Whitepaper

User Profiles

Author: Nicholas Dille (nicholas.dille@sepago.de), sepago GmbH

Location: http://blogs.sepago.de/nicholas/tag/user-profile-whitepaper/

Contributors	Topics
Nicholas Dille, sepago GmbH (http://blogs.sepago.de/nicholas)	Windows Operating Systems Presentation Server Citrix Application Streaming Profile Migration
Helge Klein, sepago GmbH (http://blogs.sepago.de/helge)	Windows Operating Systems Citrix Profile Management
Clemens Geiler, sepago GmbH	Microsoft Application Virtualization Citrix Application Streaming
Marc Schröter, sepago GmbH	Microsoft Application Virtualization
Marcel Meurer, sepago GmbH (http://twitter.com/MarcelMeurer)	Microsoft Application Virtualization Citrix Application Streaming
Sascha Juch, sepago GmbH	Profile Solution Checklist
Maik Weber, sepago GmbH	Citrix Profile Streaming

Management Summary

This technical whitepaper describes the concepts behind Windows user profiles and explains common pitfalls and how to avoid them – both with and without the profile optimization solution Citrix User Profile Manager.

User profiles store application and configuration data for individual users. Contrary to popular belief, this data **is** business critical; since each user's familiar working environment is contained within his or her profile.Thus, successfully managing this kind of data is essential for any enterprise, because inconsistent or lost personal settings cause expensive help desk calls and effectively prevent the user from working.

Instead of providing several different mechanisms to resolve the challenges of user profile management, Citrix Profile Management overcomes the inherent limitations of Windows user profiles by replacing the classic process of loading and storing personal settings with an advanced approach of merging settings from several devices and sessions. Citrix Profile Management not only supports terminal servers, but also client operating systems. As today's application delivery methods become more and more heterogeneous it is more important than ever to provide one single set of personal settings on any device via any delivery method.

As application and desktop delivery becomes more complex, the limitations of classic Windows user profiles become evident because they were designed only with fat clients in mind. But in today's world of virtualized applications and desktops, the basic assumption is not true anymore that every user accesses applications from only one device. Citrix Profile Management overcomes these fundamental limitations of classical user profiles and combines high flexibility and performance with practically maintenance-free operation.

The limitations of Windows user profiles pose several challenges to architects of modern application and desktop delivery infrastructures. For one thing, low logon times are directly related to small user profile sizes – a large profile causes the logon to be prolonged. This holds true as long as profile streaming is not used. Considering that profiles usually grow over time, the logon time continuously grows, too, which intersperses a user's workflow with artificial pauses. For another, when a user works on more than one physical or virtual device, his individual settings may be overwritten in a seemingly random manner when he logs off – this is known as Last Writer Wins.

But modern application and desktop delivery poses more challenges concerning user profiles. Virtualization enables a user to access his applications from almost any device. Without carefully designing the delivery of such applications and desktops, a user's settings are spread over multiple devices instead of travelling with the user.

Windows provides methods which are considered to be remedies for the challenges encountered in application and desktop delivery. In fact, each of these methods solves a single challenge and lessens the effect of one or more others. But even with all stops pulled out, the issues of user profile management are not adequately addressed without a solution like Citrix Profile Management.

This document closes by presenting guidelines how to choose a profile solution by offering subjects to attend to when comparing solutions and offering an insight into profile migration.

Contents

1 Introduction

Microsoft Windows is the most widely used operating system for professional office workers. Products like Microsoft Office dominate the market. The corresponding file formats for documents, spreadsheets and presentations are de facto standards for the exchange of information.

In order to communicate with business associates, employees need to be provided with a Windows-based workspace where these standards are honored. This can be a Windows-based fat client, a shared desktop provided by Citrix XenApp or personal desktops served by Citrix XenDesktop.

As modern IT infrastructures are expected to incorporate a constantly growing number of requirements, they are becoming more and more complex. The challenge, IT departments face, is to design and operate complex but not complicated environments. With respect to application delivery, several options allow for a flexible composition of the users' workspace: natively installed applications, remote applications and streamed applications. Thin clients, virtual desktops and mobile users add to the complexity.

By deploying applications using more than one mechanism or by allowing for more than one type of application, a user will be assigned more than one user profile in which to save settings and files. For the user it is not discernible that there is a technical necessity for multiple profiles, he only observes that his settings are present in one application but not in another because it was configured in only one of his profiles.

To remedy this, vendors have created products to manage settings across multiple devices.

1.1 Document Structure

This technical whitepaper offers a general overview of user profile management. There are several challenges which have to be met in order to provide a consistent user environment.

Starting with the basic principles, a general introduction to user profiles is provided describing mechanisms and common pitfalls. All four types of Windows user profiles are explained: Local, Roaming, Mandatory and Temporary.

The following chapter introduces the types of environments in which customers rely heavily on user profiles. It serves to clearly define the field of business this paper applies to.

After describing the environments in which user profiles play an important part, the document moves on to typical challenges and then elaborate why user profiles are not easily managed in the presented context.

There are some traditional remedies which are called upon to meet the challenges. After describing the idea behind the individual solutions, a discussion of advantages and disadvantages is presented.

The second to last chapter introduces a powerful solution for user profile management called Citrix Profile Management which supersedes the traditional remedies.

In the end, a set of guidelines for evaluating user profile management solutions is presented and the effect of profile migration is offered.

2 Basic Principles

User profiles are a key component ofWindows-based operating systems. Whenever a user logs into a system, he is assigned a user profile to save personal and configuration data. All information contained in a user profile is saved persistently to be restored at the time of the next login to provide a consistent environment.

There are two types of data contained in a user profile: registry and file system information. The registry data is stored in a file called `NTUSER.DAT` which resides in the root folder of the profile. Its content is loaded as `HKEY_USERS\<SID>` at the time of the login where `<SID>` represents the user's security identifier and is accessible by the alias `HKEY_CURRENT_USER` (also known as `HKCU`) from within the user's session.

Several folders within the profile have a special purpose. For example, the user's desktop is located in a subfolder of the user profile called `Desktop`. These well-known folders include the following:

- The folder `Application Data`is used by applications to store their settings which often include configuration data set by the user.
- `Local Settings` contains information which is valid on a single system only. Its contents should not be moved over to other computers. Whenever a profile is copied over the network, the contents of this folder should bediscarded.
- The folder `SendTo` holds links to applications that are frequently used to open documents. These links appear on the context menu of files in Windows Explorer. For example, a link to a text editor is often provided here to enable users to quickly edit files of any type without changing file type associations.
- The content of the Start menu is built from the two folders called `Start Menu`.One is located in each user's profile and the other inside the `AllUsers` profile on the current system.
- The folder `My Documents` stores a user's personal files.

German counterparts of the folders listed are called Desktop, Anwendungsdaten, Eigene Dateien, Lokale Einstellungen, SendTo and Startmenü.

The default location for a user's profile is `%SystemDrive%\Documents and Settings\%UserName%` on Windows Server 2003 and Windows XP or, short, `%UserProfile%`. Beginning with Windows Vista, Microsoft has rearranged directories placing user profiles in `%SystemDrive%\Users`. The traditional directory names are maintained as junctions in the NTFS. The folder name of the users' profile directory was changed to `%UserName%.%UserDNSDomain%` with Windows Server 2003 Service Pack 1 to accommodate for users with the same account name logging on from different domains (see knowledge base article 821929: http://support.microsoft.com/kb/821929/en-us).

