

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
24 December 2003 (24.12.2003)

PCT

(10) International Publication Number  
WO 03/107178 A2

- (51) International Patent Classification<sup>7</sup>: G06F 9/40
- (21) International Application Number: PCT/US03/17927
- (22) International Filing Date: 5 June 2003 (05.06.2003)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
- |            |                            |    |
|------------|----------------------------|----|
| 60/388,112 | 12 June 2002 (12.06.2002)  | US |
| 60/453,308 | 10 March 2003 (10.03.2003) | US |
| 10/414,959 | 16 April 2003 (16.04.2003) | US |
| 10/414,958 | 16 April 2003 (16.04.2003) | US |
| 10/414,887 | 16 April 2003 (16.04.2003) | US |

(74) Agent: HEFFAN, Ira, V.; Testa, Hurwitz & Thibault, LLP, High Street Tower, 125 High Street, Boston, MA 02110 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant: BLADELOGIC, INC. [US/US]; 100 Crosby Drive, Bedford, MA 01730 (US).

(72) Inventors: KRAUS, Thomas, Martin; 7 Westview Road, Natick, MA 01760 (US). MANWANI, Vijay, G.; 104 Parker Road, Needham, MA 02494 (US). MUDDANA, Sekhar; 46 Trepanier Street, South Attleboro, MA 02703 (US). SRINIVASA, Balaji; 264 Grove Street, Newton, MA 02466 (US). REDDY, Ravi; 11 Seaver Farm Lane, S. Grafton, MA 01560 (US).

Published:  
— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR SIMPLIFYING DISTRIBUTED SERVER MANAGEMENT

(57) Abstract: A method and system for managing a large number of servers and their server components distributed throughout a heterogeneous computing environment is provided. In one embodiment, an authenticated user, such as an IT system administrator, can securely and simultaneously control and configure multiple servers, supporting different operating systems, through a "virtual server." A virtual server is an abstract model representing a collection of actual target servers. To represent multiple physical servers as one virtual server, abstract system calls that extend execution of operating-system-specific system calls to multiple servers, regardless of their supported operating systems, are used. A virtual server is implemented by a virtual server client and a collection of virtual server agents associated with a collection of actual servers. A method and system for executing and undoing distributed server change operations for a collection of server objects across multiple target servers in a transaction-safe manner is provided. In one embodiment, server change operations for a collection of server objects, such as files and configuration file entries, are specified in a transaction package. The target servers to which the specified change operation is directed are also identified in the transaction package. Parameter values for each of the identified target servers are specified through a parameter file in the transaction package. The transaction package is sent to the identified target servers, which execute the change operations on the target servers in a transaction-safe manner using these parameter values. A method and system for configuring heterogeneous servers across a network through modules that can browse, snapshot, track changes, track compliance, correct server objects on each of the servers, and provision new servers is provided. In one embodiment, server objects on multiple servers can be browsed in real time. While browsing, a collection of server object identifiers can be selected and collected in a template. The values of the server objects identified in the template can be recorded for a "gold server" through a "snapshot" process, which collects the values and saves them in a reference model. By comparing other live servers to the reference model, discrepancies in configuration of the other live servers can be identified and corrected. The reference models can also be used to provision a new server. Alternative to the reference model, an arbitrary snapshot or scheduled snapshots of a server can be used to track change and compliance in that server.



WO 03/107178 A2

## METHOD AND SYSTEM FOR SIMPLIFYING DISTRIBUTED SERVER MANAGEMENT

### Cross-Reference To Related Application

[0001] This application claims priority to and the benefit of U.S. Provisional Patent Application Serial No. 60/388,112 filed June 12, 2002, entitled METHOD AND SYSTEM FOR SIMPLIFYING SERVER MANAGEMENT; U.S. Provisional Patent Application Serial No. 5 60/453,308 filed March 10, 2003, entitled METHOD AND SYSTEM FOR SIMPLIFYING SERVER MANAGEMENT; U.S. Patent Application Serial No. 10/414,958 filed April 16, 2003, entitled METHOD AND SYSTEM FOR EXECUTING AND UNDOING DISTRIBUTED SERVER CHANGE OPERATIONS; U.S. Patent Application Serial No. 10/414,959 filed April 16, 2003, entitled METHOD AND SYSTEM FOR SIMPLIFYING DISTRIBUTED SERVER 10 MANAGEMENT; and U.S. Patent Application Serial No. 10/414,887 filed April 16, 2003, entitled METHOD AND SYSTEM FOR MODEL-BASED HETEROGENEOUS SERVER CONFIGURATION MANAGEMENT the entire disclosures of which are hereby incorporated by reference.

### Technical Field

15 [0002] This invention relates to the field of server management and, more particularly, to the management of servers in a heterogeneous computing environment.

### Background Information

[0003] Information Technology (IT) administrators are facing new challenges due to a significant increase in the number of servers in an enterprise's IT infrastructure and the adoption of distributed 20 electronic business applications. These challenges have resulted from: (1) a transition from client-server to Internet-based architectures, resulting in frequent interactions between different types of servers; and (2) the use of component application servers, such as J2EE (Java 2 Platform, Enterprise Edition) and .NET, to generate components, tools, systems, and complex application models. Faced with these challenges, an IT administrator may need to juggle hundreds of 25 incompatible software application configurations and track thousands of server components for the thirty to forty servers he or she manages.

[0004] Currently available configuration tools are inadequate to manage a large number of software application configuration and server components across multiple servers in a heterogeneous computing environment. To manage and configure heterogeneous servers, particularly in the

- 2 -

complex business computing infrastructure, many IT administrators use enterprise systems management (ESM) products offering monitoring tools to automate problem identification across multiple servers. However, these monitoring tools do not provide a centralized management system with a centralized configuration database, which can centrally keep track of current server components and their interdependencies across the different servers.

[0005] In addition, these ESM products provide little or no help in correcting or configuring server components in a heterogeneous computing environment. For UNIX and Linux operating system-based servers, despite the open-source and internally developed tools and scripts to handle simple configuration changes to J2EE configurations, neither the tools nor the scripts can be easily extended to address complex distributed applications.

[0006] Microsoft Window-based operating system servers are even more difficult to correct and configure than UNIX and Linux operating system based servers, due to a large number of server components having complex interdependencies. Although system management tools are available from Microsoft, they have been designed to target only small-scale homogenous Windows-based computing environments, and not the large and heterogeneous computing environment supporting multiple operating systems that most IT administrators have to manage.

[0007] Because of the inadequacies in currently available management tools, significant portions of any server configuration change operations have to be made manually by the IT administrator for each server. Accordingly, human errors can occur from these manual change operations, and from manual monitoring and tracking of each server's configuration, resulting in frequent server misconfigurations and system downtime.

#### Summary of the Invention

[0008] To alleviate this situation, systems and methods according to the invention can be used to manage a large number of servers and their server components distributed throughout a heterogeneous computing environment.

[0009] In one embodiment, an authenticated user, such as a IT system administrator, can securely and simultaneously control and configure multiple servers, supporting different operating systems, by implementing a virtual server from the user's management system. In one embodiment, the user is authenticated by an operating-system-user-context-inheritance model or standard authentication protocols, such as a public key protocol, a Kerberos protocol, or a shared secret protocol.

[0010] In some embodiments, a "virtual server" model is used. A virtual server is an abstract model representing a collection of actual target servers. To represent these multiple physical servers as one virtual server, the abstract system calls that extend execution of operating-system-specific system calls to multiple servers regardless of their supported operating systems are used. A virtual server is

- 3 -

implemented by a virtual server client and a collection of virtual server agents associated with a collection of actual servers. The virtual server client may be implemented by a network-aware code library, such as "libnc," which is implemented as a network-aware version of the "libc" library. In another embodiment, the virtual server client is a library, such as "libnc."

5 [0011] The user's management system contains a software application system, such as a command program (also referred to as a command line interface) or a configuration manager, which generates abstract system calls to request services to be performed on the target servers. In one embodiment, the virtual server client receives the abstract system calls and instantiates the abstract system calls in a thread-safe manner. The thread-safe instantiation ensures simultaneous execution of the system  
10 calls on multiple target servers, while sharing the single virtual server client among these multiple target servers and their associated virtual server agents. In the instantiating process, the virtual server client identifies the target server(s) and their associated virtual server agent(s) to receive the abstract system calls. In one embodiment, the virtual server client identifies the target server(s) in response to a server identifier included in the abstract system call. Examples of the server identifier  
15 include a host name specified in a path and a network address. The server identifier may also be inferred from a group of servers to which the target server belongs.

[0012] Also, in the instantiating process, the virtual server client transmits the abstract system calls to the identified virtual server agent for execution on the target server. Before the transmission of the abstract system call, the virtual server client may encrypt the abstract system calls using standard  
20 encryption protocols, such as the SSL protocol, the Kerberos protocol, or the shared secret protocol, to secure communication between the virtual server client and the virtual server agent. In addition, before the transmission of the abstract system call, the virtual server client may specify priority, CPU utilization, and/or memory utilization of the abstract system call on the identified target server.

25 [0013] After the virtual server agent receives the abstract system calls from the virtual server client, the virtual server agent translates the abstract system call into an operating system-specific system call, so that system call can be executed on the operating system-specific target server. Before translating the abstract system call, in one embodiment, the virtual server agent identifies the source host of the user's management system to determine the encryption protocol used on the abstract  
30 system call. The virtual server agent decrypts the abstract system call after learning about the encryption protocol used by the virtual server client. From the decrypted abstract system call, the virtual server agent identifies the authenticated user. In addition, the virtual server agent contains software modules that can map the authenticated user (presented user) to another user (effective user) and locate a corresponding local user identity on the target server for the effective user, and

- 4 -

impersonate the effective user as a local user on the target server associated with the virtual server agent. In one embodiment, if the effective user is not identified as a recognized local user on the target server, the user is designated as a local guest user on the target server. The virtual server agent further restricts the user's access to the target server through a software module that limits the user to performing predetermined actions or accessing predetermined resources on the target server, based on a role-based access control model and/or access control lists (ACLs).

[0014] The translated system calls are then executed on the target server in a thread-safe manner and the results of the execution are transported from the virtual server agent to the virtual server client. In one embodiment, the virtual server agent maintains an audit log to record the names of users and the abstract system calls executed on the target server.

[0015] In another embodiment, the application system can aggregate multiple abstract system calls into a single high-level abstract system call, which in turn is transported to the virtual server client. After receiving the high-level abstract system call, the virtual server client disintegrates the high-level abstract system call into the original multiple abstract system calls and instantiates these original abstract system calls individually. Accordingly, the virtual server agent receives the individual abstract system calls for execution on the associated target server.

[0016] In yet another embodiment, after receiving the high-level abstract system call from the application program, the virtual server client instantiates the high-level abstract system call as a whole. Thus, the identified virtual server agent receives the high-level abstract system call, rather than the original multiple abstract system calls. The virtual server agent in turn translates the high-level abstract system into the individual operating system-specific system calls to be executed on its associated target server.

[0017] In another embodiment, the virtual server modifies an existing non-distributed application supporting only one specific operating system to function as a network-aware application that is applicable across servers or devices supporting different operating systems by substituting a non-network-aware system call with an abstract system call. In one exemplary embodiment, a non-distributed Unix shell program can function as a network-aware application program that is adaptable across multiple servers or devices supporting non-Unix operating systems. In another exemplary embodiment, non-distributed scripting languages, such as Perl and Python, can function as network aware-application programs that are applicable across multiple servers and devices supporting different operating systems.

[0018] In another embodiment, software configuration components (also referred to as server objects) having intricate interdependencies with other server components can be defined and characterized under a single unified system. Through this unified system, fine-grain application

- 5 -

change operations can be uniformly and simultaneously implemented across the heterogeneous servers, rather than implementing different application change operations for each of the servers individually.

5 [0019] In yet another embodiment, a centralized management system can automatically track changes, configure, and manage multiple servers to provide compliance in accordance with pre-defined policies by incorporating the methods and systems described above.

10 [0020] This invention also relates to a method and system for executing and undoing distributed server change operations for a collection of server objects across multiple target servers in a transaction-safe manner. Here, transaction-safe means that all required steps of each server change operation are completed before the distributed server change operation is deemed completed, and if an error occurs while performing the required steps on the target servers, any changes made from these steps are undone.

15 [0021] Examples of distributed sever change operations for a collection of server objects may be installing, copying, updating, or deleting server objects. In one exemplary embodiment, a collection of server objects can be copied from a single source to multiple remote target servers. Likewise, all the changes caused by copying this collection of server objects can be reversed on the affected multiple remote target servers.

20 [0022] In one embodiment, server change operations for a collection of server objects, such as files and configuration file entries, are specified in a transaction package. In particular, server change operations are specified in a transaction package to change code and content (files, applications, compound components, etc.), configure parameters of multiple servers simultaneously, and roll-back the changes in the event of a failure. Server change operations in the transaction package can be specified to occur on primitive server objects, compound server objects, abstract configuration server objects, and component server objects. A primitive server object is an elemental server object  
25 that serves as a basis for all other types of server objects. A compound server object is a server object containing primitive server objects and other related compound server objects. An abstract configuration server object is a special type of a primitive server object that represents an entry in a configuration file when the configuration file is mapped to a common abstract configuration file format using a configuration file-specific grammar. A component server object is a sequenced  
30 collection of server objects that contains prerequisite and inheritance information about other types of server objects.

- 6 -

[0023] In one embodiment, the server change operations in a transaction package are specified in an XML-based instruction set. In another embodiment, the server change operations are specified in a text-based instruction set.

5 [0024] In one embodiment, the transaction package includes a transaction context, a parameter file, error handling actions, a sequencing instruction for the change operations, and target server prerequisites for executing the change operations, in addition to the specified change operations. The transaction context is identified by begin-transaction and end-transaction statements that encapsulate the server object change operations. The parameter file specifies parameter values for each of the identified target servers. These parameter values are communicated to the identified  
10 target servers along with the transaction package. In one embodiment, the parameter file contains parameters referencing parameter values that are identical across the target servers. In another embodiment, the parameter file contains parameters referencing parameter values that are distinct for each of the target servers. The transaction package supports several types of errors, such as soft errors and hard errors, in its error handling actions. The sequencing instruction provides an  
15 execution sequence for the specified change operations. If this instruction is not provided locally within the transaction package, an external dependency graph is accessed to provide an execution sequence for the specified change operations. The transaction package also provides the prerequisite information for the target servers to execute the specified change operations.

20 [0025] In one embodiment, the user may optionally elect to proceed with a dry run. The dry run provides an additional set of tests to see if the server object change operations can be carried out by the recipient target servers before making any changes.

[0026] After the transaction package is communicated to the target servers, the specified change operations are executed on each of the identified target servers in a transaction-safe manner using the parameter values.

25 [0027] In one embodiment, the specified change operations can be reversed when a user makes an explicit request or when an error is detected in a transaction log maintained for the transaction package, after a partial or full execution of the change operations. The transaction log keeps track of details of all the steps performed, so that each performed step of a change operation can be retraced and reversed from the affected target servers.

30 [0028] In another embodiment, multiple transaction packages can be assembled into a transaction project. All the change operations specified in a transaction project can be executed in a transaction-safe manner.

[0029] This invention also relates to a method and system for configuring heterogeneous servers across a network by providing modules that can browse, snapshot, track changes, track compliance, restore previous configuration, make updates on each of the servers, and provision new servers and applications.

5 [0030] A server object is one or a collection of related configuration parameters and server assets, such as files, directories, registries, patches, packages, services, and applications. In one embodiment, there are four types of server objects: a primitive server object, a compound server object, an abstract configuration server object, and a component server object. A primitive server object is an elemental server object that serves as a basis for all other types of server objects. A  
10 compound server object is a server object containing primitive server objects and other related compound server objects. An abstract configuration server object is a special type of a primitive server object that represents an entry in a configuration file when the configuration file is mapped to a common abstract configuration file format using a configuration file-specific grammar. A component server object is a sequenced collection of server objects that contains prerequisite and  
15 inheritance information about other types of server objects.

