Realtime publishers

The Shortcut Guide™ To

User Workspace Management

sponsored by

RES software

Greg Shields

Chapter 4: Transforming to an Environment of User Workspace Management 43
Delivering User Workspace Management 44
The Workspace Composer Agent 47
The Centralized Database 48
The Workspace Designer 49
Controlling Applications Through the Workspace 50
Migrating to User Workspace Management 51
Desktop Sampling 52
Workspace Design 52
Initial Agent Installation 53
Environment Control and Tuning 53
Extending Agent Coverage 53
Environment Transformation: Two Real-World Examples 54
Migration Scenario—Upgrades 54
Green Field Scenario—VDI 55
Improving Your Life. Improving the Lives of Your Users 56

Copyright Statement

© 2010 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This book was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology books from Realtime Publishers can be found at http://nexus.realtimepublishers.com.]

Chapter 4: Transforming to an Environment of User Workspace Management

I've been working with IT systems, both servers and workstations, since before the days we had management tools. Back in those days, the idea of automation centered around "getting enough technicians into the field to sweep the hallways." I still shudder as I remember a few multi-site, company-wide configuration updates that didn't change all that much but required dozens of people and massive coordination to get the job done. Good riddance to manual administration.

Also a part of my professional history is what seems to be a constant struggle with Windows profiles. Whether fixing local profiles gone wrong on individual desktops or managing thousands of remote ones for large-scale remote application infrastructures, Windows profiles have tended to be that technology that keeps me in the office during evenings and weekends.

It is that pain, combined with the pain I see in the eyes of my users, that makes User Workspace Management solutions so attractive. Their ability to take *the profile* out of the user's profile eliminates a massive administrative pain while improving the experience of every user.

The technological bits and bytes that actually accomplish that decoupling is a topic that's been touched upon throughout this guide. You've already come to understand the workspace itself, and how that workspace can be made pervasive across the spectrum of delivery mechanisms. You should at this point also recognize how that workspace is composed from an integration of content, context, and security. Most importantly, you should appreciate how an environment of pervasive personality brings with it key security capabilities that improve your overall security posture.

But, as I mentioned in the conclusion of the previous chapter, the real technological detail of User Workspace Management is a topic that's best left for this final chapter. Now that you understand the value and the positioning of this solution's paradigm, your final questions should center around "How do I get this implemented in my environment?"

Answering that question is the primary topic of this final chapter. In it, you'll learn the details of the workspace composition process, including all the components that are necessary to enable its functionality. You'll also discover how the process of transforming to this new paradigm needn't necessarily be a forklift process. Using a selection of tools that are available today, you can incrementally implement this technology with a low level of risk to your operations.

Delivering User Workspace Management

Understanding the technology that enables User Workspace Management first requires a thorough understanding of the steps involved in *workspace composition*. This composition process is used by User Workspace Management software solutions in dynamically constructing the workspace at the moment the user needs it.

Important to recognize is that this composition process is fundamentally different than what you're used to seeing with roaming user profiles. In fact, from this point on, forget everything you ever knew about roaming user profiles:

- Ignore the fact that they are file-based constructs that are copied en masse from a storage location to the target device.
- Ignore that the logon process requires and waits for (most of) that file copy to complete before it hands control over to the user.
- Ignore the fact that the data in roaming user profiles must eventually be copied back to the central storage location if it is to be available for future logins. With roaming user profiles, this return of user data has traditionally been done only at logoff; although Windows 7 and Windows Server 2008 R2 now support a simplified background upload of some roaming profile data.

Instead, replace the profiles paradigm that you've been working with for over a decade with a new one that that focuses on *dynamic composition*.

In a composed environment, the user's workspace isn't reliant on a set of files and registry hives that must be first copied from a file share. Instead, a composed environment dynamically creates each and every user setting *on the device* and *at the point of login*.

To help envision this further, consider the average Windows desktop (see Figure 4.1). This Windows desktop isn't part of a remote application infrastructure, nor is it virtualized. It is simply your basic, run-of-the-mill desktop that a user works with to do their job.