In the following four sections, different types of user profiles are described. Each type provides a unique set of features and is applicable to a separate environment and type of use.

2.1 Local Profile

The local profile is the default type of user profile. It is generated for users who do not have a profile location assigned as described in chapter 2.7.

If a user has not logged on to the local system before, a new local profile is derived from the default user profile (see chapter 2.5 for details). After logging off, a local profile is neither deleted nor stored centrally but is retained on the local system.

2.2 Roaming Profile

Roaming profiles are widely used in environments in which users frequently log on to different systems.

Roaming profiles are stored on a central file share, copied to a computer during logon and cached locally in a subfolder of the profile directory (default on Windows XP and Server 2003: `%SystemDrive%\Documents and Settings`; default on Windows Vista and Server 2008: `%SystemDrive%\Users`). All changes made during a session are stored in the local copy. They are propagated to the central profile file share when a user logs off. A roaming profile is loaded from or written to the network share file-by-file, based on each file's modification time stamp.

If the file share does not contain a roaming profile for a user when he logs on, a new profile is created locally which is propagated to the file share upon logoff.

Roaming profiles allow for stateless workstations which do not contain any configuration data.

In most cases profiles should not be used on different versions of Windows – i.e. a profile that has been created on Windows XP should not be used on Windows Server 2003.

Microsoft provides an article describing how to configure permissions on a profile share ensuring the user's privacy: Security Considerations when Configuring Roaming User Profiles (http://technet.microsoft.com/en-us/library/cc737633.aspx)

2.3 Mandatory Profile

In some setups it is beneficiary if settings are discarded after the user has logged off. Such a user profile is called mandatory (Mandatory Profile). It is created by renaming the registry file `NTUSER.DAT` to `NTUSER.MAN`.

A mandatory profile works just like a roaming profile with one big exception: when a user logs off, the local copy of hisprofile is not copied back to the file server. Instead it is deleted and all changes made during the session are lost.

Mandatory profiles are typically very small and thus allow for fast logons. They are mainly used on kiosk systems where users only need a temporary work environment that need not be retained.

Using mandatory profiles causes several problems and, thereby, restraining the user: Private keys cannot be saved in the key store causing signatures and encryption to stop working. The permissions of the user's registry are different from a personal profile because a single profile is used for many users. All users are able to browse and modify the registry hives loaded under HKU. The latter presents a major security breach.

2.4 Temporary Profile

Whenever the system fails to assign a proper profile to a user, a temporary profile is created in the default location (`%SystemDrive%\Documents and Settings` or `%SystemDrive%\Users`). Although a user is able to work and modify all available user settings, the temporary profile is deleted as soon as the user logs off resulting in all customizations to be lost.

Temporary profiles are used by Microsoft Windows as a last resort when a session needs to be created but network problems or misconfiguration prevents access to the centrally stored user profile.

2.5 Special Profile Folders

Windows-based operating systems contain several special user profile folders.

There is a special folder called `AllUsers` which contains common configuration data which is used in all user sessions. The folders `Start Menu` and `SendTo` are especially important. In Windows Vista and Windows Server 2008, this folder is now a junction pointing to `%SystemRoot%\ProgramData` inside the default profile location.

The `DefaultUser` profile is used to create a new profile if a user does not have a profile yet (either locally or on a file server). This folder is now a junction in Windows Vista and Windows Server 2008 pointing to `%SystemRoot%\Users\Default`.

The registry contains a hive called `HKU\.DEFAULT` which is often mistaken as the default user profile. In fact, it provides user configuration data before a user has logged on. For example, the wallpaper for the login screen and the state of the NumLock key is configured there.

Windows also provides a profile for the local system account which is located under `%System-Root%\System32\Config\Systemprofile`.

2.6 Troubleshooting User Profiles

Some errors are written to the Application Event Log but a detailed log can be enabled by setting the registry value `UserEnvDebugLevel` as a `REG_DWORD` to 0x10002 under `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon`. The log file can be found at `%WinDir%\Debug\UserMode\UserEnv.log`. It is not necessary to restart the machine for the change to take effect.

This feature has been removed from Windows Vista and Windows Server 2008. There is no replacement for troubleshooting logons.

2.7 Assigning User Profiles

There are several ways to assign a profile to a user. Each of these techniques has its advantages and disadvantages which are discussed in this chapter.

- **Active Directory User Object.** A user profile is configured in Active Directory by using the *Profile* or *Terminal Server* tabs ofthe user object properties dialog. The path to the user profile is to be entered in UNC format.
  The user object's profile path property can be set by scripts, e.g. if a customer needs to distribute user profiles across several file servers. This makes the assignment of profiles very flexible but the downside is that it is difficult to figure out where an individual user's profile is located.
- **Active Directory Group Policies.** Starting with Windows Server 2003, a user profile can be assigned by Group Policy[1] but is restricted to terminal server. This mechanism allows profiles to be tied to the location of computer objects in Active Directory. In Windows Vista and Windows Server 2008, the profile path can be assigned for all machines (see section 5.7.1) including clients and servers without terminal services.
  Due to the fact that Group Policies are tied to organizational units, assigned profile locations on a single server are usually easy to resolve. On the other hand, the fact that this setting is machine-based, this mechanism does not allow users on a single machine to have entirely different profile locations.

These two options either allow for flexibility or manageability and it is for the administrator to decide which method to use.

[1] Computer Configuration → Administrative Templates → Windows Components → Terminal Services → Set path for TS Roaming Profiles

2.8 Managing Cached User Profiles

As explained in the introduction to this chapter, user profiles are cached in a single directory (default: `%SystemRoot%\Documents and Settings` on Windows XP/Server 2003 and `%SystemRoot%\Users` on Windows Vista/Server 2008). Unfortunately, it is not possible to determine which profile has which type by simply listing the profile directory's contents. Instead Windows operating systems provide a dialog to manage local or cached profiles, which is located in the Control Panel[2].

This dialog lists all profiles that are stored on a computer along with their type (roaming, local, mandatory or temporary) and the user they belong to. The administrator can select individual profiles and delete them or move them to a different location.

Deleting unneeded profiles can also be achieved by configuring a setting in a Group Policy which forces systems to remove cached roaming profiles after a user has logged off[3].

[2] *System*→ Tab: *Advanced*→ Section: *User Profiles*→ Button: *Settings*

[3] Computer Configuration → Administrative Templates → System → User Profiles → Delete cached copies of roaming profiles

3 Environment

This chapter describes which environments and products this whitepaper applies to.

3.1 Remote Desktop Services

In Windows-based operating systems since Windows 2000[4], Microsoft integrates Remote Desktop Services (RDS)[5] to deliver applications and remote desktops. Users are enabled to access applications installed on a centrally located server, the Remote Desktop Server, which sends display information about the desktop and applications to the user's workstation and reads control data (e.g. keyboard and mouse) from it. Therefore, these applications are controlled remotely by the user. The protocol used by Microsoft is called Remote Desktop Protocol (RDP).

Although a user needs a permanent network connection to the Remote Desktop Server, this infrastructure allows for several changes with respect to system administration. The user's workstation does not need to have all applications installed locally, reducing the complexity of the system and allowing for Thin Clients to be used.

