



WHITE PAPER

Home Directories on Snap Server® GuardianOS®

Introduction

Home directories have become commonplace in today's corporate computing environments. Home directories present a central location for all end user data that can be centrally backed up and accessed.

In a networked environment, dependence on vital corporate data residing on end users' local hard disks is very risky. Implementing and maintaining backups of that data can be a significant challenge, especially when proper backup relies on end users saving their data in a prescribed folder hierarchy. For remote laptop users, backing up local data may be the only viable option – but for users with workstations connected directly to the corporate LAN or even via a VPN, centralizing and consolidating user data in a single repository is a much better solution to the need to protect corporate assets.

Because Snap Servers support heterogeneous file sharing for Windows (CIFS/SMB), UNIX (NFS), Apple (AFP), HTTP, and FTP, end users need a way to seamlessly access their data without restructuring their entire storage infrastructure or access methods. The new Home Directory feature introduced in GuardianOS 5.0 does just that, with a robust and flexible Home Directory implementation that is available for all client types.

What are Home Directories?

A Home Directory is a directory in a central location that contains the personal files of a particular user. Separating user data from system-wide data avoids redundancy and makes backups of important files relatively simple. Also, virus threats and worms running as a specific user will be limited by that user's privileges and will likely only be able to affect the files to which that user has access, thus protecting the rest of the data in a corporate network. The Home Directories feature on GuardianOS-powered Snap Servers creates a private directory in a specific location for every user that accesses the system.

Enabling Home Directories on a Snap Server

Taking advantage of the Home Directory feature is done by enabling Home Directories from the *Security > Home Directories* page in the Web Browser Administration Tool. From this screen, administrators can select which volume to use and create a Home Directory root (the top-level folder, which contains the Home Directory for each Local and Windows Domain user). Administrators can also specify which network access protocols for which to enable the Home Directory feature: Windows (SMB), Linux/UNIX (NFS), Apple (AFP), Web View (HTTP/HTTPS), and FTP.

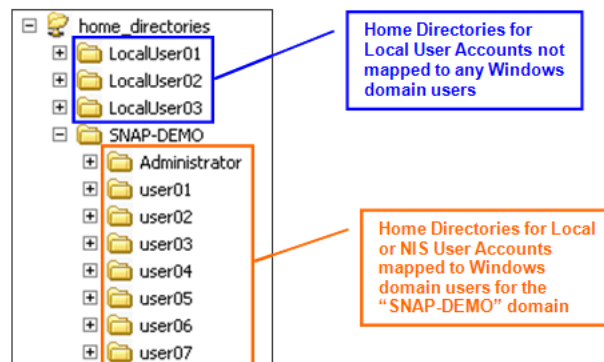
Note: Be sure the volume you select has enough disk space. Once Home Directories are established and user data begins to accumulate, relocation of the Home Directory tree can be problematic. While possible to relocate all Home Directories and reconfigure the Home Directory feature within the same Snap Server, it may require careful attention and downtime. Also, do not put Home Directories on a volume that might be deleted. If you delete the volume, you will also delete the Home Directories.

When a user logs in to the Snap Server for the first time after the administrator has enabled Home Directories, a new directory named after the username is

automatically created inside the Home Directory root, and is configured to be accessible only by that specific user and the administrators (administrators represents the Snap Server's local administrative group 'admingrp' and the Windows domain group 'Administrators'). For most network access protocols, virtualized shares are established for each user to directly access his data without passing through an intermediary share.

Home Directory Hierarchy on Snap Servers

It is important for administrators to understand the directory hierarchy created for the Home Directory feature. The Home Directory root folder path and name, as described earlier, are defined by the administrator when the Home Directory feature is enabled. All local user Home Directories are located directly underneath this root directory. If the Snap Server is joined to a Windows domain, the home directory for each domain user is located inside a subdirectory of the Home Directory root with the name of the Windows domain. The sample screenshot below shows a Home Directory hierarchy that contains home directories for both local and Windows domain users; the latter is for a domain named SNAP-DEMO.



File system security is configured on the Home Directory root to allow all users to pass through the directory (note that if an existing directory is selected as the Home Directory root, the permissions on that directory are overwritten). If located on a Windows/mixed SnapTree, the home directories for individual users are configured with a Windows ACL to allow only the user and "Administrators" full access; if located on a UNIX SnapTree, the user is set as the owner and "admingrp" is set as the owning group; permissions are set to **770 (rwxrwx---**).