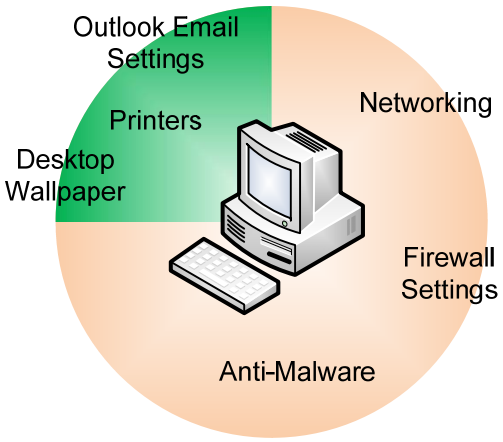

Figure 4.1: An average Windows desktop, with user-controlled settings (in green) and IT-controlled settings (in tan).

On this desktop are a number of configurations that the user has created in order to make them more productive. Those settings might be related to applications, such as email settings in Microsoft Outlook. They might be printers that are physically close to the user or have the features that the user specifically requires. They can even be personality settings such as a friendly desktop wallpaper or a series of icons on the desktop.

Some elements on this average Windows desktop might also be configured by IT. For example, IT probably handles the networking settings as well as the configuration for security software such as firewalls and anti-malware. Other settings may require administrator access, which can only be modified by a member of the IT department.

All of these settings combine to create the user's workspace. And, in an environment where that user never leaves the confines of that single machine, leaving those settings on that machine might be a completely functional solution for that user and their IT department.

Now, let's extend this example with the assumption that the user will log in elsewhere, or that the IT department wants greater control over the content and delivery of the user's workspace. At this point, the IT department has two options for delivering the user's customizations to the user. Figure 4.2 shows a graphical representation of these two options.

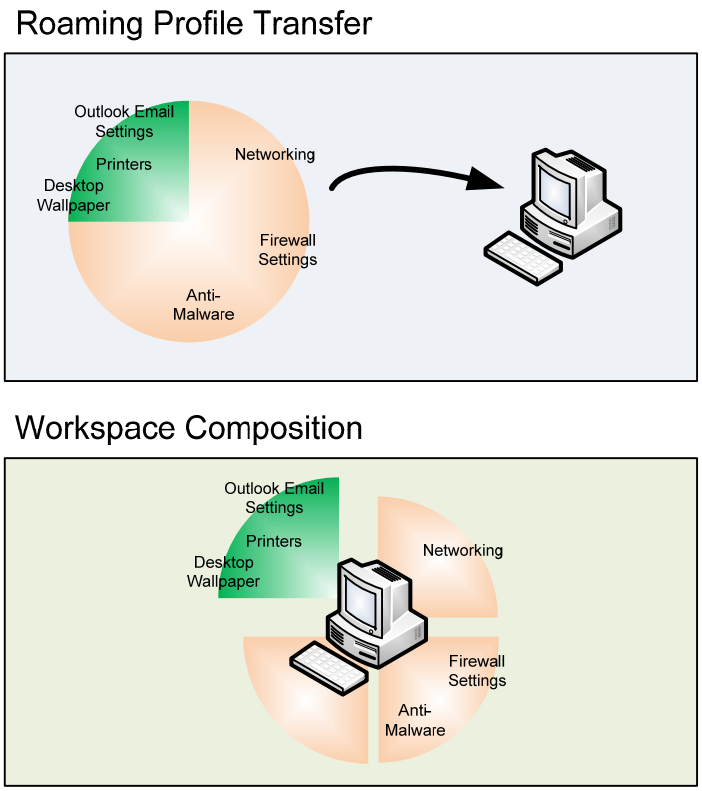

Figure 4.2: Illustrating the differences between a roaming profile transfer and desktop composition.

The transfer of a traditional roaming profile is used in Figure 4.2's top graphic. There, you can see how the profile must be transferred from some kind of external storage location (typically a file share) to the machine during the point of login. In the bottom graphic is a very different scenario. There, a User Workspace Management solution is used to construct or *compose* each of the individual configurations directly on the machine at the point of login.

Accomplishing this composition requires a set of parts that work together to enable the composition. Shown graphically in Figure 4.3, let's take a look at each in turn.

