CIFS INTEROPERABILITY TESTS FOR CISCO WAFS AND NETAPP STORAGE SYSTEMS

Network Appliance, Inc.

October 2005, TR-3427

TABLE OF CONTENTS

TABLE OF FIGURES

1. INTRODUCTION

This technical document provides an overview of how Cisco Wide Area File Services (WAFS) and NetApp fabric attached storage (FAS) technologies interoperate. The data management functionalities of NetApp storage systems were tested in the presence of Cisco WAFS. The users benefit from the LAN-speed environment provided by Cisco WAFS at the branch office while continuing to take advantage of the robust storage management capabilities offered by NetApp storage products in the data center. Note that although Cisco WAFS supports both NFS and CIFS caching, the interoperability tests in this paper were performed only for CIFS.

2. THE CHALLENGES

Enterprises that support regional and branch locations face a constant challenge ensuring reliable data service at remote sites. From the storage perspective, backup and disaster recovery procedures are often inconsistent, unreliable, or—even worse—nonexistent. Lack of skilled personnel, limited IT budgets, inconsistent policies, and inability to verify data management and protection may contribute to the problem, with potentially disastrous consequences for remote sites and the enterprise as a whole. IT also wants to enforce data retention policies to comply with regulatory directive or legal risk mitigation initiatives. From the network perspective, businesses need to provide LAN-speed access to enterprise applications for remote employees. In addition, IT desires to centralize media and web applications. How to overcome the key barriers such as bandwidth limitation, link latency and throughput, bandwidth management, and prioritization to achieve higher application performance has become a critical issue in the industry.

The combination of Cisco WAFS with NetApp storage solutions addresses the networking requirements as well as the storage and compliance requirements for data. The ease of storage management is further extended beyond the data center to remote locations with speedy and reliable access to the data.

3. SOLUTION OVERVIEW

A deployment combining Cisco WAFS and NetApp NAS facilitates an environment in which centralized NAS storage, accessed remotely, performs as if it were on the local LAN. In addition to the performance benefits, the savings in reduced WAN costs and remote storage management can be considerable and include the following:

- Uniform, simplified, and centralized backups—higher level of protection of edge data, performed by skilled IT personnel with data center quality backup software applications and NetApp features such as Snapshot™ and SnapRestore®
- Simplified compliance with regulations or data retention mandates for remote office data through LockVault™ or SnapLock®
- Increased data availability and management
- Fast global access—LAN-like access and collaboration on centralized data from any site in the enterprise
- Reduced administration—centrally managed file services such as usage quota, backups, restores, access control, security policies, etc.

Figure 1 below shows the deployment architecture of NetApp storage systems in a Cisco WAFS environment. The Cisco Edge Wide-area Application Engine (WAE) is deployed at each branch office or remote campus, replacing file and print servers and providing fast, near-LAN read and write access to the

data center file storage. Any change or modification made in the WAFS Central Manager is distributed to the Edge WAEs. The Core WAE can also be configured as a clustered pair for high availability. At the data center, the Core WAE interfaces with one or more NetApp FAS systems and provides aggregation for Edge WAEs into the centralized storage through the WAN-optimized transport mechanism. The consolidated data from the remote offices is stored in the data center either on a NetApp FAS appliance or on the SAN accessed through the NetApp V-Series product family. The NetApp award-winning storage management tools, such as Snapshot and SnapVault® offer simple, powerful data protection solutions that deliver consolidated and simplified backup operations, high availability, and—in case of disruption—rapid and complete data recovery. NetApp LockVault software integrates NetApp SnapLock and NetApp SnapVault technologies to create the only solution specifically designed to address regulatory compliance requirements for unstructured data. NetApp solutions are proven, easy to manage, and scalable and deliver a low cost of ownership.