In such environments, roaming profiles are mostly used because this type of profile enables the user to transparently log into different systems and always obtain his configuration data. He is provided with a consistent workspace.

3.2 Citrix XenApp

Citrix offers an alternative to pure Remote Desktop Services, called XenApp (previously known as Presentation Server[6]). It is a value-add to internal components of the Windows operating system. XenApp uses a proprietary communication protocol called Independent Computing Architecture (ICA) created by Citrix implementing many patented technologies to enhance the quality of the exchanged data resulting in generally lower bandwidth consumption than RDP.

Whereas RDS are hardly used in large environments, XenApp adds many features vital to larger enterprises. These features include the following:

- The concept of a server farm is introduced which allows many servers to be managed centrally from a single console.
- Servers in a farm can be configured in groups to show identical or equivalent behavior by using policies.
- Administrative rights can be delegated to individuals or groups allowing certain rights needed for daily tasks.
- A sophisticated load balancing system distributes users among servers in a farm depending on a configurable set of rules, for example, based on system performance or managed groups.

In such environments, the use of roaming profiles is even more important because users are distributed among all member servers of a farm by the load balancing system. Therefore, there is a high probability of being assigned to different servers upon consecutive logins resulting in users being very loosely coupled to servers.

---

[4] For Windows NT, a special Terminal Server Edition was created.

[5] Formerly: Windows Terminal Services (WTS)

[6] Formerly: MetaFrame Presentation Server, MetaFrame XP Presentation Server, MetaFrame, WinFrame and Windows NT Terminal Server Edition.

3.2.1 Special Folder Redirection

Beginning with XenApp 5.0, Citrix implements Special Folder Redirection for Windows Server 2008. Special folders in the user profile (see section 2.5) are redirected to the corresponding folders on the local drives of the client device.

This feature helps presenting the same environment to the user independent of the location of the session. On the client device, the users access the special folders according to the configuration of the device. In a remote session, every access to the special profile folders is redirected to the corresponding special folder in the user profile of the client device.

3.3 Citrix Application Streaming

In version 4.5 of Presentation Server, Citrix added an Application Streaming component to the product. It allows for streaming applications to clients and Presentation Servers. It is licensed through XenApp Enterprise and Platinum Editions.

Application Streaming is based on Application Isolation Environments (AIEs), which were introduced in Presentation Server 4.0 to redirect access to the file system and the registry. This mechanism allowed for applications to be deployed through Presentation Server which are not fit to be executed on Remote Desktop Services.

In Presentation Server 4.5, AIEs evolved into Application Streaming. Citrix ships a profiler which monitors the installation of applications and repackages them into an application package which are then streamed to servers or clients from a file share (CIFS) on the network. Packages are not transferred to a device as a whole but instead files contained in package are downloaded on-demand and cached in `%ProgramFiles%\Citrix\RadeCache\<Suite>` on the streaming client.

Every application package contains a set of rules which describe where read and write operations to the file system and the registry are redirected to. The following target paths are pre-defined in the profiler:

- Machine-based settings in the file system: `%ProgramFiles%\Citrix\RadeCache\<Suite>`
- Machine-based settings in the registry: `HKLM\SOFTWARE\Citrix\RadeCache\<Suite>`
- User-based settings in the file system: `%AppData%\Citrix\RadeCache\<Suite>`
- User-based settings in the registry: `HKCU\SOFTWARE\Citrix\RadeCache\<Suite>`

For a user to be able to run a streamed application, his device (client or terminal server) is required to have the RADE client installed. If a streamed application is deployed through Presentation Server, this client needs to be deployed on the server.

3.4 Microsoft App-V[7]

Softricity came to the market in 2001. With their product Softgrid Application Server they offered a Client/Server solution for streaming virtualized applications to Windows desktop clients and/or Windows Terminal Server clients. In May 2006, Microsoft acquired Softricity and integrated Softgrid Application Server into their System Center product line. It is now called Microsoft App-V.

For running virtualized applications streamed from Virtual Application Server to client devices like PCs or notebooks, users need the Client for Windows Desktop. With the Client for Terminal Server there exists an alternative for being used in environments with Remote Desktop Services or Citrix Presentation Server.

[7] Formerly: Softricity SoftGrid, Microsoft SoftGrid, Microsoft Application Virtualization

With App-V the user benefits from true application isolation and streaming capabilities. The application launch uses RTSP(S), which means the application behaves like a streamed movie. Initially, only the amount of code necessary for an application to launch is streamed down to the client (typically 20-25%) and stored in a system wide local cache directory on the system. Subsequent launches of the application will not require additional bandwidth, since the application already resides in the local cache. On consecutive launches, the only communication between client and server deals with authentication and dynamic application updates.

Besides the global settings which are valid for a whole application suite (e.g. Microsoft Office), there are numerous settings and files which are stored per user. These settings or files don't interfere with the centrally stored virtual application package. All user specific changes are stored in a so called user profile[8] which is created once per user and application package.

The default path for the user profile is `%AppData%`, which is a system variable and points to a subdirectory within the users Windows profile. Inside `%AppData%`, App-V creates a subdirectory called "Softgrid Client".

This path can be configured during the installation process or with the parameter SWIUSERDATA in an automated installation. After the installation process, the path can be changed via the Softgrid Client Management Console or by changing the values under the following registry key:

```
HKLM\Software\Softricity\SoftGrid Client\CurrentVersion\Configuration
```

In addition, the profile path can be defined centrally by using an ADM-template within a GPO.

Changes made to the key during a user session will only be processed after the user reconnects to an App-V session.

The App-V profile acts as a repository of all user-specific settings for each application. This data is maintained on per-application-per-user basis. It contains the following information:

Application Settings are maintained in the file `UsrVol_sftfs_v1.pkg`. This file contains the virtual Registry (HKLM and HKCU) for the application. Each time an application is being launched it picks up its settings from this file. During the session, changes are written to a temporary file called

```
%UserProfile%\Local Settings\Application Data\SoftGrid
Client\Streamed_App_<GUID>\UsrVol_sftfs_v1.tmp
```

As the user closes the application, changes are written to a file called

```
%USERPROFILE%\Application Data\SoftGrid Client\Streamed_App_<GUID>\
UsrVol_sftfs_v1.pkg
```

The temporary file mentioned above will be deleted at the same time and recreated at the next launch.

SoftGrid usage history is provided in a file called `sfthistory.dat`.

User Information is written to a file called `userinfo.dat`.

Shortcut information is written to a file called `shortcut_ex.dat`. This file provides information about all shortcuts for all applications the user is authorized to use.

All user specific settings are conserved even whenan application is removed from a computer. If the file `UsrVol_sftfs_v1.pkg` is deleted from a user's profile, the settings for that application are reset to the "factory settings" contained in the package.

The Microsoft SoftGrid Client Management Console has a repair function which does exactly this: The file `UsrVol_sftfs_v1.pkg` is deleted from the user's profile. At the next launch time the application creates a new personal settings file.

[8] This user profile is not to be confused with a Windows user profile.

The location of the above files can be read from the following registry values:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
```

and

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local AppData
```

3.5 Citrix XenDesktop

In the last few years, many vendors have started offering products that provide virtualized desktops. In contrast to published (shared) desktops served by XenApp, virtual desktops represent hosted desktop operating systems located in the datacenter. In addition there is an infrastructure component usually called Session Broker which assigns users to clients which is usually performed on a 1:1 basis.

