Technical Report

NFS Kerberos in ONTAP with Microsoft Active Directory

ONTAP 9.2 and later

Justin Parisi, NetApp
August 2017 | TR-4616

Abstract

This document covers NFS Kerberos support in NetApp® ONTAP® software and the configuration steps with Active Directory and Red Hat Enterprise Linux clients. This document complements, and can be considered an eventual replacement for, TR-4073: Secure Unified Authentication for NFS.

Information Classification

Public

NetApp®

Version History

Version	Date	Document Version History
Version 1.0	August 2017	Justin Parisi: Initial commit.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF CONFIGURATON STEPS

1 Overview

1.1 Document Scope

This document is intended to cover Kerberos configuration in NetApp ONTAP in a way that's easy for you to follow and to digest. To accomplish this goal, the scope is limited only to an environment with the following components:

- Microsoft Windows 2016 Active Directory Key Distribution Center (KDC)
- Red Hat Enterprise Linux (RHEL) versions 6.7 and/or 7.x
- AES-256 encryption
- ONTAP 9.2 and later

Note: The RHEL configuration can be easily applied to CentOS clients.

If you need to deviate from the preceding environment (such as the use of earlier ONTAP versions or different Linux clients), see the relevant client OS documentation, Windows documentation, and TR-4073: Secure Unified Authentication for NFS.

1.2 Kerberos Terminology

This section defines key terminology that's used when describing Kerberos processes. This section is meant to help clarify terms that might be unfamiliar to storage administrators.

Key Distribution Center

The *Key Distribution Center* (KDC) is the authentication server that includes the ticket-granting service (TGS) and the authentication service (AS). The terms KDC, AS, and TGS are used interchangeably. In Microsoft environments, an Active Directory domain controller is a KDC.

Realm (or Kerberos Realm)

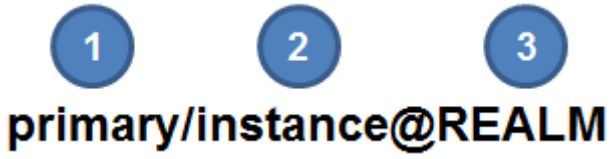
A *realm* (or Kerberos realm) can use any ASCII string. The standard is to use the domain name in uppercase; for example, `domain.com` becomes the realm `DOMAIN.COM`.

Administratively, each `principal@REALM` is unique. To avoid a single point of failure, each realm can have numerous KDCs that share the same database (principals and their passwords) and have the same KDC master keys. Microsoft Windows Active Directory does this natively by way of Active Directory replication, which takes place every 15 minutes by default.

Principal

The term *principal* refers to every entity within a Kerberos database. Users, computers, and services that run on a client are all principals. Every principal is unique within the Kerberos database and is defined by its distinguished name. A principal can be a user principal name (UPN) or a service principal name (SPN).

A principal name has three parts:



The Primary Part

The primary part can be a user or a service such as the “nfs” service. It can also be the special service “host,” which signifies that this service principal is set up to provide various network services such as ftp, rsh, nfs, and so on.

The Instance Part

This part is optional in the case of a user. A user can have more than one principal. For example, Fred might have a principal that is for everyday use and a principal that allows privileged use such as a sysadmin account. The instance is required for service principals and designates the fully qualified domain name (FQDN) of the host that provides the service.

The Realm Part

A Kerberos realm is the set of Kerberos principals that are registered within a Kerberos server. By convention, usually the realm name is the same as the DNS name, but it is converted to uppercase letters. Uppercase letters are not obligatory, but the convention allows easy distinction between the DNS name and the realm name.

Examples of principals:

```
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
```

Tickets

A *ticket* is a temporary set of credentials that verifies the identity of a principal for a service and contains the session key. A ticket can be a service or an application ticket or a ticket-granting ticket (TGT).

Secret Keys

Kerberos uses a symmetric key system in which the *secret key* is used for both encryption and decryption.

The secret key is generated from the principal’s Kerberos password with a one-way hash function. The KDC stores the password for each principal and can thus generate the principal’s secret key. For users who request a Kerberos service, the secret key is typically derived from a password that is presented to the `kinit` program. Service and daemon principals typically don’t use a password; instead, the result of the one-way hash function is stored in a keytab.

Keytab

A *keytab* contains a list of principals and their secret keys. The secret keys in a keytab are often created by using a random password and are used mostly for service or daemon principals.

1.3 Supported Encryption Types

NetApp Data ONTAP® and ONTAP technology supports NFS Kerberos with specific encryption types, depending on the operating mode and the version that you use.

So that a client uses the appropriate encryption type, limit the valid encryption types on the object principal or on the keytab file rather than in the `krb5.conf` file. This approach is much more scalable in large enterprise environments and confirms that the client can leverage stronger encryption types when they are supported.

Table 1 shows the supported encryption type based on version and mode. These types are for NFS Kerberos only and do not cover CIFS Kerberos support.

Table 1) Supported encryption types in ONTAP.

ONTAP Version and Mode	Supported Encryption Type
Data ONTAP operating in 7-Mode 7.x and later	DES and DES3 only **Note:** (RC4-HMAC works, but has no official support)
Data ONTAP 8.2.x and earlier (clustered)	DES and DES3
Data ONTAP 8.3.x	AES (128- and 256-bit), DES, and DES3
ONTAP 9.x	AES (128- and 256-bit), DES, and DES3

1.4 Supported Kerberos Security Modes

In addition to the concept of encryption types, there is also a level of security and integrity checking in Kerberos to help prevent man-in-the-middle attacks. Table 2 shows which levels of Kerberos security modes are supported in various versions of ONTAP. The security modes for Kerberos are configured on the clients and in the KDCs. Export policy rules are then configured to allow specific security modes.

Table 2) Supported Kerberos security modes in ONTAP.

ONTAP Version and Mode	Supported Kerberos Security Mode
Data ONTAP 7-Mode 7.x and later	krb5, krb5i, krb5p
Data ONTAP 8.2.x and earlier (clustered)	krb5
Data ONTAP 8.3.x	krb5, krb5i
ONTAP 9.x	krb5, krb5i, krb5p

1.5 How Kerberos Authentication Works

Kerberos is an authentication protocol that uses a secret key to validate the identity of principals.

KDCs such as Windows Active Directory maintain a database of principals and their Kerberos passwords. The secret key is nothing but the principal's password converted into a cryptographic key format. In the case of NFS servers and clients, the secret key can be generated by using a random password and is stored in a keytab on the NFS server or client.

In Kerberos, the secret key is considered as proof of unique identity. Therefore, the KDC can be trusted to authenticate any principal to any other principal, such as authenticating an NFS client SPN to an NFS server SPN at mount. It can also be trusted to authenticate a user principal to an NFS server SPN for user access to the NFS mount point. Kerberos does not send cleartext passwords for authentication across the wire.

When a Kerberos principal logs in to the Kerberos realm, the principal sends a TGT request that contains the principal but not the password or secret key to the `krb5kdc` daemon. On receiving this request, the KDC looks up the principal in the KDC database and uses the associated password from the database to encrypt the TGT response.

From the KDC, the encrypted TGT is sent to the principal. The principal decrypts the TGT response by using the secret key that was obtained from the password or from the keytab. The principal then requests authentication to the NFS server (in this case, Data ONTAP) by presenting the NFS server principal along with the encrypted TGT to the ticket-granting server (TGS). The TGS then issues a ticket for the NFS server. The ticket provides authentication to allow the principal to mount (for an NFS client SPN) or to use a specific file system that is mounted over NFS from the NetApp cluster (for a user principal).