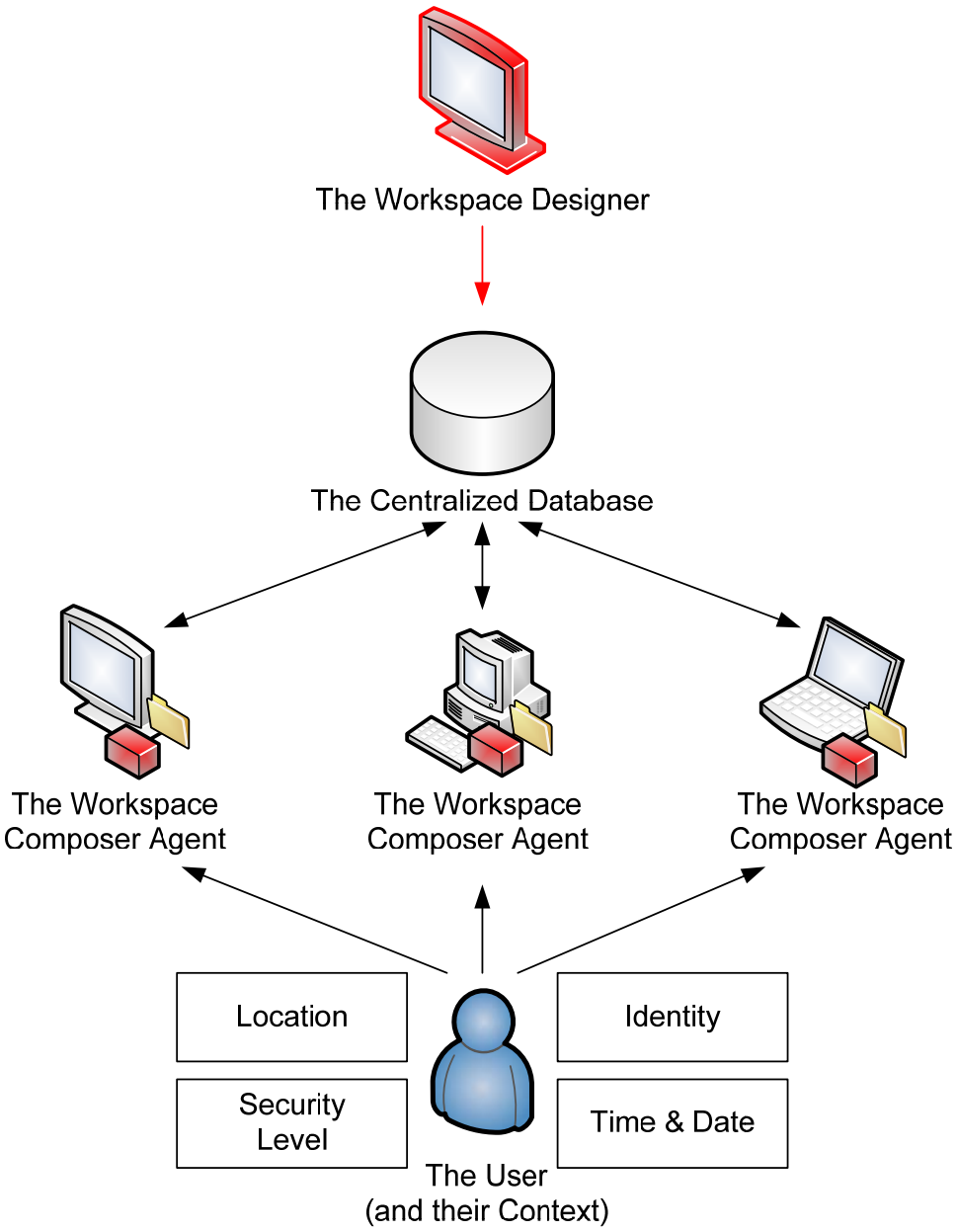

Figure 4.3: Extending Chapter 2's image to include each component of the User Workspace Management architecture.

The Workspace Composer Agent

Most of the action in this environment happens within the client agent itself. This client agent operates as the workspace composer, creating the user's environment as the user needs it. The workspace composer agent is primarily activated with the instantiation of the logon process. Installed directly to each computer instance where User Workspace Management is desired, the agent is responsible for a number of tasks.

The first job of the agent is to communicate with the User Workspace Management database to identify and cache the possible customizations that are relevant to the computer. This caching process downloads and stores the set of possible configurations, based on user information as well as user context information. The caching process is done prior to user logins to reduce the amount of time required to compose the environment and to ensure the workspace is available should the user disconnect from the network (more on this in a minute).

The client is called to action at the moment the user attempts to login. Its first job here is to identify who the user is as well as the context of the user, such as from where and via what mechanism is the user connecting. This context information is cross-referenced with cached information to identify the desktop configurations that are appropriate for the user and their context. Specific configurations at this point may be allowed or denied based on updates to the user's rights and permissions, or the context by which the user is attempting to connect.

