TRANSFER OF COMPUTING ENVIRONMENT

Field of the invention

The present invention relates to mobile computing environments and refers particularly, though not exclusively, to mobile computing environments where the software application requirements of a user are provided by an external source.

Reference to related application

Reference is made to earlier patent applications numbers PCT/SG99/00037 filed 10 March 1999, SG9903604-8 filed 24 July 1999, and SG9903866-3 filed 11 August 1999 (the "earlier applications"). The contents of the earlier applications are hereby incorporated by reference.

Background to the invention

The increasing complexity, cost and size of many software applications makes it uneconomical for many users to maintain all software applications in-house. Also some business-related software applications are used infrequently. For example, those relating to taxation returns are used once a year. This is especially important for business users as it may direct valuable resources from their core business focus. Furthermore, for small to medium sized businesses there is the added difficulty of finding and retaining competent staff familiar with, and able to handle, all the software applications they require. These, and other, factors have lead a trend to the outsourcing of software applications.

In response to this trend, a new service industry has been created – Application Service Providers (ASPs) – who supply software applications to users on a fee basis. An ASP manages and delivers software applications capabilities to multiple users from centralized data centres across a wide area network thus eliminating the need for their customers to purchase and maintain those software applications in-house. Existing ASPs include US internetworking, IBM Global Services, EDS, USWeb, FutureLink, Oracle Online, Corio, ServiceNet, and World Technology Service.

For an ASP to be effective, it must provide the following:

(a) protection of the user's data. The user must be satisfied that only those persons authorized by the user have access to the user's data, the data will not be lost or misdirected, and that the user will always have access to and be able to operate the data;

(b) reliability of service. As an ASP may have users in industries which operate 24 hours a day, seven days a week, the users must be able to operate the software applications it requires at all times. Furthermore, any upgrading by the ASP must not affect the service. Although the upgrade could happen at midnight US West Coast Time, the user may be in Singapore where it is already the middle of the following afternoon and at peak workload;

(c) responsive performance. User's should not perceive a slowing in response speed against the running of the applications on the user's machine. This requires not only sufficient capacity by the ASP, but also sufficient bandwidth and other related communication issues; and

(d) the ability to obtain software applications from multiple supplies. This is desirable as the need of the user may vary (e.g. accounting, sales, production, etc) and different suppliers may specialize in different areas.

To satisfy all of these requirements an ASP must have not only expertise in the installation, integration and maintenance of all their software applications, but must also have a reliable hosting infrastructure. This can be very expensive to establish. Therefore, the entry barriers for a good ASP are quite high.

Prior Art

Existing internet portals such as My Yahoo!, Excite and MagicalDesk provide each subscriber with an account that comes with a mailbox, starting web page, and file directory that can be accessed anywhere, as long as a browser is available. This is very useful for people who wish to stay in touch and to access their files whether they are home or in the office, especially for people who travel.

In addition, the specification of the following patents and patents applications explain methods of mapping remote storage within a native file system so that remote data can be accessed like local data. They do not address the migration of the user's entire computing environment in addition to providing access to files stored on remote servers. They also do not provide for dynamically selecting a protocol for file transfers between user and server.

WO9857250 of Microsoft Crop discloses a method through which a file's attributes are used to determine whether it belongs to remote or local storage. If it indicates remote storage, the file system driver passes control to higher level drivers which then assume control to finish processing the I/O request. The present invention does not use the file's attributes to determine whether it is local or remote. Rather, it implements a "virtual" drive and the requests destined for the virtual drive are automatically redirected to the file server by the file system monitor. In addition, Microsoft's patent supports only SMB protocol, does not have protocol adaptation, and does not cover the migration of the computing environment.

WO9746956 of AT & T Corp discloses an internet file system that provides access to resources on the internet supporting multiple protocols transparent to applications. The approach taken is to overwrite shared libraries used by an application. This implies that it cannot support applications that use static libraries. The approach by the present invention is to use the kernel driver to intercept all file system calls and then to redirect the file system call to the appropriate file server. Hence, the approach of the present invention can support applications that use either static or dynamic libraries. Moreover the reference does not cover dynamic adaptation of protocol based on what is currently available from the file server. Finally, it does not disclose the migration of the computing environment.

