



CATIA V5 Deployments with NetApp Solutions

**Rajesh Godbole and Mark Davied, Philippe ZIMNY, Dassault Systèmes,
Network Appliance, Inc.**

Updated by H. T. Sun, Network Appliance, Inc

April 2005

Updated by Rajesh Godbole, Network Appliance, Inc

August 2006 | TR-3287

Abstract

NetApp delivers a fast and efficient storage infrastructure for support of CATIA deployments. New installs or upgrades of CATIA can be quickly and easily deployed on NetApp storage infrastructure using a thin-client approach. NetApp Snapshot™ copies and SnapVault® software provide data protection to CATIA binaries, settings, and design data through online backups and near-line replication. NetApp solutions make CATIA infrastructure easy to deploy and manage, reducing costs, increasing IT and engineer efficiencies, and enabling a faster time-to-market for product manufacturers.

Table of Contents

| | |
|--|----|
| Overview | 3 |
| 1. Introduction | 3 |
| 1.1 Challenges..... | 3 |
| 1.2 Benefits..... | 3 |
| 1.3 Assumptions | 4 |
| 2. Deployment | 4 |
| 2.1 Typical Deployment..... | 4 |
| 2.2 Best-Practice Deployment..... | 5 |
| 2.3 Details: Best-Practice CATIA Deployment on NetApp..... | 6 |
| 3. Migration From Catia V4 to V5..... | 23 |
| 4. Summary..... | 24 |
| 5. References..... | 24 |
| 6. Glossary | 25 |
| 7. Revision History | 26 |

Overview

Dassault Systèmes offers a number of product lifecycle management (PLM) solutions. CATIA is the solution specific to product design in Dassault's array of PLM offerings. CATIA allows product manufacturers to simulate all industrial design processes, from the pre-project phase through to detailed design, analysis, simulation, assembly, and maintenance. Use of CATIA can assist product manufacturers in their efforts to shorten time-to-market, reduce design costs, and improve product quality.

Dassault Systèmes and Network Appliance, a leader in innovative information management solutions, are working together to develop, test, and deliver comprehensive, fully interoperable solutions to the product manufacturing market. Because of this collaboration, Dassault-NetApp solution combinations optimally address customer challenges relating to data management when deploying a PLM solution.

NetApp provides storage solutions for the entire PLM infrastructure. As such, NetApp solutions enable customers to effectively manage data and information associated with CAD, CAE, CAM, ERP, and CRM applications, among others. However, for technical clarity purposes, this paper focuses only on the CAD portion of the PLM infrastructure. Specifically, this paper is intended to provide CAD/IT managers and staff an overview concerning how to efficiently deploy and manage CATIA in its most recent version (CATIA V5)—for code serving, settings, and design files—in a NetApp environment using a shared solution implementation approach.

1. Introduction

1.1 Challenges

In order to remain competitive, companies in the product manufacturing sector must continually reduce time-to-product and time-to-market. In concert, IT departments are forced to implement and manage new technology and systems that will increase the productivity of design engineers and ensure data is always available when it is needed, where it is needed. Because of the complex, heterogeneous, and often dispersed nature of the design process, IT departments face formidable obstacles to effective deployment and management of a product design solution. Invariably, these difficulties include:

- Facilitating sharing of design files among engineers, departments, partners, and locations, regardless of point-of-origin operating system.
- Providing rapid access to older design files (e.g., CATIA v4 files), created and accessed with varying platforms (e.g., created in UNIX® and accessed from a Windows® Preserving the integrity and security of information, despite design data age, status in the information lifecycle, storage location, or present access requirements.
- Maintaining high levels of performance and data availability across the entire organization.
- Implementing a cost-effective data protection, information management, and disaster recovery plan to ensure maximum uptime and optimum business continuance in the event of regulatory request, system failure, user error, or unexpected disaster.

These challenges demand substantial IT resources—in terms of budgets as well as equipment, tools, staff, time, and skill. Failure to properly meet these requirements directly impacts an engineer's ability to perform, translating to losses in time-to-product and time-to-market.

1.2 Benefits

While CATIA software permits more efficient product design, NetApp hardware and software permit the most efficient use of resources in relation to design data management, software distribution and upgrades, local and remote collaboration, and data protection, including backup and recovery, information lifecycle management (especially for purposes of regulatory compliance), and disaster recovery. NetApp solutions

address time-to-product and time-to-market needs by reducing idle time, rework time, and administrative time.

Highly available NetApp solutions guarantee product manufacturing companies achieve high-performance delivery of vital data when and where needed. NetApp also offers these companies scalable, flexible, and cost-effective solutions that incorporate a unified, multiprotocol storage platform with feature-rich data and resource management software and that allow storage capacity additions and data protection tasks with little or no downtime. NetApp solutions deliver increased staff effectiveness, reduced operating costs, and the benefits of an innovative Dassault-NetApp partnership.

1.3 Assumptions

For purposes of this paper, it is assumed that the reader is familiar with Dassault Systèmes PLM products and has a more intimate knowledge of CATIA as a tool for CAD design. The paper also assumes that the reader is familiar with networking as well as workstation and server software and hardware platforms. Moving forward, this paper will demonstrate best practices for deploying and using CATIA in combination with NetApp solutions and how the Dassault-NetApp solution combination serves the critical needs of a high-performance CAD environment.

2. Deployment

2.1 Typical Deployment

Figure 1, below, depicts a typical Mechanical Engineering (ME) design environment that incorporates various software packages used in the PLM design process. Typically, such an environment may consist of several UNIX and/or Windows CAD workstations set up in a workgroup on a corporate LAN. The workstations may access several servers, including PDM and DB servers, as well as networked storage. The workstations, servers, and storage may be backed up to tape for archival purposes.

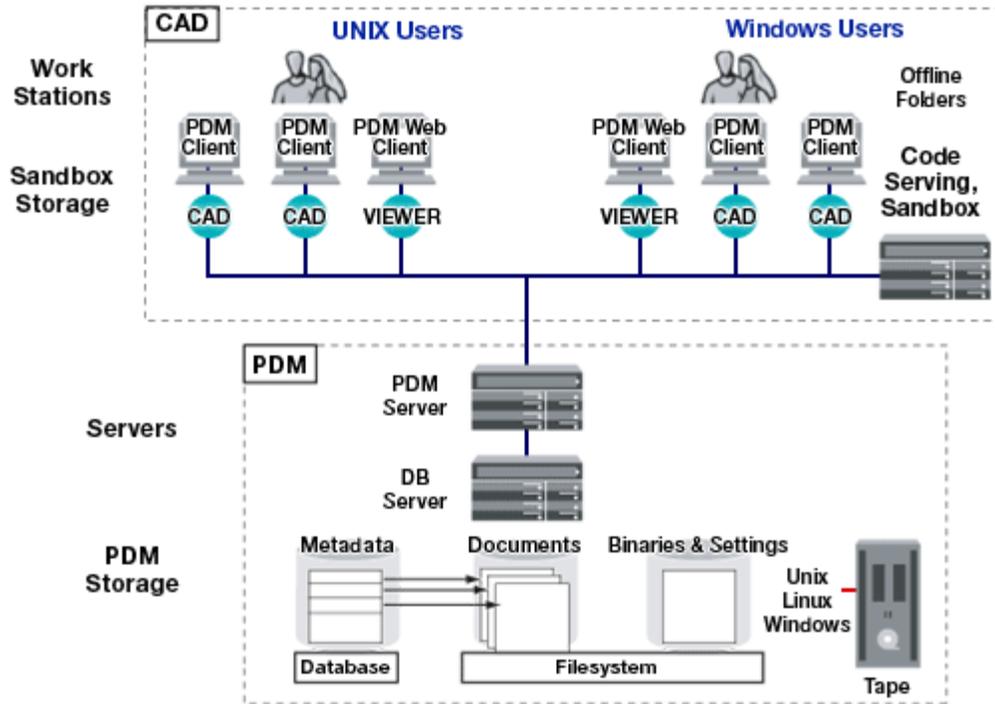


Figure 1) PLM Deployment

2.2 Best-Practice Deployment

An example of a CATIA V5-NetApp solution in a CAD environment is illustrated in figure 2, below. In the example, the CATIA binaries, environment settings, and design files are located on the storage controller with the hostname "brain." Typical production deployments will have multiple storage controller clustered in pairs for the highest levels of availability. The storage controller is backed up to a NearStore® near-line storage appliance with the hostname "r150" using NetApp SnapVault software. The NearStore appliance also serves as an archive for older design files (often reused in future designs or required for liability purposes). While not shown in the illustration that follows, additional NetApp products are available that capture, replicate, and serve data for backup, collaboration, and disaster recovery purposes. Some of these products include Snapshot, SnapMirror®, SnapRestore®, as well as NetCache® appliances.