Once the proper configuration is identified for the user—a process that takes very little time—the agent's second job is to proceed with the composition of the workspace. This composition process configures and exposes each workspace item (those discussed in Chapter 2 are excellent examples) based on the identified characteristics. This process, as shown in the bottom image of Figure 4.2, happens entirely within the local computer and without the need for the large-scale movement of files.

Control of the workspace is handed off to the user upon completing its composition. At that point, the user is able to work with the computer normally. In the background, however, the agent goes about its third responsibility. This final job for the agent is to watch for changes to the user's context as well as user-initiated changes to the content. This monitoring is exceptionally important for synchronization as well as security.

For example, if different settings are configured for different contexts, one job of the agent is to monitor and reconstruct a new workspace when that context change occurs. This dynamic reconstruction of the environment ensures that users cannot change their context without seeing a similar change to the workspace. It also assures the security configurations based on context by requiring a wholesale workspace reconstruction when that context changes.

While monitoring for context changes, that agent is also watching for content changes as well. As discussed in the earlier chapters, users want to be able to modify their desktops—perhaps adding a new icon or updating a setting—and rest assured that that change will be mirrored to their other workspaces. The final job of the agent is to monitor for those configuration changes and subsequently notify the database for update. At the same time, the agent is keeping in touch with the database in order to be notified and compensate when other workspaces have experienced changes.

The Centralized Database

Enabling the mobility aspect of the user's workspace is a centralized database. As explained in previous chapters, the User Workspace Management database operates as the central clearinghouse not only for capturing user content changes but also for storing the entire range of *potential* changes that could be made to the desktop. The database at the same time operates as a single point of control to which each agent maintains communication.

The fact that a database is used is fundamentally important to this architecture. Compare this database approach with the file-based nature of traditional roaming profiles. Using traditional profiles, user customizations are stored within the profile itself. This distribution of settings means that each individual profile stores information about that profile only. Further, making policy-based changes requires interfacing with each and every profile at the point of use. There can be substantial differences between any two profiles and their internal configurations, so the process of enforcing policies occurs as a reactive step with the profile loading process.

Using a centralized database, individual user information is consolidated with administrator and policy settings into a single storage location. There, the workspace settings for each user are dynamically composed at login, rather than occurring as an after-effect. Further, the normalization of data that occurs within a database eliminates the duplication and widespread scattering of data that is normally seen within a profile.

What About Disconnected Environments?

It should be obvious at this point that database access for agents can quickly become a problem in disconnected environments. In these environments, such as when a laptop leaves the LAN and roams outside the office, agents have no access to the database. It is for this reason that agents constantly synchronize and cache workspace characteristic data. Caching data on the local machine enables the agent to compose the user's workspace with the best possible data, even when no access to the centralized database is possible.

The Workspace Designer

This guide has discussed many times how another of the benefits of User Workspace Management is the granular administrative control over the environment. Using such a solution, administrators can lock down and otherwise control certain aspects of the workspace. Other aspects can be left for personalization by the individual user. Important to recognize here—and another important difference between this solution and traditional roaming profiles—is the ability for IT and administrators to scope which options are personalized and which are controlled.

For example, consider an environment that can be connected to via the Internet and has access to sensitive data. In that environment, IT and security administrators might want to control every aspect of the user workspace. In such a situation, a user will be delivered an extremely locked-down environment with no capacity for personalization. Another environment may be the individual desktops that are contained within the business' brick-and-mortar offices. That environment has a lower risk for exposure, and as such may have fewer areas that require control. In this second environment, IT and security administrators can control only a portion of the environment while leaving the rest open for personalization.

Important to recognize here is that both of these ideologically different environments can be administered from within the same User Workspace Management solution. Their data can be stored in the same database. Different only are the administrative controls that are assigned to the individual servers and desktops that IT has logically partitioned into each environment.

> **Note**
>
> Even the idea of assigning a "high security" label to a set of *servers* or *desktops* is no longer necessary with User Workspace Management. An effective solution will allow a further degree of granularity for different users with different contexts *on the same server*. Thus, two different users or even the same user in two different contexts can be delivered completely different experiences.

Enabling all this to occur is the workspace designer tool. This administrative console is used by the administrator to identify each of the contexts of interest as well as the content and security configurations that will be controlled. The workspace designer becomes the location where administrators identify each of these elements for distribution to the database and ultimately the workspace composer agents at each endpoint.

