手動で作成するには、次の手順を実行します。
  Active Directory:Kerberosキータブを使用してWindows以外のシステムを統合する
- FreeIPAでkeytabを手動で作成するには、「FreeIPA Kerberos」の手順に従います。
- MITまたはその他のLinux KDCでkeytabを手動で作成するには、ここで定義されているプロセスを使用します。
  https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-install/The-Keytab-File.html

手動キータブに関する考慮事項

手動キータブを作成する場合は、次の点を考慮してください。

- クライアントのキータブでは、SPNとしてhost/またはroot/を使用する必要があります（host/hostname.domain.comなど）。いずれかを選択すると、対応するUNIXユーザまたはネームマッピングルールが必要になります（「マシンアカウントのSPNからUNIXへのネームマッピング」を参照）。
- ONTAPキータブは `nfs/` SPNに使用する必要があります（など）`nfs/ontap.domain.com`。以前のリリースのONTAPでは、という名前のUNIXユーザ `nfs` またはネームマッピングルールの作成が必要になる場合があります（「NFSサービスのSPNからUNIXへのネームマッピング」を参照）。
- マウントにアクセスするユーザSPN/UPNでは、ONTAPがチケット交換のためにKDCに接続する必要はありません。Kerberosチケット交換カンバセーションは、クライアントとKDCの間で行われます。そのため、クライアントがKDCと通信できる場合は、Kerberosを使用して完全に分離されたONTAPインスタンスを作成できます。ただし、ユーザSPN/UPNには、「ユーザSPNからUNIXへのネームマッピング」のセクションに従って、有効なUNIXネームマッピングまたは解決可能なUNIXユーザ名が必要です。
- ONTAPでは、NFS KerberosでAES、DES3、およびDES暗号化タイプのみがサポートされます。そのため、keytabでは暗号化タイプ以外の暗号化タイプは使用しないでください。
- ONTAPでは、許可されている暗号化タイプをNFSサーバに割り当てることができます。keytabとNFSサーバでAES *暗号化タイプのみを指定した場合でも、許可されている他の暗号化タイプについてONTAPから苦情が表示されます。
- keytabファイルを適用した後で暗号化タイプを変更する場合は、新しいkeytabを作成し、Kerberosインターフェイスを無効または有効にする必要があります。これにより、システムが停止します。
- ONTAP内のデータLIFでKerberosを無効にする必要があり、KDCに接続していない場合は `-force`、オプションを使用します。

Kerberosキャッシュ

NFS Kerberosを設定して使用する場合は、プロセス中にキャッシュされる可能性があるため、問題が発生したときに混乱を招く可能性があることに注意してください。

たとえば、NFS Kerberosを設定しているときにエラー状態になった場合は、最初のKerberosチケットがシステムにキャッシュされている可能性があります。また、トラブルシューティング時にエラー状態の原因をクリアした場合でも、 Kerberosキャッシュが期限切れになるまで、肯定的な結果が表示されないことがあります。

ONTAP NFSサーバに対してKerberos NFSマウントが実行されると、ONTAPはチケットをサブシステムにキャッシュし、チケットの有効期限が切れるまでそのエントリを維持します。このエントリはKerberosコンテキストキャッシュに保持されます。このキャッシュは、 `kerberos-context-cache` diag権限のコマンドで管理されます。

次の例は、Kerberosを使用したマウントについて、マウントおよびNFSアクセスプロセスの各ポイントでコンテキストキャッシュがどのように処理されるかを示しています。

クライアントの初回マウント

次の例では、rootユーザが15：22にONTAPクラスタへのマウントを実行します。Kerberosチケットは1時間後に有効期限が切れるように設定されており、有効期限は16：22になります。

```
[root@centos7 ~]# mount -o sec=krb5p DEMO:/home /kerberos

cluster::*> kerberos-context-cache show -vserver DEMO -node node1
  (diag nblade nfs kerberos-context-cache show)

Vserver    : DEMO
Node       : node1
                                                                        Key
                                Aux                                    Data
                                Gid          Idle                   Enc Length
Extent   Slot    Uid    Gid Count     Duration          Expiration Type (Bytes)
------ ------ ------ ------ ----- ------------ ------------------- ---- ------
     0      1      0      1     1        0:0:3  4/27/2020 16:22:59   18   1192
     0      2      0      1     1        0:0:3  4/27/2020 16:22:59   18   1192
```

ユーザによる最初のNFSマウントアクセス

この例では、ユーザは `prof1` 15：24にKerberosクレデンシャルを使用してNFSマウントにアクセスします。チケットの有効期限は16時24分です。

```
sh-4.2$ id
uid=1002(prof1) gid=10002(ProfGroup)
groups=10002(ProfGroup),1101(group1),1202(group2),1203(group3),1220(sharedgroup),10000(Domain
Users)
sh-4.2$ kinit
Password for prof1@NTAP.LOCAL:
sh-4.2$ cd /kerberos/
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 15:25:05 04/27/2020 16:24:59 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/04/2020 15:24:59
04/27/2020 15:24:59 04/27/2020 16:24:59 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/04/2020 15:24:59

cluster::*> kerberos-context-cache show -vserver DEMO -node node1
  (diag nblade nfs kerberos-context-cache show)

Vserver    : DEMO
Node       : node1
                                                                                  Key
                                  Aux                                            Data
                                  Gid          Idle                         Enc Length
Extent   Slot    Uid    Gid Count      Duration          Expiration          Type (Bytes)
------ ------ ------ ------ ----- ------------ ------------------- -------- ------
     0      0      0      1     1       0:0:21  4/27/2020 16:22:59   18    1192
     0      1      0      1     1       0:0:32  4/27/2020 16:22:59   18    1192
     0      2      0      1     1       0:0:52  4/27/2020 16:22:59   18    1192
     0      3   1002  10002     6        0:0:8  4/27/2020 16:24:59   18    1192
```

ユーザによる以降のマウントアクセス

次に、ユーザは `student2` 15：37に同じNFSマウントにアクセスします。チケットは1時間で期限切れになります。

```
sh-4.2$ id
uid=1302(student2) gid=1101(group1)
groups=1101(group1),1202(group2),1203(group3),1220(sharedgroup),10000(Domain Users)
sh-4.2$ kinit
Password for student2@NTAP.LOCAL:
sh-4.2$ cd /Kerberos
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1302:1302
Default principal: student2@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 15:37:21  04/27/2020 16:37:15  nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/04/2020 15:37:15
04/27/2020 15:37:15  04/27/2020 16:37:15  krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/04/2020 15:37:15

cluster::*> kerberos-context-cache show -vserver DEMO -node node1
  (diag nblade nfs kerberos-context-cache show)

Vserver    : DEMO
Node       : node1
                                                                                  Key
                                  Aux                                            Data
                                  Gid          Idle                         Enc  Length
Extent   Slot    Uid    Gid Count      Duration          Expiration          Type (Bytes)
------ ------ ------ ------ ----- ------------ ------------------- -------- ------
     0      1      0      1     1       0:0:19  4/27/2020 16:22:59   18    1192
     0      2      0      1     1      0:25:25  4/27/2020 16:22:59   18    1192
```

```
     0       3   1002 10002       6       0:2:33 4/27/2020 16:24:59    18    1192
     0       5   1302   1101       5      0:12:26 4/27/2020 16:37:15    18    1192
```

次の例では、別のユーザがKerberosマウントにアクセスします。

```
cluster::*> kerberos-context-cache show -vserver DEMO -node node1
  (diag nblade nfs kerberos-context-cache show)

Vserver     : DEMO
Node        : node1
                                                                                Key
                                  Aux                                          Data
                                  Gid          Idle                       Enc Length
Extent    Slot     Uid     Gid Count      Duration          Expiration Type (Bytes)
--------- -------- ------- ------- ------ ---------- ------------------- ---- ------
     0       1       0       1      1        0:0:9  4/27/2020 16:22:59   18    1192
     0       2       0       1      1       0:7:30  4/27/2020 16:22:59   18    1192
     0       3    1002   10002      6      0:13:59  4/27/2020 16:24:59   18    1192
     0       5    1302    1101      5       0:7:44  4/27/2020 16:37:15   18    1192
     0       6    1301    1101      3        0:0:1  4/27/2020 16:59:42   18    1192
```

前の例では、スロット番号にすべてのエントリが表示されないことに注意してください。これらのエントリは、クライアントが特定の処理を要求すると表示（または再表示）されます。たとえば student2、プロンプトを終了すると、スロットテーブルの位置を考えると、実際には古いエントリである2つの新しいエントリが表示されます。

```
cluster::*> kerberos-context-cache show -vserver DEMO -node node1
  (diag nblade nfs kerberos-context-cache show)

Vserver     : DEMO
Node        : node1
                                                                                Key
                                  Aux                                          Data
                                  Gid          Idle                       Enc Length
Extent    Slot     Uid     Gid Count      Duration          Expiration Type (Bytes)
--------- -------- ------- ------- ------ ---------- ------------------- ---- ------
     0       1       0       1      1       0:0:10  4/27/2020 16:22:59   18    1192
     0       2       0       1      1      0:28:16  4/27/2020 16:22:59   18    1192
     0       3    1002   10002      6       0:5:24  4/27/2020 16:24:59   18    1192
     0       4       0       1      1        0:0:1  4/27/2020 16:22:59   18    1192
     0       5    1302    1101      5      0:15:17  4/27/2020 16:37:15   18    1192
     0       6    1302    1101      5        0:0:1  4/27/2020 16:37:15   18    1192
```

encタイプは、チケットが使用した暗号化タイプを示します。この場合、すべてのチケットはencタイプ18で、Kerberosパラメータのリストにあるようにに AES-256にマップされます。

ONTAPのKerberosキャッシュは、次のコマンドを使用してクリアできます。

```
cluster::*> kerberos-context-cache clear?
  (diag nblade nfs kerberos-context-cache clear)
  clear                         *Clear the context cache entries
  clear-all                     *Clear the entire context cache
```

コンテキストキャッシュをクリアすると、Kerberosのマウントエラー時に入力された古いエントリが取り除かれ、初期設定時に後続のエラーが原因になる可能性があります。

コンテキストキャッシュに加えて、krb-unix Kerberos認証中に発生するネームマッピングのネームマッピングエントリを削除するには、クレデンシャルキャッシュをフラッシュする必要があります。ただし、プロセス中は注意が必要です。詳細はBug1224820を参照してください。

注： バグリンクを表示するには、NetAppサポートへのログインが必要になる場合があります。

Kerberosコンテキストキャッシュに対するアンマウントの影響

クライアントがNFS Kerberosマウントをアンマウントすると、コンテキストキャッシュエントリが削除されます。ただし、krb-unix ネームマッピングのクレデンシャル（nfs/service UNIXユーザNFSなど）はキャッシュされたままです。デフォルト値は24時間で、name-service cache unix-user コマンドで制御されます。

```
cluster::*> name-service cache unix-user settings show -vserver DEMO

Vserver         Enabled Negative-cache TTL        Negative TTL Propagation
                        Enabled                               Enabled
--------------- ------- ------------------ ------------ ------------ -----------
DEMO            true    true               24h          1m           true
```

NFSクレデンシャル キャッシュ

Kerberosマウントが実行されると、krb-unix 認証用に複数のネームマッピングが実行されます（詳細については、「KRB-UNIXネームマッピングの動作」を参照してください）。これらのマッピングはNFSクレデンシャルキャッシュにキャッシュされるため、トラブルシューティング時のKerberosの動作に影響する可能性があります。たとえば、NFSサービスプリンシパルのネームマッピングが存在しないときにKerberosでマウントしようとすると、最初の問題を修正したあとでもキャッシュが発生して原因エラーが発生する可能性があります。

クレデンシャルキャッシュは nfs credential、advanced権限のコマンドで管理します。

```
cluster::*> nfs credentials ?
  count                       *Count credentials cached by NFS
  flush                       *Flush credentials cached by NFS
  show                        *Show credentials cached by NFS
```

NFSクレデンシャルのタイムアウト設定には、次のNFSサーバオプションを使用します。これらのオプションは、必要に応じて小さい値に変更できます。

```
cluster::*> nfs server show -vserver DEMO -fields cached-cred-positive-ttl,cached-cred-negative-
ttl,cached-cred-harvest-timeout
vserver cached-cred-positive-ttl cached-cred-negative-ttl cached-cred-harvest-timeout
------- ------------------------ ------------------------ -----------------------------------
NFS     86400000                 7200000                  86400000
```