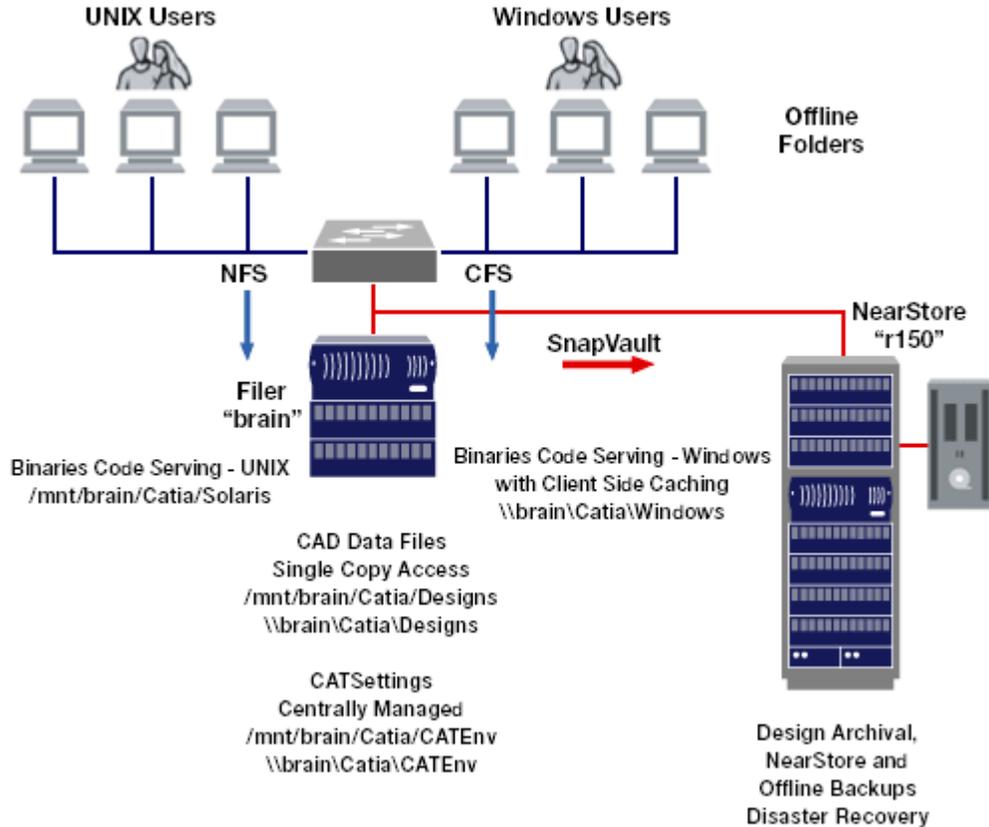


Figure 2) CATIA V5 Multiprotocol Deployment

2.3 Details: Best-Practice CATIA Deployment on NetApp

This section of the paper is divided into two parts, each detailing CATIA deployment on NetApp best practices in the respective areas:

- Installing the CATIA binaries and global environment settings for both UNIX and Windows clients
- Creating heterogeneous storage (UNIX and Windows) for design files, including maximizing data availability for design reuse

Installing CATIA Binaries and Global Environment Settings Older versions of CATIA software were available only for UNIX platforms, which supported installation over an NFS mounted partition from a NetApp appliance. CATIA V5 is available for both Windows and UNIX platforms. A network-based install is supported in CATIA V5 for both UNIX and Windows platforms and is covered in the CATIA Infrastructure Installation Guide, which is available in the CATIA V5 CD set (listed in the "Accessing the Software from a Thin Client" section in "Distributing Code").

The benefits of accessing CATIA software from a thin client are:

- Caching of files locally. The client-side caching feature of offline folders in Windows allows caching of binaries locally on the storage. This approach reduces load on the network resources while eliminating the need for local installs on the clients.

- Reduction in administrative overhead. The approach allows workstations to become thin clients. This benefit is especially significant to Windows workstations.
- Reduction in time required for local install. The code and environment are installed only once to a storage appliance from a CATIA workstation. “Thin client” workstations can access the code and environment from the appliance after the creation of a run-time environment on the client. The install process is now reduced to a small number of automated steps.
- Service pack installs are simplified. The thin-client approach simplifies the installation of CATIA service packs significantly. Service pack updates are applied once to the installation on the storage appliance. Offline folders can be set to sync upon login or logout, so offline folder caches are updated whenever a service pack is installed.

These benefits are detailed via deployment practices on the pages that follow.

Windows Executables (CIFS with Client-Side Caching)

Shared Installation on Storage for Code Serving

- Create a volume “vol1” on the storage controller. In this example, the Web-based administrative tool from NetApp FilerView® is used to create vol1 on the storage controller named “brain” using the Volumes -> Add screen.

The screenshot displays the NetApp FilerView web interface for configuring a new volume. The interface is organized into a sidebar on the left and a main content area on the right. The sidebar, under the 'brain' storage controller, lists various management options including File, Volumes, Storage, SnapMirror, CIFS, NFS, HTTP, LUNs, DAFS, MultiStore, Network, and Security. The main content area is titled 'Add New Volume' and contains the following configuration fields:

- New Volume Name:** A text input field containing 'vol1'.
- Raid Group Size:** A text input field containing '8'.
- Language:** A dropdown menu set to 'POSIX'.
- Automatic Disk Selection:** A radio button that is selected (checked).
- Number of Disks:** A text input field containing '12'.
- Disk Size:** A dropdown menu set to 'Any size disks'.

Figure 3) Creating “vol1” on the Storage controller

- Create a qtree “Catia” in vol1 with security type “mixed.” The Volumes -> qtrees -> Add screen is used in this example. The mixed security style allows the qtree to contain both objects with UNIX and NTFS style attributes. Objects in the qtree can be modified from both UNIX and Windows clients.

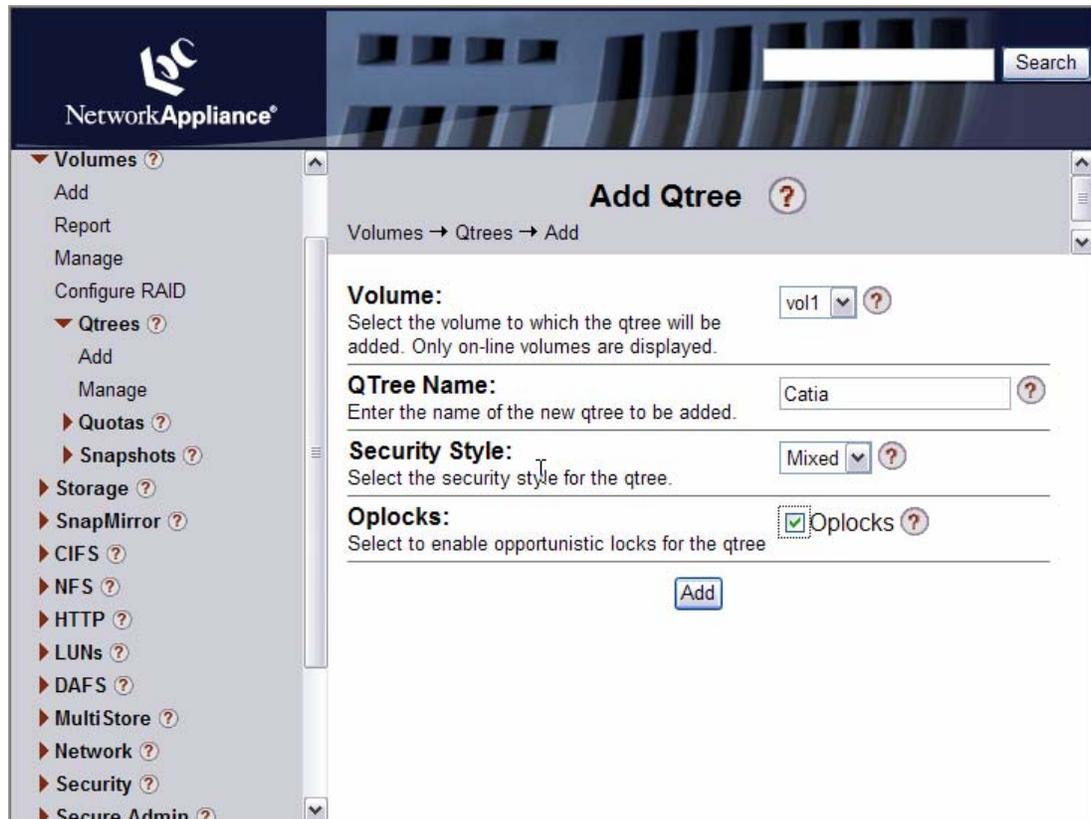


Figure 4) Creating qtree Catia in vol1

- Create CIFS share “Catia” using the CIFS -> Shares -> Add screen.