Controlling Applications Through the Workspace

This guide's ongoing discussion of how User Workspace Management enables "granular control" and "eliminates the file-based nature of traditional roaming" should at this point begin begging an important question. That question relates to the actual processes by which such a solution can actually manage your applications.

A central problem with the centralized management of applications has to do with how those applications store their information. Some applications store customizations within the registry, while others store their information within files that can be located anywhere on the local system. Even among those that store their information in the registry, there can be multiple places within that registry where the data is ultimately deposited (HKEY_LOCAL_MACHINE versus HKEY_CURRENT_USER as well as subkeys of both immediately come to mind).

The technical aspect of controlling those applications comes in managing each application's customizations. This is done by overwriting the applications' default customization information with another set that is appropriate for the user's workspace. The process of locating and documenting where these customizations are made involves a bit of sleuthing on the part of the administrator, seeking out potential areas in the registry and within files.

For example, Microsoft's Notepad application can be equipped with a status bar that provides information about the current cursor position within the document. That status bar is not enabled by default; however, its information can be of use to a user who is searching through that document.

The configuration for enabling Notepad's status bar is found within the registry, specifically in the key HKEY_CURRENT_USER\Software\Microsoft\Notepad\StatusBar. When the value for this key is set to 0, the bar is not present; when it is set to 1, the bar will be displayed the next time Notepad is run (see Figure 4.4).

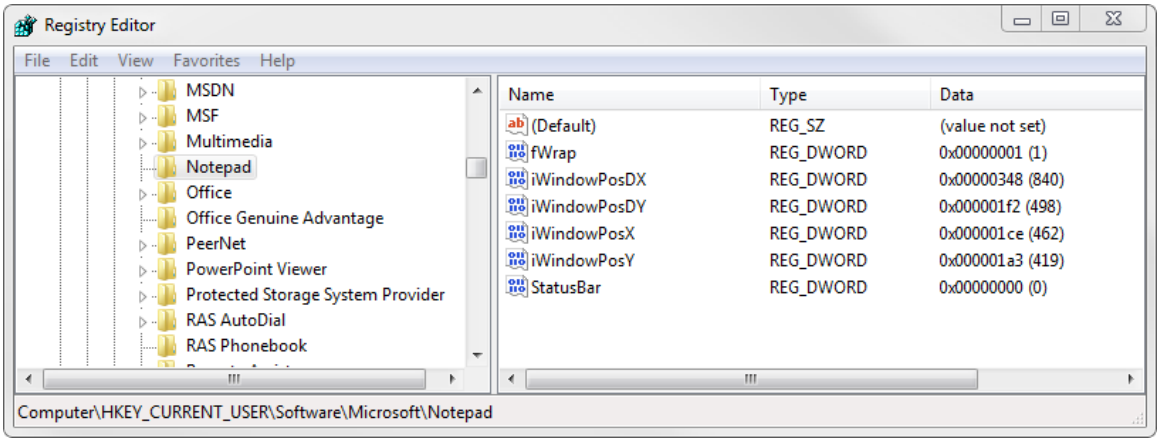

Figure 4.4: Notepad's registry location for defining the configuration of its status bar.

A User Workspace Management solution provides the enforcement mechanism for defining the application's configuration. This mechanism is commonly manifested through the solution's workspace designer console. In that console will be areas where the Notepad application can be defined, and with that definition will be the ability to insert custom configurations. Once defined within the designer, the application configuration is then available for distribution to agents and storage within the centralized database.

Such solutions, however, tend not to include the tools that assist the administrator with actually locating and identifying the correct registry key or file location where the configuration is held by the application. That process is best left for external tools that can watch for and alert on changes as configurations are made. When considering a User Workspace Management solution, you may also consider looking for additional tools that assist with your application customization needs.

Migrating to User Workspace Management

Yet another benefit of the agent plus centralized database approach used by many User Workspace Management solutions is in how this architecture impacts the implementation process. Actually getting to that end state of full User Workspace Management needn't necessarily require a full-scale forklift of every server, desktop, and endpoint all at once.

In fact, attempting to move an entire environment all at once is not considered a best practice with most solutions. By slowly and iteratively migrating your chosen solution into your environment, you can ensure that user information is not lost and that services remain intact throughout the project.