Kerberosコンテキストキャッシュでの-instanceの使用

-instance kerberos-context-cacheを指定すると、Kerberosセキュリティの種類、暗号化タイプの文字列、グループリスト、ホスト情報など、多数の有用な情報が得られます。

```
cluster::*> kerberos-context-cache show -vserver DEMO -slot-index 6 -extent-id 0
  (diag nblade nfs kerberos-context-cache show)

                     Vserver: DEMO
                        Node: node1
                   Extent ID: 0
                  Slot Index: 6
                     User ID: 1301
                    Group ID: 1101
               Aux Gid Count: 3
              Expiration Time: 4/27/2020 16:59:42
               Last Used Time: 4/27/2020 16:42:40
                Idle Duration: 0:1:29
GSS Context (Network Bytes): c9eb619133980006
              Encryption Type: 18
     Encryption Type String: aes256-cts-hmac-sha1-96
    Key Data Length (Bytes): 1192
                Aux Gid List: 1101, 1203, 1220
              Reference Count: 1
    Is Marked For Deletion?: false
           Client IP Address: 10.x.x.x
           Logical Interface: data
           RPCSECGSS Service: krb5p
```

Kerberosチケットの有効期間-クライアントキャッシュ

一部のクライアント（Red Hatなど）は `ticket_lifetime krb5.conf`、ファイルのオプションで定義された期間、Kerberosチケットをキャッシュします。デフォルト値は24時間です。

Kerberosチケットがクライアントによってキャッシュされると、すでにKerberosを使用して認証されているユーザは、期限切れになるまでローカルキャッシュにチケットを保持します。これは、パフォーマンスを考慮した設計になっています。

このようなシナリオでは、ユーザが `kdestroy` コマンドを実行した場合でも、Kerberosチケットはキャッシュされたままになり、アクセスが許可されます。Red Hat Bugzilla 93891ではこの動作について説明しています。

チケットの有効期間を短くする必要がある場合は、 `krb5.conf` の値を小さくするようにを設定します `ticket_lifetime`。

注: クライアントは `ticket_lifetime` KDCの値よりも大きい値を設定することはできません。

`ticket_lifetime` が指定されていない場合、またはコメントアウトされている場合のKerberosチケットの有効期間は、KDCが設定されている値になります。この場合、チケットの有効期間は1時間です。

```
[libdefaults]
 dns_lookup_realm = false
# ticket_lifetime = 24h
# renew_lifetime = 24h

# date
Tue May 19 09:13:24 EDT 2020

# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_V4nxJya
Default principal: student1@NTAP.LOCAL

Valid starting       Expires              Service principal
05/19/2020 09:13:47 05/19/2020 10:13:47 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 09:13:44
```

ファイルが10時間に設定されている場合でも、クライアントはKDCの設定に従って1時間でチケットの有効期限を切れます。

```
[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 10h
 renew_lifetime = 10h

# date
Tue May 19 09:17:24 EDT 2020

# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_V4nxJya
Default principal: student1@NTAP.LOCAL

Valid starting       Expires              Service principal
05/19/2020 09:15:24 05/19/2020 10:15:24 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/19/2020 19:15:21
```

チケットの有効期間が10分に設定されている場合、有効期限は10分に変更されます。

```
[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 10m
 renew_lifetime = 10h

# date
Tue May 19 09:29:34 EDT 2020

# klist
Ticket cache: KEYRING:persistent:0:krb_ccache_V4nxJya
Default principal: student1@NTAP.LOCAL

Valid starting       Expires              Service principal
05/19/2020 09:29:22 05/19/2020 09:39:20 krbtgt/NTAP.LOCAL@NTAP.LOCAL
```

```
        renew until 05/19/2020 19:29:20
```

注： に変更を加える `krb5.conf` と、Kerberosサービスの再起動が必要になります。

チケットの有効期間はKerberosセットアップのトラブルシューティングに影響する可能性があるため、設定作業中にクライアントのチケットの有効期間値をより短いタイムアウトに変更することを推奨します。

Kerberosチケットの有効期限の動作

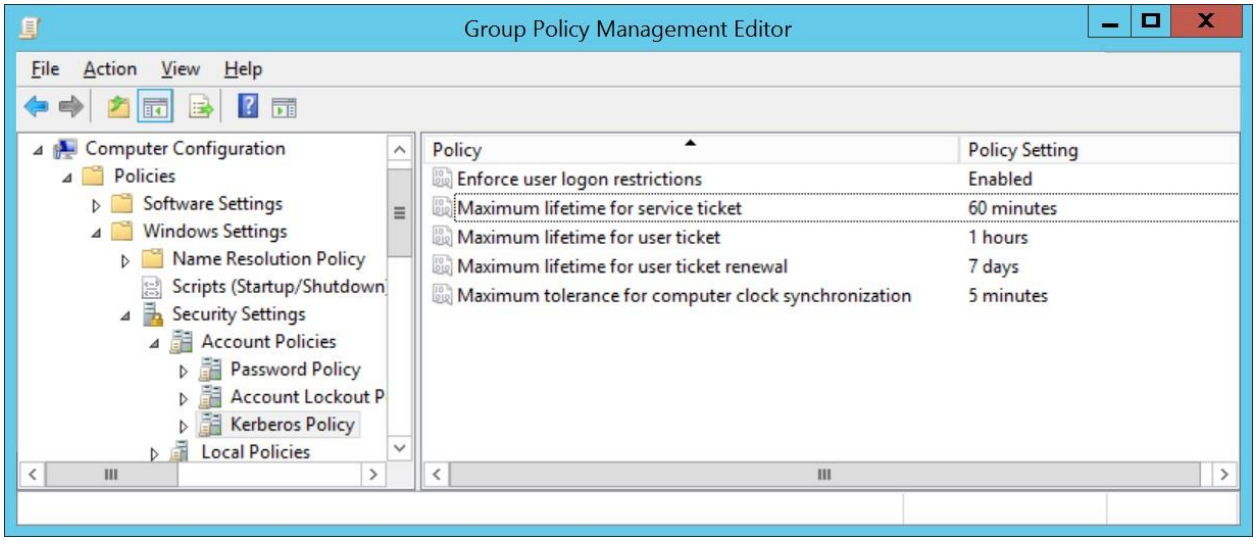
Kerberosチケットの有効期間はKDCで設定され、Kerberosチケットの有効期間が決定されます。チケットの有効期間は、賢明なセキュリティとKDCの負荷軽減のバランスをとることを目的として設定されています。たとえば、チケットの有効期間を1年に設定すると、KDCの負荷が低くなる可能性がありますが、ユーザーが再認証する必要があるのは年に1回だけなので、セキュリティリスクも高まります。デフォルトでは、Microsoft Kerberosチケットは10時間有効で、7日ごとに更新する必要があります。これはクライアントの `krb5.conf` ファイル設定でより低い値に上書きできますが、より長い有効期限に設定することはできません。

チケットの有効期限が切れると、ユーザがを使用してKDCに再認証するまで、Kerberos経由のNFSマウントへのアクセスは成功しません `kinit`。

Kerberosチケットの有効期限が切れた場合の動作

たとえば、次のユーザ（`prof1`）が1時間続くチケットを要求し、NFSマウントにアクセスしたとします。図7では 、ユーザチケットとサービスチケットの両方が16:24:59に期限切れになることがわかります。これは、Windows KDCが1時間のチケット有効期限ポリシーを使用するように設定されているためです。Windows Active DirectoryでKerberosチケットポリシーを設定する方法については、「サービスチケットの最大有効期間」を参照してください。

図7）Kerberosチケットの有効期間管理-Microsoft Windowsグループポリシー



ここでは、クライアントのKerberosチケットと有効期限のリストを確認できます。

```
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 15:25:05 04/27/2020 16:24:59 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/04/2020 15:24:59
04/27/2020 15:24:59 04/27/2020 16:24:59 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/04/2020 15:24:59
```

チケットの有効期限が切れると、チケットの有効期限がフラッシュされたことがわかります。

```
sh-4.2$ date
```

```
Mon Apr 27 16:25:00 EDT 2020
sh-4.2$ klist
klist: Credentials cache keyring 'persistent:1002:1002' not found
```

NFS Kerberosマウントにはアクセスできなくなります。

```
sh-4.2$ cd /kerberos
sh: cd: /kerberos: Not a directory
```

再認証後、新しい有効期限付きのアクセスと新しいチケットを取得します。

```
sh-4.2$ kinit
Password for prof1@NTAP.LOCAL:
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:27:32 04/27/2020 17:27:32 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 16:27:32
sh-4.2$ cd /kerberos
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:27:39 04/27/2020 16:37:39 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/20/2020 16:27:32
04/27/2020 16:27:32 04/27/2020 17:27:32 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 16:27:32
```

注： 次のセクションをテストするために、サービスチケットの有効期限を10分に変更しました。

サービスチケットだけが期限切れになった場合の動作

場合によっては、ユーザチケットが期限切れになる前にサービスチケットが期限切れになることがあります。その場合、クライアントには次のようにチケットが表示されます。

```
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
klist: No credentials cache found while retrieving a ticket
```

ユーザがNFS Kerberosマウントに属している場合、`ls` は新しいサービスチケットが取得されるまで失敗します。

```
sh-4.2$ ls
ls: cannot open directory .: Permission denied
sh-4.2$ pwd
/kerberos
```

新しいチケットを取得すると、アクセスが復元されます。

```
sh-4.2$ kinit
Password for prof1@NTAP.LOCAL:
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:38:46 04/27/2020 17:38:46   krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 16:38:46
sh-4.2$ ls
dir dynamicuid flexgroup ftp ftpuser      mtuser nfs4 oracle prof1 root silly student1
student2 test unix
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1002:1002
```

```
Default principal: prof1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:39:01  04/27/2020 16:49:01  nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/20/2020 16:38:46
04/27/2020 16:38:46  04/27/2020 17:38:46  krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 16:38:46
```

チケットが手動で破棄された場合の動作

kdestroy クライアント上でを使用してチケットを手動で破棄すると、Kerberosチケットが期限切れになるか、ONTAPキャッシュから手動でクリアされるまでアクセスが許可されます。

```
[root@centos7 /]# su student1
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1301:1301
Default principal: student1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:01:12 04/27/2020 16:59:42 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/04/2020 15:59:42
04/27/2020 15:59:42 04/27/2020 16:59:42 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/04/2020 15:59:42
sh-4.2$ kdestroy
sh-4.2$ klist
klist: Credentials cache keyring 'persistent:1301:1301' not found
```

チケットをONTAP SVMから削除すると、クレデンシャルを破棄したユーザは再認証するまでアクセスを拒否されます。

```
cluster::*> kerberos-context-cache clear -vserver DEMO
  (diag nblade nfs kerberos-context-cache clear)

Warning: This command removes all context cache entries for the Vserver "DEMO" on node "node1".
Do you want to continue? {y|n}: y

Successfully removed 3 context cache entries on node "cluster-01". The entries which were in use
will be removed when they are no longer used.

sh-4.2$ klist
klist: Credentials cache keyring 'persistent:1301:1301' not found
sh-4.2$ ls
ls: cannot open directory .: Permission denied
sh-4.2$ pwd
/kerberos
```

ユーザが再発行する kinitと、再びアクセスできるようになります。

```
sh-4.2$ kinit
Password for student1@NTAP.LOCAL:
sh-4.2$ ls
dir dynamicuid flexgroup ftp ftpuser mtuser nfs4 oracle prof1  root  silly student1
student2 test unix
sh-4.2$ klist
Ticket cache: KEYRING:persistent:1301:1301
Default principal: student1@NTAP.LOCAL

Valid starting       Expires              Service principal
04/27/2020 16:50:17  04/27/2020 17:00:17  nfs/demo.ntap.local@NTAP.LOCAL
        renew until 05/20/2020 16:50:15
04/27/2020 16:50:15  04/27/2020 17:50:15  krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 05/20/2020 16:50:15
```

NFS Kerberosパフォーマンステスト

コンセプトの実証ラボでは、NFS Kerberos（krb5、krb5i、krb5p）を使用したNFSv3とNFSv4.1のテストを先日実施しました。これらの数値は、最高のパフォーマンスを示すものではなく、KerberosがNFS処理にどのような影響を与えるかを示すものです。

- 使用したテストスイートはvdbenchで、読み取り/書き込みの比率は50/50で、100%ランダムで、ブロックサイズは32Kでした。
- 単一のCentOS 7.9クライアントを使用して、ONTAP 9.8を実行するNetApp A400システムをマウントしました。MTUサイズは9000、rsize/wsizeは64Kです。これらの値の計算には、4回のテスト実行の平均が使用されました。
- NFSv4.1ではpNFSが使用されていました。

表3 に、MFS Kerberosの結果を示します。

表3）NFS Kerberosの結果

テスト	平均 IOPS	平均スループット（MB/秒）	平均レイテンシ（ミリ秒）
NFSv3-sys	～23839	～745	～0.5
NFSv3-krb5	～12158	～380	～2.9
NFSv3-krb5i	～10688	～334	~1.1
NFSv3-krb5p	～5633	～176	~2.2
NFSv4.1-sys	～24102	～753	～0.5
NFSv4.1-krb5	～11351	～355	~3.2
NFSv4.1-krb5i	～10856	～338	~1.1
NFSv4.1-krb5p	~5579	～174	～2.1