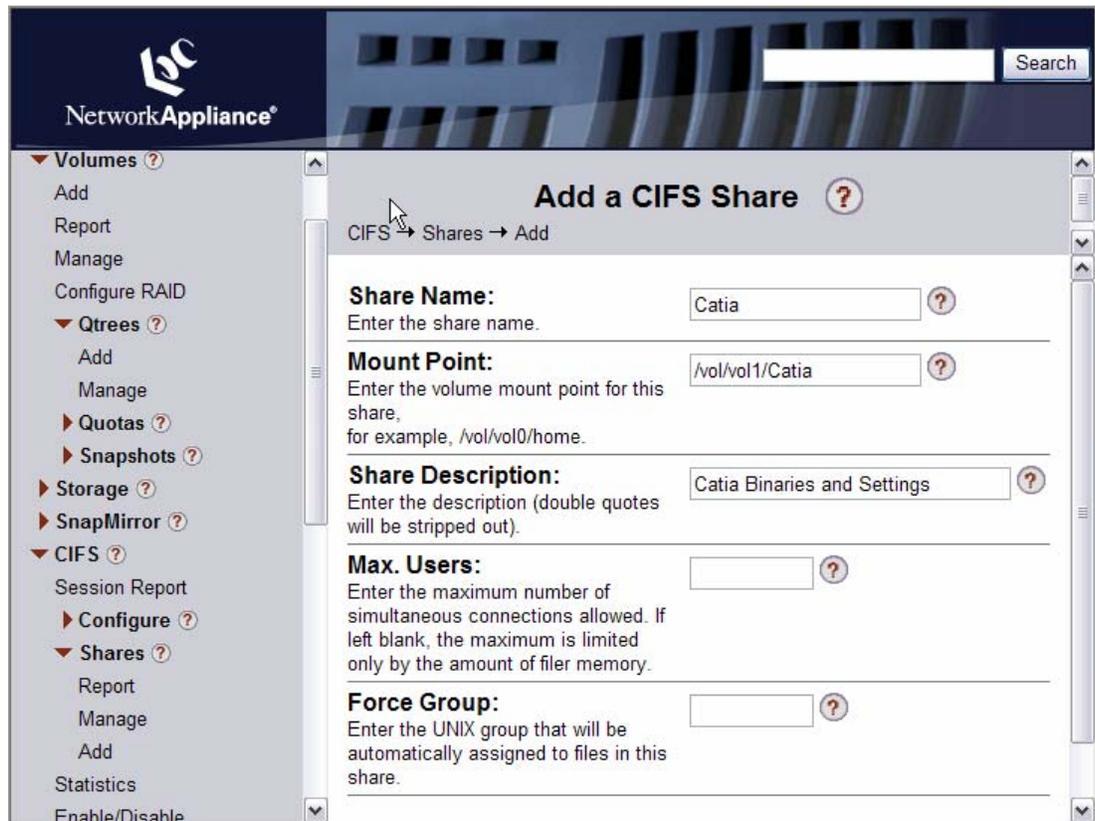


Figure 5) Creating CIFS Share Catia

- Log in to a CATIA workstation as “administrator.” Use the management console to connect to the storage controller “brain” and modify the share Catia’s properties. Under the “general” tab, click on “caching ...” Make sure that the “allow caching of files” in this shared folder is checked and change the cache setting to “allow caching for programs.” The ability to change the cache setting is available in NetApp Data ONTAP® release 6.3.2, 6.4.1, and 6.4.1P1 or better. See the NetApp [NOW™](#) site for details.

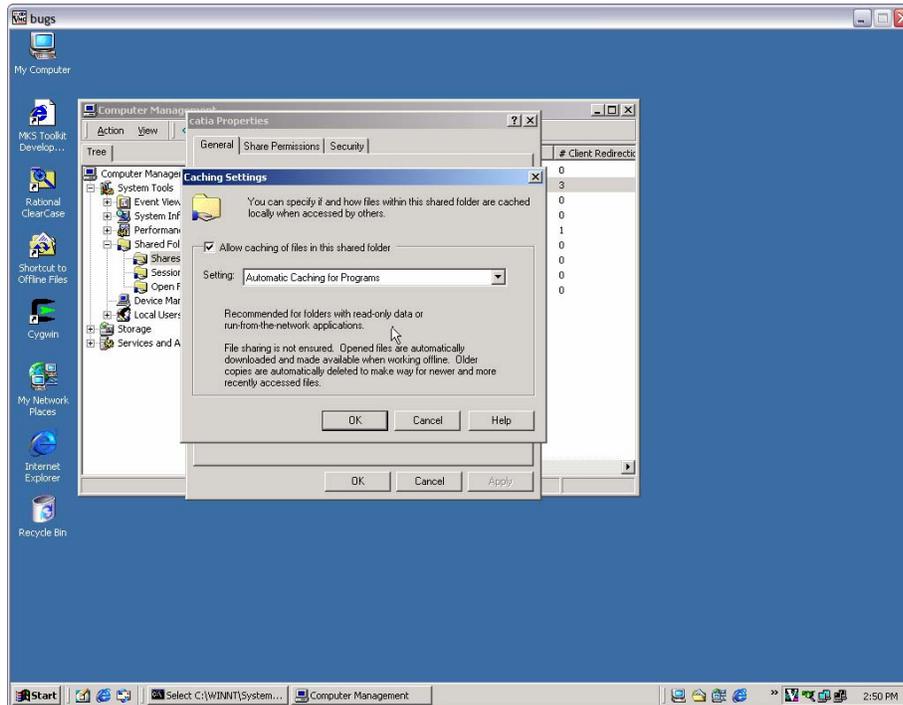


Figure 6) Permitting Caching for Share Catia

When sharing a folder on a network, one must decide whether people can work with the contents of the folder when they are offline. With Offline Folders, others on the network can open and update the files in shared folders even if they currently are disconnected from the network. Offline Folders can be configured using three settings. The *Automatic Caching for Programs* setting may be used for best results.

The *Automatic Caching for Programs* option allows programs that are being stored offline to be accessed locally and helps reduce network traffic. Use of Offline Folders can reduce the start time and network bandwidth usage and therefore allow a NetApp appliance to support larger numbers of CATIA workstations. Additionally, this setting prevents changes made offline from being synchronized back to the code server. For more information see the [Microsoft®](#) Web site.

- Under “share permissions,” change the default permissions for “everyone” to “read” only. Add “full access” to the administrator account.

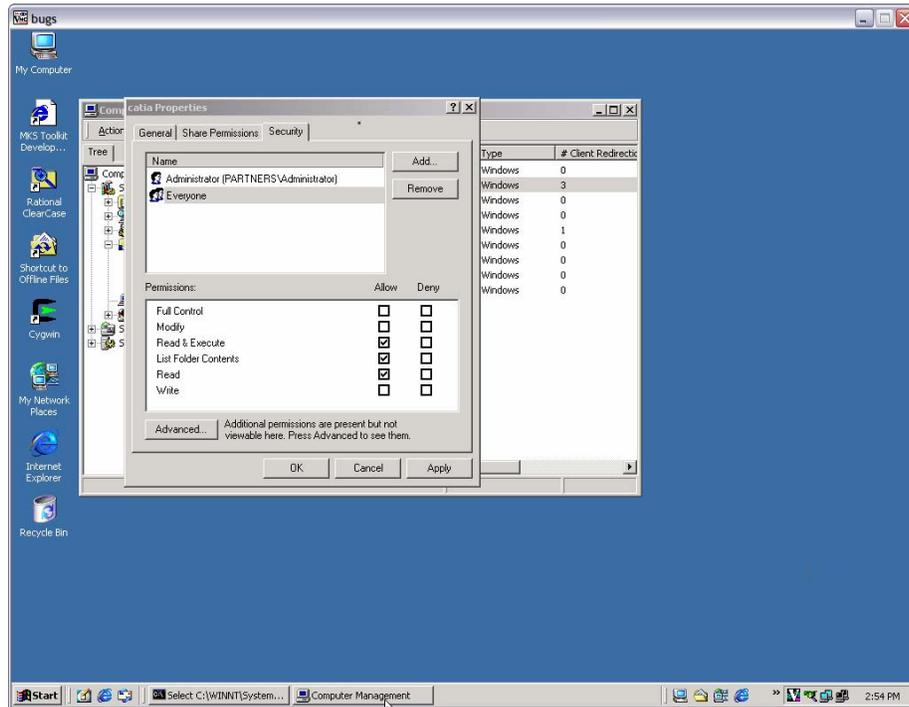


Figure 7) Changing Share Permissions

- Map the Windows share from the storage controller to the workstation using Windows Explorer (Drive F: in this example).
- Install CATIA V5 on the workstation. Change the install path for the installation folder to F:\Windows (F: is mapped from [\\brain\Catia](#)).

