WHITE PAPER

Acronis®

How Microsoft® DFS Home Directories Work with ExtremeZ-IP®

A Technical Best Practices Whitepaper

Microsoft® DFS and Home Directories

Home directories are defined to be either portable home directories or network home directories. Both store users' home directory folders on a network file server, but portable home directories perform a file synchronization either on a timed value or at login & logout to bring the user's files locally to the machine while they work for faster access. Conversely with network home directories the user works directly off of the network mount all the time.

The user's home directory is stored as an attribute of their profile in Active Directory. When they log on to a computer, this attribute is read and used by the computer to locate and mount their home directory.

Many organizations use DFS to host user home directories in order to gain redundancy (when the home directory data is replicated across two or more servers), scalability (when users are load balanced across replicated servers), and administrative flexibility (where volumes can be moved between machines without having to change the location of the user's home directory in Active Directory).

However, Mac® OS X does not have built-in support for DFS, so integrating Macs into a DFS infrastructure has been challenging. In other instances organizations have deferred implementation of DFS until they could achieve Mac support.

Microsoft® DFS Background

Microsoft Distributed File System (DFS) is a powerful set of technologies used to present a single virtual namespace to a collection of file servers and manage replication of data between those servers. Microsoft DFS consists of two technologies:

- DFS Replication (DFS-R): which provides facilities for replicating file server data between locations and servers.
- DFS Namespaces (DFS-N): which allows administrators to group file server shares on disparate machines into a single virtual namespace so end users can access files without needing to know exactly where the files are located.

In addition to providing end users with a simplified, single view of the file sharing namespace, the key business benefits of using DFS are:

- Flexible Provizioning: DFS provides administrators the ability to relocate a sharepoint to another server without having to change the network path used by clients to connect to the share. This provides IT staff flexibility to optimise server configuration and re-provizion storage without having change user's workflows.
- High Availability: Uptime guarantees and Service Level Agreements (SLAs) can be achieved using DFS when combined with file system replication (DFSR). If one file server goes down, then DFS can redirect users to an alternative target file server with minimal interruption.
- Optimized WAN Performance: When file shares are replicated between servers in different locations, DFS site costing allows users to be directed to the file server closest to them. This prevents excessive traffic from going over the corporate WAN, and improves user productivity by giving them fast access times since the data is local.

Background

In this example, we will be describing how the logon process works for a user named "Tom" with a home directory with the UNC path of: \\GLILABS\DFSHOMES\SALES\TOM

Here GLILABS\DFSHOMES is the name of the DFS namespace that hosts the DFS home directories. The DFS root is "DFSHOMES".

An important note - GLILABS is not an actual server on the network. Windows computers can detect this is a DFS namespace and do the proper work behind the scenes to find the user's home directories. But Mac computers cannot naturally resolve this UNC path since it doesn't map directly to a server. This will be addressed in the example below.

High Level Configuration

In this example we will be referring to three computers that have the following setup:

Mac Client:
This is a Mac OS X 10.5 ("Leopard") or later Mac which is bound to Active Directory where the user will be logging on to access their home directory. This Mac has the ExtremeZ-IP DFS client installed and configured.

Please Note - Due to changes made in Mac OS X 10.7 ("Lion"), DFS home directories are not supported by ExtremeZ-IP as of OS X 10.7.0.

A fix for this issue is currently under investigation.

EZDFS:
This is an ExtremeZ-IP® 7.0 server that is acting as the virtual DFS server for Mac clients. It does not have to be running on the same server that is hosting the Windows DFS service.

EZTarget:
This is another ExtremeZ-IP server that contains the home directory folders for user "Tom". This is where Windows and Macintosh clients will be redirected during the logon process.

In order to simplify this description, we are explicitly leaving the following, more advanced configurations out, but they can all be supported with ExtremeZ-IP 7.0:

- Support for redundancy / failover of the DFS virtual root server
- Support for redundancy / scalability / failover of the targets servers containing the home directories
- Support for SMB-based targets

Detailed Configuration

Below is a more detailed description of the configuration of each of the servers in this example. This section also describes how the components work to enable DFS support in the Mac.

EZTARGET Server
This server is located at EZTARGET.GLILABS.COM
It contains a volume called "Sales", which is a DFS target in the DFS Namespace.

EZDFS Server
This server is located at EZDFS.GLILABS.COM
Its root volume is called "GLILABS".

> Autofs
> ExtremeZ-IP's DFS implementation leverages a capability of Mac OS X 10.5 and later called "autofs". Autofs allows a directory on the local Mac to be redirected to a remote server that is automatically mounted only when that local directory is accessed. For example, if the directory "/AnotherServer" was configured in autofs to map to "afp://anotherserver.glilabs.com", then when the Mac navigates to "/AnotherServer", autofs will automatically mount the server into this location seamlessly to the end user. The autofs configuration is stored in something called an autofs map file.