表4 に、MFS Kerberosのパフォーマンス比較を示します。

表4）NFS Kerberos：パフォーマンスと非暗号化ベースラインの比較

テスト	IOPS	スループット（MB/秒）	レイテンシ（ミリ秒）
NFSv3-krb5	-49%	-49%	+480%
NFSv3-krb5i	-55%	-55%	+120%
NFSv3-krb5p	-76%	-76%	+340%
NFSv4.1-krb5	-53%	-53%	+540%
NFSv4.1-krb5i	-55%	-55%	+120%
NFSv4.1-krb5p	-77%	-77%	+320 %

所見

全体として、NFS Kerberosを使用すると、すべてのNFSバージョンのパフォーマンスが大幅に低下します。暗号化されたパケットの処理にストレージで時間がかかり、その間もレイテンシが増加するため、IOPSとスループットが低下します。すべてのワークロードが同じ影響を受けるわけではないので、必ずご使用の環境でテストしてください。

一般的な問題

このセクションでは、NetApp ONTAPでNFS Kerberosを設定するプロセスで発生する最も一般的な問題のいくつかについて説明します。また、問題がどのように現れ、問題を解決するかについても説明します。このセクションは包括的ではありませんが、最も一般的に見られる問題のいくつかを提示しようとします。Kerberosにはさまざまな要素があるため、場合によっては、ストレージ管理者、Windows KDC管理者、

DNS管理者、NFSクライアント管理者の関与が必要になります。

エクスポートポリシーのトラブルシューティング

通常、エクスポートポリシーは次のような場合に発生する問題の原因です。

- マウントが失敗しました。
- 読み取りまたは書き込みが失敗します。
- ルートアクセスに失敗します。
- ユーザに正しいファイル所有権が表示されない。
- 許可されるアクセス数が多すぎます。

これらの問題は、アクセスが拒否された、読み取り専用のファイルシステム、またはさまざまな根本原因にまたがるその他のエラーとしてクライアントに表示されます。ただし、原則として、NFSアクセスの問題のトラブルシューティングを行う際には、エクスポートポリシーとルールを確認することが最初に実行する手順の1つです。

エクスポートポリシーチェックアクセス

NFSエクスポートへのアクセスをチェックする最も簡単な方法は、を使用することです `export-policy check-access`。この方法を使用すると、エクスポートポリシーのアクセスルールセットをクライアントのアクセスと照合して、エクスポートポリシールールが導入前およびトラブルシューティングの際に適切に機能しているかどうかを判断できます。

このコマンドは、NFSクライアントからの標準マウントで使用される通常のネームサービス通信とキャッシュのやり取りを使用します。

次の例を参照してください `export-policy check-access`。

```
cluster1::*> vserver export-policy check-access -vserver vs1 -client-ip x.x.x.x -volume flex_vol
-authentication-method sys -protocol nfs3 -access-type read

                                          Policy    Policy       Rule
Path                            Policy    Owner     Owner Type  Index Access
------------------------------- --------- --------- ----------- ----- ------------
/                               default   vs1_root  volume          1 read
/dir1                           default   vs1_root  volume          1 read
/dir1/dir2                      default   vs1_root  volume          1 read
/dir1/dir2/flex1                data      flex_vol  volume         10 read
```

また、このチェックは親エクスポートをトラバースして、パスのすべての部分に意図したアクセス権があることを確認します。エクスポートチェックが失敗すると、失敗したボリュームまたはqtreeでエクスポートチェックが停止します。次の例では、vsrootエクスポートポリシーによってボリュームへのアクセスが拒否されてい `flexvol`ます。クライアントがマウント用に他のボリュームをトラバースできるように、Vsrootはエクスポートポリシーで読み取りアクセスを許可する必要があります。vsrootアクセスのロックダウンについては、TR-4067：『Network File Systems（NFS）in NetApp ONTAP』を参照してください。

`export-policy check-access` vsrootでの障害の例を次に示します。

```
cluster::*> export-policy check-access -vserver DEMO -volume flexvol -client-ip x.x.x.x -
authentication-method sys -protocol nfs3 -access-type read
                                          Policy    Policy       Rule
Path                            Policy    Owner     Owner Type  Index Access
------------------------------- --------- --------- ----------- ----- ------------
/                               empty     vsroot    volume          0 denied
```

このコマンドを使用してKerberosアクセスを確認することもできます。エクスポートポリシーとルールでKerberosアクセスが許可されているかどうかが検証されます。Kerberosマウント全体（ネームマッピング、SPN検索、パスワードなど）が成功するかどうかはチェックされません。

`export-policy check-access` Kerberosアクセスについては、次の例を参照してください。

```
cluster::*> export-policy check-access -vserver DEMO -volume flexvol -client-ip x.x.x.x -
authentication-method krb5p -protocol nfs4 -access-type read-write
```

```
                                                Policy    Policy       Rule
Path                                Policy      Owner     Owner Type   Index Access
----------------------------------- ----------- --------- ------------ ----- ------
/                                   default     vsroot    volume           2 read
/flexvol                            default     flexvol   volume           2 read-write
```

エクスポートポリシーキャッシュ

エクスポートポリシールール、クライアントホスト名、ネットグループ情報はONTAPにキャッシュされ、クラスタへの要求数を削減します。キャッシュを使用すると、要求のパフォーマンスが向上し、ネットワークやネームサービスサーバの負荷が軽減されます。

clientmatchキャッシュ

clientmatchエントリがキャッシュされる場合、そのエントリはSVMに対してローカルなままになり、キャッシュタイムアウト時間に達した場合、またはエクスポートポリシールールテーブルが変更された場合にフラッシュされます。デフォルトのキャッシュタイムアウト時間はONTAPのバージョンによって異なり、 `export-policy access- cache config show` admin権限でコマンドを使用して確認できます。

ONTAP 9.7のデフォルト値は次のとおりです。

```
TTL For Positive Entries (Secs): 3600
TTL For Negative Entries (Secs): 3600
Harvest Timeout (Secs): 86400
```

で特定のクライアントを表示するには `export policy access-cache`、次のadvanced権限のコマンドを実行します。

```
cluster::*> export-policy access-cache show -node node2 -vserver NFS -policy default -address
x.x.x.x

                                    Node: node2
                                 Vserver: NFS
                             Policy Name: default
                              IP Address: x.x.x.x
                   Access Cache Entry Flags: has-usable-data
                                Result Code: 0
                First Unresolved Rule Index: -
                     Unresolved Clientmatch: -
             Number of Matched Policy Rules: 1
         List of Matched Policy Rule Indexes: 2
                               Age of Entry: 11589s
                Access Cache Entry Polarity: positive
Time Elapsed since Last Use for Access Check: 11298s
      Time Elapsed since Last Update Attempt: 11589s
               Result of Last Update Attempt: 0
                List of Client Match Strings: 0.0.0.0/0
```

エクスポートポリシーキャッシュエントリを個別にフラッシュするには、次のコマンドを実行します。

```
cluster::*> export-policy access-cache flush -vserver DEMO -node node1 -policy default -address
x.x.x.x
```

ホスト名/ DNSキャッシュ

clientmatchにホスト名を設定すると、その名前がIPアドレスに解決されます。これは、SVMのネームサービススイッチ（`ns-switch`）で使用される順序に基づいて行われます。たとえば、 `ns-switch` ホストデータベースがに設定されている場合 `files,dns`、ONTAPはローカルホストファイルで一致するクライアントを検索し、次にDNSを検索します。

名前検索後、ONTAPは結果をホストキャッシュにキャッシュします。このキャッシュの設定は変更可能で、advanced権限でONTAP CLIから照会およびフラッシュできます。

1. キャッシュを照会します。

```
cluster::*> name-service cache hosts forward-lookup show -vserver NFS
(vserver services name-service cache hosts forward-lookup show)
                    IP       Address IP                       Create
Vserver   Host      Protocol Family Address          Source Time         TTL(sec)
--------- --------- -------- ------ ---------------- ------ ------------ ----------
NFS       centos7.ntap.local
                    Any      Ipv4   x.x.x.x dns      3/26/2020 3600
                                                     16:31:11
```

2. ホストキャッシュ設定を表示します。

```
cluster::*> name-service cache hosts settings show -vserver NFS -instance
  (vserver services name-service cache hosts settings show)

                    Vserver: NFS
          Is Cache Enabled?: true
Is Negative Cache Enabled?: true
               Time to Live: 24h
     Negative Time to Live: 1m
     Is TTL Taken from DNS: true
```

場合によっては、NFSクライアントのIPアドレスが変更されたときに、アクセスの問題を修正するためにhostsエントリのフラッシュが必要になることがあります。

3. ホストのキャッシュエントリをフラッシュします。

```
cluster::*> name-service cache hosts forward-lookup delete -vserver NFS ?
     -host      -protocol -sock-type -flags      -family
```

ネットグループキャッシング

clientmatchフィールドのネットグループをエクスポートルールに使用している場合、ONTAPはネットグループネームサービスサーバに接続してネットグループ情報を展開する追加の作業を実行します。ns-switchのネットグループデータベースは、ONTAPがネットグループを照会する順序を決定します。また、ONTAPがネットグループのサポートに使用する方法は、netgroup.byhostのサポートが有効になっているか無効になっているかによって異なります。netgroup.byhostの詳細については、TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

- netgroup.byhostが無効になっている場合、ONTAPはネットグループ全体を照会し、すべてのネットグループエントリをキャッシュに取り込みます。ネットグループに数千のクライアントがある場合、そのプロセスが完了するまでに時間がかかることがあります。netgroup.byhostはデフォルトで無効になっています。
- netgroup.byhostが有効になっている場合、ONTAPはネームサービスに対してホストエントリと関連するネットグループマッピングのみを照会します。これにより、潜在的に数千のクライアントを検索する必要がないため、ネットグループのクエリに必要な時間が大幅に短縮されます。

これらのエントリは vserver services name-service cache、コマンド内のネットグループキャッシュに追加されます。これらのキャッシュエントリは表示またはフラッシュでき、タイムアウト値を設定できます。

ネットグループキャッシュ設定を表示します。

```
cluster::*> name-service cache netgroups settings show -vserver NFS -instance
  (vserver services name-service cache netgroups settings show)

                    Vserver: NFS
          Is Cache Enabled?: true
Is Negative Cache Enabled?: true
               Time to Live: 24h
     Negative Time to Live: 1m
  TTL for netgroup members: 30m
```

ネットグループ全体がキャッシュされると、そのネットグループはメンバーキャッシュに配置されます。

```
cluster::*> name-service cache netgroups members show -vserver DEMO -netgroup netgroup1
  (vserver services name-service cache netgroups members show)

            Vserver: DEMO
```

```
           Netgroup: netgroup1
              Hosts: sles15-1,x.x.x.x
        Create Time: 3/26/2020 12:40:56
Source of the Entry: ldap
```

キャッシュされているネットグループエントリが1つだけの場合、IP-to-netgroupキャッシュおよびホストのリバースルックアップキャッシュにエントリが入力されます。

```
cluster::*> name-service cache netgroups ip-to-netgroup show -vserver DEMO -host x.x.x.z
  (vserver services name-service cache netgroups ip-to-netgroup show)
Vserver     IP Address Netgroup       Source Create Time
----------- ---------- ---------------- ---------- ---------------
DEMO        x.x.x.z
                       netgroup1     ldap     3/26/2020 17:13:09

cluster::*> name-service cache hosts reverse-lookup show -vserver DEMO -ip x.x.x.z
  (vserver services name-service cache hosts reverse-lookup show)
Vserver     IP Address       Host                    Source Create Time     TTL(sec)
----------- ---------------- ------------------------ -------- -------------------- -----------
DEMO        x.x.x.z    centos8-ipa.centos-ldap.local
                                                    dns    3/26/2020 17:13:09
                                                                        3600
```

キャッシュタイムアウトの変更に関する考慮事項

必要に応じて、キャッシュ設定を別の値に変更できます。

- タイムアウト値を大きくするとキャッシュエントリが長く保持されますが、クライアントがIPアドレスを変更した場合（クライアントIPアドレスにDHCPが使用されていてDNSが更新されていない場合や、エクスポートルールでIPアドレスが使用されている場合など）、クライアントアクセスの不整合が発生する可能性があります。
- タイムアウト値を小さくすると、キャッシュがより頻繁にフラッシュされ、より最新の情報が得られます。ただし、ネームサービスサーバへの負荷が増大し、クライアントからのマウント要求のレイテンシが増大する可能性があります。

ほとんどの場合、キャッシュタイムアウト値をそのままにしておくのが最善の方法です。詳細とガイダンスについては、TR-4668：『Name Services Best Practices』および TR-4835：『How to Configure LDAP in ONTAP』を参照してください。

