

Using Multiple Protocols

Nasuni Corporation – Boston, MA

Introduction

The Nasuni Filer provides efficient and convenient global access to your data. Nasuni's patented file system, UniFS[®], combines the performance and consistency of a traditional file system with the scalability and stability of cloud storage.

Nasuni offers a number of protocols with which to access data in the UniFS file system, including CIFS, iSCSI, NFS, and FTP protocols. You can think of these protocols as gateways to the UniFS file system. Some clients might find one protocol more useful than another protocol.

However, you might also want to provide access to the same data for several different types of clients. For this reason, the Nasuni Filer supports assigning multiple protocols to volumes of data.

This document discusses some typical scenarios requiring particular access to data, and how different combinations of protocols can help provide the access that clients need.

***Note:** You cannot enable Global Locking for a volume that has multiple protocols enabled.*

Protocols

This section discusses the protocols available for volumes on Nasuni Filers.

Original Protocols

When you create a volume on the Nasuni Filer, you have three choices for the original protocol of the volume:

- **iSCSI (Internet Small Computer System Interface):** iSCSI is an Internet Protocol (IP)-based storage networking standard for linking data storage facilities. iSCSI is a Storage Area Network (SAN) protocol. The iSCSI protocol supports the use of blocks of data.
- **CIFS (Common Internet File Service):** The CIFS protocol is typically used to provide data to clients on Microsoft Windows or OS X systems. The CIFS protocol supports the use of folders and files.
- **NFS (Network File System):** NFS is a protocol and file system for accessing and sharing files across a computer network using UNIX or Linux. The NFS protocol supports the use of folders and files.

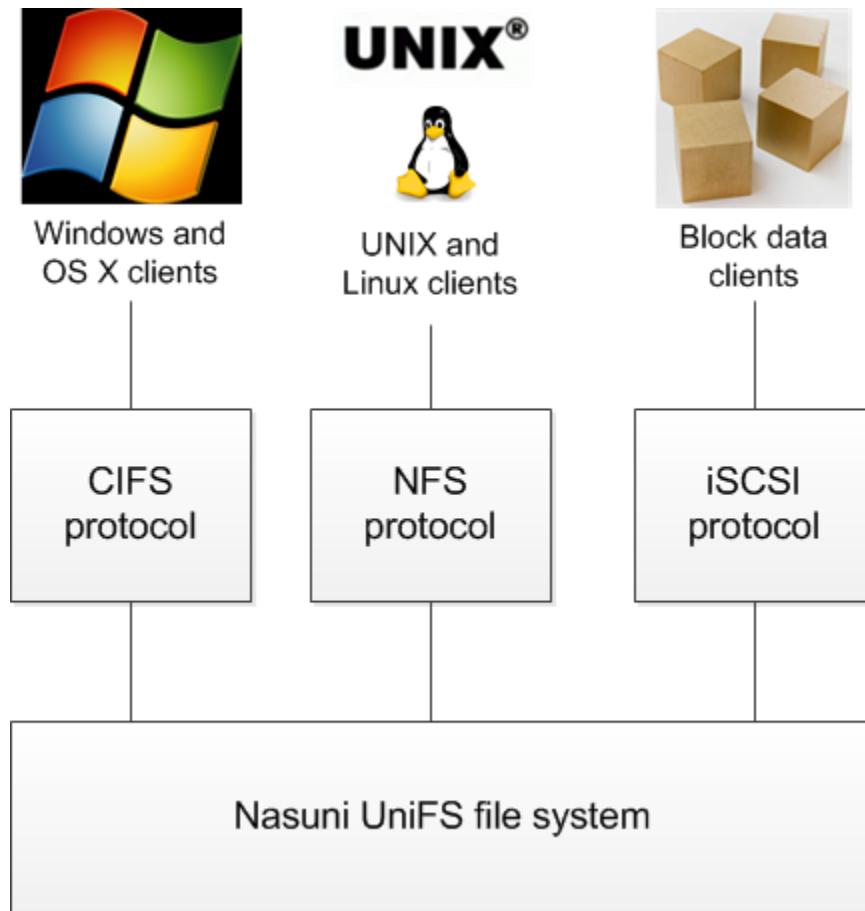


Figure 1. Original protocols available for volumes include CIFS, NFS, and iSCSI.

Enabling Additional Protocols

After you create a volume on the Nasuni Filer and select the original protocol of the volume, you can enable other protocols for the volume.

Note: You cannot enable other protocols for iSCSI volumes.

Warning: Protocols work in parallel. Enabling an additional protocol to an original protocol does not affect the original protocol. However, writing data to the volume using one protocol can affect the permissions or other metadata used by another protocol. This can inadvertently affect permissions in unexpected ways.

Warning: If you enable an additional protocol for a volume, you cannot remove that protocol.