Such desktops are usually provided to off-shore developers and users running applications with high requirements regarding system resources. Due to the nature of how the presentation of an application is sent to the user, virtual desktops are bound to experience the same restrictions as shared desktops because the same communication protocols (ICA or RDP) are used. Vendors are putting a lot of effort in making virtual desktops execute graphic intense application through remoting audio, video, Flash, DirectX, OpenGL and even the GPU.

4 Challenges

In today's complex IT environments administrators face several challenges in implementing user profiles. Not only do the users want short logon and logoff times, they also expect their personal settings to be present in any session on any device they work on. Administrators, on the other hand, need a reliable solution that is easy to maintain while the management focuses on low operations costs.

Most organizations use roaming profiles to store their user's settings. The roaming profiles are stored on one or more file servers on the network. In an ideal world each user would have one roaming profile that would contain all his personal settings (in real life often more than one profile per user is used, see chapter 5.1). These settings would be loaded on each device during logon and written back to the central file share during logoff. While this sounds like the perfect solution in fact it has several drawbacks which will be discussed in this chapter.

Let us have a look at what happens when a user logs on to a Windows machine. After verifying credentials the operating system determines the type of user profile to be used. If the user has a roaming profile configured Windows connects a drive letter to the profile share and copies all files stored in the profile directory down to the local machine. However, before copying the profile directory tree Windows checks whether a local copy of the profile exists by comparing the date of the local copy of `NTUSER.DAT` with the date of its network twin. If both dates are identical the local copy is current and there is no need to copy the profile over the network.

While the user works in his session the local copy of the user profile is updated.

As the user logs off Windows checks which files have been changed and copies back only those to the file server.

4.1 Last Writer Wins

A classic in terminal server environments, this problem is easy to explain but not easy to remedy. It is inherent in the way Windows handles roaming profiles.

The last section explained how the operating system copies roaming profiles from a file share to the local disk during logon and copies changed files back to the network during logoff. While this works well in simple one-user-per-desktop scenarios, it gets problematic in terminal server environments where often silos are used. Think of a silo as a group of servers that have the same set of applications installed. Thus silos are a way of partitioning servers into different groups that offer different applications. With silos users typically access applications from more than one silo concurrently. As a consequence multiple copies of their profile are being used and changed – one copy per terminal server the user is accessing.

This gets problematic during logoff. In the first session to close Windows determines which files inside the profile have been changed and writes back those files to the file server. Things work as expected until now. But when the next session ends Windows writes the changed files from that session to the same location overwriting any older version that already exists there. Changes of the first session are being overwritten and thus are lost. This is called the **Last Writer Wins** problem.

One might argue that different applications change different files so that files from different silos do not overwrite each other. This may be true for the file system, depending on the setup of your environment, but the user's registry is stored in asingle file called `NTUSER.DAT` which is always written back during logoff.

To sum this up, if one roaming profile per user is used in a siloed terminal server environment only the registry changes from the last session to close persist. Depending on the silo design the same is true for files stored within the user's profile.

4.2 Profile Size and Logon Speed

During logon Windows checks whether it is necessary to copy a roaming profile down to the local machine. This is the case if either no locally cached **current** version of the profile exists or if the local copy of the profile is older than the copy on the file server. In terminal server environments cached copies of roaming profiles are typically deleted at logoff so that Windows always copies the profile over the network.

Logon time is obviously prolonged by the time it takes to transfer the whole profile over the network. Since user profiles can grow quite large, the logon time is usually adversely affected by this behavior. Another, not well known factor for slowing down the copy time substantially, is the number of files within the profile. It takes considerably longer to copy 100 files of 10 KB size each than one single file of 1 MB size. Unfortunately, user profiles are often comprised of large numbers of small files – several thousand files per profile are not uncommon. To conclude, the larger your profiles are and the more files they contain the slower your logons will be.

A new approach to increasing logon speed is transferring individual files in the profile on-demand. Although workspace is available much faster, accessing large files may take some time to retrieve the file from the central store. In addition, there are grave issues regarding consistency of the data contained in the profile. If logically connected data is only partly used in separate session, writing back modifications may result in inconsistencies because the individual pieces do not add up to a logically consistent application data. Profile streaming will also cause pains for mobile or offline users forcing the implementation to provide a locally cached copy.

4.3 Profile Inconsistency

A user profile is a set of related files and folders. Since the chance of transmission errors in today's networks is extremely low, you might conclude profile corruption is a theoretical problem. Yet, the problem is real. It is responsible for a nice percentage of user management and support cost.

This is due to the fact that a user profile comprises an entity where the various parts depend on each other. For example, if an application changes a registry value that points to a certain directory but "forgets" to create the folder, the settings in the profile become inconsistent. That is what so-called corrupt user profiles should really be called: *inconsistent*.

The problem with inconsistent profiles is that they can cause any number of strange errors that are very hard to debug. So most administrators tend to delete a profile first and ask questions later. In many cases weird problems can be fixed in this way. But what about users who spent valuable time configuring all those settings stored in their profile? Apart from being frustrated they are going to configure it all over again, burning money in the process.

4.4 Citrix Streamed Applications

Applications delivered by the streaming component of Presentation Server 4.5 are virtualized and thus isolated from the underlying operating system. Since the whole point of application virtualization is to sandbox programs, write operations to the file system or the registry have to be redirected so that the "real" registry and file system remain unchanged. Citrix chose the user profile as the redirection target, specifically `%Userprofile%\Application Data\Citrix\RadeCache` for files and `HKCU\Software\Citrix\RadeCache` for registry keys. Since redirected files and keys are stored in the user profile Citrix application streaming is susceptible to the problems described earlier (see chapter 4.1): increased profile size and low logon speed.

As these settings are stored inside the user profile, they are synchronized with the profile and are made available in consecutive sessions. However, there is no use case for providing a single application on the local machine and as a streamed application. This scenario only causes administrative

overhead due to several deployment methods. Therefore, a profile solution does not need to redirect settings between the Rade Cache and the original location.

4.5 Mobile Users

Mobile users running Windows on their laptops typically have local profiles configured to be independent of network connectivity. This leads to several problems:

- There is no easy way to backup local user profiles on laptops. If a machine has to be replaced due to hard- or software failures the user's settings are lost.
- Mobile users often not only access locally installed applications but also connect to terminal servers where they get a different user profile. Since their personal settings are stored in two or more locations they spend valuable time redundantly configuring their environment according to their personal taste.

4.6 Dual-Mode Streaming

The streaming component of Citrix Presentation Server 4.5 has a very interesting feature called **Dual-Mode Streaming**. It essentially works as follows: If a user starts a streamed application over the WebInterface the server decides whether the client is "fit" to run the streamed application locally or whether the package should rather be streamed to a terminal server and launched there. As versatile as this feature is, it creates the problem that one application, say Microsoft Outlook, is sometimes executed on a client OS and sometimes on a terminal server. Since in most environments user profiles are strictly separated between clients and terminal servers this, too, leads to the situation that one and the same setting needs to be configured twice. This can be confusing and irritating for users.

4.7 Platform Boundaries

Although the format of user profiles has not changed a lot since Windows NT, many administrators are reluctant to share one profile across platform boundaries. This is partly due to the fact that it could lead to significant problems when applied to NT4 and Windows 2000. The real reason why in most cases profiles cannot be shared across platforms is that user profiles contain many platform specific settings like the paths to applications and their data. Using one profile on multiple platforms is only feasible if the configuration of the operating system and all additional applications is identical on the participating systems.