[0031] In one embodiment, server objects in multiple servers can be browsed in real time. While browsing, a collection of server object identifiers (without values) can be selected and manually collected in a template. In another embodiment, the template may be imported from an external vendor. In yet another embodiment, the template may include one or more previously defined  
20 templates.

[0032] The values of the server objects identified in the template can be recorded for a specific server (also referred to as a "gold server") through a process called "snapshot," which collects the values (also referred to as "snapshot results") and saves them in a reference model. In one embodiment, the reference model may be an imported reference model created by an external  
25 vendor. In another embodiment, the reference model may include one or more previously defined reference models. In one embodiment, the reference model may be used to derive compliance rules, such as baseline configuration values and compliance ranges, from the collected values for other servers on the network. By comparing other live servers to the reference model, the systems and methods track compliance and changes in the configuration of the other servers on the network.

30 [0033] Alternatively, instead of saving the snapshot results in the reference model, a snapshot result can be used to capture the configuration of a server at an arbitrary point in time. The configuration may include server objects that are explicitly selected from a server or that are implicitly selected via



- 8 -

the template. In another embodiment, the snapshot results can also be recurring snapshots of a server taken at scheduled time intervals. In this embodiment, the first snapshot serves as a baseline for subsequent snapshots, so that for the subsequent snapshots, only the changes against the baseline are captured. Thus, any snapshot can be reconstructed to show the entire configuration of a server at a specific time in the time intervals by combining the baseline with the incremental changes saved for the particular snapshot results. In addition, these snapshots taken over a period of time can be used by the user to analyze changes on the server over time. Moreover, a single snapshot or recurring snapshots can be used to track change at an arbitrary point in time or over a scheduled period of time.

5 [0034] After comparing servers on the network and identifying the discrepancies present in the compared servers, server change operations are generated to correct these discrepancies. In one embodiment, these server change operations can be presented to the servers as a transaction package so that the change operations can be executed across multiple servers in a transaction-safe manner to synchronize the target servers to the reference model or to the snapshots. Similarly, to update target servers, the user updates the reference model and packages the updates in a transaction packages to synchronize the target servers to the reference model.

[0035] In one embodiment, the reference model can be used to provision a new server that is newly added to the network to ensure consistency in the configuration of the servers on the network.

20 [0036] In another embodiment, the servers on the network can restore their previous configuration from the reference model or the snapshots, so that in case of server failure, the server can be restored to recover its existing configuration and contents.

[0037] In yet another embodiment, a live server can be compared against another live server by comparing the server objects identified in the template. In another embodiment, the user can explicitly select server objects that are commonly shared between these live servers and compare them accordingly.

25 [0038] In one embodiment, the systems and methods according to the invention manage categorically related configuration parameters across different servers by modeling the parameters in templates. Server objects (also referred to as configuration parameters) are categorized in a template per server type categories, such as an application server category, a database server category, and a web server category. In the same template, the server objects are then categorized by configuration parameter type categories (e.g., network parameters, capacity parameters, availability parameters, performance parameters, and security parameters), sub-categories, and associate key words based on

its function. A new template can be derived from the first template that combines the categorically related server objects across the server categories manages the configuration parameters as if they belonged to a single server. For example, the configuration parameters of an individual web server related to security can be changed in concert with security parameters of an application server and a database server.

#### Brief Description of the Drawings

[0039] In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

10 [0040] FIG. 1 is a block diagram depicting an embodiment of a system for managing multiple servers in a heterogeneous computing environment.

[0041] FIG. 2 is a block diagram depicting a virtual server client in accordance with an embodiment of the invention.

15 [0042] FIG. 3 is a block diagram depicting a virtual server agent in accordance with an embodiment of the invention.

[0043] FIG. 4 is a flowchart depicting an embodiment of a method for receiving and executing a system call from an application program.

[0044] FIG. 5 is a flowchart depicting the details of instantiating an abstract system call in one embodiment of the method of FIG. 4.

20 [0045] FIG. 6 is a screen shot of an embodiment of a system implementing the method of FIG. 4.

[0046] FIG. 7 is a block diagram depicting an embodiment of a system for executing and undoing distributed server change operations in a transaction-safe manner.

[0047] FIG. 8 is a flowchart depicting an embodiment of a system for executing and undoing distributed server change operations in a transaction-safe manner.

25 [0048] FIG. 9 is a flowchart depicting an embodiment of a method for executing and undoing distributed server change operations in a transaction-safe manner.

[0049] FIG. 10 is a block diagram depicting an embodiment of a system for configuring multiple servers in a heterogeneous computing environment.

30 [0050] FIG. 11 is a flowchart depicting an embodiment of a method for configuring multiple servers in a heterogeneous computing environment.

[0051] FIG. 12 is a block diagram depicting an embodiment of a system for managing server objects as described in a embodiment of the invention.

[0052] FIG. 13 is a block diagram depicting an exemplary embodiment of the system of FIG. 12.

[0053] FIG. 14 is a user interface display in an embodiment for a system implementing the method of FIG. 11.

#### Detailed Description

[0054] Referring to FIG. 1, a user 10, such as a system administrator, manages a number of servers 15A, 15B, 15C, 15D, generally 15, which are computers, each of which can be of the same or of different types than the other servers 15. The servers 15 are typically server-class general-purpose computers, which provide services (e.g. software applications and/or data) to other computers via one or more computer networks. For example, the servers may be application servers, routers, firewalls, load balancers, storage controllers, or a combination of these or other computers or network devices.

[0055] Examples of application servers are databases, such as the Oracle database from Oracle Corporation of Redwood City, California or other business applications. Application servers may also include web servers, such as the Apache web server from the Apache Foundation, and Internet Information Server (IIS) from Microsoft Corporation of Redmond, WA. In addition to these examples, other programs can be provided by the servers 15. It should be understood that as used herein, the term "server" is not limited to server-class computers or application servers, but refers generally to computers on which the embodiments of the invention operate, which may include other types of computers or network devices.

[0056] As shown, each of the servers 15 may use a different operating system. For example, server 15A uses MICROSOFT WINDOWS (e.g., WINDOWS NT and WINDOWS 2000), available from Microsoft Corporation of Redmond, WA; server 15B uses SUN SOLARIS, available from Sun Microsystems, Inc. of Santa Clara, CA; server 15C uses RED HAT LINUX, available from Red Hat, Inc. of Durham, N.C.; and server 15D uses IBM AIX, available from IBM of Armonk, NY. It will be understood that this is just one example of the operating systems that may be used on the servers 15, and other combinations and operating systems may be used on the servers 15 in accordance with embodiments of the invention. One of the benefits of the system is its ability to operate in an environment having heterogeneous servers.

[0057] In one embodiment, the user 10 manages the servers 15 via a management system 20. The management system 20 is typically a server-class computer that provides the user 10 with an ability to manager servers 15 in a consistent manner through use of application programs 25. The management system 20 may be one of the servers 15, or any server-class computer that can communicate with the servers 15 over a network. Any of the target servers 15 can be designated as the management system, as long as the designated server includes appropriate application programs and software modules to manage remotely located servers.

- 11 -

[0058] Application programs 25 in the management system 20 can include one or more of a command-line shell program 25A and related programs for executing shell commands (e.g., UNIX shell commands such as ls, mv, rm, etc.), a configuration manager 25B for managing system configuration, and/or other applications 25C. The application programs 25, which in some implementations are “network-aware,” communicate abstract system calls to a virtual server client 5 30, which in turn communicates the abstract system calls to the servers 15 that are the target(s) for execution of the operations requested by the abstract system calls. Advantageously, through use of the abstract system calls, the “network-aware” applications are able to request services from heterogeneous servers supporting different operating systems without having to modify their architecture to support each of the different operating systems. 10

[0059] For example, the user 10 enters commands, such as Unix shell commands, to the shell program 25A via a command line interface. Commands can be entered, for example, to distribute files, directories, software packages, and patches to the target servers 15. Commands can also be entered to edit configuration files of the target servers 15. In addition, commands can be entered to 15 remotely reboot the target servers 15, and stop and start change operation on the target servers 15.

[0060] For example, in one implementation, the Unix shell command “ls,” which requests a server computer to list a directory of files, may be modified to be used with the user’s management system 20 and the virtual server client 30 to list a directory of files from any of the target servers 15. From the user’s 10 perspective, the “ls” command is used in the normal manner, except that the user 10 can identify a target server 15 for the command in a path associated with the command. For example, if the target server 15A is named “targetserver1,” the user 10 may enter the command “ls //targetserver1/path/” to list the files in the specified path on the target server 15A. 20

[0061] To implement this ls command of the shell program 25A on the user’s management system 20, the shell program 25A translates the system calls called by the “ls” command into one or more abstract system calls. These abstract system calls are sent to the virtual server client 30, which in 25 turn sends the abstract system calls to appropriate target servers 15, in this case, the target server 15A. After execution of the command on the target servers 15, the results are communicated back to the user 10 via the application programs 25 and the virtual server client 30.

[0062] Other programs can be made “network aware”. For example, in some implementation, script interpreters, such as interpreters for the Perl and Python scripting languages can be modified 30 to work with the virtual server client 30. Generally, selected system calls made by an application program are translated into abstract system calls, which are communicated through the virtual server client 30 to the servers 15.

- 12 -

**[0063]** In addition to providing shell commands and other application programs, the management system 20 may include a configuration manager 25B. In one embodiment, the configuration manager 25B is used to configure one or more of the servers 15. The configuration manager is a software application program that implements server change operations that are in turn translated into the corresponding operating system specific commands on the target servers 15.

**[0064]** In one implementation, an application program 25 directs abstract system calls to specific target servers 15. In another implementation, the application program 25 can also direct abstract system calls to a group of servers. A group of servers can be pre-defined or dynamically defined based on attributes such as operating systems, capacity, IP address ranges, and installed applications.

For example, the application program 25 can direct an abstract system call to a group of servers, consisting of a subset of servers 15 running the Linux operating system. Application program 25 thus can deploy a command onto a server in this group without specifying a particular server in the subset. In this way, the application program 25 does not need to keep track of each server, nor determine which servers have sufficient capacity or features to run the program; rather, the application program 25 can deploy commands (or change operations) to a predetermined group, and the virtual server client 30 decides which specific server should run these operations.

**[0065]** The virtual server client 30, which may be included in the management system 20, presents the servers 15 to the application programs 25 as a single “virtual server” on which system call operations can be executed. The virtual server client 30 is implemented by a software library, which in one implementation is roughly analogous to the C library, libc. The application programs 25 can be statically or dynamically linked to the virtual server library, which is called libnc. In one embodiment, non network-aware application programs 25 are converted to network-aware programs by replacing calls to the libc library with equivalent calls to the libnc library, which provides abstract network-aware system calls.

**[0066]** In an alternative embodiment, the virtual server client 30 may be implemented as part of an operating system. For example, the operating system running the user’s management system 20 can receive abstract system calls and communicate them to the remote target servers 15. Accordingly, for purposes of executing an abstract system call a target servers 15, the source of the abstract system call is immaterial.

**[0067]** In some embodiments, the virtual server client 30 communicates with the servers 15 through virtual server agents 35 associated with the servers 15, which will be described in detail below. The virtual server client 30 communicates with virtual server agents 35 to present the multiple physical target servers 15 as a single virtual server to the application programs 25. As an abstract representation of a collection of the physical servers 15, the virtual server intercepts the abstract

- 13 -

system calls via the virtual server client 30 and routes the abstract system calls to the virtual server agents 35.

5 [0068] When the virtual server client 30 receives an abstract system call from an application program 25, the virtual server client 30 checks the abstract system call to determine whether this system call is a local call or a remote call. If the abstract system call is a local call, then the operating system running the management system 20 executes the system call locally. If the abstract system call is determined to be a remote call, the virtual server client 30 sends the abstract system call to a virtual server agent 35 associated with a target server 15 via a message protocol. For example, when an “ropen” abstract system call, representing a remote file open command, is received by the virtual server client 30, the data representing the “ropen” command and parameters associated with the “ropen” command are sent to appropriate virtual server agents 35. The target-servers 15 for a system call are identified by the user 10 or the application programs 25. The virtual server client 30 identifies the target servers 15 from their virtual server agents 35 and determines where the system call should be directed.

15 [0069] The virtual server agents 35 receive abstract system calls from the virtual server client 30 and prepare the abstract system calls for their associated target servers 15. When the virtual server client 30 determines to which virtual server agents an abstract system call should be directed, each of the virtual server agents 35 receives the abstract system call. As a part of preparing the abstract system call for the associated target servers 15, the virtual server agents 35 provide security measures to ensure that the user 10 is authorized to access the target servers 15, and that the virtual server agent 35 controls the user access, as provided by the associated target server 15. Once the user 10 is authorized, the virtual server agent 35 translates the abstract system call into an operating system specific call directed to its associated target server 15. The target server 15 executes the abstract system call and returns the results back to the virtual server agent 35, which in turn sends the results back to the appropriate application programs 25 via the virtual server client 30.

25 [0070] In one embodiment, the virtual server agents 35 (also referred to as Remote System Call Daemon or RSCD agents) are software modules attached to their corresponding target servers 15. In another embodiment, the virtual server agents 35 are software modules that are not attached to their corresponding target servers 15, but are in communication with their associated remotely located target servers 15.

30 [0071] In some embodiments, instead of acting as a messenger that sends an abstract system call to a specific target server 15, one of the virtual server agents 35 can represent a group of physical servers. Thus, if the same command needs to be executed on multiple servers, these servers can be

- 14 -

aggregated into a group, represented by a single virtual server agent 35, so that appropriate system calls can be made to a group of servers simultaneously via that virtual server agent 35.

[0072] Generally, abstract system calls may include all types of system calls including file system calls, operating system calls, and the like. An abstract system call typically is implemented as a  
5 modification of an analogous standard operating system specific call. For example, the abstract system call “ropen” is analogous to a standard system call “open,” which opens a file on a server.

[0073] With minor modifications to an application program’s source code, any application program can make operating system agnostic abstract system calls. By changing the system calls to abstract system calls, any generic application program can be made into a network aware-application that can  
10 operate transparently across servers supporting different operating systems.

[0074] In one embodiment, only the system calls that are applicable to all of the target servers 15 can be modeled as abstract system calls. For example, if the target servers 15 include Unix-based servers, it may not be possible to model a system call to update a registry as an abstract system call, since a registry, which is a Windows specific object, does not exist and has no relevance for Unix-  
15 based server platforms.

[0075] Referring to FIG. 2, in one embodiment, the virtual server client 30 includes various software modules which implement its functionality. These modules include a receiver 40 that receives an abstract system call made by an application program 25, and forwards the abstract system call to an instantiator 42. The receiver 40 is a software module that acts a messenger  
20 between the software application programs 25 and the instantiator 42. In one embodiment, the receiver 40 receives the abstract system call from one of the software application programs 25 used by the user 10. The receiver 40 then forwards the abstract system call directly to the instantiator 42. In another embodiment, the receiver 40 may receive standard operating system specific system calls from an application program 25. The receiver forwards such standard system calls to the  
25 instantiator 42 for the instantiator 42 to decide to where the system calls should be directed.