- **FTP (File Transfer Protocol) and SFTP (SSH File Transfer Protocol or Secure File Transfer Protocol)** (for CIFS or NFS volume only): FTP is a standard network protocol to transfer files over a TCP-based network, such as the Internet. FTP clients may authenticate themselves using a username and password, but can connect anonymously if the server is configured to allow it. FTP is often used to enable contractors or other outside entities to add or retrieve data files using anonymous access. You can configure FTP directories, read-only access, visibility of FTP directories, allowed hosts, allowed users, allowed groups, and anonymous access.
- **Web Access** (for volume with CIFS enabled): A Nasuni technology that enables access to data using a Web browser.
- **Sync and Mobile Access (MA)** (for volume with CIFS enabled): A Nasuni technology that enables access to data using mobile devices, including iOS-based devices (such as iPhone and iPad) and Android phones. With Mobile Access, you can enable, disable, or delete specific mobile devices. You can also limit access to certain classes of mobile devices. With Desktop Access, you can access data by using the Nasuni Desktop Client.

Table 1. Original protocols, and available additional protocols.

Original Protocol	Additional Protocol Available	Additional Protocol Available
iSCSI	None	None
CIFS	FTP/SFTP	
CIFS	NFS	
CIFS	Web Access	
CIFS	Sync and Mobile Access	
NFS	FTP/SFTP	
NFS	CIFS	
NFS	CIFS	FTP/SFTP (enable CIFS first)
NFS	CIFS	Web Access (enable CIFS first)
NFS	CIFS	Sync and Mobile Access (enable CIFS first)

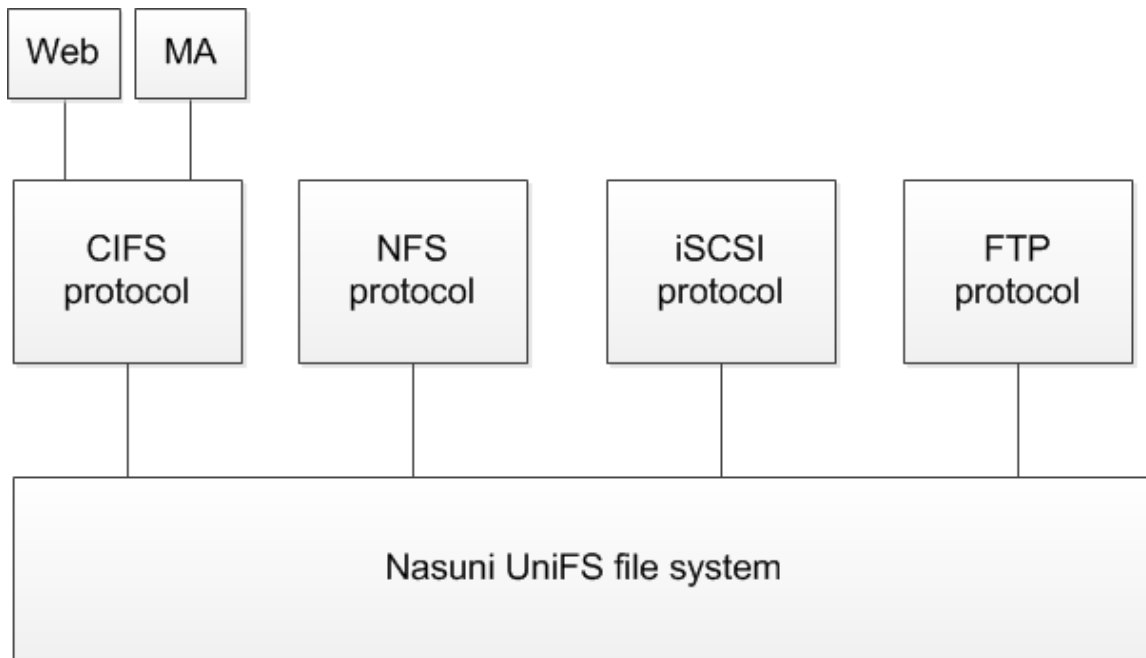


Figure 2. Additional protocols include FTP, Web Access, and Sync and Mobile Access (MA).

Volume Permissions Policies

When you enable CIFS, NFS, or FTP protocols on an original CIFS or NFS volume, you can also select a permissions policy for the volume. These volume permissions policies enable you to define volume permissions for specific situations.

- **UNIX/NFS Permissions Only Mode:** Default mode for NFS volumes. Recommended for primary or heavy NFS use. Not recommended for Windows users. Only the traditional UNIX mode bits control permissions. Windows can view permissions as access control lists (ACLs), but cannot add or remove access control entries (ACEs). Windows CIFS users can change permissions using the Security tab of the Windows Properties dialog box.
- **NTFS Compatible Mode:** Default mode for CIFS volumes on Nasuni Filers joined to Active Directory. Recommended for volumes with only CIFS protocol enabled, or for volumes with CIFS and FTP protocols enabled, but with read-only FTP or only occasional FTP writes. Not recommended for mixed protocol support when writing is enabled for all protocols. Full NTFS permissions as supported on CIFS/SMB. Windows clients obey inheritance rules. NFS and FTP protocols cannot see all NTFS permissions and do not obey all access rules in NTFS permissions. NFS and FTP protocols obey only the POSIX access control list (ACL) component of inheritance rules.