Accessing Home Directories

Depending on the client access protocol, Home Directories are accessed by users either via a user-specific virtual share (exclusively visible to and accessible by that user), or via a common share pointing to the Home Directory root. As mentioned above, Home Directories are supported for Windows, Linux/UNIX, Apple, Web, and FTP clients, as well as their respective client access protocols. Since the behavior of the Home Directory feature is based solely on the client access protocol, the descriptions below are based on the protocol being used by the client, as opposed to by client 'type'.

GuardianOS supports some unique cross-platform functionality with the Home Directory feature. A given user accessing his or her home directory from any of the supported protocols can seamlessly access the same Home Directory data, providing a distinct advantage over other Home Directory implementations, which differentiate home directories by protocol or client OS. No extra configuration is required to enable this powerful capability.

Windows Clients (SMB/CIFS)

Windows clients access Home Directories via CIFS/SMB through a virtual share based on the username. The virtual share is *exclusively* visible to and accessible by that username. For example, a user logged in with the username *jdoe* cannot view or access the virtual share for the username *jsmith* and vice-versa.

Users can utilize a number of methods to access the virtual share:

- Manually mapping a drive letter each time the user logs on to Windows.
- Automatically mapping a drive letter upon Windows logon via a logon script configured by the administrator.
- Automatically mapping a drive letter upon Windows logon via the Home Folder feature built into Windows domain user management. The administrator simply maps to the Snap Server name followed by the username (`\\snapserver\username`). For example, to configure a mapped drive letter for home directory for the domain user *jdoe* for a Snap Server named *MySnap*, the mapped Home Directory path would be `\\MySnap\jdoe\`. See the “Integrating with the Windows Built-in Home Folder Feature” section for additional details.

Windows users can also use a Home Directory on a Snap Server as a roaming profile directory. The roaming profile directory is specified in the domain user’s account settings using the same format as the domain user home directory, i.e.: `\\snapserver\username`. See the “Windows Roaming Profiles and Home Directories” section for additional details.

Note: Users are not limited only to their virtual shares; all other shares on the Snap Server continue to be accessible in the usual fashion.

UNIX Clients (NFS)

UNIX clients access their Home Directories via NFS through an export to the Home Directory root folder named “*home_dir*”. When a user mounts *home_dir* over NFS, all Home Directories are visible; however, the user’s Home Directory is accessible only by the logged in user and administrators of the Snap Server.

The exported path for the Home Directory root folder is the Snap Server name followed by *home_dir* ; and some NFS clients can also mount directly to the specific user’s home directory. For example, to mount to the Home Directory root via NFS on a Snap Server named *MySnap*, the mount path to the export is *MySnap:/home_dir*. To mount directly to the user’s home directory, the mount path is *MySnap:/home_dir/username*.

Note: If the NFS user is mapped to a Windows domain user on the Snap Server, then the Home Directory will be located beneath a directory named after the Windows domain; otherwise it will be located directly beneath the Home Directory root. See the “ID Mapping and Home Directories” section for more details.

If desired, administrators can configure UNIX clients to use a Snap Server’s Home

Directory for their system Home Directories. To accomplish this, the administrator would first configure the clients to mount the Home Directory root, then configure each user account on the respective clients to use the username-specific directory on the Snap Server as each user's Home Directory.

Apple Clients

Clients accessing Home Directories via Apple have the same experience as users accessing their Home Directories via Windows (SMB/CIFS). A virtual share is only visible and accessible for the username that is logged in.

Web Clients (HTTP/HTTPS)

Just like Windows and Apple clients, Home Directories are presented to users accessing from a web browser over HTTP or HTTPS as a virtual share for the username. As before, this share is only visible to and accessible by that user.

Since HTTP and HTTPS only authenticate using Local user accounts, administrators interested in allowing cross-platform access to Home Directories for those Local user accounts and Windows domain user accounts must enable and configure the ID Mapping feature on the Snap Server. This will be described later in this document.

Note: Web access via HTTP or HTTPS to files stored on a Snap Server is READ ONLY.