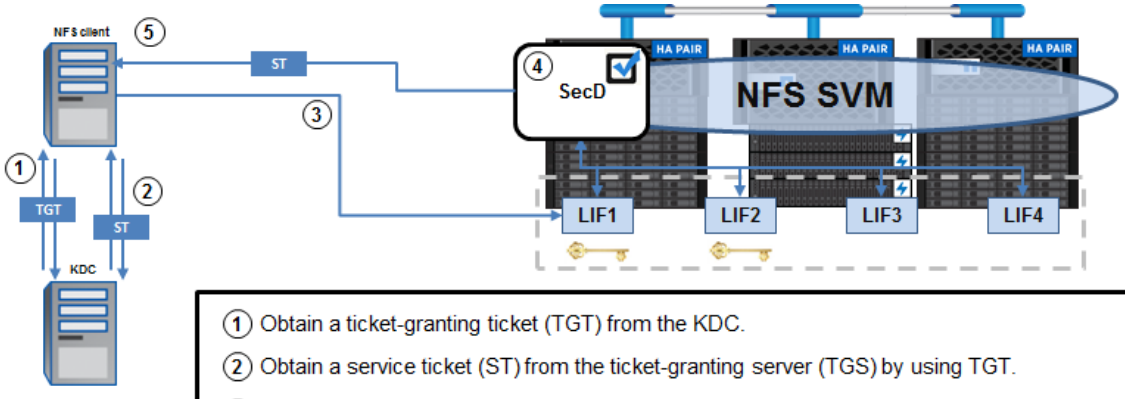
No Kerberos communication takes place between the NFS server and the KDC because the NFS server decrypts its portion of the TGS by using its keytab entry. The ticket is cached on the NetApp storage system until it is flushed. Figure 1 shows the Kerberos workflow between the client, the KDC, and the NFS server.

In Data ONTAP, the Kerberos ticket is cached until the cache is cleared, the node is rebooted, or the SecD process is restarted.

To see this cache, use the following command:

```
cluster::> set diag
cluster::*> diag secd cache show-krb-creds -node [nodename] -vserver [vservername]
```

Figure 1) Kerberos workflow between the client, the KDC, and the NFS server on NetApp storage.



To clear the Kerberos ticket cache in ONTAP, use the following commands:

```
cluster::> set diag
cluster::*> diag secd cache clear-krb-creds -node [nodename] -vserver [vservername]
```

When an object (in this case, an Active Directory machine or user account) is created for use by an SPN on the Active Directory domain controller, the user principal name (UPN) is also set when the `ktpass` utility is used. An object can have numerous SPNs but only one UPN. When the NFS client attempts a Kerberos connection with a credential that was established by using an SPN from a keytab file, Active Directory maps the incoming connection request to a UPN to find the appropriate account.

In the environment that this document covers, only one machine account is needed, with one UPN/SPN. This approach is a departure from previous methods that created three separate accounts.

The `rpc.gssd` service on a Linux client searches for SPNs in a specific order. That order is shown in the rpc.gssd manual pages and in the following list.

Kerberos SPN Types

`root/host.domain.com`: used by the NFS client for mount requests

`nfs/host.domain.com`: required to be used by the NFS server (for example, `nfs/cluster.domain.com`)

`host/host.domain.com`: used by the NFS client, usually for third-party applications such as SSSD

Any of the preceding types can be used to create a principal in Active Directory, but only one is required. This document covers the use of only the root SPN in most cases, but you can use other SPNs if you prefer. Some client operating systems require nonroot SPNs to use Kerberos, such as Red Hat 5.x and earlier versions.

2 Benefits of Using Kerberized NFS

Kerberos is a mode of authentication for users and for hosts. Sometimes this authentication is confused with authorization, which uses access control lists (ACLs) or mode bits on files and directories to determine a user's access. Authorization is performed after authenticating the user or host.

***Authentication* proves who you are; *authorization* allows you to do what you need to do after you have been authenticated.**

For example, if you buy a subway ticket, you are allowed through the turnstile (authentication). But after you are inside the station, you might not be able to travel to your destination if the ticket does not allow you to get there (authorization).

The benefits of using NFS Kerberos in ONTAP include:

- Prevention of plaintext passwords from being passed over a network
- End-to-end, enterprise-class encryption through AES-256 and AES-128
- Control over SPN to user mappings through the `krb-unix` name-mapping rule
- Increased group membership limits (32 maximum) as compared with standard AUTH_SYS (16 maximum).

Note: In ONTAP 8.3 and later, the AUTH_SYS and AUTH_GSS limits can be raised to 1,024 for both AUTH_SYS and AUTH_GSS. For more information about extending the auxiliary group limits for NFS in ONTAP, see TR-4067: NFS Best Practice and Implementation Guide.

3 ONTAP Configuration

This section covers how to configure NetApp ONTAP for the configuration of NFS Kerberos.

3.1 Configure the NFS Server

For the NFS server, you should enable and configure options to provide clients with the functionality that you need. You should make decisions about the NFS versions to use, which options to choose, and so on, before you configure NFS Kerberos. To help you make those decisions, see TR-4067. For NFS Kerberos, you should also consider the following:

- **NFSv3 doesn't Kerberize everything.**

  NFSv3 has ancillary protocols such as mount, port mapper, NLM, and so on. Kerberos in ONTAP covers only the NFS portion of the protocol version. NFSv4.x can Kerberize the entire stack, because it's all combined as per the standard. Therefore, if you want to use Kerberos for NFSv3, make sure that the export policy rules allow `sys` and `krb5*`.

- **Consider removing less secure encryption types.**

  By default, NFS servers in ONTAP allow the following enctypes on creation:

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

  DES and DES3 are much less secure enctypes. In fact, DES is disabled by default in modern Windows KDCs. If you don't need DES or DES3, remove them from the list. When Kerberos is enabled in an ONTAP storage virtual machine (SVM), removing enctypes requires downtime. It's better to remove the enctypes before you enable Kerberos in ONTAP.

  To disable DES and DES3 in ONTAP SVMs:

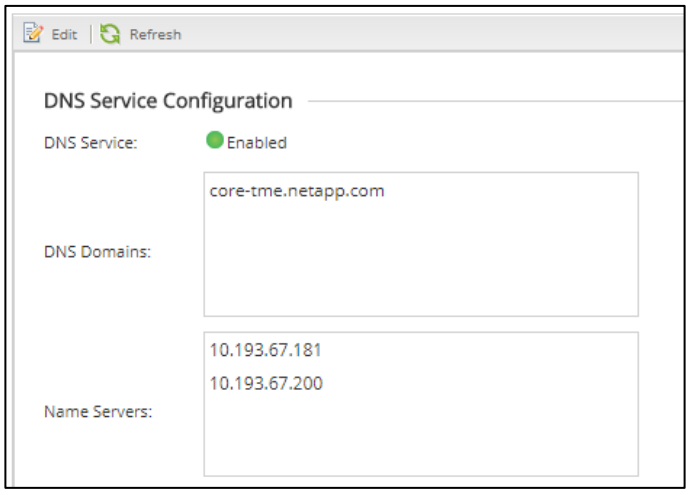
  ```
  cluster::> nfs modify -vserver [vserver] -permitted-enc-types aes-*
  ```

  Note: NetApp OnCommand® System Manager currently cannot be used to modify the permitted encryption types.

3.2 Configure DNS Settings in ONTAP

To make DNS lookups work properly for Active Directory connectivity and for Kerberos functionality, you must configure the DNS at the SVM level. You can configure the DNS in OnCommand System Manager or through the command line. The DNS servers must be able to resolve the cluster data LIFs and the client's host name, either through A/AAAA records or through DNS forwarding/delegations.

To configure DNS settings in **System Manager**, go to SVMs > SVM Settings > DNS/DDNS.



To configure DNS settings in the CLI, use the following command.

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

Add DNS Records or Configure On-Box DNS for the SVM Data LIFs

You should add to DNS the data LIFs in the SVM that will be participating in NFS Kerberos. You can add the LIFs either through A/AAAA and PTR records or by leveraging the on-box DNS. Work with your DNS administrator to accomplish this task. For information about configuring on-box DNS or adding records to DNS, see TR-4523.