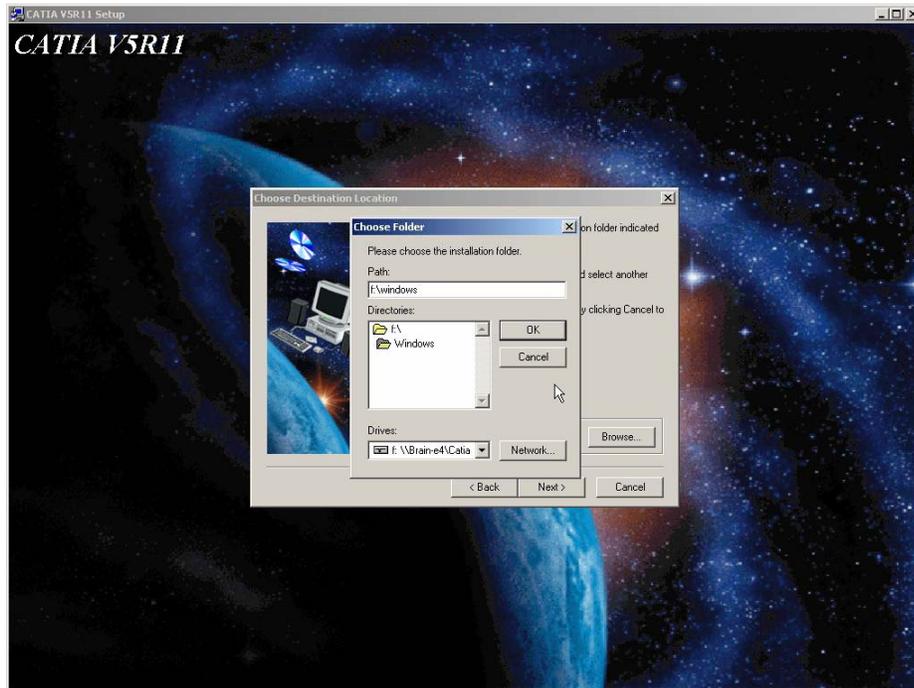


Figure 8) Installing CATIA V5 on the Workstation

- The default location of the CATIA environment is in the “all users” profile on the server, which is

```
C:\%WINDIR%\Profiles\All
Users\Application\Data\DassaultSystemes\CATEnv
```

To facilitate access to the runtime environment over the network, the environment must be located on a CIFS share on the storage controller and not in the default location. Change this location to the drive F:\Windows\Catia.

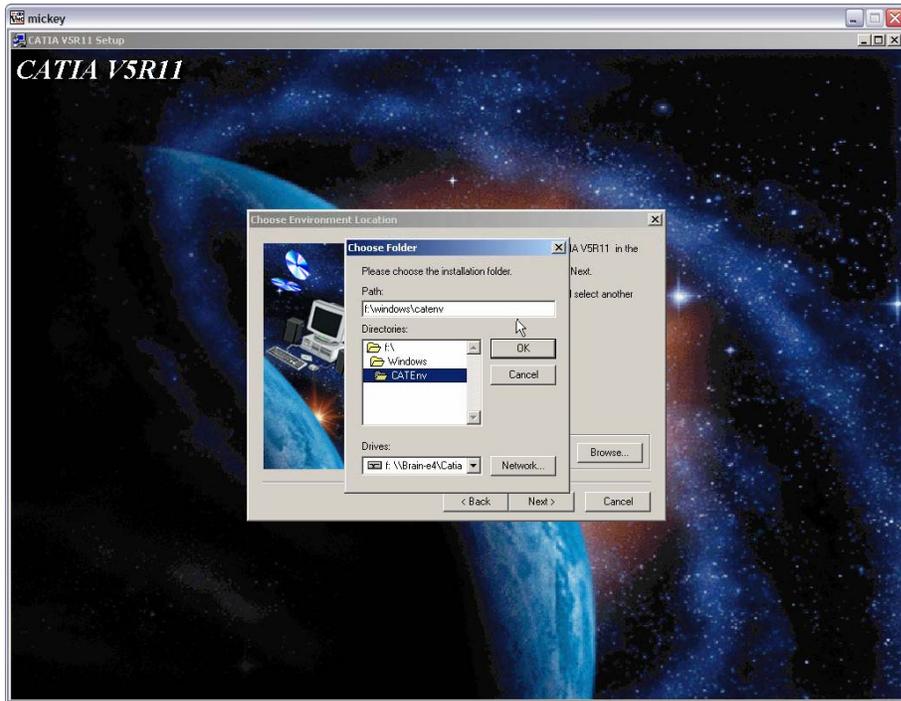


Figure 9) Changing the Catia Share Location

- Create a new global environment on the CATIA workstation using the following command:


```
setcatenv -e CatiaV5 -d \\brain\Catia\CATEnv -a global -p \\brain\Catia\Windows -desktop no
```
- Edit the global environment to tailor it to reflect your environment. Commonly modified global settings are `CATUserSettingPath` and `CATReferenceSettingPath`, which define the location of the global settings.

Creating a global environment on a storage controller CIFS share eases administration of CATIA workstations by allowing the administrator to make global changes via change to a single environment.

The same methodology can be used for global settings in both the Windows and UNIX environments. Additionally, settings can be managed on one storage controller from a single location.

Installation of CATIA Runtime Environment on Thin Clients The process for installing the CATIA runtime environment on thin clients should be scripted to suit your environment. Scripting this process will allow the deployment expert to extract the full value from a thin-client configuration by reducing administration on CATIA workstations. The process outlined below shows an example of such an install.

- Map the storage controller share on which CATIA was installed in the process above to the thin client. For example [\\brain\Catia](#) is mapped to the F: drive. CATIA was installed into [\\brain\Catia\Windows](#).
- Open a command prompt window in the directory `F:\Windows\intel_a\code\bin`.
- Check that the system DLLs on the client are up to date by running:

```
F:\Windows\intel_a\code\bin>CATSoftwareMgtB -P
```

If the system DLLs are not up to date, the following command from the installation CD will install the required DLLs. Note that the computer will need to be restarted after the DLLs have been updated.

```
D:\INTEL>startb -DLL
```

- Update OLE support by updating the registry via running the command below. This ensures that double-clicking CATIA V5 documents on the client will run a V5 session.

```
cnxet /regserver -e CatiaV5 -d \\brain\Catia\CATEnv
```

- To add a shortcut to the CATIA V5 environment to the desktop for easy access, run the command:

```
setcatenv -e CatiaV5 -d \\brain\Catia\CATEnv -p  
\\brain\Catia\Windows
```

- To set up links to CATIA programs in the Start->Programs menu, run the command:

```
setcatenv -e CatiaV5 -d \\brain\Catia\CATEnv -p  
\\brain\Catia\Windows -tools -cs CATIA
```

- If you require extended font support, run the following command from the F:\Windows\intel_a\code\bin directory:

```
F:\Windows\intel_a\code\bin>VE0rootIFONT -env CatiaV5 -direnv  
\\brain\Catia\CATEnv
```

- If you want to record and play macros, you may have to install Microsoft Visual Basic for Applications, version 6.0, if not already installed, from the product CD-ROM.

```
Msiexec /q /I pathcdrom\VBA\VBA6.msi
```

- To set up the communications backbone used to support process interoperability between CATIA and DMU, add the following default port settings

```
catiaV5bb 6666/tcp  
catiaV5run 6667/tcp
```

to the file

```
%windir%\system32\drivers\etc\services
```

- the following command located in the D:\INTEL directory on the product CD-ROM (mounted on the D: drive)

```
D:\INTEL>startb -UpdateServices
```

- Enable client-side caching to the UNC path to the folder [\\brain\Catia](#). This can be accomplished by opening the UNC path [\\brain\Catia](#) in Windows Explorer, selecting Tools -> Folder Options, then the "enable offline files" checkbox..

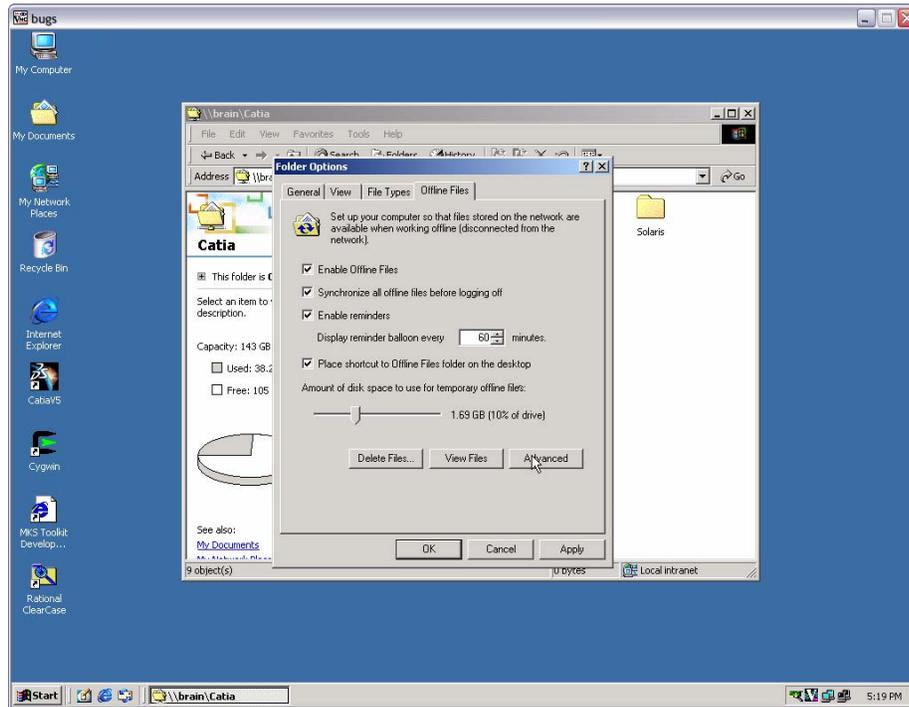


Figure 10) Enabling Client-Side Caching

Select “ synchronize all offline files before logging off” so changes to the CATIA environment on the storage controller are updated on the client.