EP0774723 of Matsushita Corp discloses a distributed server environment, where a central file management apparatus maintains a virtual file management table that indicates the file's virtual identity and the physical location of the file. Requests are directed from the file management apparatus to the appropriate server based on the actual location. The system of the present application does not need a special server/machine, can work with standard file servers without modification, and all the information regarding remote files is maintained on the user's machine.

US5845282: This patent describes a method that establishes a data transfer link between a pen-based computer and a remote desktop computer, displays the files available for retrieval from the remote computer and translates each file that is selected to be transferred. This is essentially a file/directory mapping product.

US5864853: Here there is disclosed a portable file system that includes:

(a) at least one portable data processing device having a memory unit for storing file data and file management data of portable side files,
(b) at least one stationary data processing device having a processing unit for executing desired processing by making accesses to the portable side files and,
(c) a conversion unit for converting at least one of the file data and the management data of each requested file among the portable side files for which a file access request is issued by the processing unit, into a form suitable for the stationary data processing device.

The conversion enables the processing unit to access each request file among the portable side files according to converted file data/file management data obtained by the conversion unit. This is essentially a file/directory mapping product.

US5561799: This relates to an extensible file system which layers a new file system over an old file system to provide coherent file data and describes a mechanism for layering a new file system over an existing file system, possibly residing in different computers. A data movement facility connects the pager program in the existing file system to the cache program in the new file system, thus supplying coherent file data between them. This is also essentially a file/directory mapping product.

Further prior art can be found in the "follow me" systems in "WINDOWS 2000", IntelliMirrors, and Netware Z.E.N. These software applications enable a desktop, including user settings and software applications on the desktop, to "follow" its "owner" to any of a group of machines on a network that is served by the same directory tree and have the same operating system.

Objects of the invention

It is the principal object of the present invention to provide a mobile computing environment where the software application requirements of a user are provided by an external source and where the mobile computing environment is mobile across domains.
A further object is to provide such a mobile computing environment that can migrate across operating systems.

Yet another object is to provide such a mobile computing environment where a data centre is provided and which can host mobile computing environments created by a plurality of ASPs.

Summary of the inventions

With the above and other objects in mind the present invention provides a method for transferring a computing environment from a supplier to a user, the method including the steps of:

(a) loading a mobile computing environment on a machine of the supplier;
(b) configuring the mobile computing environment;
(c) saving the configured mobile computing environment as image data;
(d) transferring the image data to a data centre and saving it at the data centre;
(e) transferring the image data to a user's machine; and
(f) recreating the configured mobile computing environment on the user's machine from the image data.

Preferably, the supplier is an Application Service Provider. More preferably, the transferring steps (d) and (e) occur over a network selected from the group consisting of a local area network, metropolitan area network, and wide area network. The wide area network may be the internet. Advantageously, the suppliers' machine and the data centre may be on separate servers, or on the same server. The user can use the configured mobile computing environment subsequent to its recreation in step (f), but unauthorized changes to the configured mobile computing environment by the user may not be propagated back to the image data. Preferably upon the use by the user ending, the image data is transferred back to the data centre. Both the supplier's machine and the data centre may have a server administration module, the server administration module in the suppliers machine creating mobile computing environments. Preferably, the server administration module also modifies existing mobile computing environments. More preferably the server administration module in the data centre manages user accounts. Furthermore, the server administration module in the data centre may regulate the transference of steps (d) and (e).

The transference of steps (d) and (e) may be on a physical storage medium. For step (e) the image data may be first received and saved in a user's server for use over several sessions, and the use may be by multiple users. The image data may contain a limit on how many users are inclined in the multiple users and the limit is set by the supplier as part of step (b). The limit is advantageously enforced by the recreated mobile computing environment. Preferably, a tracking agent is notified when the recreated mobile computing environment is installed on the user's machine. More preferably, authorization is sought by the recreated mobile computing environment to permit use by the user.

At least one user-specified component may be attached to the recreated mobile computing environment. The at least one user-specific component may include a personal data directory.