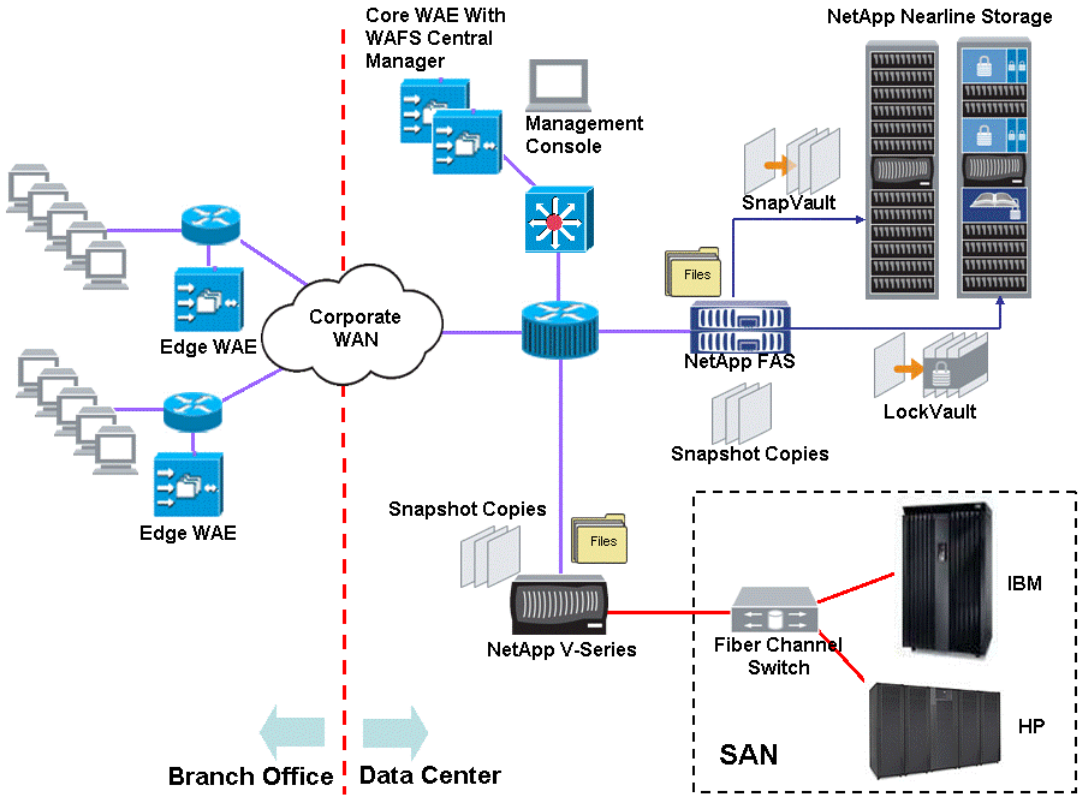

Figure 1) NetApp and Cisco WAFS development solution.

4. INTEROPERABILITY TESTS

4.1 TEST CONFIGURATIONS

In the simulated data center (see Figure 2 below), a Core WAE interfaces with NetApp FAS system, while an Edge WAE was deployed at the branch office to provide local data access through CIFS. A Windows® 2003 domain controller (DC) is used at the data center to provide services for domain authentication, virus scanning and distributed file system (DFS). A NetApp FAS cluster (running Data ONTAP™ 7G with failover support enabled) is used to provide Windows file services for the branch office. Between the data center and branch office, a BSD-based WAN simulator is used to generate desired latency and bandwidth throughput. In the test, a typical T1 line with a bandwidth of 1.544 Mbps and a transoceanic latency of 140 milliseconds (round trip) with a packet loss ratio of 0.01 was simulated.

Several interoperability tests were performed based on the configuration described above. They are discussed separately below.

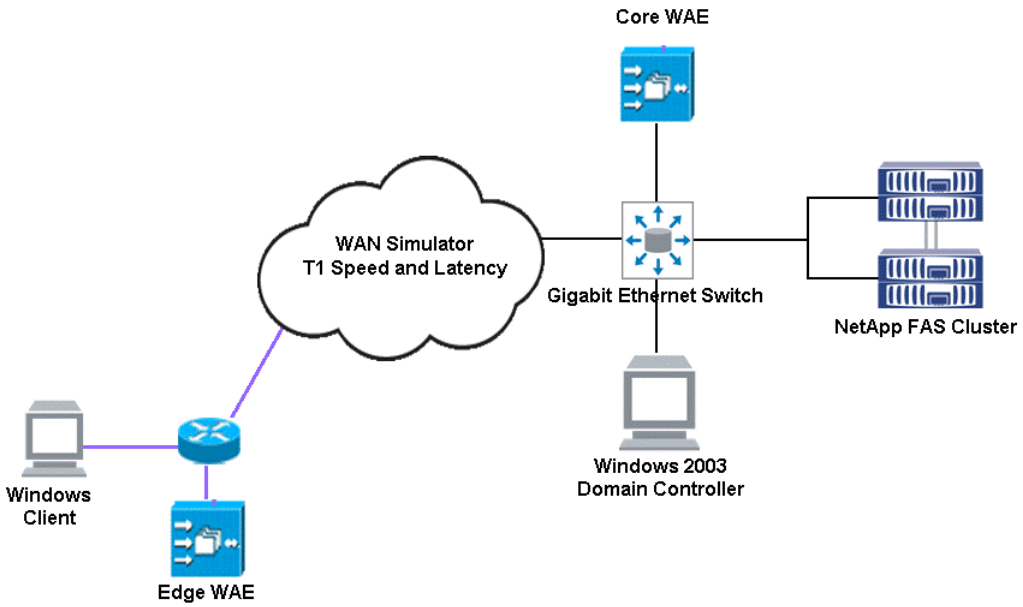

Figure 2 Interoperability test configuration.

4.2 SNAPSHOT COPIES

System administrators use Snapshot copies to facilitate frequent, low-impact, user-recoverable backups of files, directory hierarchies, LUNs, and/or application data.