Solaris Executables (NFS)

Shared Installation on Storage for Code Serving

- Log in as “root” to a CATIA UNIX workstation. The example used here is the machine “grumpy” running Solaris.
- Mount the storage controller share created when using Windows. In this example, the qtree /vol/voll/Catia is mounted using NFS on the mount point /mnt/brain.

```
mount -F nfs brain:/vol/voll/Catia /mnt/brain
```

An entry for this mount may be created by adding the following entry in the /etc/vfstab file so that the qtree is mounted on the UNIX workstation automatically upon reboot:

```
brain:/vol/voll/Catia - /mnt/brain nfs - yes
```

An alternative approach may be via the use of the automounter to mount the directory automatically upon access.

- Make the CATIA installation CD available by copying its contents to an NFS share on a storage controller. Mount the CATIA installation directory from the NFS share on the storage controller to the CATIA Sun™ workstation.
- Start the CATIA install by running “start” from the CATIA CD-ROM mount-point.

- When prompted, change the CATIA on this mount-point by changing the install path to the /mnt/brain/Solaris.

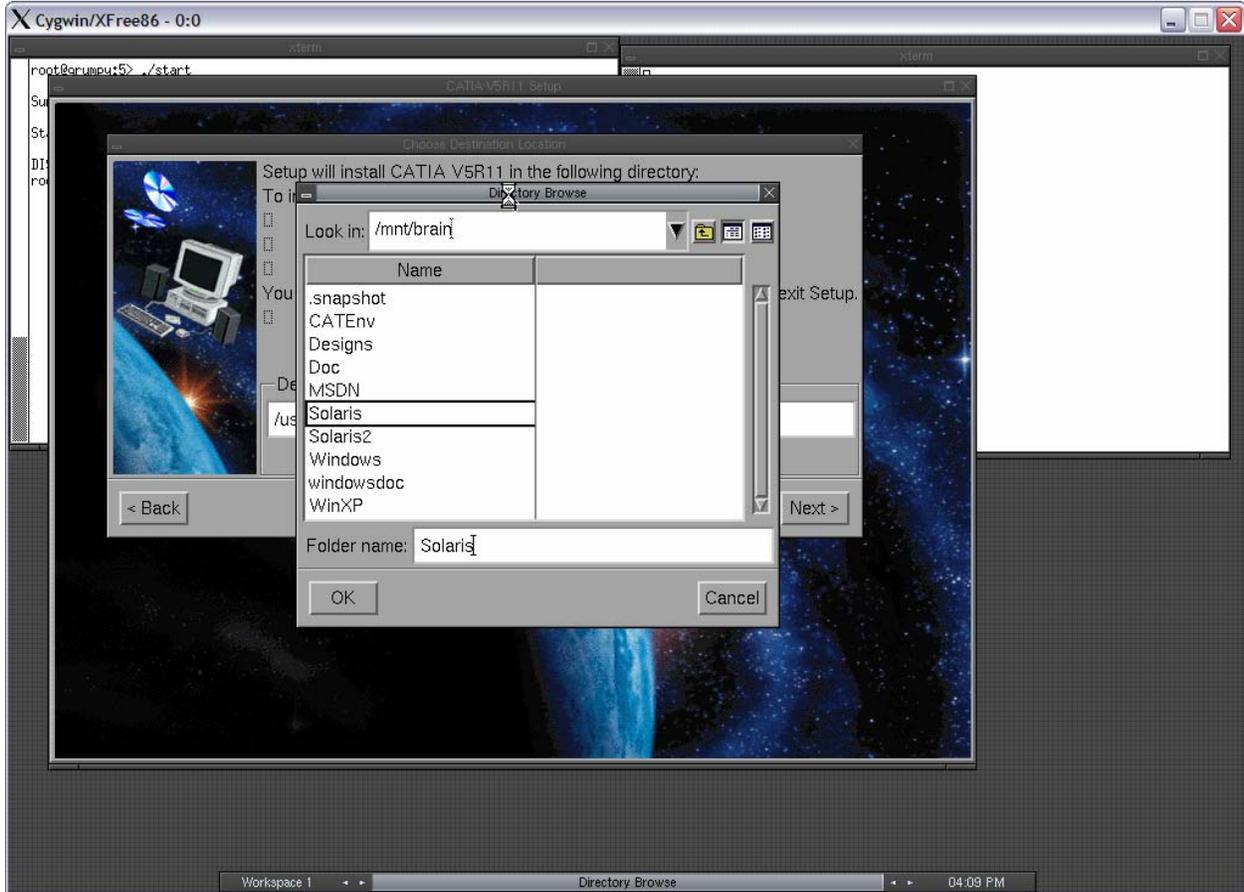


Figure 11) Changing the Install Path to Solaris

- When prompted for the CATIA environment directory, select a global CATEnv directory from the NFS share from a storage controller. If a global CATEnv directory was selected during a prior Windows install of CATIA, the same share can be accessed over both the NFS and CIFS protocols. The example used here is /mnt/brain/CATEnv over NFS, which is the same as the UNC CIFS path [\\brain\Catia\CATEnv](#) in our Windows environment above.

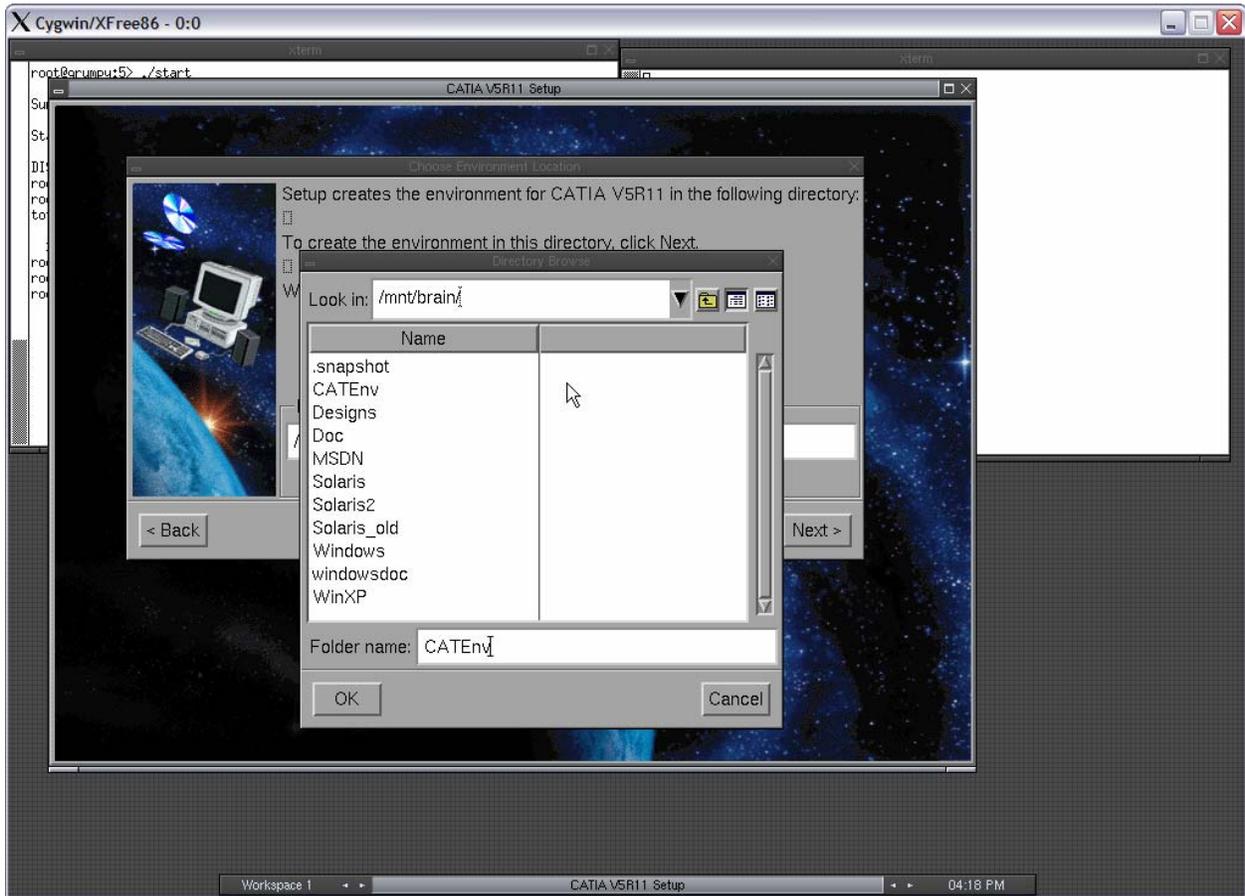


Figure 12) Selecting a Global CATIA Environment Directory

A storage controller allows multiprotocol access to a single shared directory and simplifies global administration of CATIA settings by modifying them in a single location in order to make a global change.