FTP Clients

For FTP, users are automatically placed in their private Home Directory when they log in. Access to the Home Directory is facilitated through a *home_dir* share pointing to the Home Directory root. Users can still change to the top-level directory to access all other shares and directory structures. As with Home Directory access for other protocols, individual user home directories are accessible only by the authenticated user and a Snap administrator.

Just like HTTP, FTP authenticates utilizing Local user accounts, and therefore must leverage the ID Mapping feature on the Snap Server to have cross-platform access to the Home Directories.

ID Mapping and Home Directories

Individual end users who access the Snap Server from different workstations using assorted protocols and authenticating via various security mechanisms (e.g.: Windows domain and NIS) are normally treated as separate users when they are simultaneously connected. Therefore, distinct security will apply to each login they utilize, and each user is provided with a unique home directory.

However, with ID Mapping, administrators can configure user accounts to permit end users to access the same Home Directory seamlessly from any of the supported protocols. Using the ID Mapping feature to map a Windows domain user to a NIS or

Local Snap user instructs the Snap Server to consider the two users as the same identity for general security enforcement and Home Directory access.

When a Windows domain user is mapped to a NIS or Local Snap user via the ID Mapping feature, the user will always be directed to the Windows domain user's Home Directory – regardless of the network protocol or authentication method used to access the server (in the case of NFS access, the NIS user still mounts the *home_dir* export, but can access the domain user's Home Directory). Home directories for Local or NIS users not mapped to domain usernames continue to be created directly beneath the Home Directory root folder.

Note that ID Mapping is not necessary to enable cross-platform access between Local users and NIS users. Cross-platform access to Home Directories for any of the protocols using a Local user account for authentication is facilitated by ensuring that the UID for the Local user account matches that of the NIS user account.

Best Practices

Enabling and using the Home Directory feature is quite straight forward, but some areas deserve special attention for administrators of Home Directories.

Home Directory Administrative Access

In some circumstances, such as to repair permissions for file or folders that the end user has inadvertently made inaccessible, or to handle the disposition of Home Directory data for an employee who is no longer with the organization, a Snap administrator may need to directly access an end-user's Home Directory.

Administrative access to Home Directories can be easily set up by creating a hidden share that provides access to either a parent of the Home Directory root, or to the Home Directory root itself. Security on this share can be configured so that only Snap administrative users have access. Since by default all user Home Directories grant full access to Snap administrators, administrators can connect to the server via this special administrative share and traverse through the Home Directory root into any user Home Directory.

Shares can be created through the Web Browser Administration Tool in [Security > Shares > New](#), and can be hidden by enabling the *Hide this share* option in the *Advanced* section of the share creation screen. Access to this share can be controlled in [Security > Shares > Access](#) by removing access for all users except administrative users.

Backup of Home Directories

There are several methods for backing up data that is located on a Snap Server, all of which can also be employed to backup Home Directory data. Whether using the included snapshot technology, BakBone NetVault:Backup software, or third-party backup packages, administrators only need to be sure to include the location that contains the Home Directory data when specifying the backup source.

If utilizing a file sharing protocol to back up Home Directories over the network, administrators need to ensure that a share exists above the Home Directory root. This can be accomplished by setting up a hidden share, similar to the administrative access share that refers to the section “Home Directory Administrative Access.” Once this hidden share is created, the administrator can simply configure the backup application to use the explicit share path to the Home Directory root as the backup source. As with the administrative access share described above, it is important to limit access to the Home Directory root share to only those administrative accounts that require access to all user Home Directories.

Windows Roaming Profiles and Home Directories

Another interesting way to take advantage of the new Home Directory feature is to utilize the virtual share and inherent user-level permissions for Roaming Profiles for Windows domain users. Utilizing the Home Directory structure will ease the trouble of setting up another structure just for roaming profiles.

Configuring a Windows domain user to use a Home Directory stored on a Snap Server is simple. Once Home Directories for SMB/CIFS have been enabled, go to the domain user’s account settings and specify a UNC path to the user’s virtual Home Directory share on the Snap Server (e.g.: `\\MySnap\jdoe`).

By specifying the path using the Windows “%username%” variable, this task can be further simplified to a standard, generic path that Windows will translate to a specific path using the username. For example, if specifying “`\\MySnap\%username%`” as the roaming profile path for user “jdoe”, Windows will automatically convert the path to “`\\MySnap\jdoe`”. Windows scripting tools can subsequently be used to apply this roaming profile path to multiple or all users in a Windows domain without the need to manually configure each user.