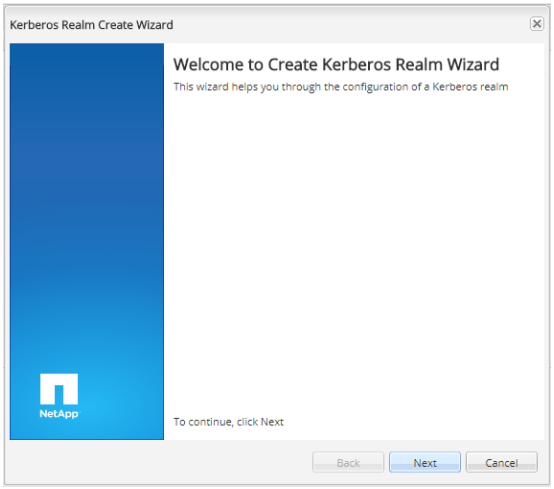
3.3 Create the Kerberos Realm

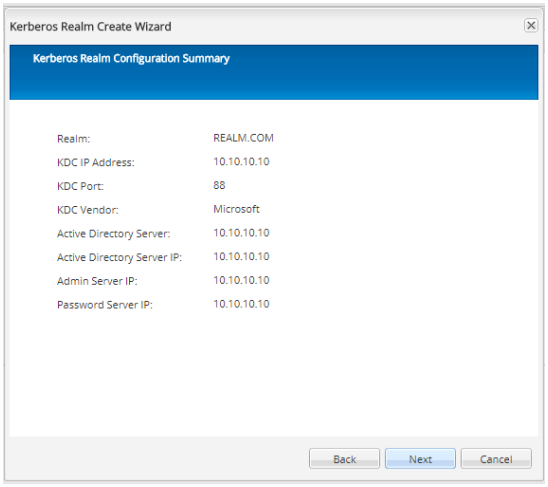
You need a Kerberos realm so that the cluster knows how to format Kerberos ticket requests. Creating the realm is similar to configuring `/etc/krb5.conf` on NFS clients. The IP addresses that are specified in the Kerberos realm commands are used only during creation of the machine account object or SPN; these IP addresses are not used for actual Kerberized NFS traffic. Therefore, you don't need to worry about failover or DNS aliases for these commands. KDC failover for Kerberized traffic is handled by using DNS SRV records. For more information, see TR-4073.

Note: You can create Kerberos realms by using OnCommand System Manager or by using the CLI.

To create a Kerberos realm in **System Manager:**

1. Go to SVMs > SVM Settings > Services > Kerberos Realm.
2. The realm configuration appears as a wizard. Enter your values and click Next for each screen.





To create a Kerberos realm in the **CLI**, use the following command.

```
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
```

3.4 Enable Kerberos on the Data LIFs

To use Kerberos for NFS, you must enable Kerberos on a data LIF in the SVM. When Kerberos is enabled, the SPN is defined and a principal is created on the KDC that was defined in the realm configuration. This machine account uses only the first 15 characters of the NFS SPN, including the `nfs/` portion. Therefore, if you want to have multiple Kerberos-enabled data LIFs, you should use names that

are unique within the first 15 characters. And to help avoid issues later with duplicate machine object names, you can also rename machine account objects after the fact.

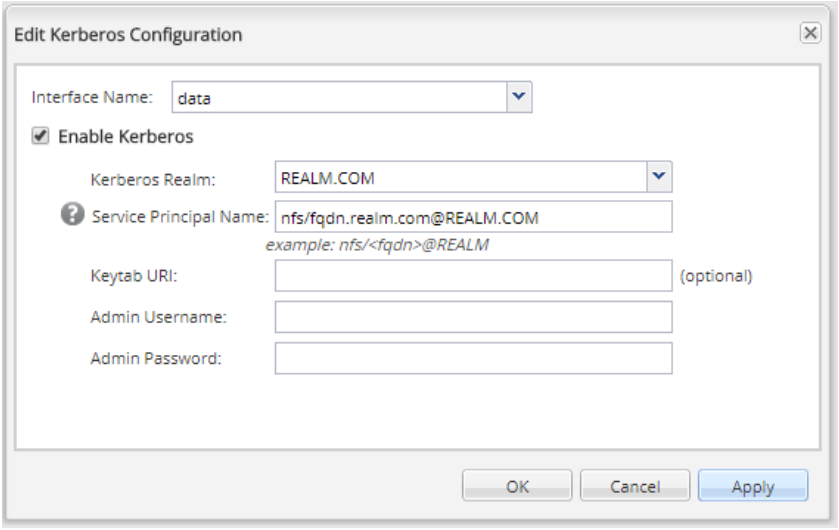
When Kerberos is enabled in ONTAP, the KDC is contacted and a user name and password prompt are issued by using the CLI. The user name that you provide must have the rights to create objects in the computer's organizational unit (OU) in Active Directory. This user can be a domain administrator or a user who has had rights delegated to manage that OU.

The SPN must use the format in the example of `primary/instance@REALM`, where `REALM` is always in ALL CAPS. If you don't use this format, the command fails.

Some other factors that you should consider include:

- This process is performed one data LIF at a time.
- You can use the same SPN for multiple LIFs or use different SPNs for different data LIFs.
- For every new SPN that is specified, a new machine account is created in Active Directory with the name `NFS-SPN-NAME`, up to 15 characters.
- For data LIFs with the same SPN, only one machine account is created.
- You need a domain user who has the permissions to create objects in the specified domain OU. The default OU is `DC=DOMAIN, DC=COM`.
- If you specify an OU, don't include `DC=DOMAIN, DC=COM`; the base DN is implied.
- The SPN is created as: `nfs/[desired DNS name for access]@REALM.IN.CAPS.COM`.

To create the user and group in **OnCommand System Manager**, go to SVM > SVM Settings, under Services > Kerberos Interface.



To create the user and group in the **CLI**, use the following command.

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

3.5 Modify Export Policy Rules to Allow Kerberos

Export polices in ONTAP are containers for export policy rules. Export policy rules are the share-level permissions that are applied to NFS exports. Access is provided or is denied based on host identity, such as IP address, host name, netgroup, or Kerberos authentication.

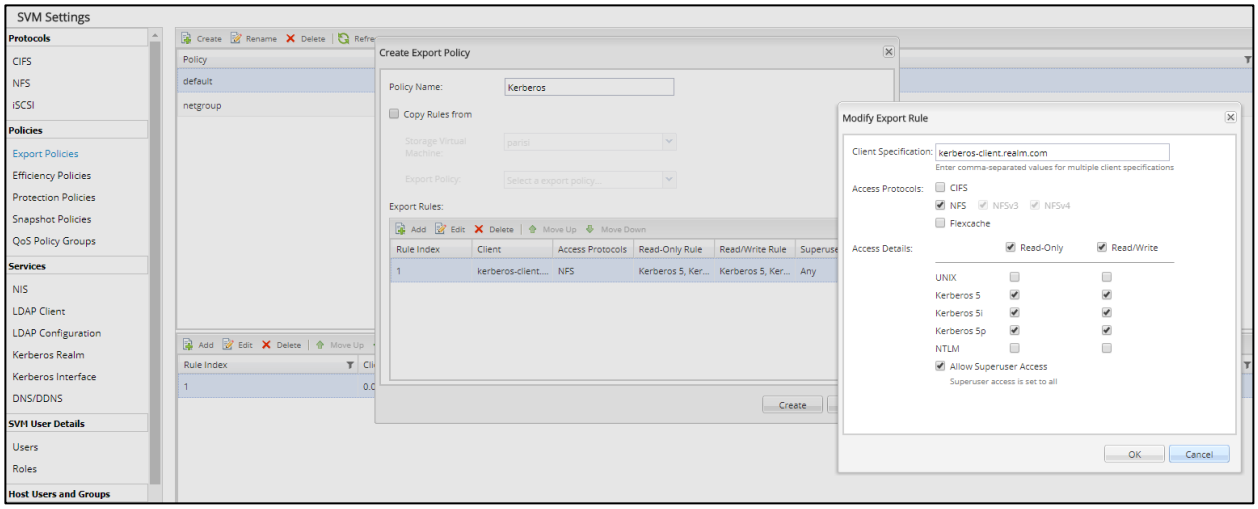
You can specify Kerberos security in the `rorule`, `rwrule`, and `superuser` fields of an export policy rule. Several different versions of Kerberos security are available in ONTAP 9 and later:

- **krb5** uses Kerberos V5 instead of local UNIX user IDs (UIDs) and group IDs (GIDs) to authenticate users.
- **krb5i** uses Kerberos V5 for user authentication and performs integrity checking of NFS operations by using secure checksums to prevent data tampering.
- **krb5p** uses Kerberos V5 for user authentication and integrity checking, and it encrypts NFS traffic to prevent traffic sniffing. This setting is the most secure, but it also involves the most performance overhead.