ONTAPテノKerberosインタアフエイスノユウコウカヘンコウマタハサクセイシノエラア

KerberosのデータLIFの初期設定時や既存のデータLIFの変更時にエラーが表示された場合は、表5を参考にして問題を解決してください。

表5）ONTAPでKerberosインターフェイスを作成または変更する際の問題の特定と解決

問題	エラーの表示方法	解決手順
インターフェイスを変更しようとするユーザには、指定したOUでマシンアカウントを作成または変更するKDCに対する権限がありません。	• event log show • コマンドが失敗した場合に返されるエラー出力	• アクセス権を持つユーザ（ドメイン管理者など）に切り替えます。 • OUの制御をユーザーに委任します。 • Kerberos設定で指定されているOUを、ユーザが作成アクセス権を持つOUに変更します。
Kerberosインターフェイスの変更が失敗し、有効なKDCに接続できないことが挙げられます。	• event log show • コマンドが失敗した場合に返されるエラー出力	• Kerberos Realmの設定をチェックし、正しく設定されていることを確認します。 • SVMのDNS設定を確認します。 • データLIFがKDCにルーティングできることを確認します。 • SVMにデフォルトルートが存在することを確認します。

問題	エラーの表示方法	解決手順
Kerberosインターフェイスの作成または変更が失敗し、タイムスキュー問題が発生します。	• event log show • コマンドが失敗した場合に返されるエラー出力 • SecDログ	• クラスタ時間をWindows KDCから5分以内に変更します。 • クラスタのタイムゾーンがKDCのタイムゾーンと一致していることを確認します。 • 環境全体で時刻を同期するには、NTPを使用します。
Kerberosインターフェイスの作成がkrb5kdc_ERR_ETYPE_NOSUPPERRORで失敗します。	• event log show • コマンドが失敗した場合に返されるエラー出力 • SecDログ	• NFSサーバの設定 - `permitted-enc-types` が、KDCで許可されているKerberos暗号化タイプと一致していることを確認します。 • たとえば `-permitted-enc- types`、がAES-256に設定されていて、KDCでDESのみが許可されている場合、コマンドは失敗します。
Kerberosインターフェイスの作成が失敗し、CIFS SMB krb5 Realmの不一致が発生します。	• event log show • コマンドが失敗した場合に返されるエラー出力 • SecDログ	• Kerberosを有効にするために使用されているユーザ名が小文字のドメインプリンシパルを使用していないことを確認します。 • たとえば、RealmがNTAP.LOCALの場合、KDCへの認証に使用するユーザはuser@ntap.locaではなく、user@NTAP.LOCAまたはuserだけを使用する必要があります。

クライアントからNFS Kerberosをマウントする際のエラー

クライアントからKerberosを使用したNFSの初回マウント時にエラーが表示された場合は、表6 にいくつかの潜在的な問題を確認してください。この情報は、Kerberosマウントの初回試行時のエラーにのみ適用されます。

表6）NFS Kerberosエクスポートをマウントする際の問題の特定と解決

問題	エラーの表示方法	解決手順
アクセス/権限の拒否	• mountコマンドの出力 • ONTAPのイベントログ • パケットトレース	• SVMルートボリューム（/）およびデータボリューム（`/path`）のエクスポートポリシールールを確認します。qtreeエクスポートを使用している場合は、qtreeのポリシーを確認します。`ro/rw` ルールでkrb5が許可され、NFSクライアントがエクスポートポリシールールのクライアント一致で許可されている必要があります。 • `export-policy check-access` コマンドを使用して、指定したクライアントがアクセスできることを確認します。 • ONTAPのイベントログ（`event log show`）で、`krb-unix` NFSクライアントのネームマッピングに関するエラーを確認します。エラーが発生した場合は、ローカルUNIXユーザまたはネームマッピングルールを作成して問題を解決します。通常、NFSサービスプリンシパル/ユーザは初期マウントには適用されません。NFSプリンシパルは、Kerberosマウントにアクセスする際に認証を行います。 • ONTAPのイベントログ(`event log show`)で、サポートされていない暗号化タイプに関するエラーを確認します。Active Directoryとの共通の問題には、RC4-HMACを使用して認証を試みるクライアントが含まれます。ONTAPでは、NFS KerberosでRC4-HMACをサポートしていません。

問題	エラーの表示方法	解決手順
		この問題を解決するには、マシンアカウントを変更して、リストからRC4を削除します。マシンアカウントを変更したあと、keytabを削除するために、キャッシュのフラッシュやKerberosの無効化/有効化が必要になる場合があります。
サポートされていないプロトコル	• mountコマンドの出力 • パケットトレース	• マウントされているNFSのバージョンを確認し、ONTAP NFSサーバで有効になっているバージョンと比較します。 • クライアントは、サーバで有効になっている最も高いNFSバージョンをネゴシエートしようとします。 • ONTAPは、NetApp FlexVol® ボリュームではNFSv3、NFSv4.0、NFSv4.1をサポートし、ONTAP FlexGroupボリュームではNFSv3をサポートします。
該当するファイルまたはディレクトリがありません	• mountコマンドの出力 • パケットトレース	• mountコマンドで指定したパスが、ONTAPにジャンクションパスとして存在することを確認します。この手順は、System ManagerまたはCLIを使用して実行できます。
マウントポイント""が存在しません	• mountコマンドの出力	• 指定したマウントポイントフォルダがローカルクライアントに存在することを確認します。
マウントオプションが正しくありません	• mountコマンドの出力	• 指定したマウントコマンドオプションを確認します。実際には、クライアントのドキュメントに従って存在していますか。 • krb5を指定する場合は、rpcgssdサービスが開始され、NFSクライアントでsecure_nfsが許可されていることを確認します。
マウントのハング	• mountコマンドの出力 • パケット トレース	• マウントがハングしている場合は、クライアントまたはサーバがパケットに応答しないことを意味します。一般に、この問題はネットワーク問題、ファイアウォール、またはサーバ設定問題のいずれかになります。

アクセス、読み取り、または書き込みの試行時のNFS Kerberosエラー

表7 に、Kerberos NFSエクスポートが正常にマウントされたあとに発生する可能性がある問題を示します。このカテゴリでは、トラバーサル、読み取り、および/または書き込みによってエラーが発生します。

表7）ONTAPでKerberos NFSエクスポートにアクセスする際の問題の特定と解決

問題	エラーの表示方法	解決手順
マウントをトラバースしようとしたときにアクセス/権限が拒否されました	コマンドライン出力	• ONTAPのイベントログ（`event log show`）で、`krb-unix` NFSサービスプリンシパルのネームマッピングに関するエラーを確認します。エラーが発生した場合は、問題のローカルUNIXユーザまたはネームマッピングルールを作成して、`nfs/name.realm.com` SPNを解決します。 • `export-policy check-access` コマンドを使用して、クライアントがkrb5を介してエクスポートに対して読み取りおよび書き込みを許可されているかどうかを確認します。 • mountコマンドを実行して、Kerberos経由で実際にマウントされたことを確認します。

問題	エラーの表示方法	解決手順
		• エクスポートポリシーとルールで、krb5による `ro rw` ルールとルールへのアクセスが許可されていることを確認します。 • `kinit` Kerberos TGTを生成するためにユーザとしてログインしたことを確認します。 • `klist -e` Kerberosチケットの有効期限が切れていないことを確認するために使用します。 • rootユーザの場合は、ONTAPイベントログでrootユーザの認証を試行しているユーザを確認します。 • `vserver security file-directory show` エクスポートに対するファイルレベルの権限を確認するために使用します。 • ボリューム/ qtreeのセキュリティ形式がNTFSの場合は、アクセスを試行しているUNIXユーザに有効なUNIXとWindowsのネームマッピングが設定されていることを確認します。
エクスポートの読み取りまたは書き込み時に問題が発生します。	CLI出力	• `vserver security file-directory show` エクスポートに対するファイルレベルの権限を確認するために使用します。 • NFSv4.xを使用している場合は、NFSv4.xが適切に設定されていることを確認します（TR-4067を参照）。 • `chown` またはを使用しようとしたときに[操作は許可されていません]と表示された場合は `chmod`、フォルダに対する権限とエクスポートポリシールールの設定を確認してください。

注： 表7に記載されていないその他のNFSの一般的な問題については、TR-4067を参照してください。

NFS Kerberosに関連するONTAPの一般的なイベントログエラー

場合によっては、ONTAPでイベントログを表示することで、Kerberosアクセスとマウントで発生する問題を切り分けることができます。表8 に、イベントログのフィルタリングに使用できるエラーのリストと、エラーの一般的な原因を示します。

CLIでは、これらのエラーの詳細な説明をコマンドで確認できます `event route show - messagename -instance`。

表8）ONTAPの一般的なイベントログエラー

EMSイベント	一般的な原因
secd.kerberos.clockskew secd.kerberos.lookupFailed secd.curberos.noAuthdata secd.kerberos.preauth secd.kerberos.tkt期限切れ secd.kerberos.tktnyv	ほとんどの場合、これらのエラーはSMB / CIFSサーバでのKerberosに関連しています。
secd.nfsAuth.noNameMap	このエラーは、ネームマッピング問題に関連しています。NFS Kerberosでは、通常、クライアントSPN（host $@ domain.comなど）またはユーザSPN（user@domain.comなど）に対するkrb-UNIXネームマッピングが使用されます。エラーを確認し、該当するネームマッピングを追加します。LDAPなどの外部ネームサービスを使用している場合は、LDAPが正常に機能していること、およびONTAPからのLDAPクエリが機能していることを確認します。
secd.nfsAuth.problem	このエラーは、NFS Kerberosではさまざまな理由で発生します。一般的に、これには、次のようなKerberos固有のエラーが伴います。

EMSイベント	一般的な原因
	• サポートされない暗号化タイプ • ネームマッピングエラー • 復号化の整合性チェック 復号化整合性チェックエラーはかなり一般的であり、パケットトレースやクライアントログなど、さらにトラブルシューティングを行う必要があります。通常、このエラーは、クライアントが使用するチケットがONTAPから適切なNFSサービスクレデンシャルを取得できない場合に発生します。問題を解決するには、クライアントのKerberosサービスを再起動するか、SVMでKerberos設定を再作成します。
エクスポート。*	エクスポート*エラーを確認し、設定ミスの可能性がないか調査する必要があります。NFS Kerberosでは引き続きNFSと同じ設定が使用されます。マウントを機能させるには、クライアントがNFSエクスポートにアクセスできる必要があります。
nfs.krb.lif.disabled	このエラーは、Kerberosクレデンシャルが誤ってSVM間で共有された場合にのみトリガーされるため、かなりまれです。この場合、KerberosがデータLIFとして無効になるため、クライアントからのアクセスが失敗します。Kerberosを再度有効にすると、問題が解決されます。

Kerberos keytabのトラブルシューティング

Kerberos keytabが正しく設定されているかどうかをトラブルシューティングする際には、次の点を考慮する必要があります。

- SPNは正しく定義されていますか？
- KDCにプリンシパルを作成しましたか?
- 暗号化タイプは正しく、サポートされていますか。
- keytabは正しくインポートされていますか？
- keytabのバージョン番号は、すべてのクライアント、サーバ、KDCで同じですか。

これらの問題を除外するために、keytabの機能を確認するためのトラブルシューティングのヒントがいくつかあります。

イベント ログ

イベントログを確認します。keytabファイルが問題の場合、暗号化タイプまたは整合性チェックに関するエラーが表示されることがあります。イベントログに表示されるエラーの詳細については、「NFS Kerberosに関連するONTAPの一般的なイベントログエラー」を参照してください。」と入力します

キーバージョン番号の確認

クライアントとONTAP SVMのキーのバージョン番号（kvno）を確認します。

クライアント/Linux KDCでkvnoを確認するには、次のコマンドを実行します。

```
# kinit username
# kvno nfs/hostname.domain.com@REALM.COM
```

ONTAPでは、kvnoはKerberosキーブロックとともに保存されます。これらは、インターフェイスでKerberosを有効にすると作成されます。keytabファイルには、暗号化タイプごとに作成されたキーブロックが表示されます。コマンドの `kerberos keyblocks show` 権限はdiagです。

注: キーブロックには作成、削除、変更の各オプションがあります。NetAppサポートから指示がない限り、これらのオプションは使用しないでください。

```
cluster::*> kerberos keyblocks show ?
  (vserver nfs kerberos keyblocks show)
  [ -instance | -fields <fieldname>, ... ]
```

```
  [[-service-type] {CIFS|NFS}]    *Types of Service CIFS|NFS
  [ -vserver <vserver> ]          *Vserver ID
  [[-lif] <integer>]              *Logical Interface ID
  [[-key-version] <integer>]      *Key Version Number
  [[-encryption-type] <integer>] *Encryption Type
  [ -timestamp <integer> ]        *Time Stamp
  [ -keyblock <Hex String> ]      *Keyblock
  [ -spn <text> ]                 *Service principal name
  [ -machine-account <text> ]     *Machine Account Name
```