Five general process steps (see Figure 4.5) are commonly used with User Workspace Management solutions to fulfill the iterative approach. Those five steps involve the sampling of the environment, using information from that sampling to create an initial design, implementing that design to a limited area, incrementally adding points of control and tuning the design, and finally extending agent coverage to other parts of the network. Each of those steps is further explained in the sections that follow.

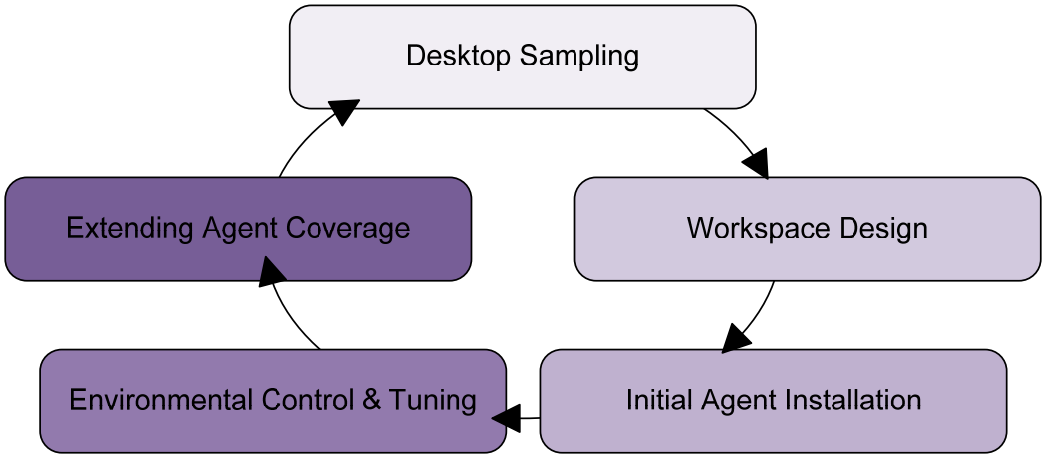

Figure 4.5: The five steps in migrating to a User Workspace Management solution.

Desktop Sampling

Before you can create a well-defined workspace, you first need to understand the movements and actions that are common to your user base. This part is fundamentally necessary to a smart design because it allows IT to use a data-driven approach to environment control rather than making decisions in a vacuum.

One method for desktop sampling uses manual methods such as observation and user interviews. These tools enable the project team to identify where users are connecting into the environment, what tasks they are accomplishing, what resources they need, and how they go about completing the tasks associated with their job role.

Although observation and user interviews are indeed helpful for any implementation project, their manual methods tend to lead to gaps in coverage of control options. Users may be wary of increasing control and change their responses or observed behaviors in anticipation of the new technology. Other users may not see the efficacy in such a solution, and may provide misleading results.

An alternative approach may use automated sampling tools that are provided by the User Workspace Management software vendor. These tools keep a constant monitor on the environment while working in the background. Allowing these tools to monitor and report on behaviors provides a better sense of data over and above the manual steps previously discussed.

> **Note**
>
> Some products include the sampling activity as a component of the workspace composer agent itself. This merging of responsibilities enables you to deploy only a single agent to accomplish both tasks.

Workspace Design

Information gathered through the desktop sampling process will fill out the picture of user behaviors on your managed systems. It at the same time should highlight some of the areas of gap in your security policies and practices that can be fixed through the control of the workspace. Most importantly, the sampling process will provide your project team with the added situational awareness needed to better control workspaces throughout your environment's many contexts. It will also serve as the data that can be used for quantifying what those contexts are as well as which you want to bring under control.

Leveraging the information gained through the first step, it becomes possible to begin creating an initial workspace design. This design will likely be based on a subset of user contexts in order to keep the project manageable during its initial phases. This initial workspace design will focus on identifying which areas are to be controlled by IT and business policies as well as which will remain customizable by the individual user.

> **Note**
> Important to note here is that any workspace design is an iterative process. You will find in your first run through the process that you've missed areas or that you've configured too much control into others. This right-sizing should be expected and is an excellent reason why it is important to start small.

Initial Agent Installation

Remember that the workhorse of any User Workspace Management solution is its workspace composer agent. A system that does not have this agent does not fall under the control of your User Workspace Management solution. Conversely, when agents are installed to computers, those computers can incrementally be brought under centralized control.