During the test, the option `cifs.show_snapshot` was enabled on the filer to let the users view and access the content of the `~snapshot` folder after a Snapshot copy was created at the data center. As expected, the newly created Snapshot copy was immediately available at the branch site for the Windows client. The remote user could then readily go into the `~snapshot` folder to retrieve the previous copy of a corrupted or lost file.

4.3 CIFS HOME DIRECTORY

NetApp Data ONTAP software offers the flexibility of assigning a user's home directory to a predefined location in the storage space. In the test, we created a qtree `/vol/vol1/ntfs` on filer `jeckle` and then shared it using the following command:

```
cifs shares –add ntfs /vol/vol1/ntfs
```

In `/etc/cifs_homedir.cfg`, we then inserted the following qtree path, which was intended as storage for home directories:

```
/vol/vol1/ntfs
```

The home directory storage creation then took effect using the `cifs homedir load` command. We associated a branch office user `wafs` to his or her home directory by creating a folder with appropriate access permissions in qtree `/vol/vol1/ntfs` called `wafs`. As soon as user `wafs` logs into the domain, the filer automatically finds the home directory with the same user name and gives him or her full access to the home folder.

Suppose that the suffix `wafs` is used in the Cisco WAFS central management GUI to create the alias at the branch office for the original filer as described in Figure 3 below. The UNC path to the home directory at the branch office automatically defaults to `\\jeckle-wafs\~wafs` and physically resides in `\\jeckle-wafs\ntfs`. See Figure 4 below. The `\\jeckle-wafs\~wafs` UNC path can be used in a Windows login script for user `wafs`.

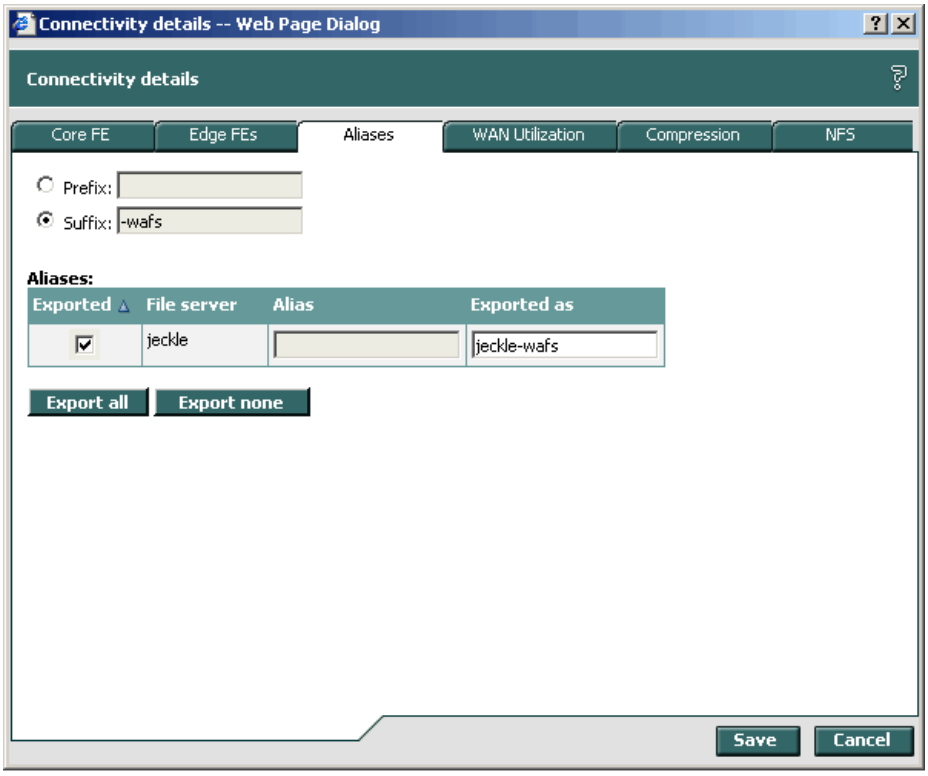

Figure 3) Creating aliases for file server using WAFS central management GUI.