[0076] The instantiator 42 instantiates abstract system calls in a thread-safe manner. The thread-safe instantiation shares a single resource between multiple operations without requiring changes to the architecture of the application programs requesting the operations. Typically, thread-safe instantiation shares the same virtual server client 30 between multiple simultaneous execution of  
30 system calls. The use of the shared resource, such as the virtual server client 30, is coordinated, so that the execution of one operation does not impact the execution of other operations. In one embodiment of the thread-safe instantiation, the application programs 25 can instantiate multiple commands (or operations) via the instantiator 42. For example, the application programs 25 may invoke multiple “ropen” system calls that are directed to one or more target servers 15. The

- 15 -

“ropen” system call is received by the instantiator 42 in the virtual server client 30. The instantiator 42 then distributes the “ropen” abstract system call to each of the virtual server agents associated with the target servers, so that multiple “ropen” calls can be executed simultaneously by the target servers 15.

5 [0077] In one embodiment, the instantiator 42 is implemented as a software library that provides routines that represent the abstract system calls. One particular implementation of the software library is called “libnc.” Libnc is a “network-aware” library that is analogous to the standard C library. The Libnc library supports the network aware application programs 25 by instantiating the abstract system calls generated by the application programs 25.

10 [0078] In one embodiment, the instantiator 42 determines to which virtual server agents 35 an abstract system call should be directed. The instantiator 42 identifies target servers 15 by finding the target server identifiers specified in the abstract system call. The target server identifier may include a path name, which in turn may include a host name or a network address (e.g., IP address) for the server. The target server 15 may also be identified by server names explicitly stated in a file which is to be run on specific named servers. Alternatively, the server identity may be inferred from a subset of servers or a group of servers (e.g., a group of Linux servers) to which the target server 15 belongs.

15 [0079] Before transmitting the abstract system call to the virtual server agents 35, the instantiator 42 can also specify the priority, CPU utilization, and memory utilization of the system call for the target servers 15, so that the identified target server 15 platforms can perform the requested services as specified by the virtual server client 30. Once the abstract system call has been instantiated, it is sent to an encryptor 44 for further processing.

20 [0080] The encryptor 44 encrypts the abstract system call before sending it to a transmitter 46 for transmission to the virtual server agents 35. The encryptor 44 uses standard encryption protocols and algorithms to secure communication between the virtual server client 30 and the virtual server agents 35. Examples of standard encryption protocols include, but are not limited to, SSL (Secure Sockets Layer), Kerberos, and Shared Secret protocols. SSL uses a public key to encrypt data. Kerberos assigns a unique key to each authorized user. Standard encryption algorithm includes, but are not limited to, DES (Data Encryption Standard), 3DES (Triple DES), Blowfish, and AES (Advanced Encryption Standard).

30 [0081] The encryption protocol and algorithm used by the encryptor 44 must be supported by each virtual server agent 35 with which the virtual server client 30 will communicate. For example, if the virtual server client 30 supports SSL, the virtual server agent 35 must be able to support SSL for that protocol to be used. If the virtual server client 30 supports Kerberos, the virtual server agent 35 must also be able to support Kerberos for that protocol to be used.



- 16 -

[0082] The transmitter 46 uses a network interface protocol, such as TCP/IP or Ethernet, to send the abstract system call over a network to the virtual server agents 35. The transmitter transmits the same abstract system call to each target virtual server agent. In one embodiment, the transmitter 46 uses an IP address to determine to which of the target servers 15 an abstract system call should be sent. An IP address may be directly included in the abstract system call or may be inferred from a server identifier included in the abstract system call. The virtual server agent 35 accepts the abstract system call containing the IP address of the target server 15 associated with that virtual server agent 35. Once the virtual server agent 35 receives the abstract system call, the virtual server agent 35 processes the abstract system call for execution on the target server 15.

[0083] Referring to FIG. 3, each virtual server agent 35 includes software modules that implement its functionality. These modules include a receiver 50, which receives abstract system calls from the virtual server client 30, and transfers the abstract system calls to a decryptor module 52.

[0084] Before the user 10 can access the user's management system 20, the user 10 is authenticated to ensure that the user 10 is in fact the person he or she claims to be. The user 10 can be authenticated in many ways. In one embodiment, the user 10 is authenticated by the operating system of the management system 20 and the target servers 15 subsequently inherit the user's 10 identity. In another embodiment, SRP (Secure Remote Password) or PKI Cryptography (X.509 Certificates) is used to authenticate user 10. In yet another embodiment, the Kerberos 5 system can be used to authenticate the user 10 by assigning a unique private key to the user 10.

[0085] The source identifier module 52 identifies the source machine, e.g., the user's management system 20. The source identifier module 52 first determines the source machine through a network address (e.g., IP address) that was submitted to the virtual server agent 35 from the virtual server client 30 with the abstract system call and checks to see if the source host is authorized.

[0086] By identifying the source machine, the source module 52 determines the security protocols to be used by the virtual server agent 35 for encryption and decryption. In one embodiment, the virtual server agent 35 can support different security protocols. For example, the virtual server agent 35 can flexibly support either SSL or Kerberos based on the security protocol of the incoming data from the virtual server client 30. Next, the abstract system call is sent to a decryptor 54, which decrypts the abstract system call. From the decrypted abstract system call, the user identifier module 55 identifies the user 10 invoking the application programs 25 from the source machine and verifies that the user 10 is authorized to access the source machine.

[0087] After the user is identified by the user identifier 55, an identity mapper 56 and an impersonator 58 provide additional security measures as the user 10 tries to access the remote target servers 15 from the user's management system 20. The identity mapper 56 optionally maps the

- 17 -

authenticated user (presented user) to another user (effective user) and locates a local user identity on the target server 15 that corresponds to the authenticated identity of the effective user. Through the impersonator 58, the user 10 is impersonated on a remote target server 15, so that if the effective user is identified and exists as a local user on the remote target server 15, the user 10 takes on the local identity of the effective user and the permissions provided by that identity on the remote target server 15. Thus, the user's 10 access to the remote target server 15 is further restricted to the appropriate levels provided by the permissions granted to the effective user's local identity on the remote server 15. For example, if the user 10 is authenticated as "Joe" on the management system 20 and mapped to an effective user "Jane", local permissions of "Jane" will be available to the user 10 on the remote target server 15. If "Jane" does not exist on the remote target server 15, then the user 10 will be given a guest account. In one embodiment, the combination of the presented user and the role, which is defined by Role Based Access Control (RBAC), is mapped to an effective user. For example, user "Joe" having the role of a junior administrator can be mapped to an effective user named "junior administrator." Another user "Bob" also having the role of a junior administrator can be mapped to the same effective user named "junior administrator."

[0088] The effective user's access for presented user 10 is further restricted by an authorizer 60, which permits the user 10 to perform predetermined actions or access predetermined resources on a particular target server 15. This is achieved by using Access Control Lists (ACLs) to manage the effective user's access to resources on the remote target servers 15. The ACL informs the operating systems of the remote target servers 15 of the access rights of the effective user on specific server resources, such as files or directories. For example, if the user 10 is mapped to the effective user "junior administrator", then the user 10 is only permitted to perform read-only commands on certain directories or files of a group of remote target servers 15 and cannot effect any changes to the target servers 15.

[0089] After the user is authorized, a translator 62 translates the abstract system call into a standard operating system call that is understandable and executable by the target server 15. The translator 62 examines the abstract system call and identifies a standard operating system specific system call that is analogous to the abstract system call and is supported by the operating system running the associated target server 15. Once the analogous standard system call is identified, the translator changes the abstract system call to the standard system call. This standard operating system call is forwarded to an executor 66 for execution on the target server 15.

[0090] Once the executor 66 receives a standard operating system call, the executor 66 performs the services that are requested by the standard system call. In one embodiment, the executor 66 is the operating system running on the target server 15. The operating system examines system calls and

- 18 -

carries out the operations requested by the system call by, for example, communicating with other applications running on the target server 15.

5 [0091] An audit log 64 is maintained by each virtual server agent 35 to keep track of the names of the users and all the activities performed by each user, and to troubleshoot server changes and configuration errors. For example, the audit log 64 saves information about the activities requested and performed by authorized users, information about data, such as the system calls and the results of the system calls, that were transferred back and forth between the virtual server client 30 and the virtual server agent 35, as well as all parameters associated with the abstract system call. The content of the audit log 64 is then transmitted to a centralized aggregated log kept for all of the virtual server agents 35.

10 [0092] A first example of security measures incorporated in an embodiment of the virtual server implementation follows. First, the user 10 logs into the management system and is authenticated as "Joe" during the login process. This authentication process can be achieved by using a known network authentication server, such as NTLM, K5, AD, APM, NIS, etc., depending on the operating system running on the management system 20. After the user "Joe" is authenticated in the management system 20, the user "Joe" is authenticated for the target servers 15 by inheriting the user "Joe" identity through the management system 20.

15 [0093] Next, the user 10 enters a "ls" command, requesting a listing of files on the remote target server 15A, through the shell command program 25A on the management system 20. The shell command program 25A generates an abstract system call in response to the command and sends the abstract system call to the virtual server client 30 to proceed with the user's 10 request. The virtual server client 30 examines the security configuration of the abstract system call and encrypts the system call using a shared secret key scheme with a encryption algorithm, such as DES, 3DES, or Blowfish. Once the abstract system call is encrypted, the system call is communicated across a network to the virtual server agent 35A of the target server 15A.

20 [0094] When the virtual server agent 35A receives the abstract system call, the target server's 15A agent 35A attempts to decrypt the message using the secret key shared with the virtual server client 30. The virtual server agent 35A checks to see if the user "Joe" is recognized as a local user on the target server 15A through an effective user. If the user "Joe" is recognized as a local user, then the virtual server agent examines the access control list to determine if the combination of the user "Joe" 10, target server 15A, and the abstract system call is allowed. If the combination is allowed, then the access control list is used to determine whether any further restrictions apply to the user's 30 10 access to the target server 15A. The virtual server agent 35A executes the system call in accordance with any security restrictions, encrypts the results using the same-shared secret key. The

results of the “ls” command are sent back to the virtual server client 30, where they are decrypted and displayed to the user.

[0095] In a second example of security measures incorporated in an embodiment of the virtual server, the user 10 is authenticated using of SRP or PKI Certificates. Once the user 10 is authenticated the user 10 enters an “ls” command, requesting a listing of files on the remote server 15A, through the shell command program 25A on the management system 20. The shell command program 25A generates an abstract system call in response to the command and sends the abstract system call to the virtual server client 30. The virtual server client 30 examines the security configuration of the abstract system call and encrypts the abstract system call using public key cryptography, standard encryption algorithms, such as DES, 3DES, or Blowfish, may be used for exchange of session key between the virtual server client 30 and the target server agent 35A to establish a communication session between them.

[0096] After decrypting the abstract system call received by the virtual server agent 35A, the virtual server agent 35A checks to see if the user “Joe” is recognized as a local user on the target server 15A through an effective user. If the user “Joe” is recognized as a local user, then the virtual server agent 35A examines the ACL to determine if the combination of the user 10, target server 15A, and the abstract system call is allowed. If the combination is allowed, then the access control list is used to determine whether any further restrictions apply to the user’s 10 access to the target server 15A. The virtual server agent 35A executes the system call in accordance with any security restrictions, and encrypts the results using the established session key. The results of the “ls” command are then sent back to the virtual server client 30, where they are decrypted and displayed to the user.

[0097] A third example of security measures incorporated in an embodiment of the virtual server implementation follows. If the management system 20 has an existing Kerberos 5 (K5) infrastructure in place, the user 10 can be authenticated by entering a Kerberos password to the management system 20. Once the user 10 is logged in as the authenticated user “Joe,” the user 10 enters the “ls” command, requesting a listing of files on the remote target server 15A, through the shell command program 25A on the management system 20. The shell command program 25A generates an abstract system call in response to the command and sends the abstract system call to the virtual server client 30 to proceed with the user’s 10 request. The virtual server client 30 then sends the abstract system call and a Kerberos ticket, which is retrieved from a Kerberos Domain Controller (KDC) to the virtual server agent 35A.

[0098] After the virtual server agent 35A receives the abstract system call and the ticket, the virtual server agent 35A validates the abstract system call by verifying the ticket via the KDC. Once validated, the virtual server agent 35A checks to see if the user “Joe” is recognized as a local user on

- 20 -

the target server 15A through an effective user. If the user "Joe" is recognized as a local user, then the virtual server agent examines the ACL to determine if the combination of the user "Joe" 10, target server 15A, and the abstract system call is allowed. If the combination is allowed, then the access control list is used to determine whether any further restrictions apply to the user's 10 access to the target server 15A. The virtual server agent 35A executes the system call in accordance with any security restrictions, encrypts the results using a Kerberos key. The results of the "ls" command are sent back to the virtual server client 30, where they are decrypted and displayed to the user.

[0099] Referring now to FIG. 4, a method for managing multiple servers as a single virtual server is described. First, in step 400, the system represents multiple servers as a single virtual server. Next, in step 410, based on a user's request for operations to be performed on target servers, the virtual server client 30 receives an abstract systems call from an application program 25. Finally, in step 420, the virtual server client instantiates the abstract system calls and sends the abstract system call to the virtual server agents 35 for execution.

[0100] FIG. 5 shows steps involved in instantiating an abstract system call. First in step 422, the virtual server client 30 identifies the target servers 15 through target server identifiers provided within the abstract system call. Once the target servers are identified, in step 424, the abstract system call is transmitted to the virtual server agents associated with the identified target servers. The virtual server agents 35 prepare the abstract system call for the target servers 15, so that the abstract system call can be the executed on the target servers 15. For example, for the target server 15A, the abstract system calls are translated into standard Windows NT/W2K specific system calls that are executable by the operating system running on the target server 15A. Upon completion of execution of the system call, in step 426, the virtual server client 30 receives the results of the execution from the virtual server agents 35.

[0101] In one embodiment, multiple commands generate multiple system calls, which can be aggregated into a single high-level abstract system call by an application program 25. For example, if two commands, such as copy and change permission commands, are to be made to a target server 15A, the abstract system calls carrying out these commands, such as ropen, read, rwrite, and rchmod system calls, can be aggregated into one high-level abstract system call. When received by the virtual server client 30, the virtual server client 30 can disintegrate the high level abstract system call into the original abstract system calls and transmit the abstract system calls separately to virtual server agent 35. In another embodiment, instead of disintegrating the high-level system call into the original abstract system calls at the virtual server client 30, the high-level abstract system call is received by a virtual server agent 35, which in turn translates the high-level abstract system call into separate operating system specific system calls to be executed on the target server 15.

- 21 -

[0102] FIG. 6 is a screenshot showing a command being issued to multiple servers through the management system 20. As shown here, server names used as parameters for commands are preceded by two slashes to distinguish them from a path name, which is generally separated by a slash. For examples, “//redhatbiz1/etc” specifies the /etc path on the server named “redhatbiz1.”  
5 Thus, as seen in the screenshot, to compare the “/etc/hosts” file on two different servers, one named “redhatbiz1,” and the other named “redhatbiz2,” the user 10 enters the command “diff //redhatbiz1/etc/hosts // redhatbiz2/etc/hosts.”

[0103] Referring back to FIG. 1, in an alternative embodiment, the user 10 manages the target servers 15 by executing and undoing distributed server change operations across the target servers  
10 15 in a transaction safe-manner, using the virtual server implementation described above.

Distributed server change operations request the operating systems of the target servers 15 to update, delete, install, and/or copy server assets and/or configuration file entries of the target servers 15. Transaction-safe server change operations ensure that all of the required steps of each server change operation are completed before the distributed server change operations are deemed  
15 completed. Further, if an error occurs while performing the required steps on the target servers 15, any changes made from these steps are undone, and values of the target servers’ 15 assets and/or configuration entries are returned to the values they had before execution of the server change operations. In one embodiment, the application programs 25 can generate a transaction package that bundles an instruction set and necessary server contents for the operating system of each of the  
20 target servers 15 to carry out the server change operations.