- Finish the installation of CATIA over a network share with the settings above.

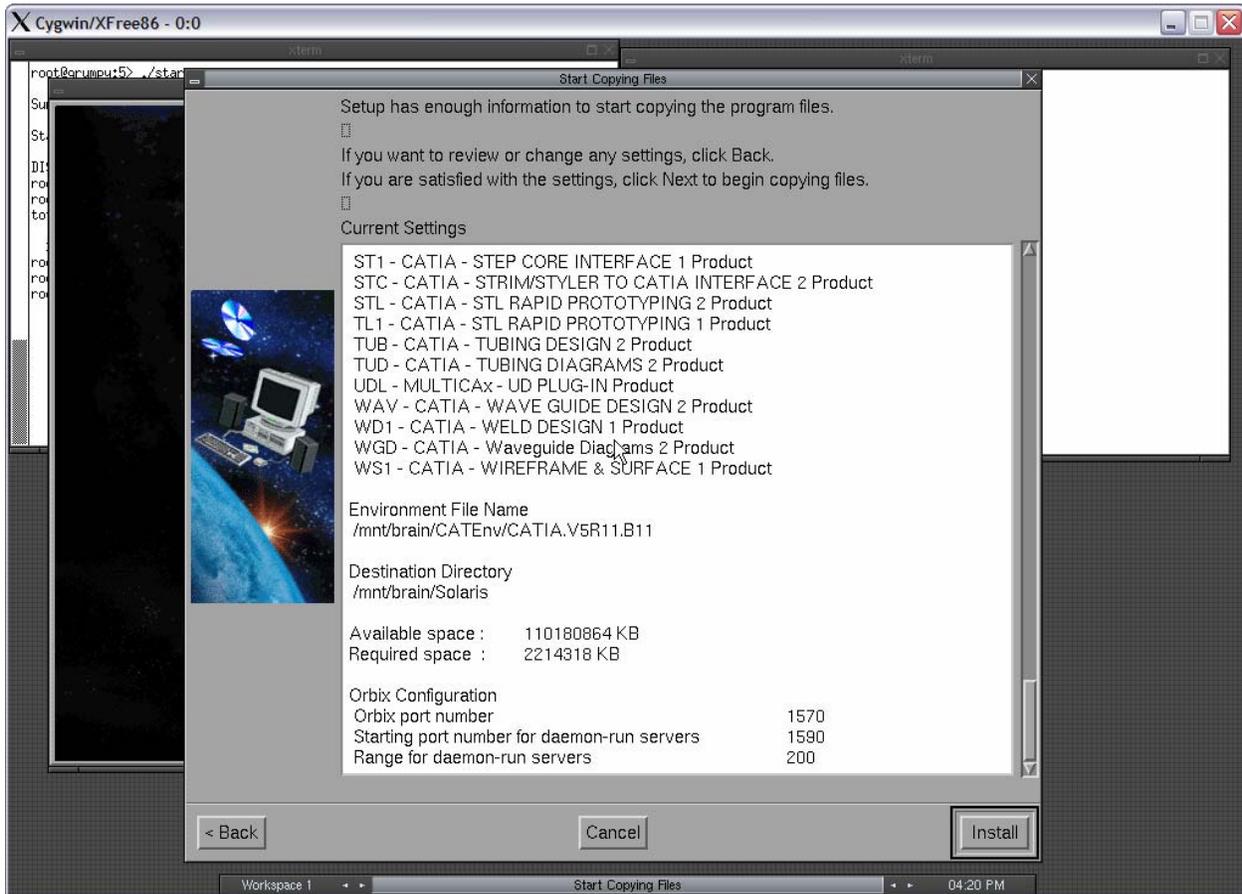


Figure 13) Finishing CATIA Installation over a Network Share

Installation of CATIA Runtime Environment on Thin Clients As before, the process for installing the CATIA runtime environment on thin clients should be scripted to suit your environment. Scripting this process will allow the deployment expert to extract the full value from a thin-client configuration by reducing administration on CATIA workstations. The process outlined below shows an example of such an install.

- Set that path of the installation directory on the server using the commands (when using `cs`h as the login shell):

```
set path=(/mnt/brain/Solaris/solaris_a/code/bin $path)
setenv LD_LIBRARY_PATH
/mnt/brain/Solaris/solaris_a/code/bin:${LD_LIBRARY_PATH}
```

- Create the following global environment, still logged in as `root`

```
setcatenv -e CatiaV5UX -p /mnt/brain/Solaris -d /mnt/brain/CATEnv -
desktop yes -new yes -a global
```

- To register document types on the client desktop, go to the directory

```
/mnt/brain/Solaris/solaris_a/code/command
```

and run:

```
./catstart -run "setcatenv -e CatiaV5UX -d  
/mnt/brain/CATEnv -regserver" -env CatiaV5UX -direnv  
/mnt/brain/CATEnv
```

- Log on using a nonprivileged user ID and verify the newly created environment.

```
cd/mnt/brain/Solaris/solaris_a/code/command;  
./catstart -env CatiaV5UX -direnv /mnt/brain/CATEnv
```

Creating Heterogeneous Storage for Design Files One of the key benefits of storing CATIA design files on a storage controller is derived from the storage controller's ability to allow multiprotocol access to the design files, both from UNIX as well as Windows workstations, and to the same set of data. A file saved from either a UNIX or Windows CATIA workstation can be accessed or modified from either a UNIX or Windows workstation using the NFS or CIFS protocols, respectively. Because of the NetApp native implementation of the NFS and CIFS protocols—they are built into Data ONTAP—users will not have to sacrifice performance for multiprotocol access to data.

In order to allow heterogeneous platforms to securely access the same set of data, file locking needs to be properly implemented. Using SecureShare®, NetApp storage controller allows UNIX clients—using the Network File System (NFS) and Network Lock Manager (NLM) protocols—and Windows systems—using the Common Internet File System (CIFS) or the (PC)NFS protocols—to share files with a high level of data integrity.

SecureShare is a multiprotocol lock management facility that is integrated into the Data ONTAP microkernel. SecureShare enables UNIX and Windows software-based applications to concurrently access and update shared files, with the integrity and cache coherency of the shared data protection by system-enforced locking and file-open semantics. At the same time, SecureShare implements a multiprotocol extrapolation of the Windows networking performance optimization known as "opportunistic locks" (oplocks). For more information on multiprotocol access and SecureShare, please see individual NetApp Technical Reports TR3014 and TR3024. For more information on opportunistic locks in Windows, see Microsoft's Knowledge Base article 129202 on the explanation of opportunistic locking.

Creating Heterogeneous Storage for Design Files Maximizing Data Availability for Design Reuse in addition to simultaneous, secure access to a single copy of design data from both UNIX and Windows, the NetApp storage controller allows access to older CATIA V4 design files. CATIA V4 files created over NFS can be accessed from a CATIA Windows workstation using CIFS. This legacy access simplifies CATIA V4 to CATIA V5 migration as well as promotes design reuse.

As design project cycles terminate and new projects are started, older projects can be archived off to a NearStore system. The benefit of using a near-line appliance for design archival is that the appliance allows easy access to the design files whenever they need to be referenced—whether for reuse in a new project or for recall based on legal or regulatory needs.

When design centers go through a CATIA upgrade from CATIA V4 to CATIA V5 to fully take advantage of the PLM features in CATIA V5, because of the design reuse tendency the centers need to be able to access CATIA V4 project files. Since CATIA V5 supports both Windows and UNIX, multiprotocol access to these older projects is important. Since NearStore runs Data ONTAP, it offers the same multiprotocol access to design data as primary storage appliances. Both the NearStore system and primary storage appliances provide significant operational benefits when upgrading from CATIA V4 to CATIA V5.

The process outlined below shows how storage for design files can be created on the appliance for use with CATIA:

- The minimum release of Data ONTAP for storage controllers serving CATIA design files is 6.3.3. This release has fixes related to CATIA and file permissions in a multiprotocol NFS and CIFS environment. For additional details, please see the NetApp [NOW](#) Web site.
- Create a qtree `CatiaDesigns` on volume `vol1` on storage controller “brain”. The example herein creates the qtree FilerView interface using the `Volumes -> qtrees -> Add` screen.