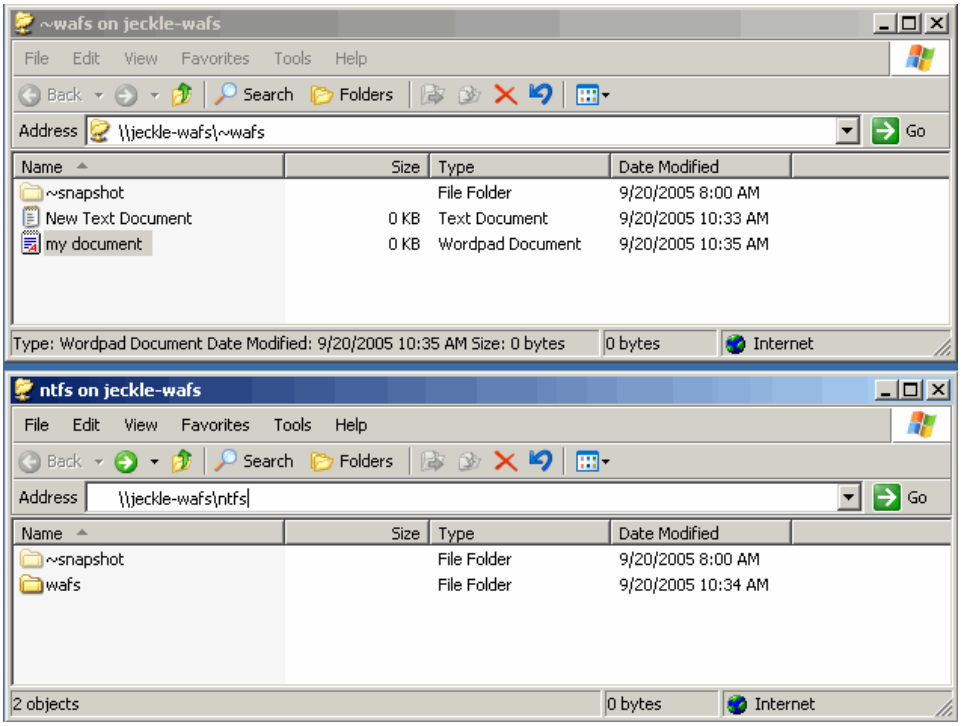

Figure 4) CIFS home directory for remote User `wafs`.

4.4 Antivirus

NetApp works with third-party antivirus software vendors to provide complete virus scanning solutions to customers. In the test, Symantec AntiVirus for NetApp Filers Version 4.0 was used for virus scanning. It is installed on the Windows 2003 DC to accept the files forwarded by the NetApp FAS through remote-procedure calls (RPCs). The vscan command enables the virus scanning service and verifies that the setup is correct and ready to scan files.

```
jeckle> vscan on
jeckle> vscan
Virus scanners(IP and Name)      P/S Connect time (dd:hh:mm) Reqs Fails
---------------------------------------------------------------------
10.32.88.203 \\DC1 Pri 05:23:15 2 0

List of extensions to scan:

??_,ARJ,ASP,BAT,BIN,CAB,CDR,CL?,COM,CSC,DL?,DOC,DOT,DRV,EML,EXE,GMS,GZ?,HLP,HT?,
IM?,INI,JS?,LZH,MD?,MPP,MPT,MSG,MSO,OCX,OFT,OLE,OV?,PIF,POT,PP?,RAR,RTF,SCR,SHS,
SMM,SWF,SYS,TXT,VBS,VS?,VXD,WBK,WPD,XL?,XML

List of extensions not to scan:
 Extensions-not-to-scan list is empty.

Number of files scanned: 340
Number of scan failures: 0
```

An infected file at the branch office was then dropped into the `\\jeckle-wafs\ntfs` folder. It was immediately detected and removed by the antivirus software. The following message on the filer console captured the event:

```
Mon Sep 19 15:35:06 PDT [vscan.virus.created:ALERT]: CIFS: Possible Virus
Detected - File ONTAP_ADMIN$\vol\vol1\ntfs\eicar.txt in share ntfs modified by
client 10.32.88.202 (TX5880) running as user administrator may be infected. The
filer received status message Infection found, repair failed and error code
[0x5] from vscan (anti-virus) server 10.32.88.203.
```

4.5 CLUSTERED FAILOVER (CFO)

NetApp cluster storage systems guarantee 99.999% uptime with the clustered failover function built into Data ONTAP software. It usually takes less than 60 seconds for clustered failover to complete in NetApp FAS systems when one of the heads becomes unavailable. This time is well within the 95 second tolerance window in Cisco WAFS where the branch office user maybe in the middle of editing a file (no saving or opening file activities occur) without noticing the filer being disconnected. During the test, one of the NetApp FAS cluster nodes was purposely brought down, and the takeover was completed within a minute without causing any disruption to the remote user. Note that if the client is in midwrite (final close) during failover, the session will hang through the disconnection period, and the remote user will be notified that the network drive is no longer online. No data will be lost on the filer. The user will be prompted to save to an alternative location.

4.6 DISTRIBUTED FILE SYSTEMS (DFS)

In order to test the interoperability of Cisco WAFS and NetApp FAS on DFS, we created a DFS root on the domain controller (`\\dc1.example.com\dfs`) and a link pointing to two storage targets `\\jeckle\ntfs` and `\\jeckle-wafs\ntfs` at the data center and branch office respectively as shown in Figure 5 below. Note that the file replication service (FRS) between these two targets was not enabled because they are essentially the same, i.e., `\\jeckle-wafs\ntfs` at the branch office is simply a mirrored version of `\\jeckle\ntfs` at the data center.