[0104] Referring to FIG. 7, in one embodiment, the configuration manager 25B generates a transaction package 700 that includes files or configuration file entries 705 (together referred to as server objects), a parameter file 710, and an instruction set 715 to carry out the server change operations on one or more target servers 15 that are specified by an external file, as requested by the  
25 configuration manager 25B.

[0105] In one embodiment, the instruction set 715 includes an execution sequence of the server change operations provided for the operating systems of the target servers 15 that carry out the server change operations. If this information is not provided in the instruction set 715 in the transaction package 700, an external dependency graph 720 is accessed to provide an execution  
30 sequence of the server change operations. For example, the external dependency graph 720 can provide information about directional relationships between server objects. In particular, if NT-based program A is a prerequisite for another NT-based program B, to successfully execute programs A and B, program A must start before program B and program B must stop before program A. Although the sequence information is used to order the sequence of change operations

- 22 -

for the server objects that are specified in the transaction package, the sequence information is also used to add implied server object change operations for related server objects, such as server objects that depend on and/or depend from these specified server objects, that are not specified in the transaction package. In particular, continuing from the previous example, if the only change instruction provided in a transaction package is to stop program A, the sequence information adds the implied instruction to stop program B and then stop program A based on the directional relationship between programs A and B. Thus, the sequence information from the dependency graph determines the sequences of server change operations to be performed not only on the specified server objects, but also on their related server objects. If an error occurs while performing the service change operations, the sequence information also causes the server change operations to stop and to be reversed not only on the specified servers, but also on the related server objects.

**[0106]** As described above, if the instruction set 715 provides the sequence information for the server change operations, the instruction set 715 overrides the sequence information provided by the dependency graph 720. Similar to the sequence information provided by the dependency graph 720, the instruction set 715 provides the information related to the order in which the server change operations should be performed. The related server objects of the specified server objects are provided, so that the server change operations can effect changes on the related server objects, as well as the specified server objects. The instruction set 715 also provides dependency information between types of servers. For example, if an application server depends on a database server, the sequence information provided in the instruction set 715 will instruct the execution of the database server change operations before the execution of the application server change operations.

**[0107]** In one embodiment, the instruction set 715 specifies server change operations to occur on any of the four types of server objects 705: primitive server objects, compound server objects, abstract configuration server objects, and component server objects. A primitive server object is an elemental server object that serves as a basis for all other types of server objects. For example, for Linux-based servers, primitive server objects include, but are not limited to, files, directories, Redhat Package Manager files, and configuration file entries for text configuration files, such as the "inetd.conf" file. For Solaris-based servers, primitive server objects include, but are not limited to, files, directories, packages, patches, and configuration files entries for configuration files, such as the "inetd.conf" file. For MS NT or W2K-based servers, primitive server objects include, but are not limited to, files, file ACLs, directories, directory ACLs, application programs, hot fixes, the registry entries, registry entry ACLs, COM/COM+ (component object model) catalog entries, Metabase entries, users, accounts, and configuration file entries for all configuration files, such as ".ini" files.

**[0108]** A compound server object is a server object containing primitive server objects and other related compound server objects. For example, an extended component object model (COM+) object, an NT or W2K-based compound server object, contains primitive server objects, such as a COM+ catalog entry, NT registry entries, and DLL files. In yet another example, an Enterprise JavaBeans (EJB) object, a compound server object, contains primitive server objects including a Java Archive (JAR) file and multiple configuration file entries. In another example, a server process is a compound server object, containing primitive server objects, such as configuration file entries (e.g., a permission entry, a priority entry, a control signal entry), files, and executables.

**[0109]** An abstract configuration server object is a special type of a primitive server object that represents an entry in a configuration file via a corresponding entry in an abstract configuration file, where mapping of a configuration file to a common abstract configuration format is provided by a configuration file-specific grammar. For example, in the MS NT/W2K environment, configuration file entries are stored in ".ini" files or XML configuration files. In the UNIX environment, configuration file entries are stored in text files such as "inetd.conf" files or "httpd.conf", or XML configuration files.

**[0110]** To reconcile the difference between the configuration file entry formats across different servers, a common abstract configuration format is provided by normalizing configuration file entries through a supported configuration file-specific grammar. By modeling each configuration file entry as an abstract configuration file entry through this normalization process, server change operations may be made based on the normalized abstract configuration file entries. The change operations requested by the abstract configuration file entries are performed, and the changes are then communicated to the actual configuration file entries. Thus, in this embodiment, configuration file entries can be individually managed through use of abstract configuration file entries, without having to change the entire configuration file each time a server change operation changes an individual entry. Configuration file-specific grammars may be provided for numerous systems, including Solaris, Linux, NT4/W2K, Apache, Web Logic, and Web Sphere.

**[0111]** A component server object is a sequenced collection of server objects. For example, an NT Service Pack is a sequenced collection of NT Hot Fixes to be applied in a predefined order. Accordingly, a collection of predefined related change operations can be effected in order through a component server.

**[0112]** In addition to the constituencies of the instruction set 715 described above, the instruction set 715 specifies the server change operations to be made across the target servers 15 on a collection of predetermined server objects by communicating with the server objects (e.g., files or configuration file entries 705), the dependency graph 720, and the parameter file 710. Server change



- 24 -

operations can be used to deploy or copy files, directories, and software packages to the target servers 15. Change operations can also be used to edit configuration file entries 705 without having to log into each target server 15. In one embodiment, the instruction set 715 provides the information needed by the target servers 15 and their associated virtual server agents 35 to carry out the server change operations. In one embodiment, the instruction set 715 provides a transaction context that is identified by begin-transaction and end-transaction statements encapsulating the server object change operations. After the begin-transaction statement is made, the instruction set provides the necessary information to perform the change operations requested by the application programs 25.

10 [0113] The instruction set 715 also provides error-handling instructions for the target servers and their associated virtual server agents. In one embodiment, several types of errors are available. Soft errors are available to alert the target servers and their virtual server agents of a likelihood of occurrence of an error during server change operations. Because no actual error has occurred, the user 10 may ignore the soft errors and continue with the execution of the server change operations. 15 Alternatively, the user 10 may instruct the virtual server agents to explicitly undo all the changes made from the execution of the server change operations after reviewing the error information returned by the soft errors.

[0114] Hard errors are available to notify the virtual server agents of an occurrence of an error during the performance of server change operations on the target servers. In one embodiment, the hard errors can be programmed to automatically trigger undo operations to undo any of the changes made during the execution of the server change operations. In another embodiment, the hard errors can be programmed to abort the execution of the remainder of transaction package change operations. The hard errors are triggered by error conditions set forth in the instruction set 715. These error conditions specify that if certain conditions occur, the hard errors should be sent to the target servers and their associated virtual server agents. 25

[0115] The instruction set 715 also includes prerequisite information for the instructions. An example of this prerequisite information can include, but are not limited to, the minimum set of change operation instructions that must be specified in a transaction package for its successful execution. For example, to successfully add a COM+ component on the target servers, instructions for adding the COM+ entry in the catalog, the corresponding Registry entry, and the corresponding DLL file must be specified in the transaction package. Another example of the prerequisite information can include types of permissions needed to carry out the change operations, minimum disk space required by the target servers 15, and the type of operating system required. In addition, the prerequisite information can also include implicit instructions for hierarchical server objects. 30

- 25 -

For example, to add a file in the target servers, the parent directory for the file should exist in the target servers, so that the file can be created under the specified parent directory in these servers.

[0116] In one embodiment, the instruction set 715 defines the changes that need to be made on the server objects by using named parameters, and later replacing the parameters with actual values  
5 obtained from a parameter file 710. The virtual server agents 35 receive the transaction package 700 on behalf of their associated target servers 15, and replace the named parameters with values obtained from the parameter file 710. These named parameters are particularly useful when performing server change operations on server objects that are directed to multiple target servers 15, because the named parameter representing the identity of each target server can be replaced with the  
10 actual server identifiers by the virtual server agents 35. For example, named parameters of an instruction can reference a path name for a target server 15 that includes a host name or an IP address of the target server 15. These parameters are replaced with actual server identifiers for each target server 15, as provided in the parameter file(s) 710.

[0117] In one embodiment, the parameter file 710 can be either a global parameter file or a host-  
15 specific parameter file. A global parameter file contains parameters that are configured by the user 10, thus the identical global parameter file is passed to all target servers 15. A host specific parameter file contains parameters that are specific to each of target servers 15, thus the host specific parameter file is different for each of target servers 15. Parameter values contained in the global parameter file are useful when copying the same server object to the same destination on  
20 multiple target servers 15. Examples of this type of parameter are the user's name and password. For parameter values contained in the host-specific parameter file, the parameter values are resolved by each of the target servers 15. Examples of these parameters are host names, and path names of the target servers 15. In addition, there are intrinsic parameters that are resolved through host environment variables on the target server. In one embodiment, one or more parameter files 710  
25 are associated with one or more target servers. For example, for a Window-based target server, "windir" and IP address are examples of host environment variables that can be used to resolve intrinsic parameters associated with one or more target servers and passed via the transaction package 700.

[0118] Referring to FIGS. 1 and 7, in one embodiment, instead of using abstract system calls to  
30 carry out server change operations generated by the application programs 25, a transaction package 700 can be used to carry out these change operations using an XML-based instruction set 715. To accommodate both system call level commands and XML-based instruction sets, each virtual server agent 35 is divided into two parts. One part of the virtual server agent 35 is an XML API that can interpret the XML-based instruction set 715 contained in the transaction package 700, and the other

- 26 -

part of the virtual server agent 35 is a system call API that can interpret abstract system calls. Thus, when a virtual server agent 35 receives an XML-based transaction package 700 through the virtual server client 30, the XML-based instruction set 715 in the transaction package 700 can be interpreted via the XML API. In an alternative embodiment, the transaction package 700 can be implemented with a text-based instruction set 715. The commands of the text-based instruction set 715 are translated into abstract system calls that are in turn interpreted by the system call API.

[0119] Below is an example of an XML-based transaction package, named "Package\_1.XML," specifying a prerequisite, transaction context, compound server object, sequence, and error handling information using an XML-based instruction set 715.

10 Package\_1.XML

```
<blpackage schema-version="2.0" created-date="02/12/03" modified-  
date="02/22/02" revision="23">
```

```
<name>
```

15 name of the blpackage

```
</name>
```

```
<description>
```

```
description of the package
```

20 </description>

```
<source type="host">web-demo1</source>
```

```
<!-- default parameters -->
```

25 <param name="\$APP\_PATH"> c:\program files\app </param>

```
<param-file>foo.params</param-file>
```

```
<applies-to>
```

```
<condition>
```

30 <os>"\$(os) = Windows"</os>

```
<os-version>$(os-version) > 5</os-version>
```

```
<service-pack>2</service-pack>
```

```
</condition>
```

```
</applies-to>
```

35

```
<!-- requires the following items before we deploy this package -->
```

```
<depends>
```

```
<condition>
```

- 27 -

```

    <application>SQL server</application>
    <version>$(version) = 8.0 </version>
  </condition>
</depends>
5
<!-- failure conditions if the following exit on target -->
<FailIf>
  <ErrorLevel <4
    />
10 </FailIf >

<transaction id="0">
  <command id = "1005" undo="net start w3svc">net stop w3svc</command>
  <service action="add" refid="1003" key="RSCDsvc">
15   <depends>
     <file refid="1002"/>
   </depends>
  </service>
  <command id = "1006" undo="net stop w3svc">net start w3svc </command>
20 <file action="add" key="%WINDIR%ado.dll" refid="1001"/>
  <file action="add" key="%WINDIR%/System32/svchost.exe" refid="1002" />

  <assets>
    <file id="1001">
25     <name>ado.dll</name>
     <source>0</source>
     <attributes>2</attributes>
     <created-date>02/12/03</created-date>
     <modified-date>02/22/03</modified-date>
30     <owner></owner>
     <group>0</group>

    <acl key="%WINDIR%ado.dll" owner="BUILTIN\Administrators">
      <ace action="add" id="1313">web admins</ace>
35     <acemode>0</acemode>
     <aceflags>3</aceflags>
     <acemask>1179817</acemask>

     <ace action="add" id="1314">dbas</ace>
40     <acemode>1</acemode>
```

- 28 -

```

    <aceflags>3</aceflags>
    <acemask>2032127</acemask>

    </acl>
5    </file>

    <file id="1002">
        <name>svchost.exe</name>
        <source>0</source>
10    <attributes>2</attributes>
        <created-date>02/12/03</created-date>
        <modified-date>02/22/03</modified-date>
        <owner></owner>
        <group>0</group>
15
        <acl key="%WINDIR%ado.dll" owner="BUILTIN\Administrators">
            <ace action="add" id="1313">web admins</ace>
            <acemode>0</acemode>
            <aceflags>3</aceflags>
20    <acemask>1179817</acemask>

            <ace action="add" id="1314">dbas</ace>
            <acemode>1</acemode>
            <aceflags>3</aceflags>
25    <acemask>2032127</acemask>

        </acl>
    </file>
30
    <service id="1003" name="RSCDsvc">
        <binary_path>%WINDIR%/System32/svchost.exe</binary_path>
        <name>RSCDsvc</name>
        <description></description>
        <state>Stopped</state>
35    <runas>
            <userid>$Token1</userid>
            <pwd>$Token2</pwd>
        </runas>
    </service>
40
```

```

    </assets>
</transaction>
</blpackage>

```

5

The Parameter file *foo.params* contains

10       **\$TOKEN1** as a parameter that corresponds to user id – “R2D2\web-admins”  
       **\$TOKEN2** as a parameter to password for R2D2\web-admins – “c3-po”

[0120] In this example, the <blpackage schema> tag denotes the beginning of the instruction set 715. The <name>, <description> and <source type> tags respectively provide the package name, description, and source server, in this example “web-demo1,” server, from where the package was  
 15       created. The <param> tag is use to specify location, in this example “c:\program files\app”, of parameters having the name of “\$APP\_PATH” within the package 700, while <param-file> tag is used to specify an external parameter file 710 called “foo.params”. In the prerequisite section, which is introduced with the <applies-to> tag, the MS Windows operating system, version greater than 5 and with service pack 2, is specified as a prerequisite to carry out this instruction set. Also in  
 20       the prerequisite section, the <depends> tag, indicates that SQL Server, version 8, is a pre-requisite for the package. The error handling information, which is introduced with the <FailIF> tag, specifies that the server operations should fail if error level falls below 4.

[0121] The <transaction id=“0”> tag introduces the set of change operations requested, and any dependency information for the specified server change operations. The execution sequence  
 25       information for the server change operations is provided under the <depends> tag. In this example, the order of the operations, -stop w3svc, add service RSCDsvc, start w3svc, add file ado.dll, and add file svchost. exe, would occur in the following order: stop w3svc, add file svchost.exe, add service RSCDsvc, start w3svc, and add file ado.dll.

[0122] The server assets that are being affected by the server change operations are specified under  
 30       the <assets> tag. This example has three assets – two files, id=1001 and id=1002, and one service, id=1003. Each file has a corresponding nested File ACL having the <acl key> tags.

[0123] The parameter file 710, “foo.params” has two parameters that are used in the transaction package 700, named as “\$TOKEN1” and “\$TOKEN2”. Instead of passing physical values directed to each target server, the named parameters are sent, and are resolved by the parameter file 710

- 30 -

when the parameter file 710 substitutes the actual values that are specific for each target servers 15 for the named parameters. As shown in this example, these values can be a path for a collection of server objects (e.g., files), a user name, or a password. In this example, the first parameter, \$TOKEN1, corresponds to the user name "R2D2\web-admins", and the parameter \$TOKEN 2  
5 corresponds to the password "c3-po."