Integrating with the Windows Built-in Home Folder Feature

Similar to roaming profiles, Windows administrators can set up “Home Folders” for Windows domain user accounts. This Home Folder feature can be easily combined with Snap Server Home Directories. However, it is important to understand the best process for setting up the Home Directory infrastructure when utilizing the Windows Home Folder feature.

Traditionally, when configuring the Home Folder of a Windows domain user to point to a directory beneath a share on a Windows server, the Windows client employed to perform this configuration task automatically connects to the server and share in the background, then creates the specified directory beneath it with specific permissions (if it does not already exist). For example, when an administrator configures the Home Folder for user “jdoe” to point to “`\\MyServer\homedirs\jdoe`”, the administrator’s client connects to “`\\MyServer\homedirs`” and creates subdirectory “jdoe” with full access permissions granted to jdoe and “Administrators”.

This traditional method can be used to point Windows domain user accounts to a specific directory on a standard share on a Snap Server without using the Home Directory feature. However, doing so will not take advantage of the capabilities of GuardianOS to centrally organize and manage Home Directories. The better solution is

to integrate Windows domain Home Folders with the Home Directories feature in GuardianOS.

To integrate a Windows domain user's Home Folder with Home Directories:

1. Enable and configure the Snap Server Home Directory feature for "Windows (SMB)" (verify that it is working as expected).
2. In the "Profile" tab for a Windows domain user in "Active Directory Users and Computers", configure the Home Folder to "Connect" a drive letter pointing to a UNC path to the user's Home Directory virtual share on the Snap Server (e.g.: "\\MySnap\jdoe" or "\\MySnap\%username%").
3. Click "OK" or "Apply" in the user profile window. This will usually return an error dialog stating that the Home Folder could not be created because the network path does not exist. This is normal and expected. This occurs because the individual user's Home Directory virtual share is exclusively visible to and accessible by the user in question; while typically this configuration task is performed from a Windows domain administrator account, which is likely a different account than the user Home Directory being configured. Dismiss this error dialog and click "OK" on the user profile window to complete the configuration.

Note: if a new user is created utilizing the above process, a brief delay is sometimes experienced before the Snap Server recognizes the new user and allows that user to access the Home Directory.

GuardianOS Home Directory Implementation Summary

Step 1: Create all Local users and groups on the Snap Server

Step 2: Integrate the Snap Server into Windows (Active Directory or NT) and/or NIS

Step 3: Configure any ID Mapping based on the Local, NIS, and Domain users and groups

Step 4: Enable Home Directories by choosing the protocols that will utilize Home Directories

Step 5: Test the creation and access of the Home Directories with the configured protocols

Conclusion

Snap Servers powered by GuardianOS have always provided advanced features that are easy to manage and use. The Home Directory feature exemplifies this core principle. The new Snap Server Home Directory feature brings the otherwise complex and daunting administrative task of creating and managing Home Directories to the masses. This tightly integrated feature allows cross-platform access to Home Directories without creating unnecessary administration and without changing the way an end user would typically access their data from any of their native access environments. Regardless of whether the user is accessing his Home Directory from Windows, UNIX, Apple, FTP, or from the Web, he will always have the ability to utilize native tools for each access method, with nothing special to remember. The simplified management and automatic directory creation requires only minutes to get up and running—whether implemented for one hundred or ten thousand Home Directories.

About Overland Storage

Overland Storage provides affordable end-to-end data protection solutions that are engineered to store smarter, protect faster and extend anywhere — across networked storage, media types, and multi-site environments.

Overland Storage products include award-winning NEO SERIES® and ARCVault™ tape libraries, REO SERIES® disk-based backup and recovery appliances with VTL capabilities, Snap Server® NAS appliances, and ULTAMUS™ RAID high-performance, high-density storage. For more information, visit www.overlandstorage.com.

WORLDWIDE HEADQUARTERS

4820 Overland Avenue
San Diego, CA 92123 USA
TEL 1-800-729-8725
1-858-571-5555
FAX 1-858-571-3664

UNITED KINGDOM (EMEA OFFICE)

Overland House, Ashville Way
Wokingham, Berkshire
RG41 2PL England
TEL +44 (0) 118-9898000
FAX +44 (0) 118-9891897