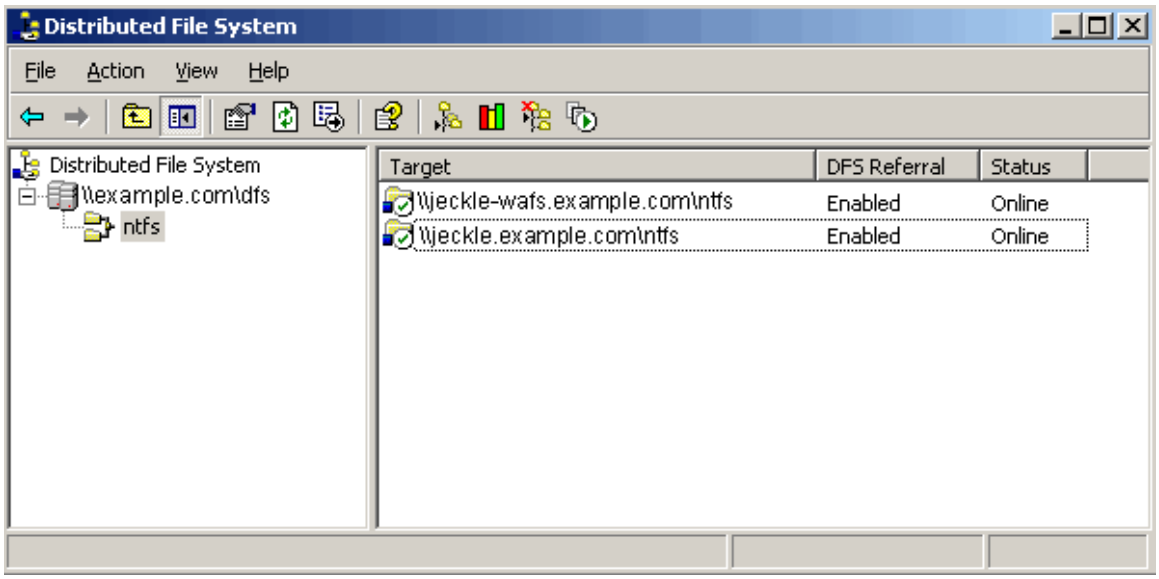

Figure 5) DFS configuration with WAFS.

We also created two Active Directory (AD) sites to capture the two physical subnets in data center and branch office as shown in Figure 6 below. An AD site is a set of IP subnets connected with fast, reliable connectivity. AD servers and clients use the site topology of a forest to route query and replication traffic efficiently. In our case, 10.32.88/24 at the data center and 192.168.0/24 at the branch office are two fast LANs connected by a less reliable WAN with lower traffic throughput.

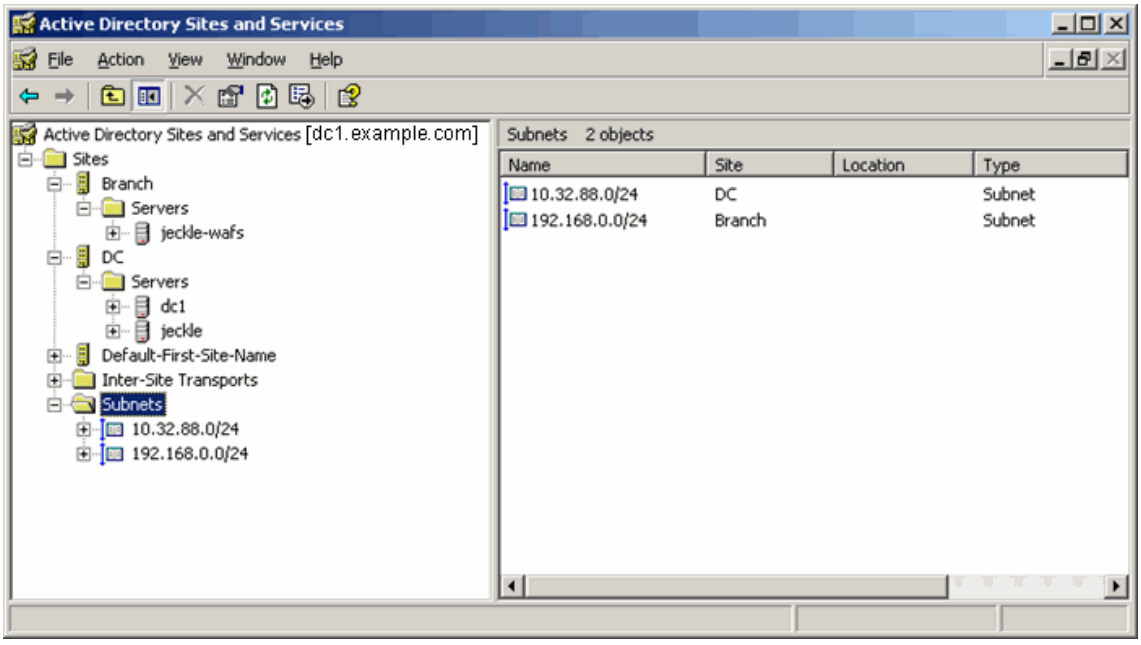

Figure 6) Active Directory sites with WAFS.