[0124] In one embodiment, multiple transaction packages can be aggregated into a transaction project 725. The transaction project 725 coordinates the transaction packages 700 and their server change operations, so that each server change operation can be executed in a transaction safe manner. Below is an example of an XML transaction project 725 containing a transaction package  
10 named "BLPkg\_web.XML," directed to six web servers, a transaction package named "BLPkg\_app.XML," directed to two application servers, and a transaction package named "BLPkg\_db.XML," directed to two database servers:

```
<PROJECT>
```

```
  <BLPkg>
```

```
15   <Name>BLPkg_web.XML</Name>
```

```
     <Hosts>Web Server1</Hosts>
```

```
     <Hosts>Web Server2</Hosts>
```

```
     <Hosts>Web Server3</Hosts>
```

```
     <Hosts>Web Server4</Hosts>
```

```
20   <Hosts>Web Server5</Hosts>
```

```
     <Hosts>Web Server6</Hosts>
```

```
  </BLPkg>
```

```
  <BLPkg>
```

```
25   <Name>BLPkg_app.XML</Name>
```

```
     <Hosts>App Server1</Hosts>
```

```
     <Hosts>App Server2</Hosts>
```

```
  </BLPkg>
```

```
30   <BLPkg>
```

```
     <Name>BLPkg_db.XML</Name>
```

```
     <Hosts>Db Server1</Hosts>
```

```
     <Hosts>Db Server2</Hosts>
```

```
  </BLPkg>
```

</PROJECT>

5 [0125] In this example, first, the package “BLPkg\_web.XML” is to be executed on six web servers named Web Server1 through Web Server6, the package “BLPkg\_app.XML” is to be executed on two application servers, and the package “BLPkg\_db.XML” is to be executed on two database servers.

10 [0126] The configuration manager 25B, or any of the application programs 25, prepares the transaction package 700 and instructs the virtual server client 30 to pass the package 700 to the virtual server agents 35 associated with the target servers. After receiving the transaction package 700, the virtual server agents 35 unpack the package 700 and execute the operations on their associated target servers 15. A method for achieving this is shown in FIG. 8

15 [0127] In Step 800, Configuration manager 25B checks the prerequisite information of the requested change operations. Examples of the prerequisite information include checks related to integrity and completeness of package such as prompting for user name and password if required, making sure simple dependencies are resolved, and making sure the corresponding files are in the package.

20 [0128] After the prerequisites are checked in step 800, in step 810, the configuration manager 25B checks for the sequence information setting forth the execution order of the requested change operations in the package’s instruction set 715. If the sequence information is not provided in the instruction set 715, the configuration manager 25B accesses the external dependency graph 720 to obtain the sequence information. After completion of step 810, in step 815, the configuration manager 25B transfers the package 700 and the associated files and parameter files to the virtual server agents 35 via the virtual server client 30.

25 [0129] In one embodiment, the virtual server agent 35 receives the completed transaction package 700 via the virtual server client 30. On the virtual server agent 35, in step 820, the named parameters are substituted with actual values. The virtual server agent 35 then executes the server change operations specified in the transaction package for its associated target server 15. In another embodiment, instead of transporting the completed transaction package 700, the virtual server client  
30 30 may transport only the parameter file 710 and the instruction set 715, without the actual files or any of the server objects, to the virtual server agent 35, in case the user 10 optionally elects to proceed with a dry run. The dry run provides an additional set of tests to see if the instruction set 715 can be carried out by the recipient virtual server agent 35 before making any changes on the target server 15. After the virtual server agent 35 receives a partial transaction package 700 from the



virtual server client 30, in step 820, the parameters are substituted with actual values as provided in the parameter file 710. After completing the dry run, the configuration manager 25B can transfer the entire package 700 to the virtual server agents 35 via the virtual server client 30 for actual execution.

5 [0130] Before executing the operations on each target server 15, in step 835, the agent updates an undo log. The undo log, which is maintained for each target server, records the executed operations, and tracks the changes made by these operations, so that if an error occurs while executing the servers change operations, the operations can be undone as recorded in the undo log. This can be achieved by tracing back the steps performed during the server change operations using  
10 the undo log records. In one embodiment, the undo log is identical in structure to the transaction package, but with the parameter files arranged in reverse order and the change operations recorded in reverse order. Finally in step 840, the server change operations are executed on the target servers 15.

[0131] Referring now to FIG. 9, a method for executing and undoing server change operation in a  
15 transaction safe manner is described. In step 900, one or more application programs 25 generate and specify change operations using a transaction package 700. Different types of server objects and corresponding target servers 15 are supported through the instruction set provided in the transaction package 700. Next, in step 910, the application program specifies the target server(s) to which the server change operations are directed. In step 920, the application program specifies the  
20 parameter file that provides parameters and their corresponding values defined for each of the target servers, and places this information in the transaction package 700. In step 930, the server client 30 sends the server change operation from the application program 25 to the virtual server agents 35 on the target servers 15. In step 940, the target servers 15 execute the server change operations in a transaction-safe manner.

#### 25 Configuration Manager

[0132] Referring now to FIG. 10, the configuration manager 25B is an exemplary application  
program 25 that tracks changes and compliance and configures target servers by generating and deploying a transaction package 700. The configuration manager 25B provides a method and system for configuring different servers using a variety of software modules, such as a browser 1000,  
30 a template 1010, a recorder 1020, a reference model 1030, a comparator 1040, and a corrector 1050.

[0133] The browser 1000 browses server objects in different servers in real time, to examine the current configuration of the server objects contained inside of the servers 15. First, the user selects a server he/she wishes to browse. Through browsing, a collection of server object identifiers that identify each server object are selected and entered into the template 1010. Alternatively, instead of

- 33 -

building the template 1010 from browsing, the template 1010 may be imported from an external vendor. The template 1010 may also be created by including one or more previously defined templates. In one embodiment, the template 1010 is an abstract template that identifies server objects contained in a server. For example, if an Apache server contains files, and configuration file entries, an Apache server template 1010 contains identifiers that are sufficient to identify the files and configuration file entries of the Apache server. After identifying server objects on the template 1010, values of these identified server objects are recorded to configure servers on the network.

[0134] In one embodiment, the recorder 1020 takes a snapshot of values (e.g., attributes) associated with a collection of server objects. In another embodiment the recorder 1020 takes a snapshot of values of the server objects identified in the template 1010. The values may come from any of the servers browsed by the browser. Alternatively, the values may come from a selected server, also referred to as a gold server. Examples of the values (or attributes) of files recorded in the snapshots include, but are not limited to, file names, sizes, permissions, owners, creation dates, modification dates, and versions. Examples of directory attributes (or values) recorded in snapshots are directory locations, permissions, creation dates, and modification dates. Examples of registry entry attributes recorded in snapshots are field names, and corresponding values.

[0135] In one embodiment, the recorded values or snapshot results of the gold server are used to derive baseline values and compliance ranges in the reference model 1030. In another embodiment, instead of creating the reference model, the snapshot results can be directly used to track changes, configure existing servers and provision new servers on the network. Snapshot results record a configuration of a server at a point in time, thus they cannot be changed. However, the reference model 1030 can be edited to represent the reference implementation for compliance or provisioning purposes.

[0136] For example, when the snapshots of the gold server are taken by the recorder 1020, the values collected in the snapshots are saved in the reference model 1030. Based on the values of the gold server, the reference model 1030 can provide information, such as baseline values and compliance ranges, for use by other servers in the network to identify their drift in comparison to the gold server. The baseline values provide basis for configuration of other servers. The compliance ranges are ranges of acceptable configuration values that are acceptable for other servers for these servers to be in compliance. Alternative to creating a reference model 1030, the reference model 1030 may be an imported reference model that was created by an external vendor. Also, the reference model 1030 may include one or more previously defined reference models. Subsequently, the comparator 1040 compares a server to the reference model 1030 to track changes and track compliance in the server.

[0137] In another example, a snapshot of a current configuration of a server captured at an arbitrary point in time can be compared against a live-version of the captured server to track changes in the captured server. The configuration of a server can include explicitly selected server objects that are on the server or implicitly selected server objects provided through the template 1010.

5 [0138] In yet another example, the snapshot results of recurring snapshots of a server taken at scheduled time intervals (e.g., daily, weekly, etc.) can be used to track changes in the captured server. In this example, the first snapshot of the server serves as a baseline, so that for subsequent snapshots, only the changes against the baseline are saved in the snapshot results. Thus, any snapshot result taken during these time intervals can be reconstructed to view its entire  
10 configuration and content by combining the baseline with the incremental changes saved in the snapshot result. Moreover, the incremental changes show changes occurred in the configuration of the server over a period of time for the user to analyze the changes of this particular server. Subsequently, the comparator 1040 compares a live-version of the server to the baseline snapshot to track and save only changes on the server.

15 [0139] In one embodiment, two live servers can be compared against each other without the snapshots or the reference model 1030, on an ad-hoc basis. In this embodiment, the user 10 may explicitly select server objects that are commonly shared between the two live servers so that the comparator 1040 can compare the values of the sever objects between these servers. In another example of this embodiment, the comparator 1040 compares the values of the server objects that  
20 are implicitly provided by the template 1010.

[0140] After comparing the servers and identifying the discrepancies present in the compared servers, the corrector 1050 corrects the discrepancies in each target server. The corrector 1050 examines the discrepancies and generates server change operations that request services from the operating systems running on the target servers to correct these discrepancies. As described  
25 previously, server change operations can be presented to the servers as a transaction package 700 to remove discrepancies and synchronize the target servers to the reference model 1030 in a transaction-safe manner. Similarly, in one embodiment, configuration updates to the target servers can be made by the transaction package 700. In particular, the configuration manager 25B first makes all the updates to the reference model 1030, which then packages the discrepancies  
30 (introduced in the reference model) as updates in the transaction package 700. The transaction package 700 is propagated to the target servers to synchronize them to the updated reference model 1030.

[0141] The reference model 1030 can also be used to provision a new server to ensure consistency in the configuration of the servers in the network when a new server is added. For example, an

- 35 -

Apache reference model 1030 can be used to provision a new Apache server so that the configuration of all Apache servers in the network are consistent with each other.

[0142] In addition, both the reference model 1030 and snapshots can be used restore a previous configuration of a server in case of a disaster recovery. In particular, in case of a server failure, this server can recover its most recent configuration and contents by reconstructing the server's configuration from the snapshots taken over a period of time. With the reference model 1030, in case of a server failure, the server can look to the basis values of the gold server in the reference model 1030 and synchronize to this configuration to be in compliance again.

[0143] FIG. 11 shows an exemplary method of tracking changes and compliance, and correcting component as well as parameter-level changes across multiple servers. In step 1100, the configuration manager 25B browses servers in the network to obtain server asset and configuration (together referred to as server objects) status information for each server. In the browsing step 1100, selected server objects and their dependent server objects are browsed in real time. In one embodiment, live servers in the network and their stored server objects can be browsed via a Graphic User Interface (GUI) which presents the servers and server objects hierarchically.

[0144] Next, in step 1105, the configuration manager 25B, selects identifiers of the browsed server objects to be in the template 1010. The identifiers can include any information about the server object that is sufficient to identify the server object. Next in step 1110, the configuration manager selects a gold server, to provide a baseline configuration and configuration ranges for other servers in the network. In step 1115 snapshots of the values of the server objects identified in the template that are present in the gold server are recorded in the reference model 1030. Based on the values recorded in the reference model 1030, in step 1115, the reference model establishes compliance rules, such as the baseline configuration and the compliance ranges. Alternatively, the snapshots of the values are not recorded in the reference model. Instead, the snapshot results of a server can be used to directly compare against a live-version of this server to track changes.

[0145] In step 1120, the configuration manager 25B selects servers and their respective configuration parameters (also referred to as server objects) to compare against the reference model 1030. These servers can be selected from any live servers on the network. Alternatively, these live-version servers can also be directly compared against their own snapshots, taken at an arbitrary point in a time, or taken over a specific period, without the reference model 1030, to track compliance and changes in these servers. The results of the comparing step 1125 can be viewed item-by-item, by showing which software (or server objects) are installed or not installed, or host-by-host, by showing each server and the server objects present on the server.

- 36 -

[0146] Finally, based on the discrepancies obtained during the comparing step 1120, a correcting step 1130 fixes the servers to be in compliance by synchronizing configuration of these servers with the reference model 1030 or the snapshots. Moreover, a newly added servers can be provisioned to be consistent with other servers by synchronizing this new server to the reference model 1030.

5 [0147] Referring to FIG. 12, in one embodiment, the configuration manager 25B can manage the same type of configuration parameters (also referred to as server objects) across different servers by specifying one or more categories for the parameters in templates. The template 1200 first specifies the "server-type" category (e.g., application server category 1210, web server category 1215, and database server category 1220) to specify to what type of server each server object in the network  
10 belongs, and then specifies the "parameter-type" category (e.g., network parameters, capacity parameters, availability parameters, performance parameters, security parameters) to specify the parameter type to which each server object belongs. Each server object in the template 1200 can be classified under one or more categories, sub-categories and keywords. In one example, for security parameters, sub-categories can include encryption type and authentication type, and keywords can  
15 include "read-only" and constant.

[0148] Referring briefly to FIG. 13, an example of the system described with reference to FIG. 12 is shown. In this example, Internet 1300 and intranet 1305 are available to different categories of servers 1215, 1210, 1220 through firewalls 1310. Web server category 1215 include an IIS server 1215A for intranet services and Apache Servers 1215B, 1215C for the HTTP/FTP and  
20 Wireless/Video Internet services respectively. Application server category 1210 include servers running sales applications 1210A, on-line brokerage applications 1210B, and customer service application 1210C. Database server category 1220 include sales, trading, and account databases 1220A, 1220B, and 1220C.

[0149] Referring again to FIG. 12, each server object in the template 1200 is placed into a  
25 parameter category based on its function and server type. For example, the server objects may be grouped into network parameters 1330, capacity parameters 1335, availability parameters 1340, performance parameters 1345, and security parameters 1350. The configuration manager 25B selects categorically related server objects from each category of servers and stores them in the template 1200. For example, all the security parameters in the application server category 1210 and  
30 all the network parameters in the application server category 1210 are stored in the template 1200.

[0150] Referring again to FIG. 13, for the web server category 1215, web server configuration parameters a, b, c, d, e are respectively categorized as network parameters 1330, capacity parameters 1335, availability parameters 1340, performance parameters 1345, and security parameters 1350. For the application server category 1210, application server configuration parameters i, ii, iii, iv, v are

- 37 -

respectively categorized as network parameters 1330, capacity parameters 1335, availability parameters 1340, performance parameters 1345, and security parameters 1350. Similarly, for the database server category 1220, database server configuration parameters I, II, III, IV, V are respectively categorized as network parameters 1330, capacity parameters 1335, availability parameters 1340, performance parameters 1345, and security parameters 1350.

**[0151]** After categorizing all the server objects in the template 1200 by the server-type categories and the parameter-type categories, a new template can be derived from the template 1200 to isolate the categorically related server objects across the server categories and manage the configuration parameters as if they belonged to a single server. For example, security configuration parameters of an individual web server can be changed in concert with other security configuration parameters for other web servers, as well as for application servers and database servers. In the example shown in FIG. 13, for instance, web server network parameter a can be changed in concert with network parameters i of the application server category 1210 and parameter I of the database server category 1220. Similarly, Web server capacity parameter b can be changed in concert with other capacity parameters ii of the application server category 1210 and II of the database server category 1220. Likewise, correlated changes of parameters can be performed for the availability parameters 1346, the performance parameters 1345, and the security parameters 1350.