The Kerberos security options are negotiated between the client and the KDC. ONTAP export policies and rules simply provide a way to allow, or even require, a specific security option. If a krb5 security option is not specified in the export policy rule, attempts to mount NFS Kerberos exports fail, with access denied or permissions issues.

Note: NetApp does not recommend that you use krb5i or krb5p in ONTAP versions earlier than 9.2.

To create or modify export policies and rules in **System Manager,** go to SVM > SVM Settings, under Policies > Export Policies.



To modify export policy rules to allow krb5 in the **CLI**, use the following command set.

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

For more details about export policies and rules, see TR-4067.

3.6 Create a UNIX User or a Name-Mapping Rule to Map the NFS Service Principal

When a client attempts to access a mount with NFS Kerberos, a service ticket is requested by using the SPN that was defined in the Kerberos configuration. This SPN attempts to map into ONTAP through a `krb-unix` name mapping, using the first portion of the SPN as the source name. For Kerberos-enabled interfaces, that name is `nfs/fqdn.realm.com@REALM.COM`.

If no name mapping or valid UNIX user exists, the Kerberos access attempt fails and the client reports access denied/permission denied. ONTAP logs the failure to the event management system (EMS) in the form of a name-mapping failure.

To see the EMS event that is logged, use the following command.

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

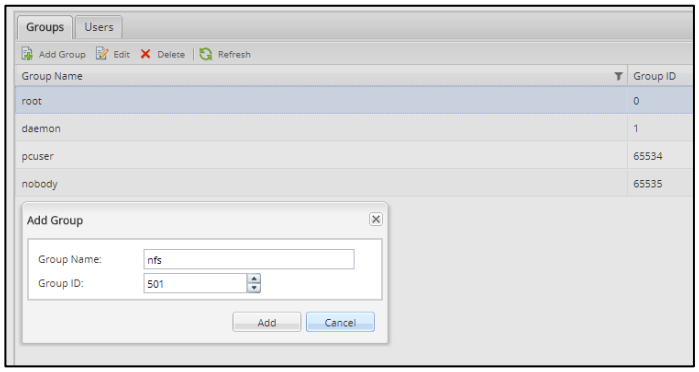
You can approach this task in either of two ways:

- Create a UNIX user named “nfs” for implicit name mapping either locally or in LDAP.
- Create a name-mapping rule for the SPN to map to an existing valid UNIX user.

Option 1: Creating a UNIX User and Group

To create a UNIX user in ONTAP, use either OnCommand System Manager or the command line to create a user and a group named “nfs” with any UID and GID that you choose. In general, service accounts use a range between 1 and 1,024 for UIDs and GIDs. Before you define a numeric UID or GID, make sure that it’s not in use elsewhere in your environment.

To create the user and group in **System Manager**, go to SVM > SVM Settings, under Host Users and Groups.



To create the user and the group in the **CLI**, use the following commands:

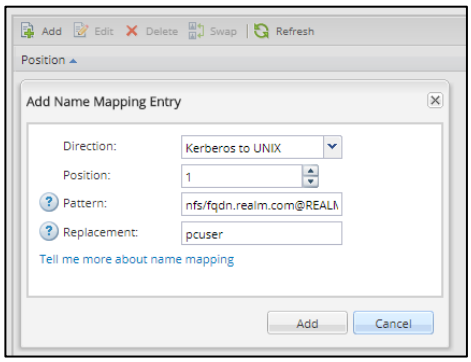
```
unix-user create -vserver [SVM] -user nfs -id [500] -primary-gid [500] -full-name "NFS Kerberos"

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

Creating a UNIX user and group is the simplest way to handle NFS Kerberos SPN `krb-unix` authentication into the cluster. Alternatively, if you have LDAP in your environment, you can create a user named “nfs” in LDAP.

Option 2: Creating a krb-unix Name-Mapping Rule

If you don’t want to create a UNIX user and group, you can create a name-mapping rule to handle NFS Kerberos SPN authentication. With this approach, the SPN `nfs/fqdn.realm.com@REALM.COM` (defined in the Kerberos interface commands) maps to the UNIX user of your choosing. In the following examples, we map the SPN to the pcuser.

To create the name mapping in **System Manager**, go to SVM > SVM Settings, under Host Users and Groups.



To create the name mapping in the **CLI**, use the following command:

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

3.7 Create a UNIX User or a Name-Mapping Rule to Map the NFS Client Principal

When an NFS client attempts to mount NFS exports in ONTAP through Kerberos, the client's principal is passed to ONTAP for authentication. The principal that the client uses for authentication depends on how Kerberos was configured. You can view it from the keytab on the client by using `klist`.

When joining a domain by using realmd or net ads, the principal is the `MACHINENAME$@REALM.COM`. In some cases, RHEL will use either `nfs/hostname` (in versions earlier than RHEL 6.x) or `root/hostname` (generally, with manual keytab creation) as the SPN.

When the mount command is issued, that principal attempts to perform a `krb-unix` name mapping into ONTAP. The default behavior for clients that used domain joins is to look for a UNIX user named "MACHINEACCOUNT$." If that user doesn't exist in local files or name services, then ONTAP looks for a name-mapping rule. If no name-mapping rule exists, the NFS Kerberos mount attempt fails with a permission or access issue. ONTAP logs the failure in EMS as a secd error.

To see the EMS event that is logged, use the following command.

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

You can approach this task in either of two ways:

- Create a name-mapping rule for the SPN/UPN to map to an existing valid UNIX user.
- Create a UNIX user "MACHINEACCOUNT$" for implicit name mapping either locally or in LDAP.

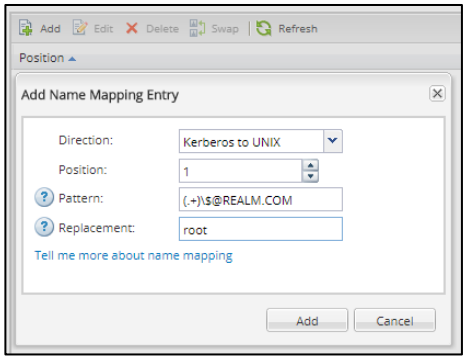
Note: In the cases where `nfs/hostname` or `root/hostname` are used as the SPNs, you should create UNIX users named "nfs" or "root." Root is always a default user in ONTAP, so no action should be required.

Option 1: Creating a Name-Mapping Rule (Recommended)

Rather than creating multiple UNIX users for RHEL clients, it makes more sense to create a global name-mapping rule to map all Linux clients that attempt to authenticate as `MACHINEACCOUNT$@REALM.COM` to root. Mapping an account to root does not grant root access; it simply allows a root user to appear as root to Kerberized mounts. You can create this global name-mapping rule in OnCommand System Manager or through the CLI.

In the following examples, we create a rule that maps any computer account name that attempts Kerberos access to root through the regular expression of `(.+)\$`. This name-mapping rule does not map user accounts to root; it maps only machine accounts (unless users are named `user$@REALM.COM`).

To create the name mapping in **System Manager**, go to SVM > SVM Settings, under Host Users and Groups.



To create the name mapping in the **CLI**, use the following command.

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

Note: The incoming NFS client principal is highly dependent on the client Linux version and how you configured Kerberos. Verify the incoming SPN when you determine how to create the name mapping. For example, some clients might use `host/name.realm.com` as their Kerberos principal. `Event log show` in ONTAP can deliver details about which principal is trying to authenticate when failures occur.

2) To test the name mappings, use the following command:

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

Option 2: Creating a UNIX User and Group (Not Recommended)

To create a UNIX user in ONTAP, use either OnCommand System Manager or the command line to create a user and a group named “MACHINEACCOUNTNAME$” with any UID and GID that you choose. In general, service accounts use a range between 1 and 1,024 for UIDs and GIDs. Before you define a numeric UID or GID, make sure that it’s not in use elsewhere in your environment. You can also perform this task in LDAP by using the existing machine account object that is created by modifying LDAP attributes. For details about creating a user and group, see TR-4073.

Note: Because an environment might contain many hundreds of RHEL clients that use Kerberos, NetApp does not recommend that you use this approach; it often becomes a scalability headache.

3.8 From Active Directory, Modify the Machine Account to Allow Only AES

Modifying the machine account to allow only AES prevents clients from trying weaker or unsupported encryption types. When you enable Kerberos in ONTAP, a NFS-specific machine account is created in Active Directory (separate from existing CIFS server machine accounts). Using Windows PowerShell is the easiest way to modify the NFS server’s machine account:

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

4 Red Hat Linux (RHEL) Client Configuration

Before the more modern RHEL clients, configuring NFS Kerberos with Active Directory KDCs was a fairly manual process that required interaction from multiple teams. Client principals in Active Directory had to

be created from the KDC, and keytab files had to be manually moved to clients. For the manual process, see TR-4073: Secure Unified Authentication for NFS.

Newer RHEL clients provide utilities to behave more like their Windows counterparts; the utilities allow the clients to automate the process by joining an Active Directory domain. When a domain is joined with realmd, the principal creation on the KDC, the client Kerberos configuration, and the keytab transfer are carried out automatically, without ever having to touch the KDC. The following RHEL packages are recommended for joining clients to Active Directory domains:

- RHEL 6.x: Winbind/Samba (through net ads)
- RHEL 7.x: Realmd

As an added bonus, domain joins also configure the LDAP client SSSD to automatically leverage the Active Directory environment for UNIX Identity Management. For more information about configuring LDAP, see TR-4073: Secure Unified Authentication for NFS.

This configuration section makes the following assumptions about the RHEL clients:

- The RHEL client has forward (A/AAAA) and reverse (PTR) records in DNS.
- AES encryption is being used.
- The RHEL client has the following packages installed (optional packages are denoted with *):
  - nfs-utils, realmd, samba, samba-client, samba-winbind, autofs*, ntp, bind-utils, tcpdump*, sssd (or other LDAP client)*, krb5-workstation, krb5-libs, auth-config-gtk

4.1 Configure Network Time Protocol (NTP) Services

Configuring time services on the RHEL client helps prevent issues with Kerberos time skew. To configure NTP services, use the following commands.

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

4.2 Verify DNS

This verification allows you to check that the client exists in DNS. DNS forward and reverse records are needed for proper Kerberos functionality. To verify DNS, use the following commands.