The personal data directory is preferably installed on any one of the group consisting of the supplier's machine, the data centre, the user's machine, a user's server. Preferably,

the recreated mobile computing environment masks off at least one component in a native computing environment on the user's machine.

The supplier may configure the mobile computing environment as a replacement for a previous mobile computing environment. Also the user may be able to return the mobile computing environment back to the supplier for troubleshooting and maintenance.

In a preferred form, the data centre forwards a notice to the user's machine to deactivate the recreated mobile computing environment. Preferably, upon deactivation the mobile computing environment is returned to the data centre

Description of drawings

In order that the invention may be better understood and readily put into practical effect there shall now be described preferred forms of the present invention, the description being with reference to the accompanying illustrative drawings in which:

Figure 1 is a basic flow chart of the supply chain of (a) the prior art, and (b) the present invention;

Figure 2 is a schematic illustration of the system architecture;

Figure 3 is a representation of the server administration interface;

Figure 4 is a representation of the mobile computing environment;

Figure 5 is a representation of the user account manager interface;

Figure 6 is a representation of the user login interface; and

Figure 7 is a flow chart of one form of the invention.

Description of preferred embodiments

In Figure 1(a) there is shown the present system used by an Application Service Provider ("ASP"). Here, a ASP 10 obtains a number of software applications from the software developer 12. The software is subjected to license conditions. A user 14 logs into the server of the ASP and in the ASP's server uses one or more software applications under appropriate commercial terms. The user 14 sends their data to the ASP 12 over the internet.

Figure 1(b) shows the supply chain according to the present invention. The ASP 10 obtains a number of software applications from the software developer 12. The software is subjected to license conditions. The ASP creates a mobile computing environment such as, for example, a virtual computer. This is configured on the ASP's server, and saved. It is then transmitted as image data to a data centre 16 which saves the image data, then onforwards it to the user 14. Once in the machine of the user 14, the mobile computing environment is recreated from the image data, and the user can use the relevant software application in the user's machine. All subsequent communication to and from the user is from the data centre 16. The

configured computing environment may include one or more of the required software applications, environment settings, screen background, drive and directory mappings, usage history, and short cuts.

By decoupling the set-up of the mobile computing environment from the hosting of the application services, the ASP is free to focus on application set up, leaving the operation infrastructure to the data centre 16. This allows higher efficiency and margins through specialization, and lower entry costs. The data centre 16 can host mobile computing environment created by several ASPs, and the user 14 can select any suitable mobile computing environment for their session, and still have access to their drive/directory for their documents and data.

To now refer to Figure 7 in conjunction with Figure 2 to 6, there is shown the deployment architecture of a preferred form of the present invention. The ASP 10 and data centre 16 each use a backend server that holds the available mobile computing environments, together with a server administration module 18. A mobile computing environment 20 is created in the ASP 10 and forwarded to the data centre16. A user login module 22 is provided in both the ASP 10 and data centre 16. A user login interface is shown. The server administration module 18 is used to create and/or modify computing environments 20, manage user 14 accounts, and regulate the transference of mobile computing environment 20.

Figure 4 shows the interface for the mobile computing environment manager, which enumerates all mobile computing environment currently registered in the ASP server giving such information as, for example, issue of the software, platform(s) supported, and user licenses. From here, the server administration module 18 can:

(a) create a new mobile computing environment 20 and load it on the ASP administration module's machine. The administration module 18 can then configure the mobile computing environment 20 including the installation of all required software. The mobile computing environment 20 is then saved on the ASP's server. At the stage of saving, the administration module 18 is able to specify the platforms in which the mobile computing environment 20 is valid, as well as being able to set passwords for activation and maintenance. The mobile computing environment 20 can be created and saved in advance of anticipated user 14 requirements.

(b) load the mobile computing environment on the ASP's administration module's machine. Any maintenance password is verified before loading. The administration module 18 can then modify the configuration of the mobile computing environment 20, including the installation and/ or removal of software. The platform settings and user password can also be changed, then the mobile computing environment 20 is saved as image data.