**[0152]** Referring to FIG. 14, an exemplary screenshot of a GUI-based configuration manager 25B includes a module referred to as an asset browser 1400, which allows a user 10 to browse live remote target servers 15, and to manage and store frequently used server assets (also referred to as server objects). The asset browser 1400 is divided into two panes. The left pane 1410 functions as either a Servers pane or a Depots pane, depending on a tab 1420 selected by the user 10. The Contents pane 1430 on the right side displays the contents of an item selected in the Servers or the Depots pane.

**[0153]** In FIG. 14, the left pane 1410 displays the Servers pane which shows a hierarchical depiction of the servers that the user 10 manages. For example, the user 10 may arrange the servers into groups based on geographical location and/or operating system. Server groups are divided into the eastern and western divisions of an enterprise, and within those groups, another level of hierarchy for Windows, UNIX, and Linux-based servers. More specifically in FIG. 14, within the servers in the Easter Division 1440, the patches object 1460 in the sun 2 server 1450 is selected. The Contents pane 1430 shows the contents of the patches object 1460.

**[0154]** The Depots pane (not shown) can display central repositories of commonly accessed server objects (e.g., all files, software to be deployed, and pointers to the content of the files and software

residing in other servers in the network). In additions, the Depots pane stores scheduled tasks to be performed, snapshots of server objects, Shell scripts, and transaction packages 700.

Example

- 5 [0155] In an overall example of operation of the configuration manage, the configuration manager browses live servers on a network, tracks changes and compliance in the servers by comparing their server objects against a reference model or a snapshot, and identifying any discrepancies from the reference model or the snapshot. By making records of the values of the gold server's server objects through a snapshot and saving the results as a reference model, the reference model may be used to audit other servers, to determine how configurations of the other servers have changed from the reference model. Alternatively, a server's own snapshot can be taken arbitrarily, or over a specific period of time to track changes in the server, without using the reference model. In one example, the server objects being compared in the audit process are provided automatically by the configuration manager via templates. In another example, the user may manually select the server objects to compare. Additionally, the audit process can be scheduled to track compliance over time.
- 10 [0156] After identifying server configuration discrepancies present in the servers, the configuration manager 25B corrects the discrepancies by generating a transaction package 700, that contains server change operations to be performed on the servers 15. The transaction package 700 bundles configuration changes operations and corresponding instructions to be deployed on remote target servers 15 to correct any discrepancies that exist in server objects contained in those servers 15.
- 20 With the transaction package 700, the configuration manager 25B can install any types of server objects from a single source to multiple locations. Similarly, the configuration manger 25B can uninstall software, and undo server object deployments on the remote target servers 15. As discussed previously, certain values inside the transaction package 700 can be parameterized and subsequently replaced with real values during the deployment of the transaction package 700 on the target servers 15, without changing the contents of the transaction package 700 for each target server 15.
- 25 [0157] In one particular example, the configuration manager 25B can be used to move a working MS SQL server database from a gold server to multiple target servers 15, to duplicate the changes made in this database to multiple servers. To achieve this duplication, the user 10 copies the changes made on the SQL Server database to the reference model, so that the configuration manager 25B can later bundle these changes to other instances of the same SQL Server database in the remote target servers 15. The reference model and the remote target servers 15 have the same initial installation of the SQL Server database. The configuration manager takes a snapshot of the gold server to create a reference model that is used as a baseline to compare the SQL Server
- 30

- 39 -

databases between the gold server and the target servers 15. The necessary database changes are first made to the gold server. Next, the configuration manager 25B creates a transaction package 700 to bundle these changes to be deployed on the target servers 15. The configuration manager 25B deploys the transaction package 700 to the virtual server agents 35 associated with the target servers 15 to request these changes to be made on their SQL Server databases.

**[0158]** In some embodiments, the functionality of the systems and methods described above may be implemented as software on one or more general purpose computers. In such an embodiment, the software may be written in any one of a number of high-level languages, such as FORTRAN, PASCAL, C, C++, LISP, JAVA, or BASIC. Further, the software may be written in a script, macro, or functionality embedded in commercially available software, such as EXCEL or VISUAL BASIC. Additionally, the software could be implemented in an assembly language directed to a microprocessor resident on a computer. For example, the software could be implemented in Intel 80x86 assembly language if it were configured to run on an IBM PC or PC clone. The software may be embedded on an article of manufacture including, but not limited to, a “computer-readable medium” such as a floppy disk, a hard disk, an optical disk, a magnetic tape, a PROM, an EPROM, or CD-ROM.

**[0159]** Variations, modifications, and other implementations of what is described herein will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

**[0160]** What is claimed is:



- 40 -

CLAIMS

- 1 1. A method for receiving and executing a system call from a software application program on  
2 one of a plurality of servers, the method comprising the steps of:
  - 3 (a) providing a representation of a plurality of servers as a single virtual server, the  
4 representation of the single virtual server implemented by a virtual server client and a  
5 plurality of virtual server agents each running on a respective one of the plurality of  
6 servers;
  - 7 (b) receiving, by the virtual server client, an abstract system call from a software  
8 application program; and
  - 9 (c) instantiating in a thread-safe manner the abstract system call by:  
10 identifying, by the virtual server client, a target server to receive the abstract system  
11 call, and identifying a corresponding virtual server agent associated with the target server;  
12 transmitting the abstract system call to the identified agent for execution on the  
13 target server; and  
14 receiving execution results from the agent.
- 1 2. The method of claim 1, wherein at least two of the plurality of servers have different  
2 operating systems.
- 1 3. The method of claim 1 further comprising the step of aggregating at least the abstract system  
2 call and a second abstract system call into a high-level abstract system call.
- 1 4. The method of claim 3 further comprising the steps of
  - 2 (i) receiving, by the virtual server client, the high-level abstract system call;
  - 3 (ii) disintegrating, by the virtual server client, the high-level abstract system call into the  
4 at least the abstract system call and the second abstract system call; and
  - 5 (iii) instantiating in a thread-safe manner each of the at least the abstract system call and  
6 the second abstract system call.
- 1 5. The method of claim 3 further comprising the steps of:
  - 2 (i) receiving, by the virtual server client, the high-level abstract system call; and
  - 3 (ii) instantiating in a thread-safe manner the high-level abstract system call.
- 1 6. The method of claim 1, wherein the instantiating step (c), the virtual server client is  
2 implemented by a network-aware code library.
- 1 7. The method of claim 6, wherein the network-aware code library is a libnc.
- 1 8. The method of claim 6, wherein the virtual server client is a libnc.

- 41 -

- 1 9. The method of claim 1, wherein the identifying step comprises identifying the target virtual  
2 server agent to receive the abstract system call in response to a server identifier included in the  
3 abstract system call.
- 1 10. The method of claim 9, wherein the server identifier comprises a host name specified in a  
2 path.
- 1 11. The method of claim 9, wherein the server identifier comprises a network address.
- 1 12. The method of claim 11, wherein the server identifier is inferred from a group of servers the  
2 target server belongs.
- 1 13. The method of claim 1, further comprising after the transmitting step, the steps of:  
2 (i) translating, by the virtual server agent, the abstract system call into an operating  
3 system specific system call to be executed by the target server; and  
4 (ii) executing, by the target server, the operating system specific system call in a thread-safe  
5 manner.
- 1 14. The method of claim 1 further comprising:  
2 before the transmitting step, specifying at least one of priority, CPU utilization, and memory  
3 utilization of the abstract system call on the target servers associated with the identified virtual server  
4 agents.
- 1 15. The method of claim 1 further comprising:  
2 (i) authenticating a user of the software application program and a management system  
3 operating the software application program;  
4 (ii) after the instantiating step (c), encrypting, by the virtual server client, the abstract  
5 system call;  
6 (iii) identifying, by the virtual server agent, the management system and the user;  
7 (iv) decrypting, by the virtual server agent, the encrypted abstract system call;  
8 (v) mapping the identified user to an associated local user of the target server;  
9 (vi) impersonating the identified user as the mapped local user on the target server;  
10 (vii) authorizing the decrypted abstract system call for the mapped local user based on at  
11 least one of role-based access control model and access control lists; and  
12 (vi) maintaining an audit log to record the name of the user and the abstract system call executed  
13 on the target server.
- 1 16. The method of claim 15, wherein the authenticating step (i) is performed substantially in  
2 accordance with a public key protocol.
- 1 17. The method of claim 15, wherein the authenticating step and the encrypting step are  
2 performed substantially in accordance with Kerberos protocol.

- 42 -

- 1 18. The method of claim 15, wherein the authenticating step and the encrypting step are  
2 performed substantially in accordance with Shared Secret protocol.
- 1 19. The method of claim 1 further comprising:  
2 modifying an existing non-distributed application to function as a network-aware application  
3 by substituting a non network-aware system call with the abstract system call.
- 1 20. The method of claim 19, wherein the modifying step comprises modifying a non-distributed  
2 Unix shell to function as the network-aware application program.
- 1 21. The method of claim 19, wherein the modifying step comprises modifying a non-distributed  
2 scripting language to function as the network aware-application program.
- 1 22. The method of claim 21, wherein the non-distributed scripting language comprises Perl.
- 1 23. The method of claim 21, wherein the non-distributed scripting language comprises Python.
- 1 24. The method of claim 1, wherein the software application program comprises a configuration  
2 manager.
- 1 25. A virtual server, having a virtual server client and a virtual server agent, for representing a  
2 plurality of servers as an abstract model, wherein the virtual server comprises,  
3 (a) a virtual server client receiver for receiving an abstract system call from a  
4 software application program;  
5 (b) a virtual server client instantiator, in communication with the virtual server  
6 client receiver, for instantiating the abstract system call in a thread-safe  
7 manner;  
8 (c) a virtual server client transmitter, in communication with the virtual server  
9 client instantiator, for transmitting the abstract system call;  
10 (d) a virtual server agent receiver for receiving the abstract system call from the  
11 virtual server client transmitter;  
12 (e) a virtual server agent translator for translating the abstract system call to an  
13 operating system specific system call; and  
14 (f) a target server executor for executing the operating system specific system  
15 call on a target server associated with the virtual server agent in a thread-safe  
16 manner.
- 1 26. The virtual server of claim 25, wherein at least two of the plurality of servers have different  
2 operating systems.
- 1 27. The virtual server of claim 25 further comprising an aggregator for aggregating at least the  
2 abstract system call and a second abstract system call into a high-level abstract system call.
- 1 28. The virtual server of claim 27 further comprising:

- 2 (i) a virtual server client receiver for receiving the high-level abstract system call and  
3 disintegrating the high-level abstract system call into the at least the abstract system call and the  
4 second abstract system call; and
- 5 (ii) the virtual server client instantiator for instantiating in a thread-safe manner each of the at  
6 least the abstract system call and the second abstract system call.
- 1 29. The virtual server of claim 27 further comprising:
- 2 (i) a virtual server client receiver for receiving the high-level abstract system call; and  
3 (ii) the virtual server client instantiator for instantiating the high-level abstract system call in a  
4 thread-safe manner.
- 1 30. The virtual server of claim 25, wherein the virtual server client is implemented by a network-  
2 aware code library.
- 1 31. The virtual server of claim 30, wherein the network-aware code library is a libnc.
- 1 32. The virtual server of claim 30, wherein the virtual server client is a libnc.
- 1 33. The virtual server of claim 25, wherein the virtual server client instantiator identifies the  
2 target virtual server agent to receive the abstract system call in response to a server identifier  
3 included in the abstract system call.
- 1 34. The virtual server of claim 33, wherein the server identifier comprises a host name specified  
2 in a path.
- 1 35. The virtual server of claim 33, wherein the server identifier comprises a network address.
- 1 36. The virtual server of claim 35, wherein the server identifier is inferred from a group of  
2 servers the target server belongs.
- 1 37. The virtual server of claim 25, whereas the virtual server client transmitter specifies at least  
2 one of priority, CPU utilization, and memory utilization of the abstract system call on the target  
3 servers associated with the identified virtual server agents.
- 1 38. The virtual server of claim 25 further comprising:
- 2 (i) an authenticator for authenticating a user of the software application program and a  
3 management system operating the software application program;
- 4 (ii) a virtual server client encryptor for encrypting the abstract system call;
- 5 (iii) a virtual server agent identifier for identifying the management system and the user;
- 6 (iv) a virtual server agent decryptor for decrypting the encrypted abstract system call;
- 7 (v) a virtual server agent mapper for mapping the identified user to an associated local  
8 user of the target server;
- 9 (vi) a virtual server agent impersonator for impersonating the identified user as the  
10 mapped local user on the target server;

- 44 -

- 11 (vii) a virtual server agent authorizer for authorizing the decrypted abstract system call for  
12 the mapped local user based on at least one of role-based access control model and access  
13 control lists; and
- 14 (vi) an audit log for recording the name of the user and the abstract system call executed  
15 on the target server.
- 1 39. The virtual server of claim 38, wherein the virtual server client encryptor performs  
2 substantially in accordance with a public key protocol.
- 1 40. The virtual server of claim 38, wherein the authenticator and the virtual server client  
2 encryptor perform substantially in accordance with a Kerberos protocol.
- 1 41. The virtual server of claim 38, wherein the authenticator and the virtual server client  
2 encryptor perform substantially in accordance with a Shared Secret protocol.
- 1 42. The virtual server of claim 25 further modifies an existing non-distributed application to  
2 function as a network-aware application by substituting a non network-aware system call with the  
3 abstract system call.
- 1 43. The virtual server of claim 42 further modifies a non-distributed Unix shell to function as  
2 the network-aware application program.
- 1 44. The virtual server of claim 42 further modifies a non-distributed scripting language to  
2 function as the network aware-application program.
- 1 45. The virtual server of claim 44, wherein the non-distributed scripting language comprises  
2 Perl.
- 1 46. The virtual server of claim 44, wherein the non-distributed scripting language comprises  
2 Python.
- 1 47. The virtual server of claim 25, wherein the software application program comprises a  
2 configuration manager.
- 1 48. A method for securely executing a system call on a remote computer, the method  
2 comprising the steps of:
- 3 (a) receiving, by a virtual server client running on a first computer, an abstract system  
4 call from an application called by an authenticated user;
- 5 (b) instantiating in a thread-safe manner the abstract system call by:  
6 identifying, by the virtual server client, a virtual server agent running on a  
7 remote computer to receive the abstract system call;
- 8 (c) encrypting, by the virtual server client, the abstract system call;
- 9 (d) communicating the encrypted abstract system call to the virtual server agent;
- 10 (e) identifying, by the virtual server agent, the first computer and the authenticated user

- 45 -

- 11 (f) decrypting, by the virtual server agent, the encrypted abstract system call;  
12 (g) mapping the authenticated user to a local user on the remote computer;  
13 (h) impersonating the authenticated user as the local user on the remote computer;  
14 (i) authorizing the decrypted abstract system call for the local user based on at least one  
15 of role-based access control model and access control lists;  
16 (j) translating the abstract system call to an operating system specific system call; and  
17 (k) executing as the local user, by the virtual server agent, the operating system specific  
18 system call on the remote computer.

1 49. The method of claim 48 further comprising:  
2 before the receiving step (a), authenticating a user using an operating system user context  
3 inheritance model.

1 50. The method of claim 48 further comprising:  
2 before the receiving step (a), authenticating a user substantially in accordance with a public  
3 key protocol.

1 51. The method of claim 48 further comprising:  
2 before the receiving step (a), authenticating a user substantially in accordance with a  
3 Kerberos protocol.

1 52. The method of claim 48, wherein the identifying step (g), if the authenticated user is not  
2 identified as a local user in the identifying step (g), then designating the authenticated user as a local  
3 guest.

1 53. The method of claim 48, wherein the authorizing step (h) comprises authorizing the  
2 decrypted first abstract system call for the local user based on at least one of role-based access  
3 control model and access control lists substantially in accordance with Kerberos protocol.