It is also important to recognize that this initial installation of agents needn't necessary *immediately* begin the control of workspaces. Remember that the goal of this process is to at the same time control the workspace while retaining user customizations within that workspace. It is for this reason why the agents in an effective solution will have the additional job of identifying and synchronizing each user's personalization data back to the central database as a first step in this process.

Environment Control and Tuning

With the agent installation and initial data synchronization complete, control of the process returns back to the project team. The initial synchronization provides the foundation upon which administrative controls can be based. The project team can then elect to throw away certain customizations, overwriting them with those as defined by IT and business policy. The remaining customizations are left to the user for creating that comfortable workspace they will eventually use across all delivery mechanisms.

This tuning process may take an extended period of time, as the project team and the users in the sample group work back and forth to identify which areas can and should be controlled. At the same time, the project team should use the data in the first cycle to identify additional contexts that may have been missed in the initial design.

Extending Agent Coverage

When ready, the final step in each iteration of this process is the extension of agent coverage to the rest of the environment. This final step serves as the rollout of the final product to the area under control. Depending on the needs of the business, that final rollout can occur by delivery mechanism or by class of user.

Environment Transformation: Two Real-World Examples

Finally, all this technical conversation leads us right back to the original position first discussed in Chapter 1. That position was outlined as the new systems management paradigm that can be enjoyed by environments that embrace User Workspace Management. At this point, you should see both the technical and business benefits that arrive with the logical encapsulation of the workspace and its decoupling from the rest of the system.

This recognition opens the door for substantially improving some steps in what are commonly considered very difficult IT projects. Because you are now able to protect the users' workspace from changes to the underlying structures, you should feel a greater comfort with proactively enacting change:

- Making changes to applications, including upgrading versions, needn't impact users
- Wholesale migrations to new operating systems (OSs) can occur seamlessly
- Replacement of traditional hardware with different or even virtual hardware won't impact the user

Two of those scenarios are worth taking a quick final look: the migration to virtual hosted desktops and the upgrade of Windows XP (or other OSs) to Windows 7.

Migration Scenario—Upgrades

The first of these real-world scenarios has to do with the desire to move off the Windows XP (or other OS) platform to Microsoft's newest Windows 7 OS. At issue for many with this upgrade is the upgrade's ratio of cost versus benefit. In effect, do the extra benefits of a new OS like Windows 7 outweigh the pains in actually migrating to it?

Using traditional systems management solutions, those pains can indeed be substantial. As discussed in Chapter 1, the process to actually migrate user settings off of a candidate system can consume substantially more time than the upgrade itself. In my own personal experience, the upgrade took 30 minutes to complete while the manual personality transfer process consumed three-and-a-half hours. Attempting to accomplish such an upgrade through manual methods often doesn't pass the cost versus benefits test for many organizations.

However, incorporating such an upgrade within the framework of a User Workspace Management solution can substantially reduce the cost side of this equation. Using such a solution, as shown in Figure 4.6, individual user data is virtually eliminated from consideration as a cost center. Once in place, users need only be instructed to log out of their sessions when they leave for the day. That logout process ensures the complete synchronization of their personal data with the centralized database. Under the covers and using traditional systems management tools, IT can then replace the existing Windows XP instance with a Windows 7 OS. Once complete, the user's workspace is then reconfigured to fit within the new OS and ultimately delivered as the user returns for the day.