The matter is further complicated by the fact that user profiles up to and including Windows Server 2003 are language dependent, though x64 versions of Windows use MUI packs and therefore the *English* user profiles.

Finally, Microsoft restructured user profiles in Windows Vista (and Server 2008). To prevent older profiles from being used on these newer operating systems the postfix `.V2` is automatically added to the profile path.

In an article about Best Practices for User Profile (http://technet.microsoft.com/en-us/library/cc784484.aspx), Microsoft describes the conditions under which a user profile can be shared between the same and different versions of operating systems. These requirements are very detailed and effectively restrict the supported scenarios.

4.8 Locked Profiles

In some situations, a user profile cannot be unloaded although the user has already logged off. This is usually due to processes keeping open a handle on a file or a registry key[9]. Windows waits indefinitely for such a process to release the handle. Consecutive logon attempts of the same user will result in a local or a temporary profile (see section 2.4) or may even fail depending on the configuration.

Anti-virus software is a very common cause for this problem. Sometimes, the issue may as well be caused by a system process belonging to Windows.

Locked profiles and the effects thereof are observed on terminal servers in particular. One cause is that many system resources are shared among users. Although locked profiles do occur on clients as well, it does not happen as frequently as on terminal servers.

4.9 Misbehaving Application

Some applications are poorly designed and use a directory outside of the user profile to store user-specific configuration data. These settings will not roam with the profile, although they are necessary for the user to experience a consistent workspace across several machines.

[9]Very occasionally, there is a valid reason for holding a lock on a file after the user has logged off. In most cases it is the result of sloppy programming.

5 Traditional Remedies

In this chapter we discuss traditional remedies, which are recommended to solve the previously presented challenges. These well-known remedies are described and related to the challenges they solve or which effect they reduce.

5.1 Multiple Profiles

A very commonly used remedy is the creation of multiple profiles for a user. Depending on the system a user logs into, he is assigned a different profile. This may be necessary due to a number of reasons including:

- When a user crosses platform boundaries, he needs separate profiles due to different languages or versions of Windows.
- When applications are served from silos, separate profiles allow individual application settings to be saved.

When configuring multiple profiles the major drawback is that users need to configure settings individually for each silo. Although this method decreases the user acceptance, it is often considered to be acceptable.

There are several challenges that can be met by this remedy. If users are assigned separate profiles for silos, the effect of Last Writer Wins situations between silos is resolved, although they are still observed in individual silos. As mentioned earlier in this section, users are enabled to work on different platforms when using multiple profiles.

The size of some or all profiles for a single user is reduced as well, because settings are separated between silos due to the use of multiple profiles. In addition, the effect of profile inconsistency is limited to a single silo.

5.2 Folder Redirection

User profiles contain several well-known folders which are called **User Shell Folders** and include:

- Personal
- Desktop
- My Music
- My Pictures
- Application Data
- SendTo
- Start Menu

The location of each User Shell Folder is defined in the registry: `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`[10].

By using folder redirection, any of the user shell folders can be redirected to another location. By default all are located inside the user profile and add to its size. By moving these folders to a path outside of the user profile (e.g. the home directory or any other network share), less data needs to be copied during logon.

In addition, this technique allows users to gain access to the same data located in user shell folders across platform boundaries when using multiple profiles.

[10] Do not use the registry key called `Shell Folders` located on the same level because it contains absolute paths which are generated from `User Shell Folders` and are therefore overwritten.

By using this mechanism the size of a profile is greatly reduced because folders containing large amounts of data are moved from the profile to a network share. It also allowed users to cross platform boundaries and still have access to personal documents.

Due to the fact that documents are not copied to the local machine during logon and, therefore, they are not overwritten during logoff, some Last Writer Wins situations are resolved. Settings contained in the registry are still lost in such situations.

Folder redirection is a standard method in Windows operating systems to reduce the effect of many challenges encountered with user profiles.

Citrix XenApp 5 for Windows Server 2008 implements a special variant of folder redirection (see chapter 3.2.1). User shell folders are redirected to the corresponding folders on the client device. Please note that this feature causes a lot of network traffic and results in a degraded user experience - especially in remote locations with limited bandwidth.

5.3 Folder Exclusion

Some applications tend to create a large number of temporary files inside the profile causing the profile to increase in size and, therefore, to load slower (see section 4.2). Considering the design of backup software, many small files may lead to problems when creating backups.

These consequences can be lessened by excluding directories containing a large number of (small) files. The corresponding option in group policy is documented in section 5.7.

5.4 Profile Quota

Introducing a profile quota allows a soft and a hard limit to be configured. When the first threshold is reached, the user is warned that the profile is filling up. Reaching the second threshold results in write errors because no further data is allowed to be saved. This will result in settings to be lost.

Apart from the impact of the warning and error messages a process called proquota.exe is executed for every user enlarging the session memory footprint.

Using profile quotas does not resolve any of the challenges besides reducing profile sizes.

5.5 Profile Reset

Many administrators still rely on deleting a user's profile in case a solution is not found quickly. Unfortunately, this does not only solve the issue at hand, this also resets all settings configured by the user to the default and deletes all documents contained in the profile.

This is not to be considered a remedy except for the gravest of circumstances.

5.6 UPHClean

Microsoft offers a tool called UPHClean[11] to address problems unloading profiles caused by locked files or registry keys (see section 4.8). It consists of a system service monitoring locks in user profiles after the corresponding user has logged off. This is achieved by remapping these stale locks.

While it is a best practice to use UPHClean on Windows Server 2003-based terminal servers, it is recommended to use UPHClean on Windows XP as well[12]. The functionality of UPHClean was included in the User Profile service of Windows Vista and Windows Server 2008[13].

[11] http://blogs.technet.com/uphclean/

[12] http://support.microsoft.com/kb/837115

5.7 Group Policies

Windows offers several configuration options to configure the behavior concerning user profiles through group policies. This section documents both well-known and unfamiliar settings.

There are several settings to configure the behavior when dealing with user profiles. Windows can be forced to delete a locally cached copy of a roaming profile after a user logs off. Changes in roaming profiles can be prevented from propagating to the central store. Usually, only the user has permissions to access the user profile directory. An option allows the administrators to be added to this directory's access control list. Users can also be prevented from logging on with a temporary profile.

```
Computer Configuration\Administrative Templates\System\User Profiles
Delete Cached Copy of Roaming Profiles
Prevent Roaming Profile changes from propagating to the server
Add the Administrator security group to roaming user profiles
Do not log users on with temporary profiles
Only Allow Local User Profiles
```

In the same location, the option `Only Allow Local User Profiles` forces Windows to use local profiles for all sessions.