1 54. The method of claim 48, wherein the authorizing step (h) comprises authorizing the  
2 decrypted first abstract system call for the local user based on at least one of role-based access  
3 control model and access control lists substantially in accordance with SSL protocol.

1 55. The method of claim 48 further comprising:  
2 after the executing step (i),  
3 encrypting results of the executing step (i); and  
4 returning the encrypted results to the virtual server client.

1 56. The method of claim 48, further comprising:  
2 maintaining an audit log, by the virtual server client and the identified virtual server agent,  
3 that includes names of the authenticated user and the abstract system call performed.

- 46 -

- 1 57. A virtual server for securely executing a system call on a remote computer, the virtual server  
2 comprising:
- 3 (a) a virtual server client receiver running on a first computer for receiving an abstract  
4 system call from an application called by an authenticated user;
  - 5 (b) a virtual server client instantiator, in communication with the virtual server client  
6 receiver, for instantiating the abstract system call in a thread-safe manner by  
7 identifying a virtual server agent running on a remote computer to receive the first  
8 abstract system call;
  - 9 (c) a virtual server client encryptor, in communication with the virtual server client  
10 instantiator, for encrypting the abstract system call;
  - 11 (d) a virtual server client transmitter for communicating the encrypted abstract system  
12 call to the virtual server agent;
  - 13 (e) a virtual server agent identifier, in communication with the virtual server agent  
14 decryptor, for identifying the authenticated user and the first computer;
  - 15 (f) a virtual server agent decryptor, in communication with the virtual server client  
16 transmitter, for decrypting the encrypted abstract system call;
  - 17 (g) a virtual server agent mapper, in communication with the identifier and the  
18 decryptor, for mapping the authenticated user to a local user on the remote  
19 computer;
  - 20 (h) a virtual server agent impersonator for impersonating the authenticated user as the  
21 local user on the remote computer;
  - 22 (i) a virtual server agent authorizer, in communication with the virtual server agent  
23 impersonator, for authorizing the decrypted abstract system call for the local user  
24 based on at least one of role-based access control model and access control lists;
  - 25 (j) a virtual server agent translator for translating the abstract system call to an operating  
26 system specific system call; and
  - 27 (k) a virtual server agent executor, in communication with the virtual server agent  
28 authorizer, for executing the operating system specific system call as the local user on  
29 the remote computer.
- 1 58. The virtual server of claim 57 further comprising:  
2 an authenticator for authenticating a user using an operating system user context inheritance  
3 model.
- 1 59. The virtual server of claim 58, wherein the authenticator performs substantially in  
2 accordance with a public key protocol.

- 1 60. The virtual server of claim 58, wherein the authenticator performs substantially in  
2 accordance with Kerberos protocol.
- 1 61. The virtual server of claim 57, if the authenticated user is not identified as a local user by the  
2 virtual server agent identifier, then designate the authenticated user as a local guest.
- 1 62. The virtual server of claim 57, wherein the virtual server agent authorizer performs  
2 substantially in accordance with Kerberos protocol.
- 1 63. The virtual server of claim 57, wherein the virtual server agent authorizer performs  
2 substantially in accordance with SSL protocol.
- 1 64. The virtual server of claim 57, wherein the virtual server agent executor  
2 encrypts results of the executing step (i); and  
3 returns the encrypted results to the virtual server client.
- 1 65. The virtual server of claim 57, further comprising:  
2 an audit log, maintained by the virtual server client and the identified virtual server agents,  
3 that includes names of the authenticated users and the abstract system call performed.
- 1 66. A method for executing change operations across a plurality of servers in a transaction-safe  
2 manner, the method comprising the steps of:  
3 (a) specifying change operations for a collection of server objects in a transaction  
4 package, wherein the objects comprise at least one of files and configuration file entries;  
5 (b) identifying at least one target server for execution of the change operations specified  
6 in the transaction package;  
7 (c) specifying parameter values for each of the identified target servers;  
8 (d) communicating the transaction package to the identified target servers; and  
9 (e) executing the specified change operations on each of the identified target servers in a  
10 transaction-safe manner using the parameter values.
- 1 67. The method of claim 66, wherein the server objects comprise at least one of a primitive  
2 server object, a compound server object, an abstract configuration server object, and a component  
3 server object.
- 1 68. The method of claim 67, wherein the primitive server object comprises an elemental server  
2 object.
- 1 69. The method of claim 67, wherein the compound server object comprises at least one of the  
2 primitive server objects and the compound server objects.
- 1 70. The method of claim 67, wherein the abstract configuration server object comprises an entry  
2 in a configuration file mapped to a corresponding entry in a common abstract configuration file  
3 format.



- 1 71. The method of claim 67, wherein the component server object comprises a sequenced  
2 collection of server objects.
- 1 72. The method of claim 66, wherein the specifying step (a), the transaction package comprises  
2 an XML-based instruction set.
- 1 73. The method of claim 66, wherein the specifying step (a), the transaction package comprises a  
2 text-based instruction set.
- 1 74. The method of claim 66, in addition to the specified change operations in the transaction  
2 package, the transaction package in the specifying step (a) further comprises:
- 3 (i) a transaction context;
  - 4 (ii) a parameter file comprising the parameter values specific to each of the identified  
5 target servers;
  - 6 (iii) error handling actions;
  - 7 (iv) a sequencing instruction for the specified change operations; and
  - 8 (v) prerequisite information.
- 1 75. The method of claim 74, wherein the (i) transaction context in the transaction package  
2 comprises begin-transaction and end-transaction statements that encapsulate the specified change  
3 operations.
- 1 76. The method of claim 74, wherein the (ii) parameter file comprises group-level parameter  
2 values that are identical across the identified target servers.
- 1 77. The method of claim 76, wherein the (ii) parameter file comprises the parameter values that  
2 are distinct for each of the identified target servers and override the group-level parameter values if  
3 specified.
- 1 78. The method of claim 74, wherein the (iii) error handling actions comprise soft error and a  
2 hard error.
- 1 79. The method of claim 74, wherein the (iv) sequencing instruction for the server change  
2 operations is provided locally from the transaction package.
- 1 80. The method of claim 79, wherein the (iv) sequencing instruction for the server change  
2 operations is provided from an external dependency graph, if the sequencing instruction is not  
3 provided locally from the transaction package.
- 1 81. The method of claim 74, wherein the (v) prerequisite information comprises prerequisite  
2 information for the identified target servers to execute the specified change operations.
- 1 82. The method of claim 66 further comprising the steps of:

- 49 -

2 (i) maintaining a transaction log for the transaction package, wherein the transaction log  
3 comprises details of all steps performed during execution of the change operations specified in the  
4 transaction package;

5 (ii) after a successful completion of the executing step (e), optionally reversing the  
6 executed change operations via an explicit user request; and

7 (iii) automatically reversing the executed change operations, after detecting an occurrence  
8 of an error.

1 83. The method of claim 66 further comprising the steps of optionally performing a dry-run on  
2 the transaction package.

1 84. The method of claim 66 further comprising:

2 (i) assembling a plurality of transaction packages into a transaction project; and

3 (ii) executing change operations specified in each transaction package in the transaction  
4 project in a transaction-safe manner.

1 85. A transaction package for executing change operations across a plurality of target servers in a  
2 transaction-safe manner, the transaction package comprising:

3 (a) an instruction set for specifying change operations for a plurality of server objects  
4 and identifying at least one target server for execution of the specified change operations on the  
5 identified target servers; and

6 (b) a parameter file, in communication with the instruction set, for comprising  
7 parameter values specific to each of the identified target servers.

1 86. The transaction package of claim 85, wherein the (b) parameter file comprises group-level  
2 parameter values that are identical across the identified target servers.

1 87. The transaction package of claim 86, wherein the (b) parameter file comprises the parameter  
2 values that are distinct for each of the identified target servers and override the group-level  
3 parameter values if specified.

1 88. The transaction package of claim 85, wherein the server objects comprise at least one of a  
2 primitive server object, a compound server object, an abstract configuration server object, and a  
3 component server object.

1 89. The transaction package of claim 88, wherein the primitive server object comprises an  
2 elemental server object.

1 90. The transaction package of claim 88, wherein the compound server object comprises at least  
2 one of the primitive server objects and the compound server objects.

- 50 -

- 1 91. The transaction package of claim 88, wherein the abstract configuration server object  
2 comprises an entry in a configuration file mapped to a corresponding entry in a common abstract  
3 configuration file format.
- 1 92. The transaction package of claim 88, wherein the component server object comprises a  
2 sequenced collection of server objects.
- 1 93. The transaction package of claim 85, wherein the instruction set is an XML-based  
2 instruction set.
- 1 94. The transaction package of claim 85, wherein the instruction set is a text-based instruction  
2 set.
- 1 95. The transaction package of claim 85, in addition to the specified change operations in the  
2 instruction set, the instruction set further comprises:
- 3 (i) a transaction context;  
4 (ii) error handling actions;  
5 (iii) a sequencing instruction for the specified change operations; and  
6 (iv) prerequisite information.
- 1 96. The transaction package of claim 95, wherein the (i) transaction context comprises begin-  
2 transaction and end-transaction statements that encapsulate the specified change operations.
- 1 97. The transaction package of claim 95, wherein the (ii) error handling actions comprise a soft  
2 error and a hard error.
- 1 98. The transaction package of claim 95, wherein the (iii) sequencing instruction for the server  
2 change operations is provided locally from instruction set.
- 1 99. The transaction package of claim 98, wherein the (iii) sequencing instruction for the server  
2 change operations is provided from an external dependency graph, if the sequencing instruction is  
3 not provided locally from the instruction set.
- 1 100. The transaction package of claim 95, wherein the (iv) prerequisite information comprises  
2 prerequisite information for the identified target servers to execute the specified change operations.
- 1 101. The transaction package of claim 85, wherein a dry-run is optionally performed on the  
2 transaction package.
- 1 102. The transaction package of claim 85, wherein the transaction package and a second  
2 transaction package is assembled into a transaction project to execute the change operations  
3 specified in each transaction package in a transaction-safe manner.
- 1 103. The transaction package of claim 85, wherein the transaction package maintains:
- 2 (i) a transaction log comprising details of all steps performed during execution of the  
3 change operations specified in the transaction package;

- 51 -

4 (ii) after a successful completion of at least one of the change operations, an explicit  
5 user request for optionally reversing the executed change operations using the details provided from  
6 the transaction log; and

7 (iii) an error signal for automatically reversing the executed change operations using the  
8 details provided from the transaction log.

1 104. A method for configuring a plurality of heterogeneous servers across a network, the method  
2 comprising:

3 (a) browsing server objects in each of a plurality of servers across a network;

4 (b) selecting identifiers of at least one browsed server objects to create a template;

5 (c) selecting a gold server from the plurality of servers;

6 (d) recording values of the server object identifiers selected in a template from the gold server to  
7 create a reference model;

8 (e) comparing a second server from the plurality of servers to the reference model; and

9 (f) correcting discrepancies of the second server against the reference model.

1 105. The method of claim 104, wherein the server objects in the browsing step (a) comprise at  
2 least one of files and configuration file entries.

1 106. The method of claim 105, wherein the server objects in the browsing step (a) comprise at  
2 least one of a primitive server object, a compound server object, an abstract configuration server  
3 object, and a component server objects.

1 107. The method of claim 106, wherein the primitive server object comprises an elemental server  
2 object.

1 108. The method of claim 106, wherein the compound server object comprises at least one of the  
2 primitive server objects, the abstract configuration server objects, the component server objects and  
3 the compound server objects.

1 109. The method of claim 106, wherein the abstract configuration server object comprises an  
2 entry in a configuration file mapped to a corresponding entry in a common abstract configuration  
3 file format.

1 110. The method of claim 106, wherein the component server object comprises a sequenced  
2 collection of server objects.

1 111. The method of claim 104, wherein the selecting step (b), the template comprises a manually  
2 created template.

1 112. The method of claim 104, wherein the selecting step (b), the template comprises an  
2 externally imported template.

- 1 113. The method of claim 104, wherein the selecting step (b), the template comprises at least one  
2 of previously defined templates.
- 1 114. The method of claim 104, wherein the recording step (d), the reference model comprises a  
2 manually created template.
- 1 115. The method of claim 104, wherein the recording step (d), the reference model comprises at  
2 least one of previously defined reference models.
- 1 116. The method of claim 104, wherein the recording step (d) comprises arbitrarily taking a  
2 snapshot of the current configuration of a first server.
- 1 117. The method of claim 116, wherein the comparing step (e) comprises comparing a live-  
2 version of the first server to the snapshot.
- 1 118. The method of claim 116, wherein the correcting step (f) further comprises restoring a  
2 previous configuration of the first server from a snapshot.
- 1 119. The method of claim 104, wherein the recording step (d) comprises recurrently taking a  
2 plurality of snapshots of a first server at predetermined time intervals, wherein a first snapshot from  
3 the plurality of snapshots forms a baseline for subsequent snapshots from the plurality of snapshots  
4 and the subsequent snapshots capture changes against the baseline over time.
- 1 120. The method of claim 119, wherein the comparing step (e) comprises recurrently taking a  
2 plurality of audits of a live server at predetermined time intervals to track compliance against at least  
3 one of the baseline snapshot and the reference model over time.
- 1 121. The method of claim 104, wherein the comparing step (e) further comprises comparing live  
2 servers by:
- 3 (i) comparing values of explicitly selected sever objects that are commonly shared  
4 between a first live server and a second live server.
- 5 (ii) comparing values of implicitly selected sever objects that are implicitly specified in  
6 the template.
- 1 122. The method of claim 104, wherein the correcting step (f) further comprises restoring a  
2 previous configuration of the second server from the reference model.
- 1 123. The method of claim 104 further comprising:  
2 provisioning a newly-added third server on the network in accordance with the reference  
3 model.
- 1 124. The method of claim 104, wherein the correcting step (f) further comprises:  
2 after the comparing the comparing step (e),  
3 collecting the discrepancies identified in a transaction package to execute a plurality of server  
4 change operations on the second server; and

5 synchronizing the second server with the reference model.

1 125. The method of claim 104 further comprising:

2 updating the reference model; and

3 propagating the updates to the plurality of servers with a transaction package.

1 126. The method of claim 104 further comprising:

2 (i) categorizing in a template each of the server objects into categories, sub-categories,  
3 and associated keywords; and

4 (ii) selecting categorically related server objects in second templates.

1 127. The method of claim 126, wherein the categorizing step (i), the categories comprise server  
2 type categories including at least one of an application server category, a web server category, and a  
3 database server category.

1 128. The method of claim 126, wherein the categorizing step (i), the categories comprise  
2 configuration parameter type categories including at least one of network parameters, capacity  
3 parameters, availability parameters, performance parameters, and security parameters.

1 129. A system for configuring a plurality of heterogeneous servers across a network, the system  
2 comprising:

3 (a) a browser for browsing server objects in each of a plurality of servers across a network;

4 (b) a template comprising a selected plurality of identifiers of at least one browsed server  
5 objects;

6 (c) a recorder for recording values of the selected plurality of server object identifiers in the  
7 template from at least one of the plurality of servers.

8 (d) a reference model comprising recorded values of the selected plurality of server object  
9 identifiers in the template from a gold server of the plurality of servers;

10 (e) a comparator, in communication with the reference model, for comparing a second server  
11 from the plurality of servers to the reference model; and

12 (f) a corrector, in communication with the comparator, for correcting discrepancies of the  
13 second server against the reference model.

1 130. The system of claim 129, wherein the server objects comprise at least one of files and  
2 configuration file entries.

1 131. The system of claim 130, wherein the server objects comprise at least one of a primitive  
2 server object, a compound server object, an abstract configuration server object, and a component  
3 server object.