Figure 14) Creating a CatiaDesigns qtree

Data ONTAP supports three qtree security styles: UNIX, NTFS, and mixed. A UNIX qtree uses the user’s “UID” and “GID,” and the UNIX software-style permission bits of the file or directory to determine user access. An NTFS-style qtree uses Windows ACLs and ACEs to determine user access. In a mixed qtree, some files in the qtree or volume have the UNIX security style and some have the NTFS security style. A file’s security style depends on whether the permission was last set from CIFS or NFS. For details on understanding file permissions, please see the NetApp Technical Report TR3079.

For an environment supporting UNIX and Windows workstations, the qtree security style should be “mixed.” The benefit of using this security style is that it allows design file permissions to be modified from both the UNIX and Windows sides.

For environments supporting UNIX workstations that would like to use the NTFS security style, the recommended Data ONTAP version is 6.3.1 or better. UNIX workstations saving to an NTFS qtree in Data ONTAP versions 6.0.3 through 6.3 may see permission errors when trying to save designs. The following setting works to silently ignore attempts to set UNIX permission on NTFS qtrees after the design file is saved:

```
options cifs.ntfs_ignore_unix_security_ops on
```

For additional details, please see the NetApp [NOW](#) Web site.

- Note that oplocks should be enabled to enable opportunistic locking of files on the Windows workstation. Oplocks are a significant performance enhancement, but have the potential to cause loss of cached data on some networks with impaired reliability or latency, particularly on wide-area networks. In general, this option should be disabled only to isolate problems
- Create an NFS share for qtree `/vol/vol1/CatiaDesigns` using NFS -> Manage Exports screen.

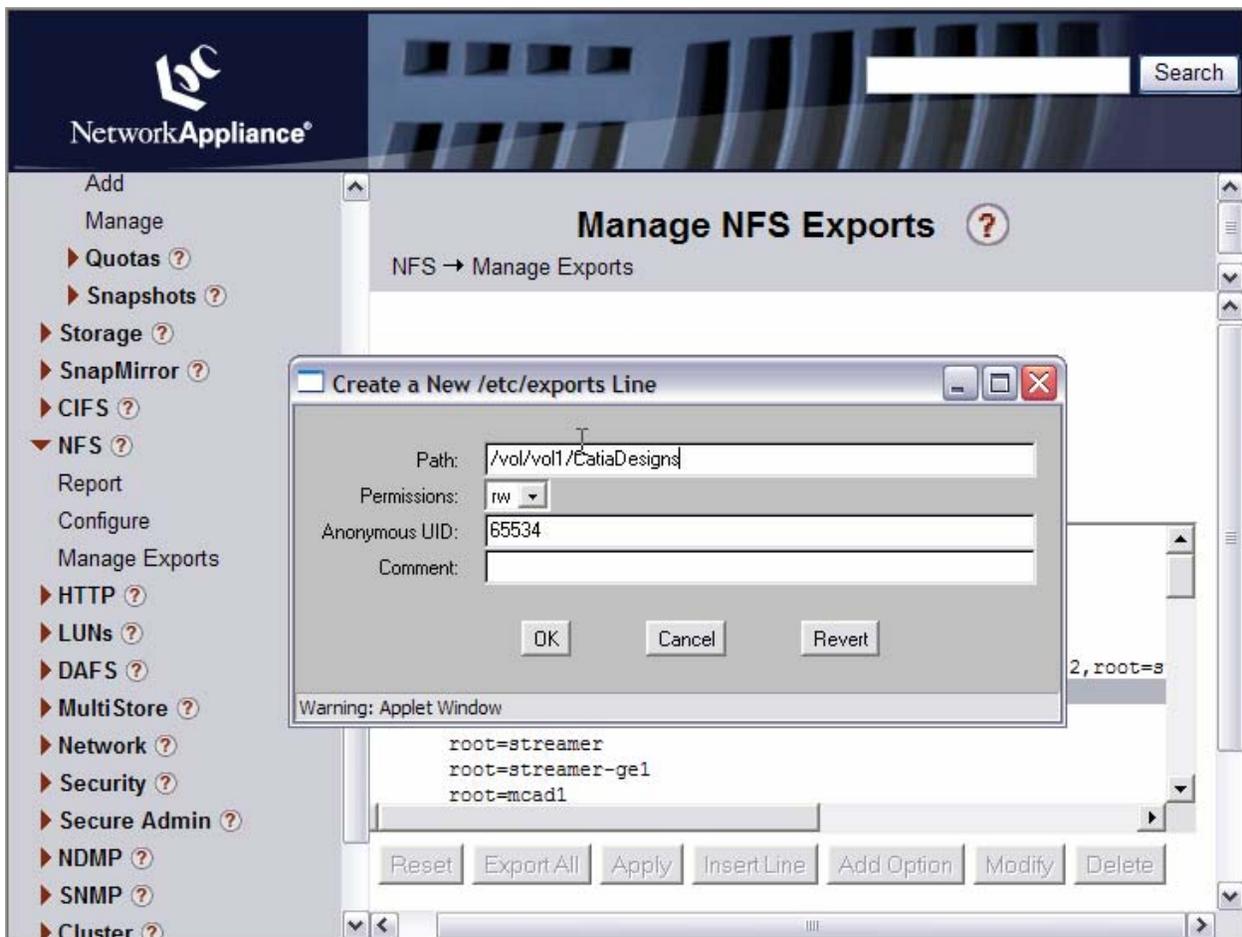


Figure 15) Creating an NFS Share for CatiaDesigns qtree

- Create a CIFS share for qtree /vol/vol1/CatiaDesigns using the CIFS -> Shares -> Add screen.

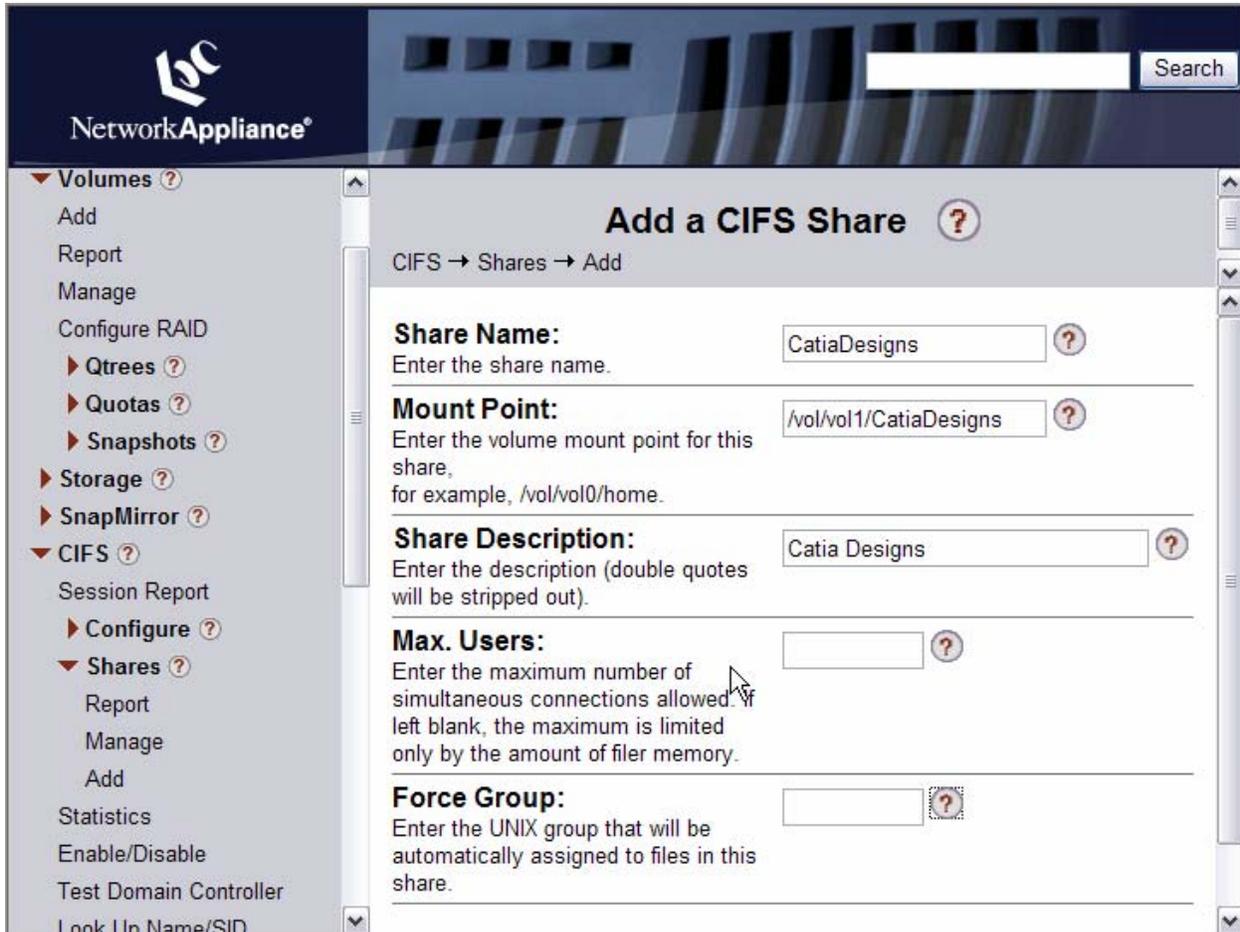


Figure 16) Creating a CIFS Share for CatiaDesigns qtree.