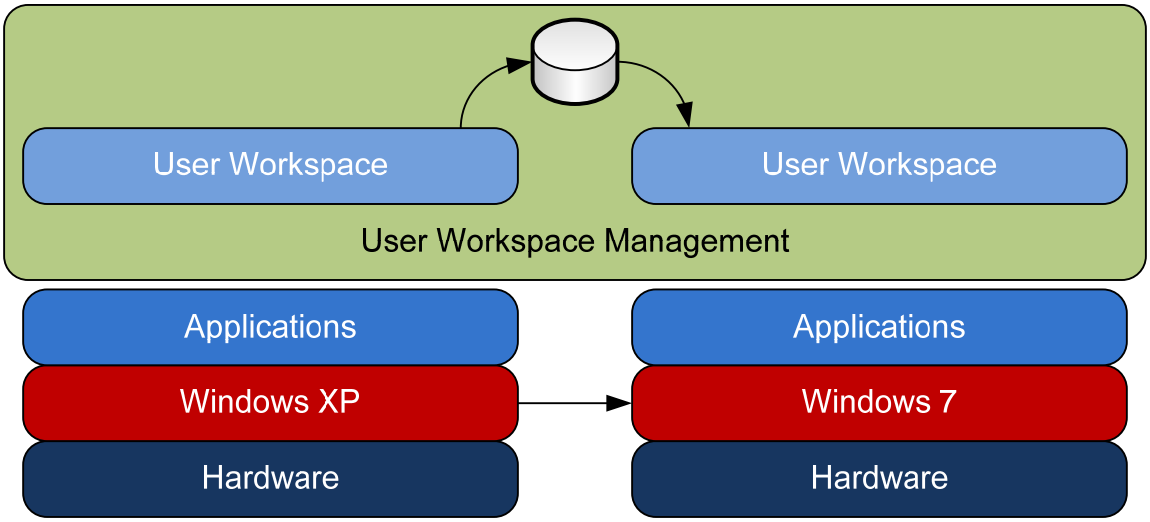

Figure 4.6: Upgrading from Windows XP to Windows 7 becomes a more trivial exercise when paired with User Workspace Management.

Green Field Scenario—VDI

The second solution is one that is growing in use throughout the IT industry. VDI or hosted virtual desktops are becoming more common in many industries due to their ability to relocate much of the processing (and, thus, security and administration) of desktops back to the data center.

However, in environments that lack User Workspace Management, actually getting users off their physical OSs and onto a virtual instance incurs the same pains as the OS upgrade discussed earlier. Moving a user from a physical instance to a virtual one incurs the same kinds of costs as a wholesale replacement of hardware.

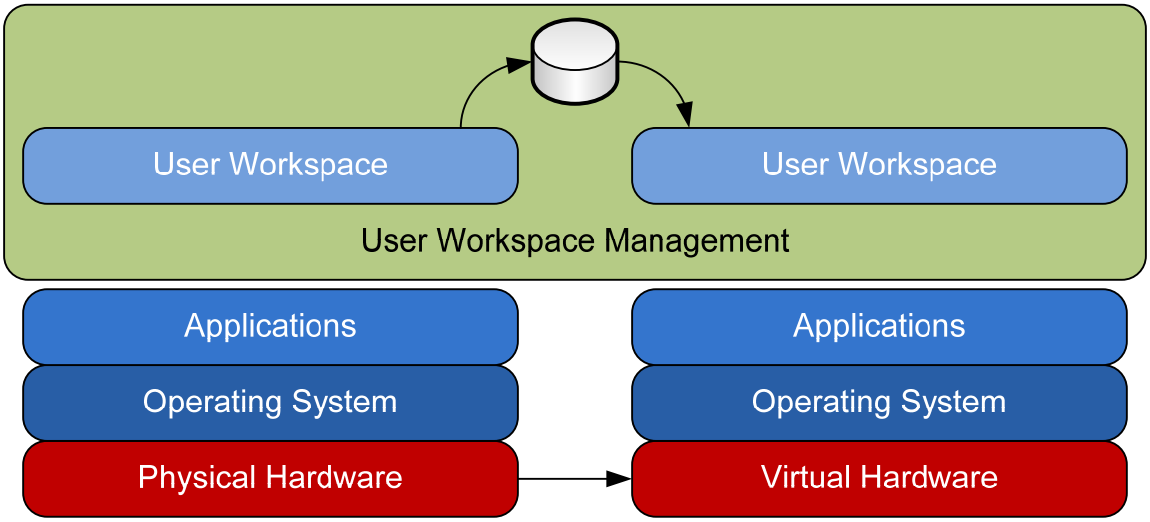

Figure 4.7: A fully-realized User Workspace Management solution also reduces many of the costs and pain points for a VDI migration.

However, a fully-realized User Workspace Management solution also assists with VDI upgrades. In the same way as the example earlier, a User Workspace Management solution enables the synchronization of user data to its centralized database, enabling IT to seamlessly replace physical hardware with virtual.

Improving Your Life. Improving the Lives of Your Users.

In the end, a User Workspace Management solution has the potential to enhance many of the traditionally-painful operations of IT. With it, difficult tasks such as OS upgrades, migrations, and wholesale paradigm changes like VDI become more-trivial solutions to incorporate. The first step is in decoupling your users from their devices.

Hopefully, this guide has given you some impression about how solutions in the User Workspace Management ecosystem can assist your business. Solutions like these bring about true management of IT's "last mile," making life easier for the IT professional and project manager while at the same time making life easier for its users.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.