- **POSIX Mixed Mode:** Recommended for combined CIFS and FTP volumes, with light NFS use. Also recommended for CIFS-only volumes with Linux or Mac clients, with UNIX extensions enabled. Access control lists (ACLs) are supported entirely through POSIX ACLs. Windows clients receive mapping of POSIX ACLs to NTFS ACLs. However, the mappings are not as complete as mappings done for NTFS Compatible Mode. Not all NFS clients can view the ACLs.
- **Unauthenticated Access Mode:** Default mode for CIFS volumes on Nasuni Filers that are not joined to Active Directory. Recommended for CIFS Public-mode volumes. For CIFS clients, this mode acts as an open share. For all other protocols, this mode acts identically to POSIX Mixed Mode.

Using Protocols

This section discusses the recommended protocols for volumes on Nasuni Filers, based on the type of client access desired.

Single-Client-Type Scenarios

If you are providing access for only a single type of client, your choices are simple:

- **Block data clients only:** Create the volume with the iSCSI protocol.
- **Microsoft Windows clients only:** Create the volume with the CIFS protocol.
- **OS X clients only:** Create the volume with the CIFS protocol.
- **UNIX or Linux clients only:** Create the volume with the NFS protocol.
- **FTP clients only:** Create the volume with the CIFS protocol, and then enable the FTP protocol for the volume.
- **Web-based clients only:** Create the volume with the CIFS protocol, and then enable Web Access for the volume.
- **Mobile device clients only:** Create the volume with the CIFS protocol, and then enable Sync and Mobile Access for the volume.
- **Nasuni Desktop Clients only:** Create the volume with the CIFS protocol, and then enable Sync and Mobile Access for the volume.



Multiple-Client-Type Scenarios

If you are providing access for multiple types of client, you can combine multiple protocols.

Mostly Microsoft Windows or OS X clients

If you are providing access mainly for Microsoft Windows or OS X clients, plus some additional different clients, you have several options:

- **Mostly Microsoft Windows or OS X clients, plus FTP clients:** Create the volume with the CIFS protocol, then enable the FTP protocol for the volume. If FTP access is solely for reading data, select the NTFS Compatible Mode of volume permissions policy. However, if FTP clients are writing data extensively, select the POSIX Mixed Mode of volume permissions policy. In this case, Windows clients receive mappings of POSIX ACLs to NTFS ACLs. However, the mappings are not as complete as mappings done with NTFS Compatible Mode.
- **Mostly Microsoft Windows or OS X clients, plus UNIX or Linux clients:** Create the volume with the CIFS protocol, then enable the NFS protocol for the volume. Select the POSIX Mixed Mode of volume permissions policy. Access control lists (ACLs) are supported entirely through POSIX ACLs. Windows clients receive mappings of POSIX ACLs to NTFS ACLs. However, the mappings are not as complete as mappings done for NTFS Compatible Mode. Not all NFS clients can view the ACLs.

Mostly UNIX or Linux clients

If you are providing access mainly for UNIX or Linux clients, plus some additional different clients, you have several options:

- **Mostly UNIX or Linux clients, plus FTP clients:** Create the volume with the NFS protocol, then enable the FTP protocol for the volume. Select the UNIX/NFS Permissions Only Mode of volume permissions policy.
- **Mostly UNIX or Linux clients, plus Microsoft Windows or OS X clients:** Create the volume with the NFS protocol, then enable the CIFS protocol for the volume. Select the UNIX/NFS Permissions Only Mode of volume permissions policy. Windows can view permissions as access control lists (ACLs), but cannot add or remove access control entries (ACEs). Windows CIFS users can change permissions using the Security tab of the Windows Properties dialog box.
- **Mostly UNIX or Linux clients, plus Web access clients:** Create the volume with the NFS protocol, and then enable the CIFS protocol for the volume, as described above. After CIFS is enabled, then enable Web Access for the volume.
- **Mostly UNIX or Linux clients, plus mobile device clients or Nasuni Desktop Clients:** Create the volume with the NFS protocol, and then enable the CIFS protocol for the volume, as described above. After CIFS is enabled, then enable Sync and Mobile Access for the volume.



Troubleshooting

If you have any questions about original or added protocols for your volume, contact Nasuni Technical Support.

PHONE: 1.857.444.8500 / 1.800.208.3418

EMAIL: support@nasuni.com

WEB: <https://www.nasuni.com/support/>

Copyright © 2010-2018 Nasuni Corporation. All rights reserved.