(c) remove the mobile computing environment 20 from the ASP's server and send it to the data centre, after verifying the maintenance password. It is there upon saved as image data, and sent to the user 14 after the appropriate verification request is sent to and approval received from, the server of the data centre.

The mobile computing environment manager also provides the interface for activating and deactivating mobile computing environment for various supported platforms.

The user account manager located in the data centre 16, the interface for which is illustrated in Figure 5, is used to create and manage user accounts. In addition to the usual user information and password, each user account also has associated with it:

(a) a " home directory" in which the user 14 can store their documents and data. The user 14 cannot store their files in the directory of the mobile computing environment 20 as the mobile environment 20 may be shared by different users; and

(b) a list of mobile computer environments 20 accessible through the particular account. The administration module 18 can add to and remove from this list.

The user login moduie 22 has an interface shown in Figure 6. When a user 14 logs in to their account at the data centre 16, the module 22 first checks whether the account is resident locally. If the account has been sent to a remote server, user 14 is given the opportunity to recall it. To do that, a request to release the account is first lodged with the outgoing request manager of the remote server, a request to receive the account is send from the remote sever to the incoming request manager of the local server, then the account is finally transferred. Until the transfer is complete, the user is not able to work on his account.

Assuming that the user account is resident locally, the module 22 then checks the mobile computing environment the user 14 has activated and notifies the user 14 if newer, updated versions are available. The user 14 can activate any mobile computing environment 20 that is made available through the user account manager.

Upon the user 14 selecting a mobile computing environment 20 to be used for the current session, if the number of users do not exceed the number of licenses available, the selected mobile environment is loaded the user's machine, recreated, then takes over from the native environment on the user's machine. At the same time the user's home directory is mapped to the mobile computing environment 20.

In addition, a file monitor is started on the user's machine. The file monitor intercepts every file system request on the mobile computing environment 20 directories. If the target file has been downloaded previously, the file monitor directs the native file system to satisfy the request from the downloaded file. If not, the file monitor downloads the target file from the file server that hosts it, decrypts the file, then directs the native file system to satisfy the request from the file. The file server could be an FTP server, an HTTP server, an SMB server, an NFS server, or a server running another protocol. Periodically, newly created files/directories and modified files/directories are uploaded to their respective host file servers.

Upon the user 14 logging out, the user 14 has the option of requesting that their account be sent to a remote server. The request will first be presented to the outgoing request manager of the local server for approval, then to the incoming request manager of the remote server, before the transfer is effected.

When the user 14 logs out, the file monitor ensures that all newly created files/ directories and modified files/ directories are uploaded. It then removes all of the user's files and directories from the user's machine before quitting. Any allowed changes to the mobile environment 20 are then propagated back to the server and the mobile

computing environment 20 is removed from the user's machine and returned to the data centre 16. The user's machine is now in its original state.

Any unauthorized changes to the mobile computing environment 20 do not permanently effect the mobile computing environment 20 as such changes are not propagated back to the image data, and the mobile computing environment is reconstructed from the image data for each subsequent use.

All transfers may be over a network, metropolitan area network or a wide area network. Alternatively an additionally a physical storage medium such as, for example, a disk or a CD ROM, may be used.

The image data may be transferred from the data centre 16 to a user's server for use over a number of sessions. Multiple users may be possible, although it is preferred that the image data contains a limit on the number of users. The limit may be set by the supplier 10 as part of the configuration of the mobile computing environment 20. The limit may be enforced by the server software at the user's machine.

Furthermore, a tracking agent may be notified whenever the mobile computing environment is loaded by the user. This may be required to enable the account manager to ensure compliance by the user with the agreed terms under which the user 14 uses the mobile computing environment 20. To assist in this, the mobile computing environment 20 preferably seeks authorization from the data centre 16 whenever the mobile computing environment is loaded on the user's machine.

The user 14 may specify a mobile computing environment 20 as a replacement for a previous mobile computing environment sent to the user 14 by data centre 16. Furthermore, the user 14 can return the mobile computing environment 20 to the ASP10 for one or more of troubleshooting, maintenance, upgrade, or the like.

If for any reason the data centre 16 requires the return of deactivation or the mobile computing environment 20 currently on the user's machine, the data centre 16 can send a notice to the mobile computing environment whereupon it is deactivated or returned, in accordance with the log out procedure described above.

