Using Kerberos with NFS for strong security

ONTAP 9

NetApp
March 11, 2023

Table of Contents

Using Kerberos with NFS for strong security

ONTAP support for Kerberos

Kerberos provides strong secure authentication for client/server applications. Authentication provides verification of user and process identities to a server. In the ONTAP environment, Kerberos provides authentication between storage virtual machines (SVMs) and NFS clients.

In ONTAP 9, the following Kerberos functionality is supported:

- Kerberos 5 authentication with integrity checking (krb5i)

  Krb5i uses checksums to verify the integrity of each NFS message transferred between client and server. This is useful both for security reasons (for example, to ensure that data has not been tampered with) and for data integrity reasons (for example, to prevent data corruption when using NFS over unreliable networks).

- Kerberos 5 authentication with privacy checking (krb5p)

  Krb5p uses checksums to encrypt all the traffic between client and the server. This is more secure and also incurs more load.

- 128-bit and 256-bit AES encryption

  Advanced Encryption Standard (AES) is an encryption algorithm for securing electronic data. ONTAP now supports AES with 128-bit keys (AES-128) and AES with 256-bit keys (AES-256) encryption for Kerberos for stronger security.

- SVM-level Kerberos realm configurations

  SVM administrators can now create Kerberos realm configurations at the SVM level. This means that SVM administrators no longer have to rely on the cluster administrator for Kerberos realm configuration and can create individual Kerberos realm configurations in a multi-tenancy environment.

Requirements for configuring Kerberos with NFS

Before you configure Kerberos with NFS on your system, you must verify that certain items in your network and storage environment are properly configured.

> The steps to configure your environment depend on what version and type of client operating system, domain controller, Kerberos, DNS, etc., that you are using. Documenting all these variables is beyond the scope of this document. For more information, see the respective documentation for each component.
>
> For a detailed example of how to set up ONTAP and Kerberos 5 with NFSv3 and NFSv4 in an environment using Windows Server 2008 R2 Active Directory and Linux hosts, see technical report 4073.

The following items should be configured first:

Network environment requirements

- Kerberos

  You must have a working Kerberos setup with a key distribution center (KDC), such as Windows Active Directory based Kerberos or MIT Kerberos.

  NFS servers must use `nfs` as the primary component of their machine principal.

- Directory service

  You must use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS.

- NTP

  You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

  Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

- User accounts

  Each client must have a user account in the Kerberos realm. NFS servers must use “nfs” as the primary component of their machine principal.

NFS client requirements

- NFS

  Each client must be properly configured to communicate over the network using NFSv3 or NFSv4.

  Clients must support RFC1964 and RFC2203.

- Kerberos

  Each client must be properly configured to use Kerberos authentication, including the following details:

  - Encryption for TGS communication is enabled.

    AES-256 for strongest security.

  - The most secure encryption type for TGT communication is enabled.
  - The Kerberos realm and domain are configured correctly.
  - GSS is enabled.

    When using machine credentials:

  - Do not run `gssd` with the `-n` parameter.
  - Do not run `kinit` as the root user.

- Each client must use the most recent and updated operating system version.

  This provides the best compatibility and reliability for AES encryption with Kerberos.

- DNS

  Each client must be properly configured to use DNS for correct name resolution.

- NTP

  Each client must be synchronizing with the NTP server.

- Host and domain information

  Each client's `/etc/hosts` and `/etc/resolv.conf` files must contain the correct host name and DNS information, respectively.

- Keytab files

  Each client must have a keytab file from the KDC. The realm must be in uppercase letters. The encryption type must be AES-256 for strongest security.

- Optional: For best performance, clients benefit from having at least two network interfaces: one for communicating with the local area network and one for communicating with the storage network.

Storage system requirements

- NFS license

  The storage system must have a valid NFS license installed.

- CIFS license

  The CIFS license is optional. It is only required for checking Windows credentials when using multiprotocol name mapping. It is not required in a strict UNIX-only environment.

- SVM

  You must have at least one SVM configured on the system.

- DNS on the SVM

  You must have configured DNS on each SVM.

- NFS server

  You must have configured NFS on the SVM.

- AES encryption

  For strongest security, you must configure the NFS server to allow only AES-256 encryption for Kerberos.

- SMB server

  If you are running a multiprotocol environment, you must have configured SMB on the SVM. The SMB server is required for multiprotocol name mapping.

- Volumes

  You must have a root volume and at least one data volume configured for use by the SVM.

- Root volume

  The root volume of the SVM must have the following configuration:

Name	Setting
Security style	UNIX
UID	root or ID 0
GID	root or ID 0
UNIX permissions	777

  In contrast to the root volume, data volumes can have either security style.

- UNIX groups

  The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0
pcuser	65534 (created automatically by ONTAP when you create the SVM)

- UNIX users

  The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase The first component of the NFS client user SPN is used as the user.

User name	User ID	Primary group ID	Comment
pcuser	65534	65534	Required for NFS and CIFS multiprotocol use Created and added to the pcuser group automatically by ONTAP when you create the SVM.
root	0	0	Required for mounting

The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.

- Export policies and rules

  You must have configured export policies with the necessary export rules for the root and data volumes and qtrees. If all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` , `krb5i`, or `krb5p`.

- Kerberos-UNIX name mapping

  If you want the user identified by the NFS client user SPN to have root permissions, you must create a name mapping to root.

Related information

NetApp Technical Report 4073: Secure Unified Authentication

NetApp Interoperability Matrix Tool

System administration

Logical storage management

Specify the user ID domain for NFSv4

To specify the user ID domain, you can set the `-v4-id-domain` option.

About this task

By default, ONTAP uses the NIS domain for NFSv4 user ID mapping, if one is set. If an NIS domain is not set, the DNS domain is used. You might need to set the user ID domain if, for example, you have multiple user ID domains. The domain name must match the domain configuration on the domain controller. It is not required for NFSv3.

Step

1. Enter the following command:

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

Copyright information

Trademark information