```
# nslookup [hostname]
# nslookup [IP address]
```

If the client is not in DNS, work with the DNS administrator to have it added or leverage the dynamic DNS functionality in RHEL.

4.3 Join the Domain

This step creates a principal in the KDC and a keytab file and configures the client for Kerberos. Joining a domain requires a user account with access to create objects in the specified Active Directory container. The default container is `OU=Computers`, but you can specify it in the commands that you use:

- For RHEL 6.x, use net ads, because realmd doesn't exist.
- For RHEL 7.x, use realmd.

4.4 Modify the Machine Account Principal

Although most of the client and KDC interaction is automated when you join the domain, there is a manual step of configuring the machine account principal to confirm that Kerberos works properly with NetApp ONTAP.

Change the Supported enctypes for the Machine Account

This step is required to prevent the client from attempting RC4-HMAC Kerberos for NFS, which ONTAP does not support. For this step, use PowerShell to modify the `msDs-SupportedEncryptionTypes` value to use AES-256 and AES-128 only.

Example of failure when using RC4-HMAC:

```
6/29/2016 16:09:56  ontap-tme-prod-03
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).
```

Optional: Add the Machine Account's Service Principal to the userPrincipalName Field

This step confirms that `kinit -k` works with the client, as well as any application (such as SSSD) that might need to use a machine account service principal for Kerberos.

Sample PowerShell command:

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

Optional: Customize the krb5.conf File

If you want the client to avoid using DNS to create the NFS service principal (that is, you have multiple A records for the ONTAP SVM), then add the following option to [`libdefaults`] in `/etc/krb5.conf`.

```
dns_canonicalize_hostname = false
```

5 Best Practices

The following is a list of best practices for using NFS Kerberos in NetApp ONTAP. They are best practices, not requirements. By following these best practices, you can achieve optimal results, but not all the steps are necessary for Kerberos to work properly.

This list is not comprehensive If you discover an issue with the best practices on this list or want to suggest an addition, please send comments to us by following the instructions in the Contact Us section. For more detailed steps and configuration information than this document provides, see TR-4073.

5.1 ONTAP Best Practices

- Add the data LIFs that participate in NFS Kerberos to DNS with forward and reverse (PTR) records.
- Set up more than one data LIF per SVM for NFS Kerberos data access; preferably, one data LIF per node per SVM. This best practice is for performance and resiliency considerations.
- DNS records for the data LIFs in the SVM should match the name set for the NFS service principal that is used in the NFS Kerberos configuration of the data LIFs (through Kerberos interface commands).
- Before you configure NFS Kerberos, remove DES and DES3 encryption types from the `permitted-enc-types` option in the NFS server. Disabling DES and DES3 after you create principals requires an outage, because you have to re-create the machine accounts to generate new keytabs.
- If you use on-box DNS load balancing or off-box DNS load balancing, enable NFS Kerberos on all data LIFs that participate in the DNS load balance zone.

- Create a local UNIX user or LDAP user named “nfs” to allow implicit `krb-unix` name mapping for the NFS service principal.
- Create a global name-mapping rule for `krb-unix` mapping of incoming NFS client machine accounts. Machine account principals will attempt to map into ONTAP and should have a valid UNIX user to map to. For further information, see section 3.7 in this document.
- Keep the SPN length of your machine account names to less than 15 characters, if possible. If your machine accounts are not unique past 15 characters, machine account creation will fail. As a workaround, rename your machine accounts after you create them.
- Ideally, configure ONTAP to use the same LDAP server as the NFS clients for identity management. For LDAP configuration information, see TR-4073.
- Verify that the SVM root volume (`/`) has an export policy rule that allows at least read access to clients. Read access is required to allow clients to traverse the top level of the namespace. See TR-4067 for details.

5.2 NFS Client Best Practices

- Use NTP to keep NFS clients in sync with the time of the KDC and the cluster. Time skews outside of 5 minutes can cause outages for NFS Kerberos.
- Add forward and reverse (PTR) records to DNS for NFS clients that use Kerberos. The DNS fully qualified domain name (FQDN) should match the client principal and what’s in the Kerberos configuration for the Kerberos realm.
- Use `klist` and `kinit` commands to view keytabs and to test Kerberos functionality. Keep in mind that any non-root user who wants to access an NFS Kerberos mount must be able to `kinit` (log in) to the KDC before it can request tickets to access the mount.
- Set the timeout value for rpcgssd to -T 60 for clients that hit timeout issues when mounting NFS Kerberos. For more information about how to set this value, see the NFS client OS guides.
- Using packet traces (`tcpdump`), `/var/log/messages`, and debug levels for rpcgssd and mount is the best way to troubleshoot most Kerberos issues. In many cases, access to the KDC and the ONTAP cluster is needed as well.
- On the KDC, make sure that the NFS client machine account has the appropriate encryption types enabled. For details about what the client can and cannot use, see the ONTAP supported encryption types.
- To avoid bugs in the NFS Kerberos stack, use the latest possible version of the client’s kernel.
- To configure NFS clients for Kerberos, use domain joins rather than manual Kerberos configuration.
- For accurate and consistent UID and GID management, use SSSD for LDAP connectivity to the Active Directory server.

5.3 Windows KDC Best Practices

- Use `setspn /q` to search the KDC for duplicate SPNs. Duplicate SPNs cause access issues that can be hard to track down.
- Make liberal use of packet traces when you troubleshoot Kerberos issues.
- To avoid time skew issues, keep the KDC’s time up to date and within 5 minutes of the ONTAP cluster and NFS clients.
- Use PowerShell as a simple way to modify machine accounts.
- Windows 2008 and later versions disable DES encryption by default. Use DES only if it’s necessary. Use AES instead, which is enabled by default in Windows KDCs.
- Windows Active Directory currently defaults to RC4-HMAC as the encryption type for Kerberos. Because ONTAP does not support RC4-HMAC for NFS Kerberos, be sure to remove RC4-HMAC as an option for NFS Kerberos clients and ONTAP servers. Section 4.4 explains how to modify the NFS client machine account. Section 3.8 covers how to modify the NFS server account.

6 Sample Configurations

This section presents a sample configuration for NFS Kerberos.

6.1 NetApp ONTAP

Kerberos Realm