In addition to these customizations of the handling of user profiles, two options influence the behavior per user. Some folders can be excluded from being propagated to the store of a roaming profile (see section 5.3) by activating `Exclude Directories in Roaming Profiles`. The profile quota (see section 5.4) is configured through `Limit Profile Size`. Both options are located under `User Configuration\Administrative Templates\System\User Profiles`:

```
User Configuration\Administrative Templates\System\User Profiles
Exclude Directories in Roaming Profiles[14]
Limit Profile Size
```

On terminal servers, two options allow for the user profile path and home path to be set centrally:

```
Computer Configuration\Administrative Templates\Windows Components\Terminal
Services
Set Path for TS Roaming Profiles
TS User Home Directory
```

Many folders in the user profile can be redirected (see section 5.2) to reduce the size and the effect of Last Writer Wins. But only four folders can be configured through managed options in group policy:

[13] http://blogs.technet.com/uphclean/archive/2008/02/28/windows-vista-windows-server-2008-and-uphclean.aspx

[14] Note that some directories are excluded by default. By activating this option, these directories are not excluded anymore. You will have to add them manually to your list.

```
User Configuration\Windows Settings\Folder Redirection
Application Data
Desktop
My Documents
Start Menu
```

To be able to redirect more folders, a new administrative templates needs to be created to define an unmanaged policy option. The folders are redirected by manipulating the registry values documented in section 5.2.

A not so well-known policy enables profile to be loaded and policies to be processed from a different forest, i.e. if the user is not located in the same forest as the machine:

```
Computer Configuration\Administrative Templates\System\Group Policy
Allow Cross-Forest User Policy and Roaming User Profiles
```

5.7.1 New Settings in Windows Vista

Beginning with Windows Vista, Microsoft introduces several new machine-based policy settings to configure the behavior regarding user profiles. They apply to Windows Server 2008 as well.

The most important addition is the option to configure a roaming profile path for Windows clients (`Set roaming profile path for all users logging onto this computer`) which is missing in versions prior to Windows Vista. If a user profile contains locked files, Windows Vista will not forcefully log off users if the corresponding option is configured.

```
Computer Configuration\Administrative Templates\System\User Profiles
Do not forcefully unload the users registry at logoff
Set roaming profile path for all users logging onto this computer
Set maximum wait time for the network if a user has a roaming profile or
remote home directory
```

5.8 Group Policy Preferences

Windows Server 2008 introduces an extension of group policies called Group Policy Preferences. Traditional group policies enforce a configuration whereas group policy preferences allow for a configuration to be deployed to the user which can be modified by the user.

Group policy preferences can only be created and modified from Windows Vista and Windows Server 2008. Older versions of Windows are only able to view and modify standard group policies.

Before being able to deploy group policy preferences to operating systems before Windows Server 2008, a client-side extension (CSE) needs to be installed.

6 Citrix Profile Management

None of the traditional attempts to solve the problems caused by Windows user profiles are fully satisfactory – each alternative has its drawbacks and pitfalls, especially when used in large heterogeneous environments.

Citrix Profile Management is a user profile optimization solution that overcomes many of the problems inherent to classical Windows user profiles. It integrates into the logon and logoff processes and uses advanced techniques for transferring and storing user profile data. The net results of these improvements are lower maintenance costs, fewer helpdesk calls and faster logon times.

6.1 Design

Citrix Profile Management is designed to overcome the limitations inherent to classic Windows user profiles. It is geared towards easy setup, low-maintenance operation, flexible configuration and high processing speed.

With Citrix Profile Management, a local profile (see chapter 2.3) is used as the basis for a user's profile. Additionally each user has a store for personal settings on a file server. During logon the Citrix Profile Management system service interrupts the logon process to load the user data from the central store. During logoff it exports changed settings and merges them with the data in the user store. This new approach was chosen to remedy the disadvantages of mandatory profiles (see section 2.3).

Several things are noteworthy about this design:

- Usage of a system service guarantees reliable and fast operation. The service can be restarted without any data being lost.
- The system service needs to be installed only on the machines the users log on to, i.e. typically XenApp servers and client systems (local devices and/or delivered desktops).
- Nothing else about the environment needs to be modified, in particular no additional servers or network services are required and no permissions need to be changed.
- The user settings managed by Citrix Profile Management can either be stored in a user's home directory or in any other file share on the network.
- Citrix Profile Management detects which files and registry keys were changed during a user session. Only the changed files and keys are saved during logoff and merged with the settings in the personal store.

6.2 Features

This section highlights the most important characteristics of User Profile Manager.

6.2.1 Low-Maintenance Operation

- Without any configuration Citrix Profile Management automatically detects and saves all registry and file system data that was changed during a user session.
- Because of the automatic detection of changed settings it is not necessary to configure Citrix Profile Management for every application on your machines. Installing, changing, removing or upgrading applications is completely transparent to Citrix Profile Management. However, application settings can be defined through include and exclude lists as well (see section 6.2.3).
- The learning curve is very low since Citrix Profile Management adheres to de facto standards and leverages technologies administrators are familiar with, like Group Policies.

6.2.2 Rugged Design

- No single point of failure: there is no single service or server which all Citrix Profile Management-enabled systems on the network depend upon. Many other profile management solutions use some kind of central database that adds complexity, increases the probability of failure and can easily become a performance bottleneck.
- Any changes and customizations in the user profile will be saved and restored, even problematic settings like:
  - Desktop properties (e.g. wallpaper, background color)
  - Display of the Windows build and version numbers[15] on the desktop
  - Certificates with private keys
  - Saved passwords
  - MUI settings
  - Keyboard scan code mappings[16] (see: How to disable the keyboard Windows key[17])

6.2.3 Flexible Configuration and Logging

- Citrix Profile Management uses managed Group Policies for configuration, a flexible and well-known mechanism for distributing settings to machines or users.
- Both in the file system and in the registry specific files, folders or keys can be excluded.
- Additionally, inclusion lists can be used to restrict the product's operation to specific areas.
- Verbose logging can be enabled that really shows what is going on. To reduce the amount of data only messages from selectable areas (e.g. registry, file system, Active Directory) can be selected for logging.

6.2.4 High Processing Speed

- The efficient design engineered for profile management only and the implementation as highly-optimized C++ code guarantee for low overhead and high processing speed.
- Directories that are configured for synchronization are monitored for changes. During logoff Citrix Profile Management only copies files over the network if their contents actually changed. For example, if a directory was renamed but is otherwise unchanged, during logoff only a rename operation is performed over the network without transferring the contents of the directory.

6.2.5 Setup and Migration

- Since no central services or databases are needed Citrix Profile Management is set up in minutes.
- Citrix Profile Management comes pre-configured with settings that are well-suited for most environments.

---

[15] http://technet2.microsoft.com/windowsserver/en/library/a6105b03-1848-4160-8858-dff4bb4a439b1033.mspx?mfr=true

[16] http://www.microsoft.com/whdc/device/input/w2kscan-map.mspx

[17] http://support.microsoft.com/?scid=kb%3Ben-us%3B216893&x=10&y=13

- Both local and roaming profiles can be live migrated to Citrix profiles. When a user logs on for the first time after Citrix Profile Management has been installed, his or her existing user profile will be migrated transparently, making the transition painless.

6.3 Solving the Challenges

In this chapter we will revisit the challenges (see chapter 4) to reliable, fast and flexible profile operations and see how many of them can be met by using Citrix Profile Management.

6.3.1 Last Writer Wins

Citrix Profile Management merges changes from multiple sessions in one place per user. This happens with a granularity of single files respectively single registry keys. Thus the problem is eliminated that data from one user session overwrites data from the previously closed session.