As expected, at the branch office, when the domain-based DFS path `\\example.com\dfs\ntfs` is opened, it correctly shows the desired content stored in the storage target on the filer as defined in Figure 5 above. See Figure 7 below.

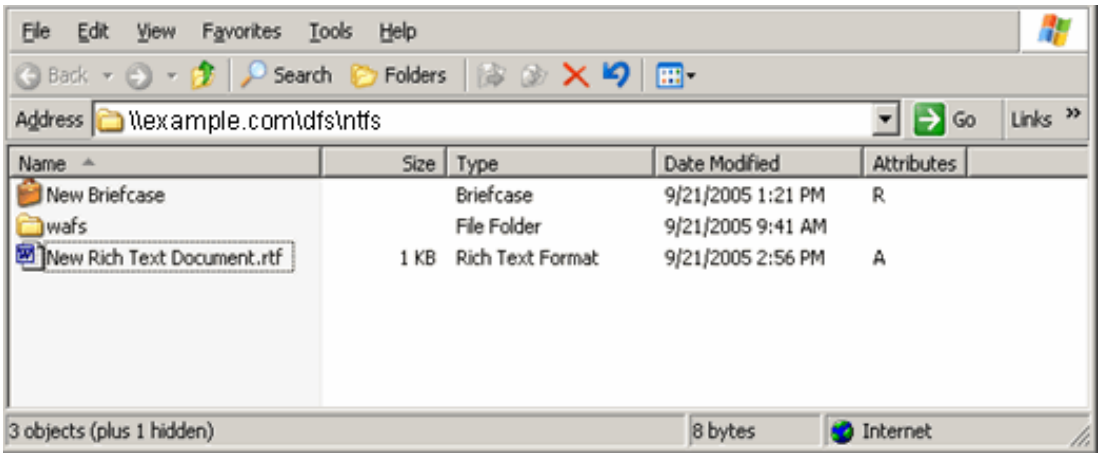

Figure 7) Opening domain-based DFS path at branch office.

4.7 SnapLock and LockVault for Regulatory Compliance

SnapLock and LockVault offer a complete solution to customers whose data has to meet certain retention and regulatory compliance requirements.

SnapLock

In the test, we created a qtree snaplock in a SnapLock volume `/vol/sl_ntfs` and shared it to the branch office as `\\jeckle-wafs\accounting`. We then created a file `payroll.txt` in the share and it was committed to a SnapLock state by changing the attribute to Read-only. We then tried deleting the file and as expected, the attempt failed. See Figures 8 and 9 below.