```
                        KDC Vendor: Microsoft
                    KDC IP Address: 10.193.67.236
                          KDC Port: 88
                        Clock Skew: 5
      Active Directory Server Name: ONEWAY
Active Directory Server IP Address: 10.193.67.236
                           Comment: -
           Admin Server IP Address: 10.193.67.236
                 Admin Server Port: 749
        Password Server IP Address: 10.193.67.236
              Password Server Port: 464
        Permitted Encryption Types: aes-256, aes-128
```

Kerberos Interfaces

```
ontap9-tme-8040::*> kerberos interface show -vserver DEMO -lif data*
  (vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
DEMO           data          10.193.67.237   enabled  nfs/demo.ntap.local@NTAP.LOCAL
DEMO           data2         10.193.67.219   enabled  nfs/demo.ntap.local@NTAP.LOCAL
2 entries were displayed.
```

Pertinent NFS Server Configuration Options

```
ontap9-tme-8040::*> nfs server show -vserver DEMO -fields permitted-enc-types,v4.0,v4.1,v4-id-
domain
vserver v4.0    v4-id-domain v4.1    permitted-enc-types
------- ------- ------------ ------- -------------------
DEMO    enabled ntap.local   enabled aes-256,aes-128
```

DNS

```
ontap9-tme-8040::*> dns show -vserver DEMO

                             Vserver: DEMO
                             Domains: NTAP.local
                        Name Servers: 10.193.67.236
      (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
```

UNIX Users and Groups

```
ontap9-tme-8040::*> 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.

ontap9-tme-8040::*> 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.
```

Name-Mapping Rules

```
ontap9-tme-8040::*> 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.
```

6.2 Windows (Machine Accounts and Principals)

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!
```

Note: The machine account in the preceding sample was renamed from “NFS-DEMO-NTAP-L” to “KERBEROS.”

NFS Client Machine Account

```
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                           : 10.193.67.225
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         : 31
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 Server Machine Account (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                           : 10.193.67.219
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
```

6.3 RHEL 7.x Client

krb.conf File

```
# 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_realm = EXAMPLE.COM
 default_ccache_name = KEYRING:persistent:%{uid}

 default_realm = NTAP.LOCAL
[realms]
# EXAMPLE.COM = {
#  kdc = kerberos.example.com
#  admin_server = kerberos.example.com
# }

 NTAP.LOCAL = {
 }

[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM
 ntap.local = NTAP.LOCAL
 .ntap.local = NTAP.LOCAL
```

Keytabs (Using klist -k)

```
# 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
```

Realm Output

```
# 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
```

Sample of Working Kerberized homedir Mount

Become a user:

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

Access is denied because we haven't "logged in" with `kinit`:

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

We have logged in and viewed the ticket-granting ticket (TGT):

```
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
```

Navigate to the homedir, which is automounted to ONTAP by using NFSv4.1 and Kerberos:

```
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=10.193.67.225,local_lock=none,addr=10.193.67.219)
```

7 Common Issues

This section covers some of the most common issues that arise in the process of configuring NFS Kerberos in NetApp ONTAP. It also explains how issues manifest and how to resolve them. This section is not comprehensive, but it tries to present some of the most commonly seen problems. Because Kerberos has numerous moving parts, you might have to involve the storage administrators, the Windows KDC administrator, DNS administrators, and the NFS client administrators.

If you have suggestions for issues to add to this section, please follow the steps in the Contact Us section of this document.

7.1 Errors During Kerberos Interface Enable, Modify, or Create in ONTAP

If you see an error during the initial configuration of a data LIF for Kerberos, or during modification of an existing data LIF, use Table 3 as a guide for resolving issues.

Table 3) Identifying and resolving issues while creating or modifying Kerberos interfaces in ONTAP.

Issue	How to View the Error	Steps to Resolution
The user who attempts to modify the interface has permissions on the KDC to create or modify machine accounts in the specified OU.	• Event log show • Error output returned by the command when it fails	• Switch to a user who has access (such as a domain administrator). • Delegate control of an OU to a user. • Change the OU that is specified in the Kerberos configuration to an OU for which the user has create access.
Kerberos interface modification fails and cites the inability to connect to a valid KDC.	• Event log show • Error output returned by the command when it fails	• Check the Kerberos realm configuration and ensure that it's configured properly. • Check the DNS configuration for the SVM. • Make sure that the data LIFs can route to the Windows Active Directory environment. • Confirm that the default route exists in the SVM.
Kerberos interface creation or modification fails and cites a time skew issue.	• Event log show • Error output returned by the command when it fails • Secd logs	• Modify the cluster time to be within 5 minutes of the Windows KDC. • Confirm that the time zone on the cluster matches the time zone on the KDC. • Leverage NTP to sync the time across the environment.

7.2 Errors During Mounting of NFS Kerberos from a Client

If you see an error during the initial NFS mount through Kerberos from a client, Table 4 offers some potential issues for you to check. This information applies only to errors during the initial Kerberos mount attempt.

Table 4) Identifying and resolving issues while mounting NFS Kerberos exports.

Issue	How to View the Error	Steps to Resolution
Access/permission denied	• Mount command output • Event log in ONTAP • Packet trace	• Check the export policy rules for the SVM root volume (`/`) and for the data volume (`/path`); if you're using qtree exports, check the policy for the qtree. Krb5 should be allowed in the `ro/rw` rules, and the NFS client should be allowed in the export policy rule's client match. • Use `export-policy check-access` commands to verify that the specified client has access. • Check the event log (`event log show`) in ONTAP for errors regarding `krb-unix` name mapping for NFS clients. If there are errors, resolve the issue by creating local UNIX users or name-mapping rules. Generally, the NFS service principal/user does not apply to initial mounts. NFS principals authenticate when attempting to access Kerberos mounts. • Check the event log (`event log show`) in ONTAP for errors regarding encryption types being unsupported. A common issue with Active Directory includes clients that are trying to use RC4-HMAC to authenticate. ONTAP doesn't support RC4-HMAC with NFS Kerberos. To resolve this issue, modify the machine accounts to remove RC4 from the list. After you modify the machine accounts, you might have to flush caches or disable/enable Kerberos to delete the keytab.
Protocol not supported	• Mount command output • Packet trace	• Verify which version of NFS is being mounted and compare it with the versions that are enabled in the ONTAP NFS server. • Clients attempt to negotiate the highest NFS version that is enabled on a server. • ONTAP supports NFSv3, NFSv4.0, and NFSv4.1 for NetApp FlexVol® volumes and supports NFSv3 for ONTAP FlexGroup volumes.
No such file or directory	• Mount command output • Packet trace	• Verify that the path specified in the mount command exists in ONTAP as a junction path. This step can be performed in System Manager or through the CLI.
Mount point "" does not exist	• Mount command output	• Verify that the specified mount point folder exists on the local client.

Incorrect mount option	• Mount command output	• Check the mount command options that are specified. Do they actually exist as per client documentation? • If specifying krb5, verify that the rpcgssd service is started and that SECURE_NFS is allowed on the NFS client.
Mount hangs	• Mount command output • Packet traces	• If a mount is hanging, it means that the client or the server is failing to respond to a packet. Generally, this problem can be a network issue or a firewall or server configuration issue.

7.3 Errors After Mounting NFS Kerberos and Attempting to Access, Read, or Write

Table 5 covers issues that might occur after a Kerberos NFS export has successfully been mounted. With this category, traversal, reading, and/or writing issues an error.