6.3.2 Profile Size and Logon Speed

Generally speaking, as many sub-folders of the user profiles as possible should be redirected to the home directory. Unfortunately this is not always possible. For example, some applications use their configuration files so heavily that it would slow them down if they were located on the network instead of a local drive. Another aspect that needs to be considered is the performance impact the file servers could take if they were to process possibly thousands of additional requests per second. For these reasons most administrators use a mix of redirected and local folders in their user profile setup.

After those folders, that can be redirected are moved out of the user profiles, the next best way of boosting the logon speed is to exclude folders from synchronization. Many (badly-designed) applications store temporary or local data in those areas of the profile designed for information that needs to roam with the user from machine to machine. By excluding such data from synchronization, profile bloat is prevented and logon speed increased (see section 6.3.6).

Also refer to section 6.3.7 about Profile Streaming to speed up the logon process.

6.3.3 Citrix Streamed Applications

Citrix Application Streaming redirects settings from virtualized applications to folders and the registry inside the user profile. The data thus redirected needs to be transferred over the network during each logon and saved back to the file server during logoff, slowing these processes considerably.

Therefore, these settings are managed by Citrix Profile Management making them available in every session to which the corresponding Citrix profile applies.

6.3.4 Dual-Mode Streaming

In a dual-mode streaming setup, different user profiles are used on fat clients and terminal servers, yet applications are used intermittently on both platforms. This creates the need for a synchronization mechanism that keeps streamed applications' settings current in both types of profiles.

In contrast to the Tech Preview of Citrix Profile Management v1, dual-mode streaming is not supported by User Profile Manager v2. Due to the changed design, Citrix Profile Management always imports the whole profile from the central store. Inclusion and exclusion lists only apply to the merge process resulting in platform-specific settings to be imported into a new session.

6.3.5 Platform Boundaries

Although Windows XP and Windows Server 2003 as well as Windows Vista and Windows Server 2008 (R2) have the same profile format (version 1 and version 2, respectively), sharing a common profile for version 1 or version 2 is not recommended due to subtle differences.

Citrix Profile Management does not support spanning multiple platforms such as Windows XP and Windows Vista in general, but enables configuration sets to be shared between all supported platforms. Using inclusion and exclusion lists, a custom synchronization list for a set of systems can be created defining the registry and file system data to export and import. As long as these paths are limited to application data and do not include Windows settings inside the user profile, sharing the configuration is supported.

6.3.6 Misbehaving Applications

Citrix Profile Management is able to synchronize directories and files from and to locations outside of the user profile and, thereby, effectively resolving problems caused by these applications.

6.3.7 Profile Streaming

Beginning with version 3, Citrix Profile Management includes a feature called profile streaming which radically changes the way profiles are handled. The default behavior of Windows is to block the logon process until the user profile is fully copied to the local system. Profile streaming introduces a filter driver which pretends that all files belonging to the user profile are already present on the local system. When such a stub file is accessed, the local service downloads the file from the central store and makes it available to the local system. This approach allows for a significant speed up of the logon process as user data can be downloaded on-demand instead of delaying the logon.

Profile streaming is configured through group policies where several options control the two modes of operation. By default, files contained in the user profile are exclusively downloaded on-demand. Alternatively, the whole profile can be cached locally without delaying the logon process. Requested files are downloaded on-demand while all other files are transferred in the background after the user has been logged on.

It is also possible to define a user group whose members will profit from profile streaming while users without the group membership will receive the standard features of Citrix Profile Management.

Please refer to the official documentation about possible issues between profile streaming and enterprise antivirus products.

6.3.8 Active Profile Write Back

Version 3 of Citrix profile management also introduced a feature called active profile write back. When users work in a very long-lived session, the profile is hardly ever written back to the central store. Active profile write back allows for files and folders to be written to the central store while a user is still logged on. This feature enables a new session to receive changes before logging off from another session.

Please note that active profile write back cannot be applied to the registry as it is contained in a single file which remains locked throughout the session and therefore cannot be written back.

6.4 Licensing

Citrix Profile Management is exclusively licensed as a part of XenApp Enterprise Edition or higher (beginning with Presentation Server 4.5 Enterprise Edition) or XenDesktop VDI Edition or higher. Its primary use is for sessions on XenApp and virtual desktops served by XenDesktop.

In addition to using Citrix Profile Management centrally in user sessions, it may be implemented on all devices used for accessing a XenApp environment. For more information, please refer to the EULA.

7 Choosing a Profile Solution

After covering the basics topic of Windows user profiles with their inherent issues and traditional remedies as well as describing how Citrix Profile Management handles the challenges, this chapter provides a set of guidelines which are vital in the evaluation of a user profile management solution.

Most companies are forced into looking for a profile solution due to preceding problems with settings in Windows profiles. At that point, it is not a question of whether a profile solution is required but rather which is chosen and implemented. To select such a solution from those available on the market, the requirements need to be thoroughly defined. But there are still subtleties that the responsible person may be unaware of.

The following sections contain several topics important to the evaluation of a profile solution in order to be able to select a product matching the requirements as well as minimize the costs required for the implementation and the maintenance of such a solution.

7.1 Consistency

The main reason for evaluating profile solutions is avoiding inconsistent user profiles which cause users to be hindered in their ability to work. Apart from users not being able to perform their given tasks, the user help desk and possibly the second level support is charged with solving the issues. This often leads to the profile being reset (see chapter 5.5) and the corresponding user losing their personal settings.

There are two kinds of inconsistencies with regard to user profiles:

1. Writing or modifying registry keys and values in an incorrect or inappropriate location causes applications to behave unexpectedly.
2. By working in two separate sessions, user data and settings from the first session are overwritten during logoff by those from the second session.

The first type of inconsistency can be met by either restoring a known working version of the affected user profile only causing the most recent settings to be lost. Another solution is resetting the user profile resulting in the loss of all data stored in the profile as well as all settings. These inconsistencies can hardly be prevented by a profile solution because they are caused by an erroneous application or system state. Nevertheless, a profile solution can lessen the effect of such unforeseeable state because user settings are stored separately from the Windows user profile. As long as these settings are unaffected, resetting a user profile has only limited effect on the user and his workspace.

The second kind of inconsistency is also known as the Last Writer Wins problem described in chapter 4.1. The remedy for this issue is simple: Only settings modified in a particular session are saved to a central store by merging them with unchanged configuration data. Thus, unrelated modifications from separate sessions are preserved and the consistency is maintained.

Several profile solutions on the market today are not able to solve the Last Writer Wins problem due to their design. Some even need to be configured for each installed application separately, causing hidden costs because applications and the related settings need to be analyzed before the profile solution is ready for action.

Apart from the integrity of the data managed by a profile solution, consistent behavior is also nevessary:

- How does the solution handle situations when it is unable to restore settings?
- Can administrators' profiles be easily excluded from being processed?

7.2 Integration

Usually, a profile solution needs to be integrated in an IT environment where profile issues have already been encountered. Before deciding on a product, the impact on the current environment needs to be determined. This includes the following topics:

- Does the solution interfere with the launch of some applications due to the mechanism used to trigger profile management?
- Is it necessary to change any logon scripts?
- Do users need to be assigned additional permissions?
- Are any additional components required for the operation? Is there a way to implement them in a redundant or highly available manner to avoid downtimes?
- How does the profile solution affect the baseline of a terminal server environment?
- Does it scale proportionally to the number of devices or the number of users?