クライアントに表示されるkvnoが、ONTAPのキーブロックに表示されるものと一致していることを確認する必要があります。kvnoが一致しないと、Kerberos認証が機能しない可能性があります（Windows KDCには必ずしもこの問題があるとは限りません）。これは、CIFS / SMBマシンアカウントをNFS Kerberosにも使用できない理由の1つです。CIFS / SMBではマシンのパスワードが常に更新され、keytab情報が増加します。パケットトレースは、これが問題のルート原因であるかどうかを確認できます。

次の例では、NFSサービスプリンシパルのkvnoが一致することを確認できます。

```
# kinit administrator
Password for administrator@NTAP.LOCAL:
[root@centos7 home]# kvno nfs/demo.ntap.local@NTAP.LOCAL
nfs/demo.ntap.local@NTAP.LOCAL: kvno = 1

cluster::*> kerberos keyblocks show -service-type NFS -vserver DEMO
  (vserver nfs kerberos keyblocks show)
Service          Interface Key     Encryption
Type     Vserver ID        Version Type        Timestamp SPN Keyblock
-------- ------- --------- ------- ----------- --------- ---------------
NFS      DEMO    1033      1       3           1588007407
                                                       nfs/demo.ntap.local@NTA .LOCAL
                                                           a2a883ec540168f8
NFS      DEMO    1033      1       17          1588007407
                                                       nfs/demo.ntap.local@NTA .LOCAL
                                                           70ec681fdcf8183a893 55901ff0385a
NFS      DEMO    1033      1       18          1588007407
                                                       nfs/demo.ntap.local@NTAP.LOCAL


4735f91db892917070c6e2ca1b1f4fdfa3d7dda0ace23226a3d28c82a37884a4
NFS      DEMO    1033      1       23          1588007407
                                                       nfs/demo.ntap.local@NTAP.LOCAL
                                                           701160a748ac404993b5fe4f0f388218
```

Kerberosコンテキストキャッシュの表示

「ユーザによる初期NFSマウントアクセス」セクションで説明したように、クライアントがKerberosチケットを使用してONTAPのKerberosマウントにアクセスするタイミングを確認できます。これらのキャッシュエントリは、アクセスの問題が発生しているときにKerberos認証が適切に機能しているかどうかを判断するのに役立ちます。

Kerberosのパケットトレースの収集と表示

Kerberosの問題をトラブルシューティングする最も効果的な方法の1つは、パケットキャプチャです。小規模な環境では、Kerberosの障害時にNFSクライアントでトレースを収集するだけで十分です。大規模な環境では、クライアント、KDC、およびONTAPクラスタでトレースの収集が必要になる場合があります。KDCが複数ある場合は、最初はONTAPクラスタとクライアントだけに焦点を当てなければならないことがあります。

パケットトレースの収集

ONTAPでのパケットトレースの収集については、次のNetAppナレッジベースの記事を参照してください。

- ONTAP 9.2+システムでパケットトレース（tcpdump）をキャプチャする方法
- ONTAP 9.1以下のシステムでpkttを使用してローリングパケットトレースを収集する方法

NFSクライアントでは、を使用して tcpdump 別のウィンドウでパケットトレースを収集できます。次のコマンドで十分です。

```
# tcpdump -s 0 -i interfacename -w /filename.trc
```

メモ： トレースファイルのサイズを制限するエラーのみをキャプチャしてみてください。

Windows KDCの場合は、Wiresharkまたは任意のパケットキャプチャ方法を使用できます。場合によっては、Windows KDC上のネットワークトレースが許可されないことがあります。これは、環境でドメインコントローラへのインストールが許可されているアプリケーションのセキュリティ制限のためです。

パケットトレースの表示

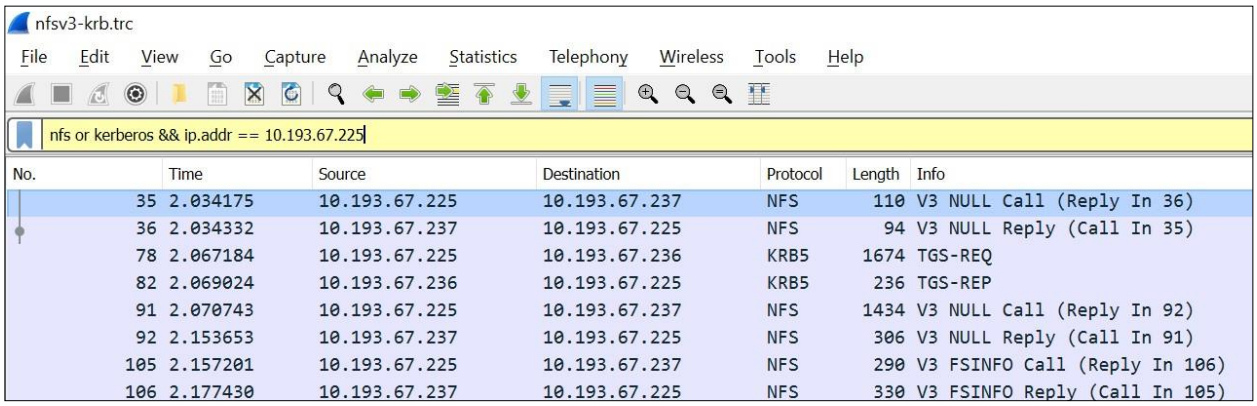
パケットトレースアプリケーションはすべて機能しますが、この例ではWiresharkを使用してKerberosパケットトレースを表示しています。パケットトレースには、提供されたフィルタを利用できるように、必要な詳細情報が含まれています。

Kerberosでは、通常、次のWiresharkフィルタを1つまたは複数使用する必要があります。

- Kerberos
- IPアドレス
- DNS
- NFS
- マウント（NFSv3のみ）

トレース内の上記の1つまたは複数の値でフィルタリングできます。たとえば、10.193.67.225 クライアントからNFSパケットとKerberosパケットだけを除外するには、図8に示すWiresharkのフィルタを使用します。

図8）Wiresharkフィルタの例



Kerberosトレースでは、使用されているKerberos SPN（NFSクライアント、ONTAP NFSサービス、ユーザSPN）、使用されている暗号化タイプ、kvno、GSSペイロードが適切に送受信されているかどうかなど、大量の情報を収集できます。また、パケットリストにKerberosエラーが表示されるため、解決のための適切な方向に進むことができます。

A 図9に示すように、SSSD LDAPクライアントは、Kerberosを使用してLDAPサーバにバインドしようとするときに存在しないSPNを使用しています。トレースには、これらのパケットが表示されます。

注: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN クライアントが要求されたSPNを見つけられなかったことを示すエラーが表示されます。

図9）Kerberosパケットキャプチャ-パケットリスト

```
294 12.438849    10.193.67.225    10.193.67.236    KRB5    1657 TGS-REQ
300 12.439183    10.193.67.225    10.193.67.236    KRB5    1671 TGS-REQ
302 12.449098    10.193.67.236    10.193.67.225    KRB5     377 KRB Error: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
318 12.450702    10.193.67.225    10.193.67.236    KRB5    1657 TGS-REQ
320 12.458210    10.193.67.236    10.193.67.225    KRB5     377 KRB Error: KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN
```

図10 に示すTGS-REQパケットは、要求されているSPN、チケットの有効期間、暗号化タイプなどを示しています。

図10）TGS-REQの詳細-パケットトレース

```
▼ sname
     name-type: kRB5-NT-SRV-HST (3)
  ▼ sname-string: 2 items
       SNameString: ldap
       SNameString: ntap.local
  till: 2020-10-30 15:12:30 (UTC)
  nonce: 1604067150
▼ etype: 2 items
     ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
     ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
```

この情報があれば、SPNを可能な問題として確認し、クライアント設定を調査することができます。上記の例では、問題はSSSDがLDAPサーバにバインドするように設定されていました。発生する可能性のあるKerberosパケットのタイプについては、「付録A：Kerberos暗号化タイプ」を参照してください。

NetAppサポートに連絡する前に収集する情報

NFS Kerberosの問題が発生して独自に解決できない場合は、NetAppのサポートをご利用ください。サポートケースをオープンした場合、テクニカルサポートエンジニアは問題のトラブルシューティングを行うためにデータを収集する必要があります。このプロセスを迅速に進めるには、以下に示す回答の質問と、サポートケースを迅速に解決するために役立つ情報を参照してください。このリストはすべてを網羅しているわけではありません。テクニカルサポートエンジニアからさらにデータを要求される場合がありますが、ここから始めましょう。

- 問題が発生した日時
- どのKDCサーバタイプとOSを使用していますか？
- どのKerberosクライアントを使用していますか？
- 影響を受けるユーザまたはグループ
- 問題はまだ発生していますか？間欠的ですか？
- テクニカルサポートエンジニアがサーバからの追加情報を必要とした場合に、KDC管理者やDNS管理者をコールに参加させることはできますか。
- 問題はすべてのノードで実行されますか。いくつかのノード？特定のIPアドレスを使用しているかどうか
- ONTAPからネットワーク経由でKDCサーバとDNSサーバにアクセスできますか。
- `-type all（autosupport invoke * -type all）`を使用して新しいAutoSupportレポートを生成します。このコマンドは、Kerberos設定、DNS、ネットワーク、イベントログなどに関する情報を収集します。
- クライアント、KDC、およびONTAPシステムからの問題中のパケットトレース。

ONTAPでのパケットトレースの収集については、次のNetAppナレッジベースの記事を参照してください。

- ONTAP 9.2+システムでパケットトレース（tcpdump）をキャプチャする方法

- ONTAP 9.1以下のシステムでpkttを使用してローリングパケットトレースを収集する方法

詳細な設定手順

このレポートの以前のセクションを整理し、わかりやすく読みやすいドキュメントを提供するために、ここまでの主な設定手順のみを紹介しました。このセクションでは、より複雑な設定手順をいくつか紹介します。

Active DirectoryでのNFS Kerberosマシンアカウントの名前変更

「データLIFでKerberosを有効にする」セクションで説明したマシンアカウント名のnfs-fqdn形式が、Active Directory環境で推奨される名前でない場合があります。たとえば、組織によってはマシンアカウントに厳密な命名規則を要求する場合があります。ONTAP 9.5以降では、Kerberosの設定時に `kerberos interface enable` コマンドオプションを使用してマシンアカウント名を指定できます `-machine-account`。最初の作成時にマシンアカウントの名前を指定しなかった場合、または指定できなかった場合は、後からクライアントの再マウントやチケットの再発行などを行わずに名前を変更できます。

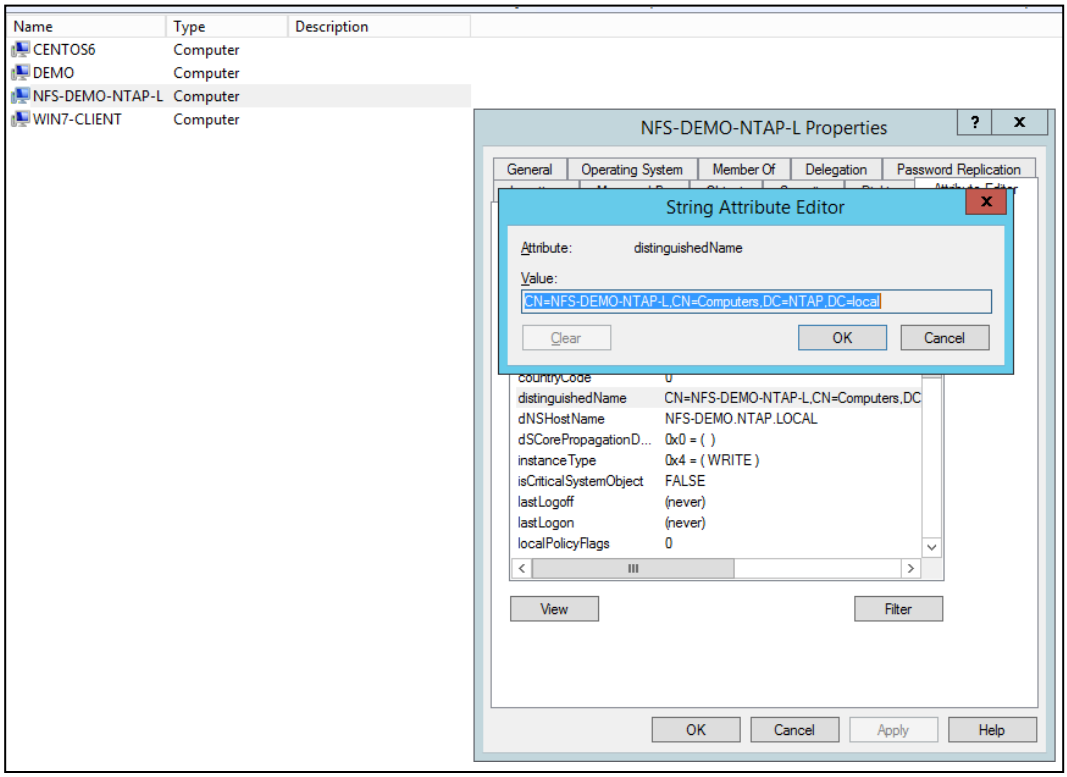
マシンアカウントの表示名はKerberos処理にとって重要ではないため、作成後に簡単に名前を変更できます。クライアントとKDC間のKerberosのやり取りで重要なことは次のとおりです。