Table 5) Identifying and resolving issues in accessing Kerberos NFS exports in ONTAP.

Issue	How to View the Error	Steps to Resolution
Access/permission denied when attempting to traverse the mount	• Command-line output	• Check the event log (`event log show`) in ONTAP for errors regarding `krb-unix` name mapping for the NFS service principal. If there are errors, resolve the issue by creating local UNIX users or name-mapping rules for the `nfs/name.realm.com` SPN. • Use `export-policy check-access` commands to see whether the client is allowed to read and write through krb5 to the export. • Verify that you actually mounted through Kerberos by issuing the mount command. • Verify that the export policy and rule allow krb5 access to `ro` and `rw` rules. • Verify that you have used `kinit` to log in as a user to generate a Kerberos ticket-granting ticket (TGT). • Use `klist -e` to verify that the Kerberos ticket has not expired. • If you are root, check the ONTAP event logs to see who root is trying to authenticate as. • Use `vserver security file-directory show` to verify the file-level permissions to the export. • If the volume/qtree security style is NTFS, verify that the UNIX user who is attempting access has a valid UNIX-Windows name mapping.

Issues when reading or writing to the export.	• CLI output	• Use `vserver security file-directory show` to verify the file-level permissions to the export. • If you're using NFSv4.x, verify that NFSv4.x is configured properly, as per TR-4073 and TR-4067. • If you see "Operation not permitted" when you try to use `chown` or `chmod`, check the permissions on the folder and the export policy rule settings.

Note: For other common NFS issues that are not listed in Table 4, see TR-4067.

8 Detailed Configuration Steps

To declutter the earlier sections of this report and to provide a cleaner, easier-to-read document, we have presented only the main configuration steps so far. In this section, we present some of the more intricate configuration steps.

8.1 Renaming NFS Kerberos Machine Accounts in Active Directory

In some cases, the NFS-FQDN-FORMAT of the machine account name is not a preferred name for the Active Directory environment. For instance, some organizations require strict naming schemes for machine accounts. Although you cannot specify a name for a machine account during its initial creation, you can rename it afterward without having to remount clients, reissue tickets, and so on.

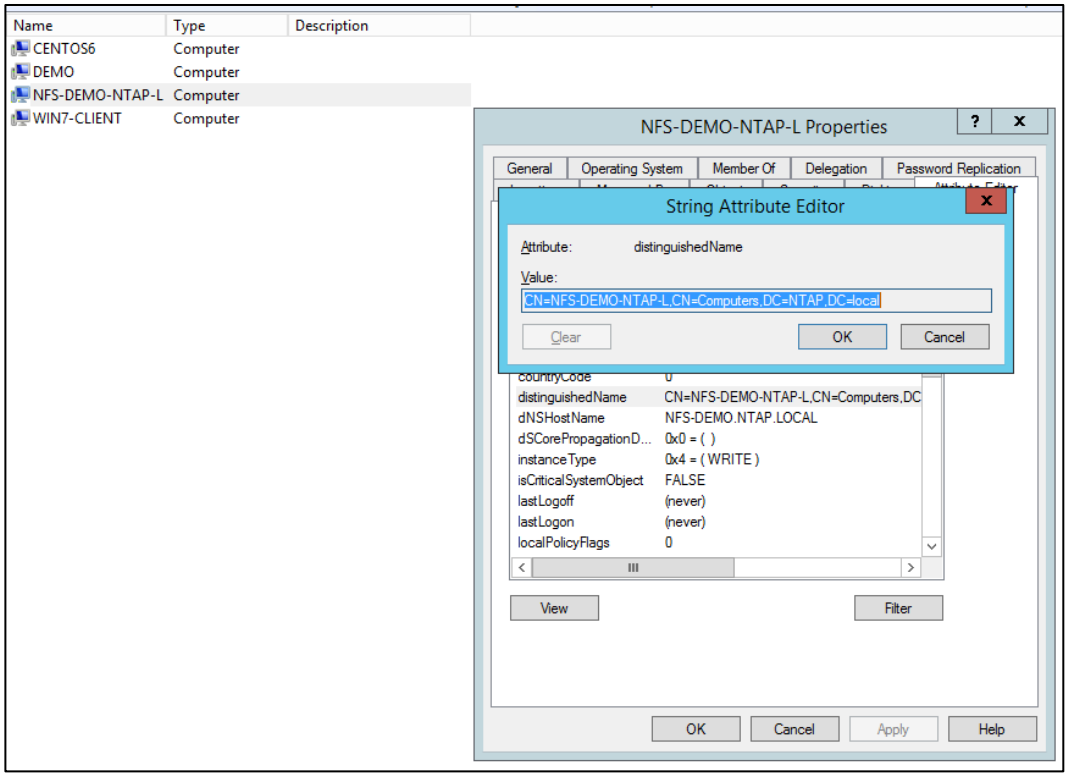
You can easily rename it after creation because the display name of the machine account is not critical to the Kerberos operations. What matters in the Kerberos interaction between clients and KDCs are:

- SPNs on the machine account
- DNS host names
- Keytab files
- `sAMAccountName` on the machine account

With Active Directory, simply changing the display name (by highlighting and changing it in GUI) does not affect any of the preceding items. In some cases, Active Directory doesn't allow name changes through the GUI by default. Instead, you have to use PowerShell. The following steps will guide you through renaming a machine account.

Configuration Steps 1) Renaming a machine account in Active Directory.

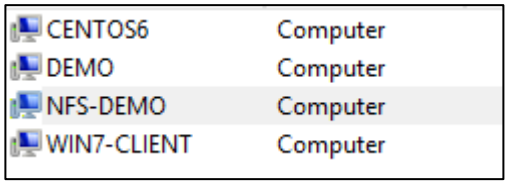
1. First, locate the machine account of the object that you want to rename in Active Directory. Open up the object in AD Users and Computers and find the DN value (you need to enable Advanced Features for this step). You need this value for your PowerShell command.

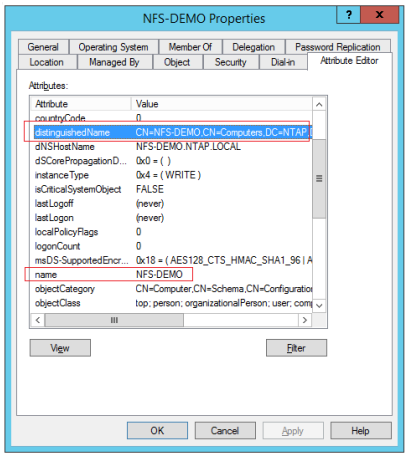


2. Open PowerShell as the domain administrator (or as another user with Active Directory renaming rights) and run the following command, replacing the objects in brackets with your desired values.

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

3. This command changes the DN and the “name” value on the computer object, as well as the displayed name in AD Users and Computers.





4. Next, change the attributes for dNSHostName and add a new SPN with the machine account name’s FQDN and short name. Use PowerShell’s Set-ADComputer for this step.


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

5. Next, test your Kerberos access. Everything should still work just fine, because the NFS SPN that is used by the data LIFs has not changed.

```
[root@centos6 /]# mount home
[root@centos6 /]# mount | grep home
demo:/home on /home type nfs
(rw,hard,intr,sec=krb5,vers=4,addr=10.193.67.219,clientaddr=10.193.67.211)
[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
```

8.2 Configuring an NFS Client to Use Kerberos with net ads join

This section shows an example of how to configure NFS clients to use Kerberos after they join a domain by using `net ads join`. You can find net ads commands with the Samba and Winbind packages.

The NFS client that we use in this example is RHEL/CentOS 7.2. We use the net ads command to join the domain. The domain is Windows Server 2012 R2 Active Directory. We use local UNIX users for name mappings.

Configuration Steps 2) Configuring an NFS client to use Kerberos with `net ads join`.