Inside the root volume on the EZDFS server is another (nested) share called "DFSHOMES". This share will be configured in ExtremeZ-IP as a DFS volume to host the DFS namespace for the home directories. This nested share approach is required in order to allow the Mac to properly traverse the UNC path of the user's home directory.
The DFSHOMES share includes a dynamically generated autofs map file that is used in mapping all of the DFS targets to their respective target file servers. This map file describes how individual folders in a specific local directory on the Mac ("/DFSHOMES") can map to target servers. In the case of this example, the map file will say:

```
DFSHomes \

            /Sales -fstype=afp afp://eztarget.glilabs.com/Sales
```

i.e., in /DFSHOMES, map /SALES to an AFP connection to the server EZTarget, volume "Sales". This means if a user accesses /DFSHOMES/SALES on their local Mac, the Sales volume of EZTarget server will automatically be mounted at /DFSHOMES/SALES.

Finally in the DFSHOMES root volume of ExtremeZ-IP, there are symlink files for each DFS target in the autofs map.

Symlinks tell the Mac that when a user accesses the symlink, they should be redirected to another location in the file system. This means that there is a symlink on the ExtremeZ-IP server for Sales, which points to the Mac's local file system as "/DFSHOMES/SALES".

If the reader has followed this description, the following behavior is now enabled: When the Mac navigates the UNC path for the user's home directory, it will connect to the DFSHOMES volume of the EZDFS server. It will then navigate to the SALES symlink which refers to /DFSHOMES/SALES on their local Mac. Because of the autofs map file, this automounts the appropriate file server target for the user's home directory.

Mac Client

Two key topics have not been described – how the autofs map configuration got to the Mac, and how the Mac found the ExtremeZ-IP DFS server to begin with from the UNC path for the home directory.

Because the home directory is mounted at login, the autofs map configuration needs to be performed before the user actually logs onto the Mac – this way when the login process runs the necessary information is available for mounting the home directory.

Additionally, because DFS home directory UNC paths do not actually refer to a real server (in fact that server in the UNC path does not exist), the Mac needs to be directed to the appropriate location when it tries to break open the UNC path.

To accomplish this, ExtremeZ-IP 7.0 provides a set of client-side scripts which can be installed or imaged / pushed to the Mac by an administrator.

A key configuration file called "dfsservers.conf" is placed in the /etc directory of the Mac which lists all of the ExtremeZ-IP DFS servers that can be used in the logon process. This is used to help identify the ExtremeZ-IP DFS server to use, and can deal with redundancy / failover in case an ExtremeZ-IP DFS server is down.

The startup script uses this information to contact a running ExtremeZ-IP DFS server to download and update the latest autofs map configuration described above. This is performed using a web service call to the ExtremeZ-IP server. Next, the Mac's hosts file is updated to map the DFS root server name that will appear in the UNC path for the user's home directory to the active ExtremeZ-IP server.

Finally a logout script is configured to run when the Mac user logs out to unmount their DFS volumes.

Step-by-Step

This section will tie all of the pieces described above together to detail the process of a Mac user logging in to access their DFS-based home directory.

1. Mac starts up and the ExtremeZ-IP dfsclient script runs automatically
    a. The list of potential servers is retrieved from /etc/dfsservers.conf
    b. The dfsclient determines which server is available and should be used for DFS operations
    c. The latest autofs map file for that DFS server is downloaded & installed/updated on the local Mac
    d. Note: this script is configured to subsequently run periodically at 5 minute intervals to keep the information current

2. The user “Tom” logs into the Mac
   a. The built-in Active Directory plug-in verifies Tom’s credentials and gets his Kerberos ticket
   b. The built-in Active Directory plug-in retrieves Tom’s home directory UNC path as \\GLILABS\DFSHOMES\SALES TOM

3. The Mac is now going to attempt to mount the home directory at this UNC path
   a. \\GLILABS will be resolved from the hosts file to EZDFS.glilabs.com
   b. The Mac will connect to EZDFS.glilabs.com and mount the volume “DFSHOMES”
   c. The Mac will navigate to the Sales portion of the UNC Path. On the ExtremeZ-IP server, this is a symlink that points to the Mac’s local file system as “/DFSHOMES/ SALES”
   d. When the Mac hits this local directory, the autofs component in the Mac will use the autofs map downloaded above to auto-mount the server EZTARGET.glilabs.com and volume Sales. This will use Tom’s Kerberos ticket for credentials
   e. The Mac will then navigate to the directory Tom on the EZTARGET/Sales server and use this for his home directory

Conclusion

This document described how DFS home directories can be used on a Mac with the new capabilities of ExtremeZ-IP 7.0.

By leveraging ExtremeZ-IP, administrators can provide Macs direct access to the DFS infrastructure for portable and network home directories. Administrators can gain the benefits of an Active Directory home profile configuration, as well as the reliability, redundancy, scalability and flexibility afforded by using Microsoft’s DFS.

About Acronis®

Acronis® is leading the next wave of data availability, accessibility and protection solutions to simplify today’s complex IT environments. Acronis technology enables organizations of all sizes to manage the always-on anywhere data access demands of users, reducing risk against the loss of valuable corporate data, and controlling management and storage costs. With proven technology for data migration and disaster recovery for physical, virtual and cloud environments, and secure enterprise file-sharing and synchronization regardless of type or platform, Acronis is enabling organizations to embrace new IT strategies and options such as BYOD and Mac in the enterprise. For additional information, please visit www.acronis.com. Follow Acronis on Twitter: http://twitter.com/acronis.

For additional information please visit http://www.acronis.com

To purchase Acronis products, visit www.acronis.com or search online for an authorized reseller.

Acronis office details can be found at http://www.acronis.com/company/worldwide.html