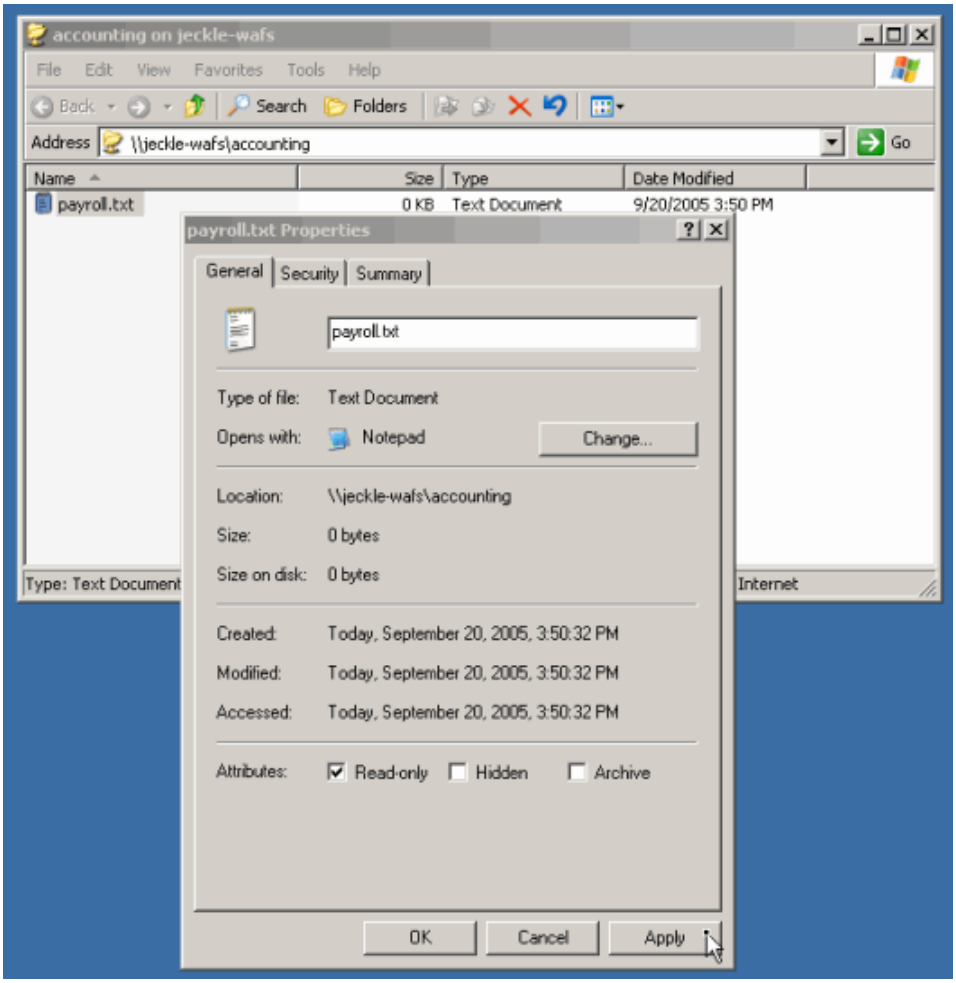

Figure 8) Committing file to SnapLock state.

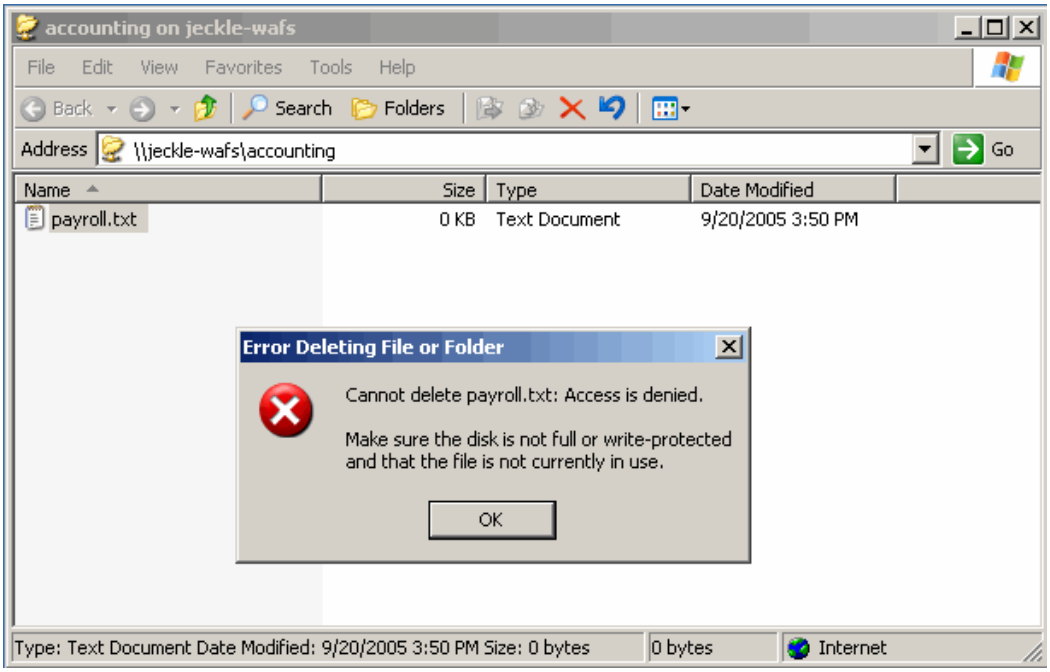

Figure 9) Access denied while deleting a SnapLock file.

Retention Period

We then modified the access time of `payroll.txt` to a future time. And when that time passed, we were able to delete `payroll.txt` to reclaim storage space as its retention period (up to the future time) was expired. This test procedure verified the SnapLock interoperability between Cisco WAFS and NetApp storage system.

LockVault

In principal, LockVault uses SnapVault to replicate unstructured data (e.g., Word, PDF, and Excel documents) from the primary to the secondary NetApp FAS storage system with SnapLock enabled to meet regulatory compliance requirements. Storage administrators may want to consider LockVault for protecting unstructured data in a two-tired storage architecture at the data center (see Figure 1 above).

4.8 OFFLINE FOLDERS AND WAFS

NetApp Data ONTAP software provides the offline folders option required by mobile Windows clients. First we opened the `\\jeckle-wafs\ntfs` share at the branch office, then we enabled the offline folder option by going to the Tools tab in Windows Explorer. We then selected Folder Options in the drop-down menu, clicked the `Offline Files` tab and clicked OK. See Figure 10 below.

Once the offline folders option was enabled, we right-clicked on a folder in the share and selected Make Available Offline. The content in the folder was then synchronized with the filer and a  sign appeared on the icon of the folder. See Figure 11 below.

The mobile Windows client can then be taken offline and the user is still able to work on the files in the locally cached folder.