- マシンアカウントのSPN
- DNSホストメイ
- keytabファイル
- `sAMAccountName` マシンアカウント

Active Directoryでは、表示名を（GUIで強調表示して変更して）変更しても、上記の項目には影響しません。Active Directoryでは、GUIを使用した名前の変更がデフォルトで許可されていない場合があります。代わりに、PowerShellを使用する必要があります。次のセクションでは、マシンアカウント名の変更について説明します。

Active Directoryでマシンアカウントの名前を変更するには、次の手順を実行します。

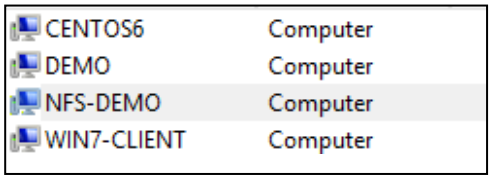
1. まず、名前を変更するオブジェクトのマシンアカウントをActive Directoryで探します。AD Users and Computersでオブジェクトを開き、DN値を見つけます（この手順ではAdvanced Featuresを有効にする必要があります）。PowerShellコマンドにはこの値が必要です。

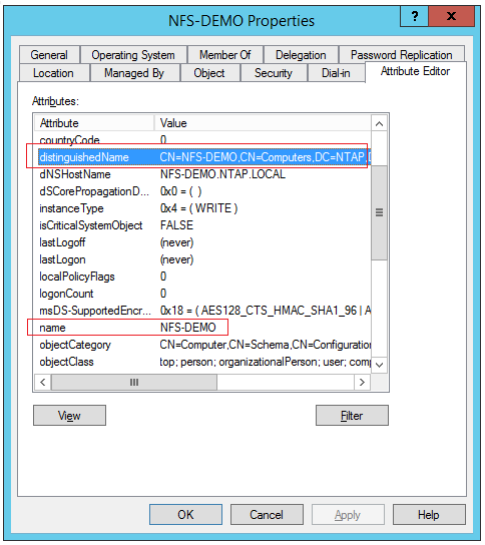


2. ドメイン管理者（またはActive Directoryの名前変更権限を持つ別のユーザ）としてPowerShellを開き、次のコマンドを実行して、角かっこ内のオブジェクトを目的の値に置き換えます。

```
PS C:\> Rename-ADObject -Identity ["CN=NAME,CN=Computers,DC=DOMAIN,DC=local"] -NewName [NEW-NAME]
```

3. このコマンドは、コンピュータオブジェクトのDNと名前の値、およびADユーザとコンピュータの表示名を変更します。





4. dNSHostNameの属性を変更し、マシンアカウント名のFQDNと短縮名を持つ新しいSPNを追加します。この手順では、PowerShellコマンドSet-ADComputerを使用します。

```
PS C:\> Set-ADComputer KERBEROS -DNSHostName demo.ntap.local -ServicePrincipalNames
@{Replace="nfs/KERBEROS", "HOST/KERBEROS", "HOST/nfs-demo-ntap-1.ntap.local", "nfs/nfs-demo-ntap-
1.ntap.local", "nfs/demo.ntap.local"}
```

5. Kerberosアクセスをテストします。データLIFで使用されるNFS SPNが変更されていないため、すべて問題なく機能します。

```
[root@centos6 /]# mount home
[root@centos6 /]# mount | grep home
demo:/home on /home type nfs (rw,hard,intr,sec=krb5,vers=4,addr=x.x.x.b,clientaddr=x.x.x.w)
[root@centos6 /]# su student2
sh-4.1$ klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_1302)
sh-4.1$ kinit
Password for student2@NTAP.LOCAL:
sh-4.1$ klist -e
Ticket cache: FILE:/tmp/krb5cc_1302
Default principal: student2@NTAP.LOCAL

Valid starting     Expires            Service principal
02/09/17 10:06:31 02/09/17 20:08:24 krbtgt/NTAP.LOCAL@NTAP.LOCAL
renew until 02/10/17 10:06:31, Etype(skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-sha1-96
sh-4.1$ cd ~
sh-4.1$ pwd
/home/student2
sh-4.1$ klist -e
Ticket cache: FILE:/tmp/krb5cc_1302
Default principal: student2@NTAP.LOCAL

Valid starting     Expires            Service principal
02/09/17 10:06:31 02/09/17 20:08:24 krbtgt/NTAP.LOCAL@NTAP.LOCAL
        renew until 02/10/17 10:06:31, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
02/09/17 10:08:35 02/09/17 20:08:24 nfs/demo.ntap.local@NTAP.LOCAL
        renew until 02/10/17 10:06:31, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

NET ADS JoinでKerberosを使用するようにNFSクライアントを設定する

このセクションでは、を使用してドメインに参加したNFSクライアントがKerberosを使用するように設定する例を示し `net ads join`ます。Sambaパッケージと Winbindパッケージを使用して、net adsコマンドを見つけることができます。

この例で使用したNFSクライアントはRHEL / CentOS 7.2です。`net ads` コマンドは、ドメインに参加するために使用します。ドメインはWindows Server 2012 R2 Active Directoryです。ローカルUNIXユーザはネームマッピングに使用されます。

でKerberosを使用するようにNFSクライアントを設定するには `net ads join`、次の手順を実行します。

1. 必要なパッケージをインストールします。

```
# yum install -y samba samba-winbind samba-winbind-clients ntp authconfig-gtk*
```

2. クライアントとドメインの時刻をチェックして、5分以内であることを確認します。この手順では、クライアントがドメインコントローラを検出できることも確認します。

```
# net time -S CORE-TME.NETAPP.COM
Mon Jul 11 16:08:00 2016

# date
Mon Jul 11 16:08:46 EDT 2016
```

3. NTPを設定します。必要に応じて、時間を手動で同期します。

```
# net time set -S CORE-TME.NETAPP.COM
```

4. クライアントがActive Directoryと同じDNSに存在し、 `nslookup` クライアントとドメインコントローラで機能することを確認します。

```
# nslookup centos7
Server:         x.x.x.c
Address:        x.x.x.c#53

Name:   centos7.core-tme.netapp.com
Address: x.x.x.x
Name:   centos7.core-tme.netapp.com
Address: 192.168.122.1

# nslookup core-tme.netapp.com
Server:         x.x.x.c
Address:        x.x.x.c#53

Name:   core-tme.netapp.com
Address: x.x.x.d
Name:   core-tme.netapp.com
Address: x.x.x.c
```

5. `/etc/krb5.conf` Active Directoryドメインを反映するようにファイルを変更します。

```
[logging]
 default =  FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = CORE-TME.NETAPP.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# EXAMPLE.COM = {
# kdc = kerberos.example.com
# admin_server = kerberos.example.com
# }
CORE-TME.NETAPP.COM = {
        kdc = dc1.core-tme.netapp.com:88
        admin_Server = dc1.core-tme.netapp.com:749
        default_domain = core-tme.netapp.com
```

```
}


[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
.core-tme.netapp.com = CORE-TME.NETAPP.COM
core-tme.netapp.com = CORE-TME.NETAPP.COM
```

6. `/etc/samba/smb.conf` ドメイン情報を使用してを設定します。

```
[global]

   workgroup = CORE-TME
   password server = stme-infra02.core-tme.netapp.com:88
   realm = CORE-TME.NETAPP.COM
   security = ads
   idmap uid = 16777216-33554431
   idmap gid = 16777216-33554431
   template shell =  /bin/bash
   winbind use default domain = false
   winbind offline logon = true

    log file = /var/log/samba/log.%m
    max log size = 50

    passdb backend = tdbsam

    load printers = yes
    cups options = raw

[homes]
    comment = Home Directories
    browseable = no
    writable = yes

[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
    guest ok = no
    writable = no
    printable = yes
```

7. SMBサービスとrpcgssdサービスを再起動します。

```
# service smb restart
# service rpcgssd restart
```

8. 管理者のKerberosチケットを取得します。

```
# kinit administrator
Password for administrator@CORE-TME.NETAPP.COM:
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
07/12/2016 11:28:54 07/12/2016 21:28:54 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/19/2016 11:28:49
```

9. ドメインに参加します。

```
# net ads join -U administrator
Enter administrator's password:
Using short domain name -- CORE-TME
Joined 'CENTOS7' to dns domain 'core-tme.netapp.com'
```

注: 通常のWindowsドメインルールがすべて適用されます。時間のずれは5分以内で、ユーザーアカウントにはコンピュータオブジェクトをドメインに追加する権限があり、DNSはドメインコントローラを見つけることができます。

10. keytabファイルを作成します。

```
# net ads keytab create -U administrator

Warning: "kerberos method" must be set to a keytab method to use keytab functions.
Enter administrator's password:
```

11. keytabファイルを確認します。

    を使用してActive Directoryにマシンアカウントを追加する `net ads keytab`と、次のSPNが `krb5.keytab` ファイルに自動的に追加されます。

```
# ktutil
ktutil: rkt /etc/krb5.keytab
ktutil: list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    3 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   2    3 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   3    3 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   4    3 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   5    3 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   6    3         host/centos7@CORE-TME.NETAPP.COM
   7    3         host/centos7@CORE-TME.NETAPP.COM
   8    3         host/centos7@CORE-TME.NETAPP.COM
   9    3         host/centos7@CORE-TME.NETAPP.COM
  10    3         host/centos7@CORE-TME.NETAPP.COM
  11    3 root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
  12    3 root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
  13    3 root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
  14    3 root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
  15    3 root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
  16    3         root/centos7@CORE-TME.NETAPP.COM
  17    3         root/centos7@CORE-TME.NETAPP.COM
  18    3         root/centos7@CORE-TME.NETAPP.COM
  19    3         root/centos7@CORE-TME.NETAPP.COM
  20    3         root/centos7@CORE-TME.NETAPP.COM
  21    3             CENTOS7$@CORE-TME.NETAPP.COM
  22    3             CENTOS7$@CORE-TME.NETAPP.COM
  23    3             CENTOS7$@CORE-TME.NETAPP.COM
  24    3             CENTOS7$@CORE-TME.NETAPP.COM
  25    3             CENTOS7$@CORE-TME.NETAPP.COM
```

マシンアカウントに他のSPNは必要ありません。特に、 `root/` keytabには用のSPNがあります。`root` SVMにはデフォルトでという名前のUNIXユーザが存在するため、別のマッピングが必要な場合を除き、クライアントのネームマッピングを考慮する必要はありません。

別のマッピングが必要な場合は、`machine$` SVM上のローカル（ネームマッピングルールまたはUNIXユーザ）またはActive Directoryオブジェクトに対するKRBからUNIXへのネームマッピングが存在している必要があります。（LDAPのuidNumber/gidNumber属性の形式）。

この問題の解決策をテストする最も簡単な方法は `unix-user`、ローカルを使用することです。

```
::*> unix-user create -vserver parisi -user CENTOS7$ -id 10001 -primary-gid 1
::*> unix-user show -vserver parisi -user CENTOS7$
         Vserver: parisi
       User Name: CENTOS7$
         User ID: 10001
Primary Group ID: 1
User's Full Name:
```

メモ： ローカルUNIXユーザを使用した解決をテストしたあと、長期的な解決策でネームマッピングルールを作成します。「UNIXユーザまたはネームマッピングルールを作成してNFSクライアントプリンシパルをマッピングする」セクションを参照してください。

12. `krb-unix` 必要に応じて、ルートSPNまたはマシンアカウントSPNのマッピングをテストします。

```
::> set diag
::*> diag secd name-mapping show -node node03 -vserver parisi -direction krb-unix -name
CENTOS7$@CORE-TME.NETAPP.COM
```

```
CENTOS7$@CORE-TME.NETAPP.COM maps to CENTOS7$

::*> diag secd name-mapping show -node node03 -vserver parisi -direction krb-unix -name
root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
root/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM maps to root
```

13. 次のサービスが実行されており、ブート時に有効になっていることを確認します。

```
systemctl start ntpd
systemctl enable ntpd
systemctl start smb
systemctl enable smb
systemctl start winbind
systemctl enable winbind
systemctl start sssd
systemctl enable sssd
```

14. ドメイン接続をテストします。