1. Install the necessary packages:

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

2. Check the time on the client and domain to ensure that you are within 5 minutes. This step also verifies that the client can find the domain controller:

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

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

Set up ntp. If necessary, sync the time manually:


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

3. Ensure that the client is in the same DNS that Active Directory uses and that `nslookup` works for the client and for the domain controllers.

```
# nslookup centos7
Server:         10.193.67.181
Address:        10.193.67.181#53

Name:   centos7.core-tme.netapp.com
Address: 10.193.67.225
Name:   centos7.core-tme.netapp.com
Address: 192.168.122.1

# nslookup core-tme.netapp.com
Server:         10.193.67.181
Address:        10.193.67.181#53

Name:   core-tme.netapp.com
Address: 10.193.67.200
Name:   core-tme.netapp.com
Address: 10.193.67.181
```

4. Modify the `/etc/krb5.conf` file to reflect the Active Directory domain:

```
[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
```

5. Configure `/etc/samba/smb.conf` with the domain information:

```
[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
```

6. Restart smb and rpcgssd services:

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

7. Get a Kerberos ticket for the administrator:

```
# 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
```

8. Join the domain:

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

Note: All normal Windows domain rules apply: The time skew is within 5 minutes; the user account has permissions to add computer objects to a domain; and the DNS can locate domain controllers.

9. Create a keytab file:

```
# net ads keytab create -U administrator

Warning: "kerberos method" must be set to a keytab method to use keytab functions.
```



```
Enter administrator's password:
```

10. Verify the keytab file.

    When a machine account is added to Active Directory by using `net ads keytab`, the following SPNs are added to the `krb5.keytab` file automatically:

```
# 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
```

No other SPNs should be required for the machine account. If you notice, there are SPNs for `root/` in the keytab. Because there is a UNIX user named “root” in the SVM by default, you don’t have to consider name mapping for the client unless you want a different mapping.

If you need a different mapping, a KRB to UNIX name mapping must exist for `machine$` either locally on the SVM (a name-mapping rule or a UNIX user) or on the Active Directory object (in the form of a uidNumber/GidNumber attribute in LDAP).

The easiest way to resolve this issue is through the local `unix-user`:

```
::*> 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:
```

11. Test the `krb-unix` mapping for the root SPN or for the machine account SPN if you prefer:

```
::> set diag
::*> diag secd name-mapping show -node ontap-tme-prod-03 -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 ontap-tme-prod-03 -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
```

12. Ensure that the following services are running and are enabled on boot:

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

13. Test the domain connectivity:

```
# net ads info
LDAP server: 10.193.67.181
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: 10.193.67.181
Server time offset: 0

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

14. Ensure that the NFS `unix-user` or equivalent name mapping is in place so that the service account (`nfs/fqdn@REALM`) can authenticate:

```
::*> 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:
```

15. On the NFS client, ensure that SSSD (or the LDAP client equivalent) is configured. Or you can use a local UNIX user in `/etc/passwd` and on the SVM.

To test LDAP:

```
# id ldapuser

# getent passwd ldapuser
```

16. Try to mount the SVM data interfaces with Kerberos. The SVM must already have the following created and configured:
    - Kerberos realm
    - Kerberos interfaces
    - DNS A/AAAA records in the DNS server (forward and reverse)
    - Permitted enctypes for Kerberos

- Export policy rules on the NFS exports and parent directories that allow Kerberos

Mount example:

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

17. `su` as a different user and `kinit`. `cd` into the mount and check for your NFS service ticket:

```
[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,retran
s=2,sec=krb5,clientaddr=10.193.67.225,local_lock=none,addr=10.193.67.226)

[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
```

8.3 Configuring an NFS Client to Use Kerberos with realm join

This section shows an example of how to configure NFS clients to use Kerberos after they join a domain. The NFS client that we use in this example is RHEL/CentOS 7.2. We use the `realm` command to join the domain. You can find the packages that you need to perform these steps in the official Red Hat documentation for Discovering and Joining Identity Domains. The domain is Windows Server 2012 R2 Active Directory. We use local UNIX users for name mappings.

Configuration Steps 3) Configuring an NFS client to use Kerberos with `realm join`.

1. Install the necessary packages:

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

2. Ensure that the DNS on the NFS client is configured to the Active Directory domain and that an A/AAAA record exists in the DNS for the Linux client. Test DNS lookups:

```
[root@centos7 /]# cat /etc/resolv.conf
# Generated by NetworkManager
search core-tme.netapp.com
nameserver 10.193.67.181

[root@centos7 /]# nslookup centos7
Server:         10.193.67.181
```

```
Address:        10.193.67.181#53

Name:   centos7.core-tme.netapp.com
Address: 10.193.67.225
```

3. Ensure that all firewall rules allow Active Directory connectivity, LDAP, Kerberos, and so on.

4. Discover the Active Directory realm:

```
# 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. Join the domain:

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

Note: All normal Windows domain rules apply: The time skew is within 5 minutes; the user account has permissions to add computer objects to a domain; and the DNS can locate domain controllers. `realm join` automatically configures SSSD to a base level and configures the Kerberos keytab files.

6. Check connectivity to the domain by performing a name lookup (this action uses SSSD for LDAP connectivity):

```
[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)
```

Note: The preceding user created a UID and GID numeric based on an algorithm in SSSD by default to approximate a user and group ID based on the SID. If you want classic UNIX user attributes, be sure to configure SSSD.

7. Run `kinit` to test Kerberos for a user:

```
[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
```

Note: As an option, you can configure `/etc/krb5.conf` with the realm information to avoid needing to append the realm to `kinit` requests.

Example:

```
[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:
```

Ensure the krb5.conf file is configured to allow only specific enctypes or that the machine account in the domain for the NFS client allows only the desired enctypes. Be sure to disallow RC4-HMAC because NetApp ONTAP does not support it.

Example of failure when using RC4-HMAC:

```
6/29/2016 16:09:56  ontap-tme-prod-03
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. When a machine account is added to Active Directory by using `realm join`, the following SPNs are added to the `krb5.keytab` file automatically:

```
[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)
```

No other SPNs should be required for the machine account. The client attempts to get a ticket by using the machine account principal (`machine$@REALM.COM`).

Therefore, a KRB to UNIX name mapping must exist for `machine`$ either locally on the SVM (a name-mapping rule or a UNIX user) or on the Active Directory object (in the form of a uidNumber/GidNumber attribute in LDAP).

Otherwise, the mount request fails with the following error:

```
6/29/2016 16:28:52  ontap-tme-prod-03
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 10.193.67.181:389 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
```

The easiest way to resolve this issue is with the local `unix-user`:

```
::*> 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. Test the `krb-unix` mapping:

```
::> set diag
::*> diag secd name-mapping show -node ontap-tme-prod-03 -vserver parisi -direction krb-unix -
name CENTOS7$@CORE-TME.NETAPP.COM
CENTOS7$@CORE-TME.NETAPP.COM maps to CENTOS7$
```

10. Ensure that the NFS `unix-user` or equivalent name mapping is in place so that the service account (`nfs/fqdn@REALM`) can authenticate:

```
::*> 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. Try to mount the SVM data interfaces with Kerberos. The SVM must already have the following created and configured:
    - Kerberos realm
    - Kerberos interfaces
    - DNS A/AAAA records in the DNS server (forward and reverse)
    - Permitted enctypes for Kerberos
    - Export policy rules on the NFS exports and parent directories that allow Kerberos

Mount example:

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

12. `su` as a different user and `kinit`. `cd` into the mount and check for your NFS service ticket:

```
[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,retran
s=2,sec=krb5,clientaddr=10.193.67.225,local_lock=none,addr=10.193.67.226)

[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
```

9 Disclaimer

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

10 Additional Resources

- TR-4067: NFS Best Practice and Implementation Guide
  www.netapp.com/us/media/tr-4067.pdf
- TR-4073: Secure Unified Authentication
  www.netapp.com/us/media/tr-4073.pdf
- TR-4379: Name Services Best Practice Guide
  www.netapp.com/us/media/tr-4379.pdf
- TR-4523: DNS Load Balancing in ONTAP
  www.netapp.com/us/media/tr-4523.pdf

11 Contact Us

Let us know how we can improve this technical report.

Contact us at docfeedback@netapp.com.

Include TECHNICAL REPORT 4616 in the subject line.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.