The complexity of implementing a profile solution increases with every component in the IT environment required to be introduced or modified. As a result, there are more contacts and, possibly, more units involved due to divided responsibilities causing additional costs on top of the licensing fees.

7.3 Investment

The last chapter already touched on a topic relevant to this section: With increasing complexity of the solution, the integration becomes more costly due to arrangements during the design and implementation.

There are additional topics adding to the investment necessary to introduce a profile solution:

- How complex and time-consuming is the configuration of the product to meet the requirements?
    - Is the configuration interface usable in an easy and intuitive manner?
    - Does the manual support the configuration by explaining concepts and configuration options as well as their interaction?
- Do administrators require training to maintain the solution?
- Does the solution allow applications to be added, upgraded and removed with minimal or no modifications to the configuration?
- Are changes to the configuration performed centrally in a single location?

All of the tasks listed above directly result in costs caused by the invested manpower.

A profile solution with few or no dependencies as well as few or no configuration changes during operation saves time and money.

7.4 Flexibility

Apart from meeting the requirements, a profile solution needs to allow for changes in the IT environment. New methods of application and desktop delivery, like application streaming and virtual desktops, require a flexible solution which does not hinder the evolution of the environment.

- Are several client as well as server Windows operating systems supported?
    - Does the same configuration apply to all supported operating systems?
    - Does it allow user settings and data to be shared in scenarios leveraging application streaming and virtual desktops?
- Are all user settings being saved and restored?
- Are inclusion and exclusion lists supported for files and registry keys as well as a combination of both?
- Does the solution scale proportionally with the number of devices or users?
- Does the solution enable the evolution of the IT environment by requiring a minimum of effort to adopt it to changes?

- Can settings be shared among different Windows operating systems, e.g. allow for the same configuration to be used for streamed applications on a fat client as well as on terminal servers?

7.5 Completeness

Although a profile solution may meet all requirements including those listed above, it may still not be able to save and restore all settings available in Windows and, more importantly, in your environment. Some even require additional tools to handle some of the settings.

- Does the solution handle problematic configuration options like setting the following registry value to `0x1`?
  `HKEY_CURRENT_USER\Control Panel\Desktop\PaintDesktopVersion`
- Are desktop settings (re)stored correctly? If so, does it require additional tools to achieve this?
- Are certificates with and without private keys (re)stored correctly?
- Are multi-lingual setups of the Windows operating systems supported?
- Are user-specific passwords handled correctly?
- Does the product work with other shells that replace Explorer.exe?

7.6 Migration

When implementing a profile solution, a feasible migration scenario is required to preserve the users' settings from the original profiles. Otherwise, the solution will not be accepted by the users because settings are lost and need to be configured manually preventing the users from doing their work.

There are several topics which heavily influence the implementation of a user profile solution:

- Can existing settings be migrated into the profile solution?
- Are all settings included in this process?
- Can settings be included and excluded to customize the resulting user profile?
- Is it possible to cleanup user profiles during the migration, e.g. remove obsolete registry keys from discontinued applications?

Vendors are usually focused on selling their product and do not offer a path back to roaming profiles. But a self-confident vendor may as well provide a migration path back to roaming profiles.

8 Profile Migration

User profile management has been around for several years and many customers have implemented one product or another to address some subset of the challenges presented in chapter 4. But by now, administrators as well as their superiors have realized that user profiles represent an issue yet again as their environment evolves to adapt to new requirements to update to current releases of IT components.

Depending on the extent of the changes required, it is often deemed a safer route to dispose of the affected user profiles. A new user profile does introduce issues caused by outdated settings. But does retaining the old user profile – containing valuable customizations – necessarily cause problems? Resetting profiles (i.e. deleting profiles) has become a bad habit even when an issue is encountered in daily help desk business.

When a user is taken away his profile, precious time of making minute customizations is wasted. Users will attempt to redo all those settings but will certainly miss one or another. In the time required to restore their customizations, work will almost entirely rest. For the user, this is annoying but for the employer deleting user profiles has a costly side effect.

Therefore, vendors have begun focusing on migrating user profiles to prevent user customizations to be lost during an extensive change in the IT environment.

8.1 Microsoft User State Migration Tool (USMT)

Microsoft offers a free program called User State Migration Tool (USMT) to support migration scenarios by lessening the effects on the user.

USMT is a command line utility for transferring user settings between clients. To make full use of the tool, a custom script must be built around USMT. It does not support migrations on server operating systems as in server-based computing environments and is limited to local user profiles.

Continue to Helge's blog for a detailed analysis von USMT.

8.2 sepago Profile Migrator

sepago, the inventors of the Citrix User Profile Management, have embraced their expertise in the area of user profiles to create a product called sepago Profile Migrator. It focuses entirely on preserving user settings across platforms managed from a graphical user interface or a command line interface.

At the core of its functionality, Profile Migrator iterates a list of user profiles, analyzes the contents and extracts the configuration settings of a configurable set of applications. These settings are inserted into a fresh profile created for the target platform. Due to the generalization of the process, Profile Migrator supports a wide range of migration scenarios to embrace upgrades of client operating systems as well as server operating systems for all Windows version supported by Microsoft[18]. In addition, an upgrade from 32 bit to 64 bit is possible.

With the release of sepago Profile Migrator 2.0, the product supports two modes for migrating profiles:

1. Offline migration of roaming and Citrix profiles
2. Online migration of profiles located on client devices

[18] As of Profile Migrator 2.0, Windows XP/Vista/7 and Windows Server 2003/2008 (R2) are supported for version upgrades.

During offline migration, Profile Migrator processes a list of profile directories on a file share or contained in Active Directory user objects. The process is initiated from a system near these profile directories and includes callbacks for custom scripts to be executed before and after the migration of individual profiles[19]. Folder Redirection is recognized and honored in the source profile.

When profiles are to be migrated between client devices or from a client device into a central environment, Profile Migrator introduces a component called **Collector** which is installed on the source device and synchronizes user profiles to a central share called the **Synchronization Point**. On the target device, a component called **Personalizer** is executed for a user to fetch application settings from a certain user profile on the Synchronization Point and to insert those settings into a fresh profile.

All settings configured in both modes can be saved to a migration project to modify and use at a later point in time.

Application settings are defined in an XML-based format called Application Configuration Set (ACS) describing user settings of one of more version for a specific application. This allows user customizations for an application to be migrated with the same or another version of the application. Although sepago offers ACS definitions for well-known applications, customers usually have several in-house applications. For these use cases, Profile Migrator offers a graphical editor for ACS definitions. In addition, the **Application Analyzer** allows for user customizations to be recorded during a launch of the application and integrates with the graphical editor to customize the resulting ACS definition.

As the process of migrating a large number of user profile can run into wide range of issues, Profile Migrator maintains a very detailed log file in CSV format for analysis in third party products. In case of an unexpected error, Profile Migrator is written to generate a crash dump helping the developers track down the issue.

8.3 Other Vendors

There are several vendors in the market offering profile migration as one in many features. This may well prove to be an advantage if you happen to be in need of several of those components. You may even own a profile migration solution as part of such a suite.

On the other hand, you may be looking for the best-of-breed profile migration solution in which case you should not take into account whether a suite offers this feature. Rather analyze your requirements and choose a profile migration solution independently.

[19] A custom post-migration script allows for domain migrations to be performed including changing the user name as well as the domain name. See Helge's blog for a detailed description of this script.