- The qtree /vol/vol1/CatiaDesigns now can be accessed using `brain:/vol/vol1/CatiaDesigns` over NFS and using the UNC path `\\brain\CatiaDesigns` over CIFS. NFS access can be automatically enabled using tools such as the automounter daemon and by updating the automounter maps for naming services, such as NIS, which will allow `brain:/vol/vol1/CatiaDesigns` to be mounted automatically without manual configuration on every CATIA UNIX workstation. In the example herein, one can create an automount entry so `brain:/vol/vol1/CatiaDesigns` will be automounted to `/mnt/brain/CatiaDesigns` on UNIX CATIA workstations.
- A logical DLName entry can now be created for this qtree to allow uniform access from both Windows and UNIX workstations. For example, the DLName `designs` can be pointed to the

Windows folder `\\brain\CatiaDesigns` and UNIX folder `/mnt/brain/CatiaDesigns`.

3. Migration From Catia V4 to V5

As CATIA customers migrate from V4, based on UNIX, to V5, based on Windows, they face a series of challenges that need to be addressed in order to minimize the impact on their product development and time-to-market cycles. NetApp Data ONTAP greatly mitigates these challenges by offering the customer the tools of flexibility and virtualization.

Filename Mapping

Challenge One challenge is that Windows considers "illegal" some special characters used in V4 UNIX filenames. For example, the characters `> < * : " ? \ | .` used in a V4 UNIX filename would not be accessible by a V5 Windows client. CATIA users must be able to reuse legacy design files as they migrate to V5 Windows workstations. Creating duplicate files or renaming files containing "illegal" characters is not an acceptable solution, because file attributes contained within filenames could be lost, and the financial and time impact would be prohibitive.

NetApp Data ONTAP addresses this issue with a filename mapping and translation mechanism between the UNIX and Windows file systems. This mechanism dynamically converts each "illegal" V4 UNIX character to another unused character that is accessible by the V5 Windows client.

For example, the mapping and translation mechanism in Data ONTAP converts the V4 UNIX filename `Ball<10mm.model` to `Ball|10mm.model` when the file is accessed by a V5 Windows client. The original filename is left in its original format to ensure future access by other users. When the new V5 Windows file is saved, it is saved with the translated characters in V5 format.

Solution In Data ONTAP releases 7.2 or greater, a way has been introduced to allow CIFS clients accessing a volume to refer to files that have NFS names that would otherwise be invalid for Windows without using the 8.3 names. This is done by specifying a mapping for the invalid characters into Unicode characters that are acceptable for both the Windows and the application. For example, here is a specification that can be used to map characters used by the CATIA application:

```
charmap desvol 3e:ff76,3c:ff77,2a:ff78,3a:ff79,22:ff7a,3f:ff7b,5c:ff7c,7c:ff7d
```

This command will map a set of characters (`>`, `<`, `*`, `:`, `"`, `?`, `\`, and `|`) into Japanese Unicode characters that are not normally used as normal characters in filenames. This mapping will apply to the volume named "desvol".

It is important to note that the Unicode characters must not appear normally in existing filenames, because otherwise unwanted mappings would occur, resulting in loss of the ability to access mapped files. For example, if `:` were mapped to `-`, but `-` appeared in files normally, a Windows client using the mapped share to access a file named "a-b" would have its request mapped to the NFS name "a:b", which is not the desired file.

Note that only CIFS client accesses will have this mapping. The on-disk names are the same as they would be if an NFS client were creating/operating using the mapped filenames. If the mapping is later changed, the UNIX names and DOS 8.3 names will not be affected.

Setup The mapping configuration is controlled with an "advanced" command `charmap`. The syntax is

```
charmap [<volname> [<mapspec>]]
```

The `<volname>` value must name one of the storage controller volumes. The format of the "`<mapspec>`" is as follows:

hh:hhh[,hh:hhh] . . .

Each "hh" represents a hexadecimal value. It does not have to be zero-padded, and upper- or lower-case hex "A"- "F" are accepted. The first value of each colon-separated pair is the hex value of the NFS byte to be translated, and the second value is the Unicode value to be substituted for CIFS use. If <mapspec> is not specified, the current mapping (if any) is displayed. If <volname> is not specified, the mapping for all volumes is displayed. To clear a mapping from a volume, specify and empty mapspec "".

Limitations

Case sensitivity Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. That means the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However the 8.3 name is available, and that is case-insensitive.

Partial/invalid mappings After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g., it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

FlexVol™ NetApp FlexVol technology delivers true storage virtualization solutions that can lower overhead and capital expenses, reduce disruption and risk, and provide the flexibility to adapt quickly and easily to the dynamic needs of the enterprise. FlexVol technology pools storage resources automatically and enables you to create multiple flexible volumes on a large pool of disks. This flexibility means you can simplify operations, gain maximum utilization and efficiency, and make changes quickly and seamlessly. Administrators can add storage when and where needed, without disruption and at the lowest incremental cost.

Prior to Data ONTAP 7G, the size of a new CATIA repository needed to be planned carefully to find a balance between future growth and efficient utilization of storage resources. Typically, storage administrators were forced to allocate more storage than required to account for future growth or inaccurate estimates of storage requirements. This practice resulted in poor utilization and increased cost of storage. Once the size was determined, it was hard to change the size of the volume. FlexVol eases the management of storage resources by giving administrators the power to adjust volume capacity on the fly according to current business requirements. In the process of V4 to V5 migration, a small V5 flexible volume can be created initially; as more and more V4 files are migrated, the V5 volume can be expanded dynamically to accommodate more files. When transient design files are deleted, the volume can be reclaimed for other purposes.

4. Summary

NetApp delivers a fast and efficient storage infrastructure for support of CATIA deployments. New installs or upgrades of CATIA can be quickly and easily deployed on NetApp storage infrastructure using a thin-client approach. NetApp Snapshot copies and SnapVault software provide data protection to CATIA binaries, settings, and design data through online backups and near-line replication. NetApp solutions make a CATIA infrastructure easy to deploy and manage, reducing costs, increasing IT and engineer efficiencies, and enabling a faster time-to-market for product manufacturers.

5. References

NetApp Technical Library

| Document | Link* |
|---|---|
| TR 3001: Storage Networking Appliance | http://www.netapp.com/library/tr/3001.pdf |
| TR3014: Multiprotocol Data Access: NFS, CIFS, and HTTP | http://www.netapp.com/library/tr/3014.pdf |
| TR3024: SecureShare®: Guaranteed Multiprotocol File Locking | http://www.netapp.com/library/tr/3024.pdf |

Microsoft Professional Support

| Document | Link* |
|---|---|
| Explanation of Opportunistic Locking | http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q129202& |
| Client-Side Caching and Offline Files and Folders | http://www.microsoft.com/windows2000/en/professional/help/default.asp?url=/windows2000/en/professional/help/file_srv_csc_and_shares.htm |
| TR3024: SecureShare®: Guaranteed Multiprotocol File Locking | http://www.netapp.com/library/tr/3024.pdf |

6. Glossary

Terms

ACE: Access Control Entries
 ACL: Access Control List
 CAD: Computer-Aided Design
 CAE: Computer-Aided Engineering
 CAM: Computer-Assisted Modeling
 CIFS: Common Internet File System
 CRM: Customer Relationship Management
 DB: Database
 DLL: Dynamic Link Library
 DLName: Dynamic Link Name
 DMU: Digital Mock-Up
 ERP: Enterprise Resource Planning
 NFS: Network File System

NLM: Network Lock Manager

NTFS: (Microsoft Windows) NT File System

OLE: Object Linking and Embedding

PDM: Product Data Management

PLM: Product Lifecycle Management

UNC: Universal Naming Convention

NetApp Products

[Data ONTAP](#): Software; highly optimized and scalable operating system for unified information management in heterogeneous environments.

[Filer/FAS](#): Hardware; powerful, high-performance, high-availability enterprise servers and file servers.

[NearStore](#): Hardware; cost-effective, fast-access, online archival (near-line) storage.

[Snapshot](#): Software; up to 255 instantaneous online copies of online data.

[SnapRestore](#): Software; restores data in record time.

[SnapVault](#): Software; simple and efficient data protection.

7. Revision History

| Date | Name | Description |
|------------|----------------|-------------|
| June 2006 | Rajesh Godbole | Update |
| April 2005 | H. T. Sun | Update |