```
# net ads info
LDAP server: x.x.x.c
LDAP server name: stme-infra02.core-tme.netapp.com
Realm: CORE-TME.NETAPP.COM
Bind Path: dc=CORE-TME,dc=NETAPP,dc=COM
LDAP port: 389
Server time: Tue, 12 Jul 2016 11:33:29 EDT
KDC server: x.x.x.c
Server time offset: 0

# wbinfo -t
checking the trust secret for domain CORE-TME via RPC calls succeeded
```

15. `unix-user` サービスアカウント（`nfs/fqdn@REALM`）が認証できるように、NFSまたは同等のネームマッピングが設定されていることを確認します。

```
::*> unix-user create -vserver parisi -user nfs -id 10002 -primary-gid 1
::*> unix-user show -vserver parisi -user nfs
         Vserver: parisi
       User Name: nfs
         User ID: 10002
Primary Group ID: 1
User's Full Name:
```

16. NFSクライアントで、SSSD（またはLDAPクライアントの同等機能）が設定されていることを確認します。詳細については、TR-4835を参照してください。または、`/etc/passwd` SVMのとでローカルUNIXユーザを使用することもできます。

    LDAPをテストするには、次のコマンドを実行します。

```
# id ldapuser

# getent passwd ldapuser
```

17. Kerberosを使用してSVMデータインターフェイスをマウントしてみます。SVMで次の項目を作成して設定しておく必要があります。
    - Kerberos Realm
    - Kerberosインターフェイス
    - DNSサーバ内のDNS A/AAAAレコード（フォワードおよびリバース）
    - Kerberosで許可されるエンコーディングタイプ
    - Kerberosを許可するNFSエクスポートおよび親ディレクトリのエクスポートポリシールールについては、次のマウント例を参照してください。

```
[root@centos7 /]# mount -o sec=krb5 parisi-nfs:/nfs /kerberos
[root@centos7 /]#
```

18. `su` 別のユーザーとしておよび `kinit`。`cd` マウントに移動し、NFSサービスチケットを確認します。

```
[root@centos7 /]# su test@CORE-TME.NETAPP.COM
```

```
[test@core-tme.netapp.com@centos7 /]$ kinit test@CORE-TME.NETAPP.COM
Password for test@CORE-TME.NETAPP.COM:
[test@core-tme.netapp.com@centos7 /]$ klist
Ticket cache: KEYRING:persistent:106003697:106003697
Default principal: test@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
06/29/2016 16:38:26 06/30/2016 02:38:26 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21

[test@core-tme.netapp.com@centos7 /]$ mount | grep kerberos
parisi-nfs:/nfs on /kerberos type nfs4
(rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=
2,sec=krb5,clientaddr=x.x.x.x,local_lock=none,addr=x.x.x.b)

[test@core-tme.netapp.com@centos7 /]$ cd /kerberos

[test@core-tme.netapp.com@centos7 kerberos]$ klist -e
Ticket cache: KEYRING:persistent:106003697:106003697
Default principal: test@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
06/29/2016 16:39:43 06/30/2016 02:38:26 nfs/parisi-nfs.core-tme.netapp.com@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
06/29/2016 16:38:26 06/30/2016 02:38:26 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

KerberosとRealm Joinを使用するようにNFSクライアントを設定する

このセクションでは、ドメインに参加したNFSクライアントがKerberosを使用するように設定する方法の例を示します。この例で使用するNFSクライアントはRHEL / CentOS 7.2です。`realm` コマンドを使用して、ドメインに参加します。これらの手順を実行するために必要なパッケージは、アイデンティティドメインの検出と参加に関するRed Hatの公式ドキュメントに記載されています。ドメインはWindows Server 2012 R2 Active Directoryです。ネームマッピングにはローカルUNIXユーザを使用します。

でKerberosを使用するようにNFSクライアントを設定するには `realm join`、次の手順を実行します。

1. 必要なパッケージをインストールします。

```
yum -y install realmd sssd oddjob oddjob-mkhomedir adcli samba-common krb5-workstation ntp
```

2. NFSクライアントのDNSがActive Directoryドメインに設定されていること、およびLinuxクライアントのDNSにA/AAAAレコードが存在することを確認します。DNSルックアップをテストします。

```
[root@centos7 /]# cat /etc/resolv.conf
# Generated by NetworkManager
search core-tme.netapp.com
nameserver x.x.x.c

[root@centos7 /]# nslookup centos7
Server:         x.x.x.c
Address:        x.x.x.c#53

Name:   centos7.core-tme.netapp.com
Address: x.x.x.x
```

3. すべてのファイアウォールルールでActive Directory接続、LDAP、Kerberosなどが許可されていることを確認します。

4. Active Directoryレルムを検出します。

```
# realm discover core-tme.netapp.com
core-tme.netapp.com
  type: kerberos
  realm-name: CORE-TME.NETAPP.COM
  domain-name: core-tme.netapp.com
  configured: no
  server-software: active-directory
```

```
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

5. ドメインに参加します。

```
[root@centos7 ~]# realm join CORE-TME.NETAPP.COM
Password for Administrator:
```

注: すべての通常のWindowsドメインルールが適用されます。タイムスキューは5分以内で、ユーザアカウントにはコンピュータオブジェクトをドメインに追加する権限があり、DNSはドメインコントローラを見つけることができます。`realm join` SSSDをベースレベルに自動的に設定し、Kerberos keytabファイルを設定します。

6. 名前検索を実行してドメインへの接続を確認します（このアクションではLDAP接続にSSSDを使用します）。

```
[root@centos7 ~]# id CORE-TME\\test
uid=106003697(test@core-tme.netapp.com) gid=106000513(domain users@core-tme.netapp.com)
groups=106000513(domain users@core-tme.netapp.com)
```

注： 上記のユーザは、デフォルトでSSSDのアルゴリズムに基づいてUIDとGIDの数値を作成し、SIDに基づいてユーザとグループのIDを近似します。従来のUNIXユーザ属性が必要な場合は、TR-4835の説明に従ってSSSDを設定してください。

7. を実行し `kinit` てユーザのKerberosをテストします。

```
[root@centos7 ~]# kinit test@CORE-TME.NETAPP.COM
Password for test@CORE-TME.NETAPP.COM:

[root@centos7 ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: test@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
06/29/2016 15:23:54 06/30/2016 01:23:54 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/06/2016 15:23:50
```

注: オプションとして、 `/etc/krb5.conf` レルム情報を使用してを構成し、`kinit` 要求にレルムを追加する必要がないようにすることができます。

次の例を参照してください。

```
[root@centos7 /]# cat /etc/krb5.conf
[logging]
 default =  FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = true
 dns_lookup_kdc = true
 default_tkt_enctypes = aes256-cts-hmac-sha1-96
 default_tgs_enctypes = aes256-cts-hmac-sha1-96
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = CORE-TME.NETAPP.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# EXAMPLE.COM = {
# kdc = kerberos.example.com
# admin_server = kerberos.example.com
# }
CORE-TME.NETAPP.COM = {
```

```
        kdc = dc1.core-tme.netapp.com:88
        admin_Server = dc1.core-tme.netapp.com:749
        default_domain = core-tme.netapp.com
}


[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
.core-tme.netapp.com = CORE-TME.NETAPP.COM
core-tme.netapp.com = CORE-TME.NETAPP.COM

[root@centos7 ~]# kinit test
Password for test@CORE-TME.NETAPP.COM:
```

krb5.confファイルが、特定のエンタイプのみを許可するように設定されていること、またはNFSクライアントのドメイン内のマシンアカウントが目的のエンタイプのみを許可するように設定されていることを確認してください。NetApp ONTAPはRC4-HMACをサポートしていないため、RC4-HMACを許可しないようにしてください。

RC4-HMACを使用している場合の障害の例を次に示します。

```
6/29/2016 16:09:56 node03
WARNING       secd.nfsAuth.problem: vserver (parisi) General NFS authorization problem. Error:
RPC accept GSS token procedure failed
  [ 0 ms] Using the NFS service credential for logical interface 1035 (SPN='nfs/parisi-nfs.core-
tme.netapp.com@CORE-TME.NETAPP.COM') from cache.
**[     1] FAILURE: Failed to accept the context: Unspecified GSS failure. Minor code may
provide more information (minor: Encryption type ArcFour with HMAC/md5 not permitted).
```

8. を使用してActive Directoryにマシンアカウントを追加する `realm join`と、次のSPNが `krb5.keytab` ファイルに自動的に追加されます。

```
[root@centos7 ~]# ktutil
ktutil: rkt /etc/krb5.keytab
ktutil: list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------------------------------------------------------
   1    2 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   2    2 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   3    2 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   4    2 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   5    2 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM
   6    2         host/centos7@CORE-TME.NETAPP.COM
   7    2         host/centos7@CORE-TME.NETAPP.COM
   8    2         host/centos7@CORE-TME.NETAPP.COM
   9    2         host/centos7@CORE-TME.NETAPP.COM
  10    2         host/centos7@CORE-TME.NETAPP.COM
  11    2             CENTOS7$@CORE-TME.NETAPP.COM
  12    2             CENTOS7$@CORE-TME.NETAPP.COM
  13    2             CENTOS7$@CORE-TME.NETAPP.COM
  14    2             CENTOS7$@CORE-TME.NETAPP.COM
  15    2             CENTOS7$@CORE-TME.NETAPP.COM

[root@centos7 /]# klist -kte
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------------------------------------------------------
   2 06/29/2016 15:16:49 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM (des-cbc-crc)
   2 06/29/2016 15:16:49 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM (des-cbc-md5)
   2 06/29/2016 15:16:50 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM (aes128-cts-hmac-
sha1-96)
   2 06/29/2016 15:16:50 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM (aes256-cts-hmac-
sha1-96)
   2 06/29/2016 15:16:50 host/centos7.core-tme.netapp.com@CORE-TME.NETAPP.COM (arcfour-hmac)
   2 06/29/2016 15:16:50 host/centos7@CORE-TME.NETAPP.COM (des-cbc-crc)
   2 06/29/2016 15:16:50 host/centos7@CORE-TME.NETAPP.COM (des-cbc-md5)
   2 06/29/2016 15:16:50 host/centos7@CORE-TME.NETAPP.COM (aes128-cts-hmac-sha1-96)
   2 06/29/2016 15:16:51 host/centos7@CORE-TME.NETAPP.COM (aes256-cts-hmac-sha1-96)
   2 06/29/2016 15:16:51 host/centos7@CORE-TME.NETAPP.COM (arcfour-hmac)
   2 06/29/2016 15:16:51 CENTOS7$@CORE-TME.NETAPP.COM (des-cbc-crc)
   2 06/29/2016 15:16:51 CENTOS7$@CORE-TME.NETAPP.COM (des-cbc-md5)
```

```
   2 06/29/2016 15:16:51 CENTOS7$@CORE-TME.NETAPP.COM (aes128-cts-hmac-sha1-96)
   2 06/29/2016 15:16:52 CENTOS7$@CORE-TME.NETAPP.COM (aes256-cts-hmac-sha1-96)
   2 06/29/2016 15:16:52 CENTOS7$@CORE-TME.NETAPP.COM (arcfour-hmac)
```

マシンアカウントに他のSPNは必要ありません。クライアントは、マシンアカウントプリンシパル(machine$@REALM.COM)を使用してチケットを取得しようとします。

したがって、KRBからUNIXへのネームマッピングはmachine$、SVM上のローカル（ネームマッピングルールまたはUNIXユーザ）またはActive Directoryオブジェクト（LDAPのuidNumber/gidNumber属性の形式）のいずれかで存在している必要があります。そうしないと、次のエラーでマウント要求が失敗します。

```
6/29/2016 16:28:52 node03
WARNING       secd.nfsAuth.problem: vserver (parisi) General NFS authorization problem. Error:
RPC accept GSS token procedure failed
  [ 0 ms] Using the NFS service credential for logical interface 1035 (SPN='nfs/parisi-nfs.core-
tme.netapp.com@CORE-TME.NETAPP.COM') from cache.
  [     1] GSS_S_COMPLETE: client = 'CENTOS7$@CORE-TME.NETAPP.COM'
  [     2] Extracted KG_USAGE_ACCEPTOR_SIGN Derived Key
  [     2] Extracted KG_USAGE_INITIATOR_SIGN Derived Key
  [     2] Exported lucid context
  [     5] Trying to map SPN 'CENTOS7$@CORE-TME.NETAPP.COM' to UNIX user 'CENTOS7$' using
implicit mapping
  [     6] Entry for user-name: CENTOS7$ not found in the current source: FILES. Ignoring and
trying next available source
  [     7] Failed to initiate Kerberos authentication. Trying NTLM.
  [    11] Successfully connected to x.x.x.c:389 using TCP
**[    91] FAILURE: User 'CENTOS7$' not found in UNIX authorization source LDAP.
  [    91] Entry for user-name: CENTOS7$ not found in the current source: LDAP. Entry for user-
name: CENTOS7$ not found in any of the available sources
  [    91] Unable to map SPN 'CENTOS7$@CORE-TME.NETAPP.COM'
  [    91] Unable to map Kerberos NFS user 'CENTOS7$@CORE-TME.NETAPP.COM' to appropriate UNIX
user
  [    91] Failed to accept the context: The routine completed successfully (minor: Unknown
error). Result = 6916
```

この問題を解決する最も簡単な方法は unix-user、ローカルを使用することです。