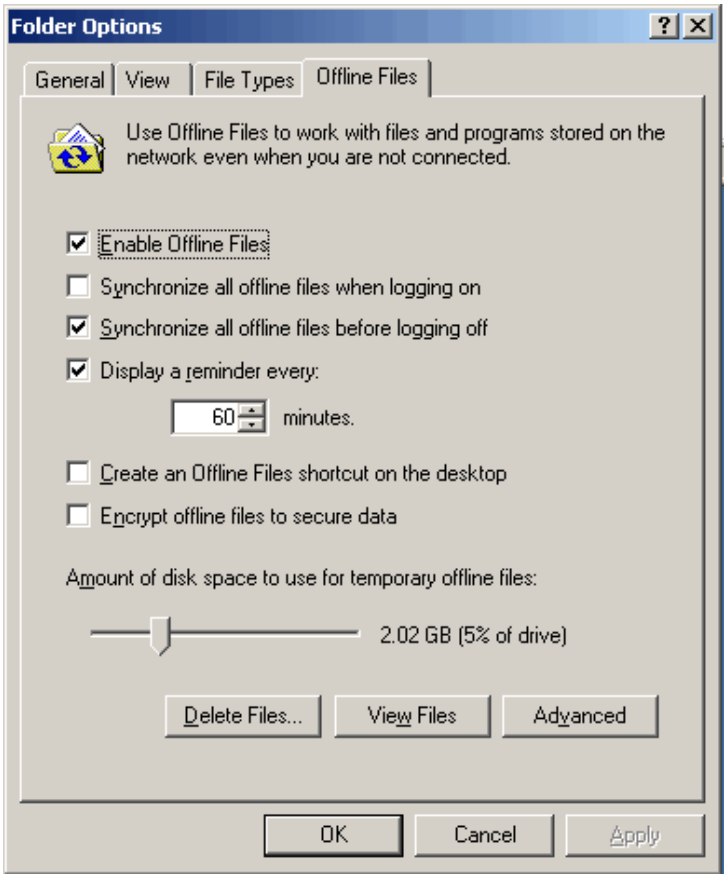

Figure 10) Enabling the offline folders option.

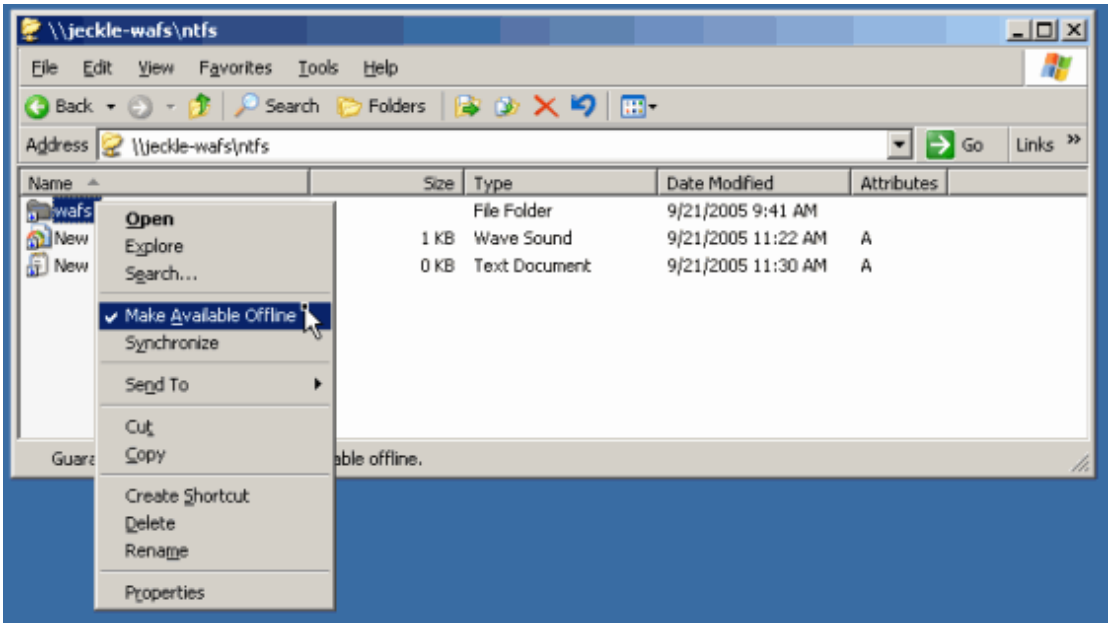

Figure 11) Synchronizing offline folders.

5. CONCLUSION

Our tests show that Cisco WAFS and NetApp storage systems interoperate flawlessly and give us a high level of confidence in the integration of the two technologies. The integration provides customers with a compelling end-to-end storage consolidation and compliance solution for the distributed enterprise. These technologies significantly lower the TCO by reducing server proliferation and storage administration costs, simplifying compliance with regulatory mandates, and eliminating remote office backups. The end result is a solution that enables cost-effective compliance with regulations or retention mandates, while delivering near-LAN read and write performance across the WAN and providing a very fast investment payback period—typically less than six months.