Whilst there has been described in the foregoing description preferred forms of the method of the present invention, it will be understood by those skilled in the technology concerned that many variations modifications may be made without departing from the present invention.

The claims

1. A method for transferring a computing environment from a supplier to a user, the method including the steps of :

   (a) loading a mobile computing environment on a machine of the supplier;
   (b) configuring the mobile computing environment;
   (c) saving the configured mobile computing environment as image data;
   (d) transferring the image data to a data centre and saving it at the data centre;
   (d) transferring the image data to a user's machine; and
   (e) recreating the configured mobile computing environment on the user's machine from the image data.

2. A method as claimed in claim 1, wherein the supplier is an Application Service Provider.

3. A method as claimed in claim 1 and claim 2, wherein the transferring steps (d) and (e) occur over a network selected from the group consisting of a local area network, metropolitan area network, wide area network.

4. A method as claimed in claim 3, wherein the wide area network is the internet.

5. A method as claimed is any one of claims 1 to 4, wherein the supplier's machine and the data centre are separate servers.

6. A method as claimed is any of claims 1 to 4, wherein the suppliers machine and the data centre are on the same server.

7. A method as claimed in any one of claims 1 to 6, wherein the user can use the configured mobile computing environment subsequent to its recreation in step (e).

8. A method as claimed in any one of claims 1 to 6, wherein unauthorized changes to the configured mobile computing environment by the user are not propagated back to the image data.

9. A method as claimed in claim 7 or claim 8, wherein upon the use by the user ending, the image data is transferred back to the data centre.

10. A method as claimed in any one of claims 1 to 9, wherein both the supplier's machine and the data centre have a server administration module.

11. A method as claimed in claim 10, wherein the server administration module in the supplier's machine creates mobile computing environments.

12. A method as claimed in claim 10 and claim 11, wherein the server administration module in the supplier's machine modifies existing mobile computing environments.

13. A method as claimed in any one of claims 10 to 12, wherein the server administration module in the data centre manages user accounts.

14. A method as claimed in any one of claims 10 to 13, wherein the server administration module regulates the transference of steps (d) and (e).

15. A method as claimed is any one claims 1,2, or 5 to 14, wherein the transference of steps (d) and (e) is on a physical storage medium.

16. A method as claimed in any one of claims 1 to 15, wherein in step (e) the image data is first received and saved in a user's server for use over several sessions.

17. A method as claimed in claim 16, wherein the use is by multiple users.

18. A method as claimed in claim 17, wherein the image data contains a limit on how many users are included in the multiple users.

19. A method as claimed in claim 18, wherein the limit is set by the supplier as part of step (b).

20. A method as claimed in claim 19, wherein the limit is enforced by the recreated mobile computing environment.

21. A method as claimed in any one of claims 1 to 20, wherein a tracking agent is notified when the recreated mobile computing environment is installed on the user's machine.

22. A method as claimed in any one of claims 1 to 20, wherein authorization is sought by the file recreated mobile computing environment prior to use by the user.

23. A method as claimed in any one of claims 1 to 22, wherein at least one user-specified component is attached to the recreated mobile computing environment.

24. A method as claimed in claim 23, wherein the at least one user-specific component includes a personal data directory.

25. A method as claimed in claim 24, wherein the personal data directory is installed on any one of the group consisting of the supplier's machine, the data centre, the user's machine, the user's server.

26. A method as claimed in claim 24 or claim 25, wherein the recreated mobile computing environment masks off at least one component in a native computing environment on the user's machine.

27. A method as claimed in any one of claims 1 to 26, wherein the supplier configures the mobile computing environment as a replacement for a previous mobile computing environment.

28. A method as claimed in any one of claims 1 to 27, wherein the user returns the mobile computing environment to the supplier for troubleshooting and maintenance.

29. A method as claimed in any one of claim 1 to 28, wherein the data centre forwards a notice to the user's machine to deactivate the recreated mobile computing environment.

30. A method as claimed in claim 29, wherein upon deactivation the mobile computing environment is returned to the data centre.