```
::*> unix-user create -vserver parisi -user CENTOS7$ -id 10001 -primary-gid 1
::*> unix-user show -vserver parisi -user CENTOS7$
         Vserver: parisi
       User Name: CENTOS7$
         User ID: 10001
Primary Group ID: 1
User's Full Name:
```

9. krb-unix マッピングをテストします。

```
::> set diag
::*> diag secd name-mapping show -node node03 -vserver parisi -direction krb-unix -name
CENTOS7$@CORE-TME.NETAPP.COM
CENTOS7$@CORE-TME.NETAPP.COM maps to CENTOS7$
```

10. unix-user サービスアカウント（nfs/fqdn@REALM）が認証できるように、NFSまたは同等のネームマッピングが設定されていることを確認します。

```
::*> unix-user create -vserver parisi -user nfs -id 10002 -primary-gid 1
::*> unix-user show -vserver parisi -user nfs
         Vserver: parisi
       User Name: nfs
         User ID: 10002
Primary Group ID: 1
User's Full Name:
```

11. Kerberosを使用してSVMデータインターフェイスをマウントしてみます。SVMで次の項目を作成して設定しておく必要があります。
    - Kerberos Realm
    - Kerberosインターフェイス

- DNSサーバ内のDNS A/AAAAレコード（フォワードおよびリバース）
- Kerberosで許可されるエンコーディングタイプ
- Kerberosを許可するNFSエクスポートおよび親ディレクトリのエクスポートポリシールールについては、次のマウント例を参照してください。

```
[root@centos7 /]# mount -o sec=krb5 parisi-nfs:/nfs /kerberos
[root@centos7 /]#
```

12. `su` 別のユーザーとしておよび `kinit`。`cd` マウントに移動し、NFSサービスチケットを確認します。

```
[root@centos7 /]# su test@CORE-TME.NETAPP.COM
[test@core-tme.netapp.com@centos7 /]$ kinit test@CORE-TME.NETAPP.COM
Password for test@CORE-TME.NETAPP.COM:
[test@core-tme.netapp.com@centos7 /]$ klist
Ticket cache: KEYRING:persistent:106003697:106003697
Default principal: test@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
06/29/2016 16:38:26 06/30/2016 02:38:26 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21

[test@core-tme.netapp.com@centos7 /]$ mount | grep kerberos
parisi-nfs:/nfs on /kerberos type nfs4
(rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=
2,sec=krb5,clientaddr=x.x.x.x,local_lock=none,addr=x.x.x.b)

[test@core-tme.netapp.com@centos7 /]$ cd /kerberos

[test@core-tme.netapp.com@centos7 kerberos]$ klist -e
Ticket cache: KEYRING:persistent:106003697:106003697
Default principal: test@CORE-TME.NETAPP.COM

Valid starting       Expires              Service principal
06/29/2016 16:39:43 06/30/2016 02:38:26 nfs/parisi-nfs.core-tme.netapp.com@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
06/29/2016 16:38:26 06/30/2016 02:38:26 krbtgt/CORE-TME.NETAPP.COM@CORE-TME.NETAPP.COM
        renew until 07/06/2016 16:38:21, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-
hmac-sha1-96
```

付録A：Kerberos暗号化タイプ

Kerberos V5では、複数のエンタイプがサポートされます。特定のインスタンスで使用されるタイプは、クライアントとKerberos KDCサーバの間で自動的にネゴシエートされます。ネゴシエーションは、クライアントとサーバの設定、およびユーザとサービスプリンシパルのパスワードの暗号化に使用される暗号化タイプに基づいて行われます。

表9 に、Kerberos v5で使用されるさまざまなエンコードタイプを示します。

表9）Kerberos暗号化タイプ

エンタイプ	暗号アルゴリズム	暗号モード	キーの長さ	HMAC	長所
AES256-CTS AES256-CTS-HMAC-sha1-96	AES	CBC+CTS	256ビット	SHA-1 96ビット	最強
AES128-CTS AES128-CTS-HMAC-sha1-96	AES	CBC+CTS	128 ビット	SHA-1 96ビット	付随する
RC4-HMAC	RC4		128 ビット	SHA-1 96ビット	付随する
des3-CBC-sha1	3DES	CBC	168ビット	SHA-1 96ビット	付随する
des-cbc-crc	DES	CBC	56ビット	CRC 32ビット	弱

エンタイプ	暗号アルゴリズム	暗号モード	キーの長さ	HMAC	長所
DES-CBC-MD5	DES	CBC	56ビット	MD5 96ビット	弱いが最強のシングルDES

付録B：マシンアカウントの属性

msDS-SupportedEncryptionTypes属性は、Kerberos認証で使用される暗号化タイプを指定するために使用されます。値は、一連の値を一緒に追加することによって指定されます。

`msDS-SupportedEncryptionTypes` 値は27（16進数の0x19）に設定されます。この値は、DESおよびAES暗号化タイプのみを許可することになります。ONTAPではNFS Kerberos用のRC4-HMACがサポートされないため、RC4は省略されます。表10 に、有効な値を示します。値27は、DES-CBC-CRC+DES-CBC-MD5+AES128+AES256（1+2+8+16）に指定された10進値を合計して算出されます。

表10）有効な `msDS-SupportedEncryptionTypes` 属性値

プロパティフラグ	16進数の値	10進数の値
DES-CBC-CRC	0x01	1
DES-CBC-MD5	0x02	2
RC4-HMAC	0x04	4
AES128-CTS-HMAC-SHA1-96	0x08	8
AES256-CTS-HMAC-SHA1-96	0x10	16

付録C：Kerberosパケットタイプ、エラー、用語

表11、表12、および 表13 は、ネットワークを介して行われるKerberos要求のタイプと、要求時に返されるエラーコードを示しています。この情報は、各リクエストの処理内容を説明することでトラブルシューティングを支援することを目的としています。

表11）Kerberosパケット

Kerberosパケット	キノウ
AS-REQ	認証サービス要求：TGTを取得するためにユーザ名とパスワードを検索します。また、セッションキーも要求します。
AS-REP	Authentication Service reply：TGTとセッションキーを配信します。
AP-REQ	アプリケーションサーバー要求:サーバーが再生を検出するのに役立つように、送信者が付随するチケットの暗号化キーについて最新の知識を持っていることをサーバーに証明します。この要求は、特定のセッションで使用する「真のセッションキー」の選択にも役立ちます。
AP-REP	アプリケーションサーバの応答：セッションキーとシーケンス番号が含まれます。
TGS-REQ	Ticket-granting-server request：TGTを使用してサービスチケット（ST）を取得します。
TGS-REP	ticket-granting-server reply：STを配信します。

表12）ネットワークキャプチャのKerberosエラー

Kerberosエラー	意味
KDC_ERR_S_PRINCIPAL_UNKNOWN	SPNが存在しないか、KDCに重複したSPNがあります。エラーの「S」が表示されていることに注意してください。これは「SPN」または「service」の略です。

Kerberosエラー	意味
KDC_ERR_C_PRINCIAL_UNKNOWN	UPNが存在しないか、KDCに重複するUPNがあります。エラーの「C」に注意してください。これは「client」を意味し、サービスプリンシパルではなくユーザプリンシパルを指します。
KDC_ERR_ETYPE_NOTSUPP	クライアントから要求された暗号化タイプがKDCでサポートされていません。これはDESおよびWindows 2008 R2で一般的です。
KDC_ERR_PREAUTH_REQUIRED	このエラーは、KDCが認証を試行するアカウントのパスワードを要求していることを意味します。これは問題のないエラーです。
KDC_ERR_PREAUTH_FAILED	事前認証に失敗しました。一般に、パスワードが正しくないためです。
krb_ap_err_skew	時間が許容されるスキューウィンドウの外側にあります。通常は5分です。
krb_AP_ERR_REPEAT	これは、リプレイ攻撃を防止するためのセキュリティメカニズムです。オーセンティケータのサーバー名、クライアント名、時刻、およびマイクロ秒のフィールドがキャッシュ内の最近検出されたエントリと一致した場合、このエラーが発生します。
krb_AP_ERR_MODIFIED	このエラーは、サービスが提供されたチケットを復号化できなかったことを示します。一般的な原因は、SPNが間違ったアカウントに登録されているためです。もう1つの可能性のある原因は、フォレスト内の2つの異なるドメインに重複するSPNです。このエラーは、元のチケットが発行されたKDCがオフラインで、クライアントが新しいKDCに対して再認証する必要がある場合にも発生する可能性があります。

表13）CentOS.orgおよびIBM.comで提供されているKerberos用語

期間	定義
KDC	Key Distribution Center：Kerberosチケットを発行するサービス。通常、チケット交付サーバ（TGS）と同じホストで実行されます。
TGT	チケット交付チケット:クライアントがKDCから申請せずに追加のチケットを取得できる特別なチケット。例：krbtgt/domain@realm。 このプリンシパルは、Microsoft Windows Active Directoryのkrbtgtという名前のユーザアカウントとして存在します。
TGS	チケット交付サーバー:目的のサービスのチケットを発行し、サービスにアクセスするためにユーザーに与えられるサーバー。TGSは通常、KDCと同じホストで実行されます。
SPN	Service Principal Name：service/instance@realmの形式でサービスに関連付けられたKerberosプリンシパル。 例： ldap / server.netapp.com@NETAPP.COM。
UPN	User Principal Name：user@realmの形式でユーザ名に関連付けられたKerberosプリンシパル。 例 ：ldapuser@NETAPP.COM。
セッション キー	2つのプリンシパル間で使用される一時的な暗号化キー。ライフタイムは1つのログインセッションの期間に制限されます。
セント	Service Ticket：特定のサービスに対して発行されるチケット。たとえば、NFSサービスの場合はnfs/instance@realm、LDAPサービスの場合はldap/instance@realmなどです。
AS	認証サーバー:目的のサービスのチケットを発行し、サービスにアクセスするためにユーザーに提供されるサーバー。ASは、要求を持つクレデンシャルを持っていない、または送信していないクライアントからの要求に応答します。このサーバは通常、TGTを発行してチケット交付サーバ（TGS）サービスにアクセスするために使用されます。ASは通常、KDCと同じホストで実行されます。

期間	定義
Realm	Kerberosを使用するネットワーク。KDCと呼ばれる1つ以上のサーバと、潜在的に多数のクライアントで構成されます。
GSS-API	Generic Security Service Application Program Interface（Internet Engineering Task Forceによって公開されたRFC-2743で定義されている）：セキュリティサービスを提供する一連の機能。このAPIは、クライアントとサービスが、基盤となるメカニズムに関する特定の知識を持つプログラムを持たずに相互認証するために使用されます。ネットワークサービス（cyrus-imapなど）がGSS-APIを使用している場合、Kerberosを使用して認証できます。

免責事項

NetAppは、本ドキュメントで提供されるいかなる情報または推奨事項の正確性、信頼性、有用性についても、または本ドキュメントで提供されるいかなる情報の使用または推奨事項の遵守によって得られる結果についても、表明または保証は一切行いません。本ドキュメントの情報は現状のまま提供され、本ドキュメントの情報の使用または推奨内容や手法の実施は、お客様の評価および業務環境への統合能力に基づいて、お客様の責任で行われるものとします。本ドキュメントおよびここに記載されている情報は、本ドキュメントで説明しているNetApp製品に関連してのみ使用できます。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを確認してください。

- TR-4067：『NFS Best Practice and Implementation Guide』
  www.netapp.com/us/media/tr-4067.pdf
- TR-4668：『Name Services Best Practice Guide』
  www.netapp.com/us/media/tr-4668.pdf
- TR-4523：『ONTAPにおけるDNSロードバランシング』
  www.netapp.com/us/media/tr-4523.pdf
- TR-4835：『How to Configure LDAP in ONTAP』
  www.netapp.com/us/media/tr-4835.pdf

お問い合わせ

本テクニカルレポートの改善点については、docfeedback@netapp.comまでお問い合わせください。
件名に「TECHNICAL REPORT 4616」と添えてください。

バージョン履歴

バージョン	日付	ドキュメントの改訂履歴
バージョン1.0	2017年8月	初回コミット
バージョン1.1	2020年6月	マイナーリビジョン、ONTAP 9.7情報
バージョン1.2	2021年2月	マイナーリビジョン、ONTAP 9.8情報
バージョン1.2.1	2021年6月	マイナーリビジョン、ONTAP 9.9.1の情報

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4616-0621-JP

NetApp