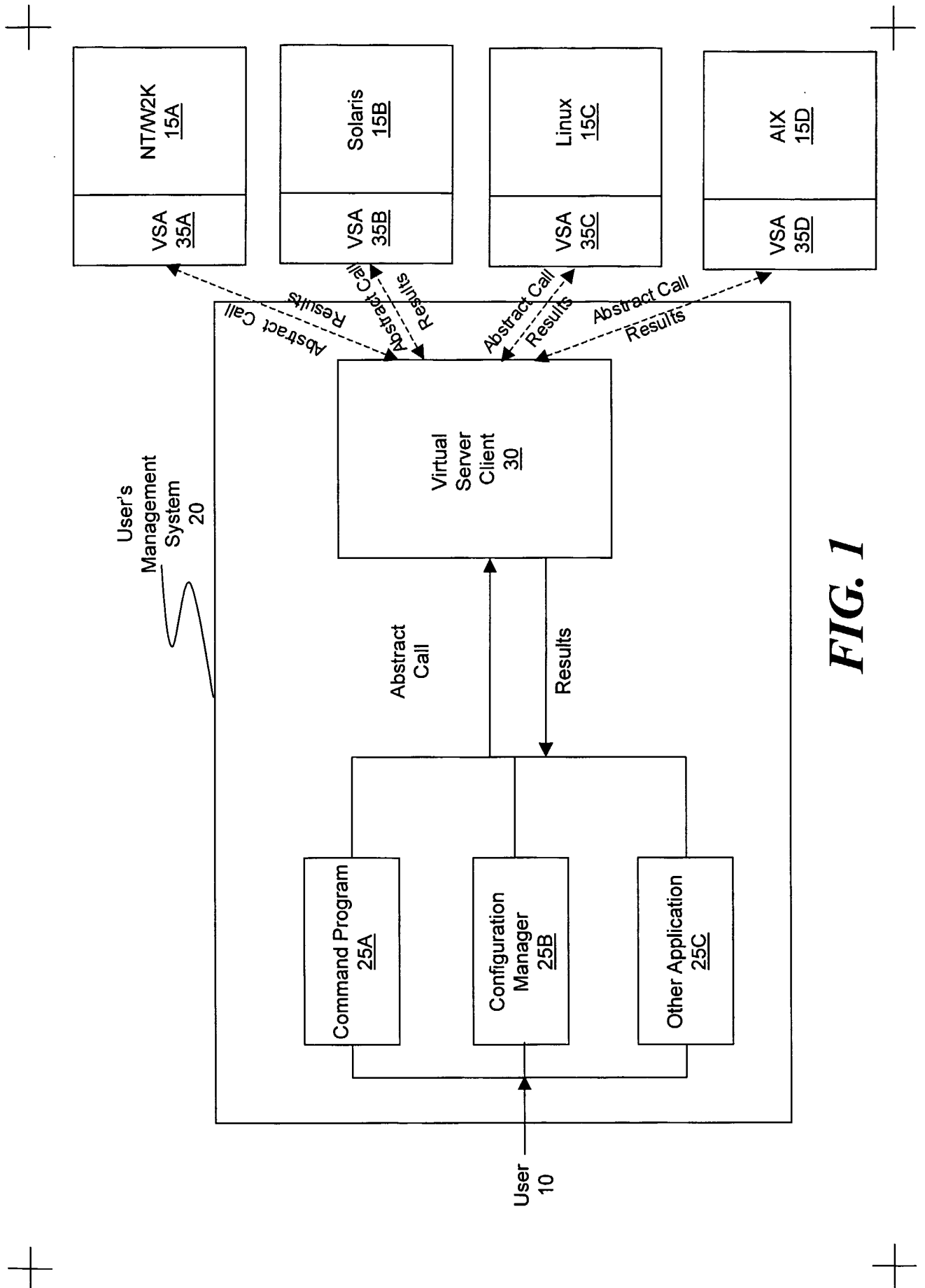
1 132. The system of claim 131, wherein the primitive server object comprises an elemental server  
2 object.

- 54 -

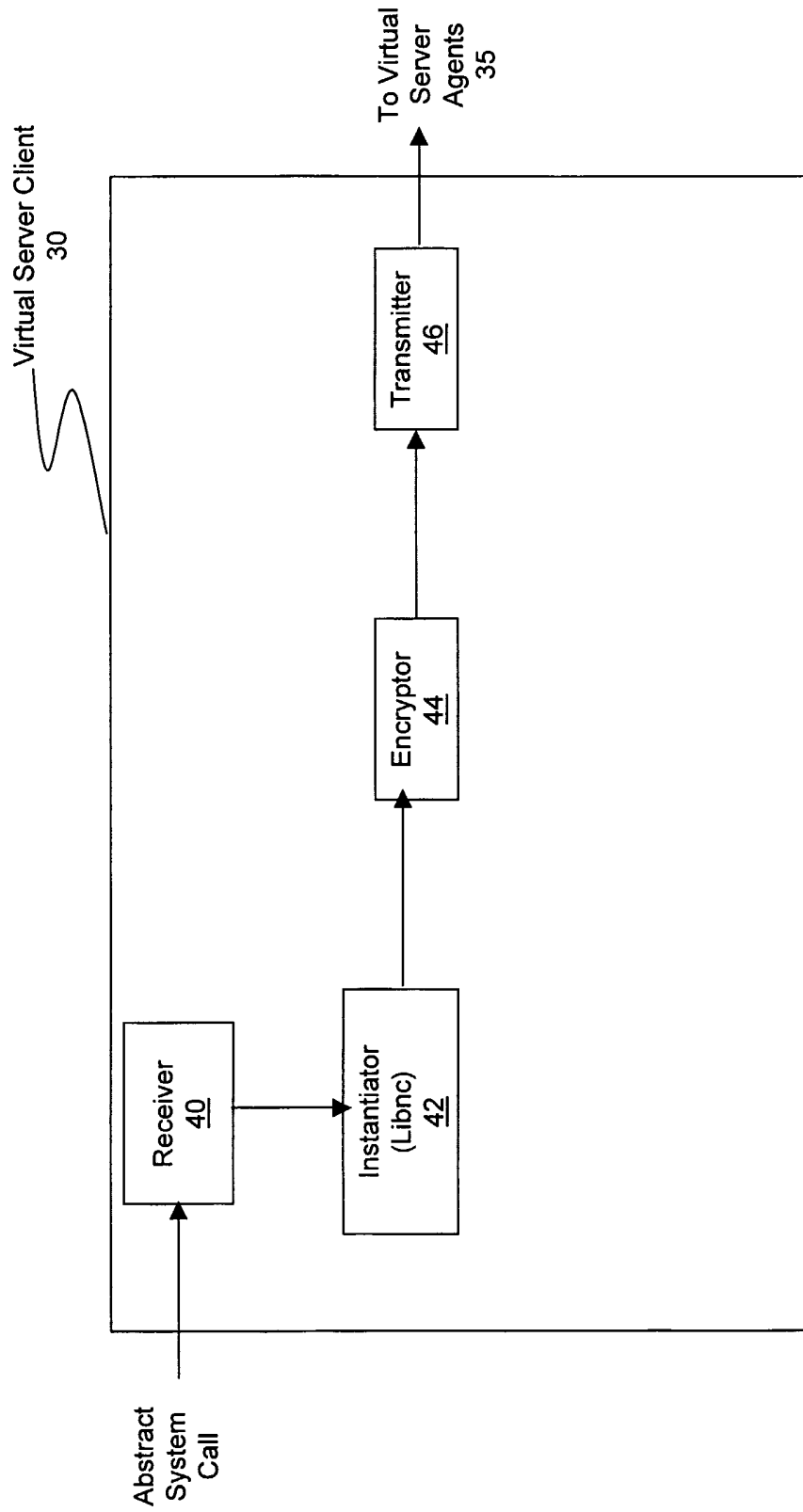
- 1 133. The system of claim 131, wherein the compound server object comprises at least one of the  
2 primitive server objects, the abstract configuration server objects, the component server objects, and  
3 the compound server objects.
- 1 134. The system of claim 131, wherein the abstract configuration server object comprises an entry  
2 in a configuration file mapped to a corresponding entry in a common abstract configuration file  
3 format.
- 1 135. The system of claim 131, wherein the component server object comprises a sequenced  
2 collection of server objects.
- 1 136. The system of claim 129, wherein the template comprises a manually created template.
- 1 137. The system of claim 129, wherein the template comprises an externally imported template.
- 1 138. The system of claim 129, wherein the template comprises at least one of previously defined  
2 templates.
- 1 139. The system of claim 129, wherein the reference model comprises a manually created  
2 template.
- 1 140. The system of claim 129, wherein the reference model comprises at least one of previously  
2 defined reference models.
- 1 141. The system of claim 129, wherein the recorder arbitrarily takes a snapshot of the current  
2 configuration of a first server.
- 1 142. The system of claim 141, wherein the comparator compares a live-version of the first server  
2 to the snapshot.
- 1 143. The system of claim 141, wherein the corrector further restores a previous configuration of  
2 the first server from the snapshot.
- 1 144. The system of claim 129, wherein the recorder recurrently takes a plurality of snapshots of a  
2 first server at predetermined time intervals, wherein a first snapshot from the plurality of snapshots  
3 forms a baseline for subsequent snapshots of the plurality of snapshots and the subsequent  
4 snapshots capture changes against the baseline over time.
- 1 145. The system of claim 144, wherein the comparator recurrently takes a plurality of audits of a  
2 live server at predetermined time intervals to track compliance against at least one of the baseline  
3 snapshot and the reference model over time.
- 1 146. The system of claim 129, wherein the comparator compares live servers by:  
2 (i) comparing values of explicitly selected sever objects that are commonly shared  
3 between a first live server and a second live server.  
4 (ii) comparing values of implicitly selected sever objects that are implicitly specified in  
5 the template.

- 1 147. The system of claim 129, wherein the corrector further restores a previous configuration of  
2 the second server from the reference model.
- 1 148. The system of claim 129 further comprising:  
2 provisioning a newly-added third server on the network in accordance with the reference  
3 model.
- 1 149. The system of claim 129, wherein the correcting step further  
2 collects the discrepancies identified in a transaction package to execute a plurality of server  
3 change operations on the second server; and  
4 synchronizing the second server with the reference model.
- 1 150. The system of claim 129 further comprising:  
2 an updater for updating the reference model and  
3 propagating the updates to the plurality of servers with a transaction package.
- 1 151. The system of claim 129 further comprising:  
2 (i) a first template categorizing each of the server objects into categories, sub-categories,  
3 and associated keywords; and  
4 (ii) second templates including a selected group of categorically related server objects by  
5 server type categories.
- 1 152. The system of claim 151, wherein the categories comprise server type categories including at  
2 least one of an application server category, a web server category, and a database server category.
- 1 153. The system of claim 151, wherein the categories comprise configuration parameter type  
2 categories including at least one of network parameters, capacity parameters, availability parameters,  
3 performance parameters, and security parameters.
- 1 154. The system of claim 129, wherein the reference model comprises an externally imported  
2 template.

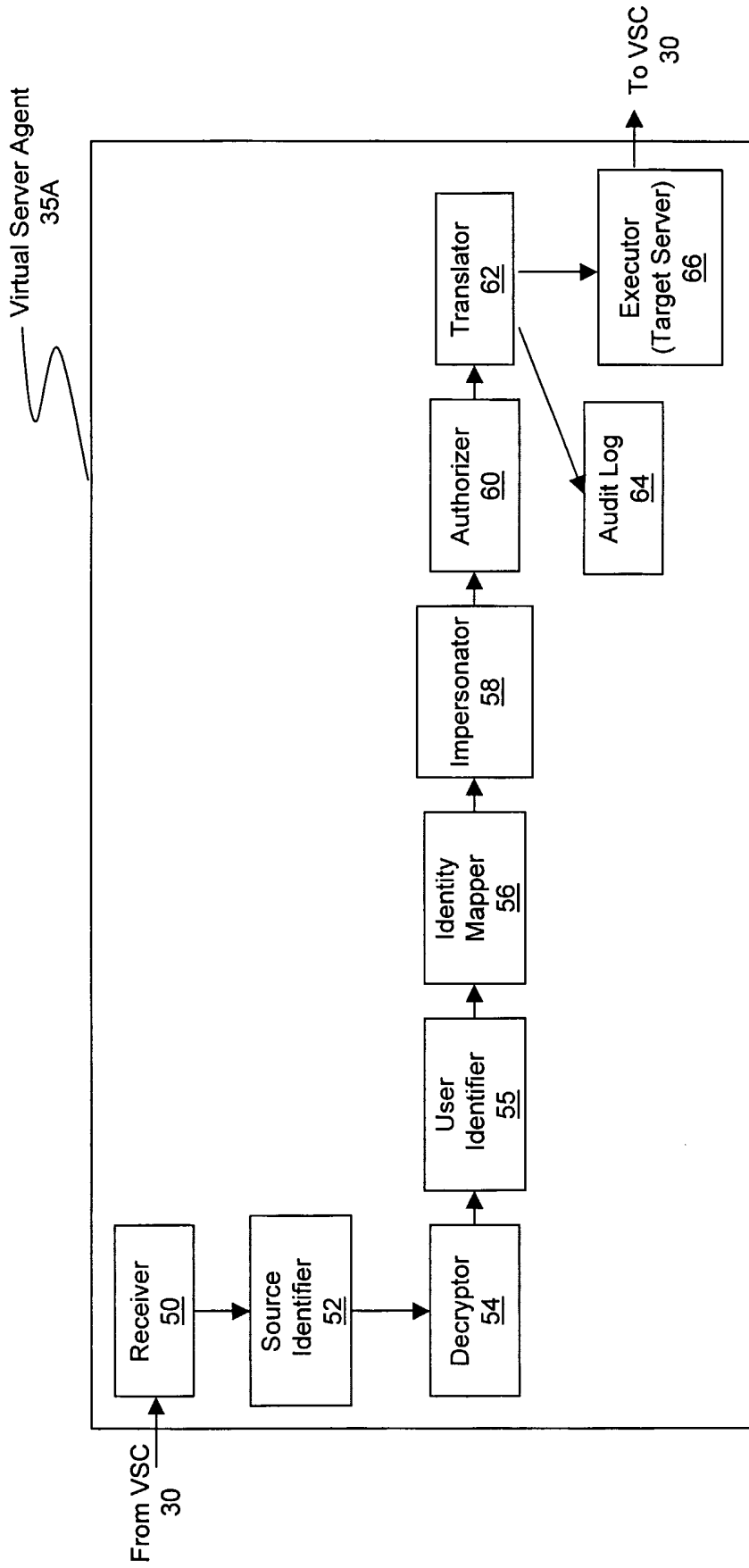




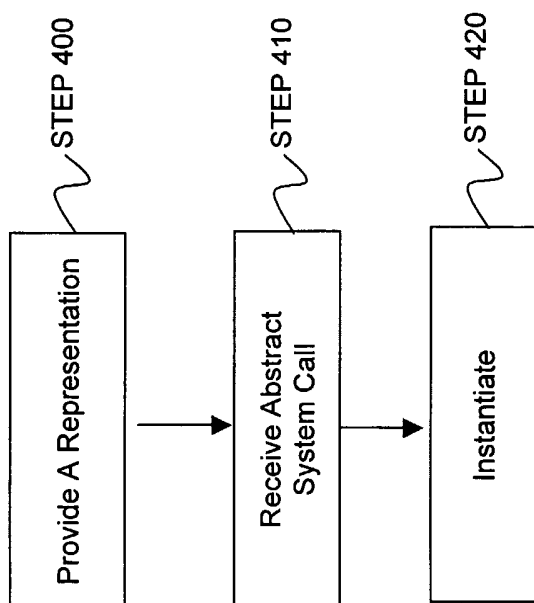
**FIG. 1**



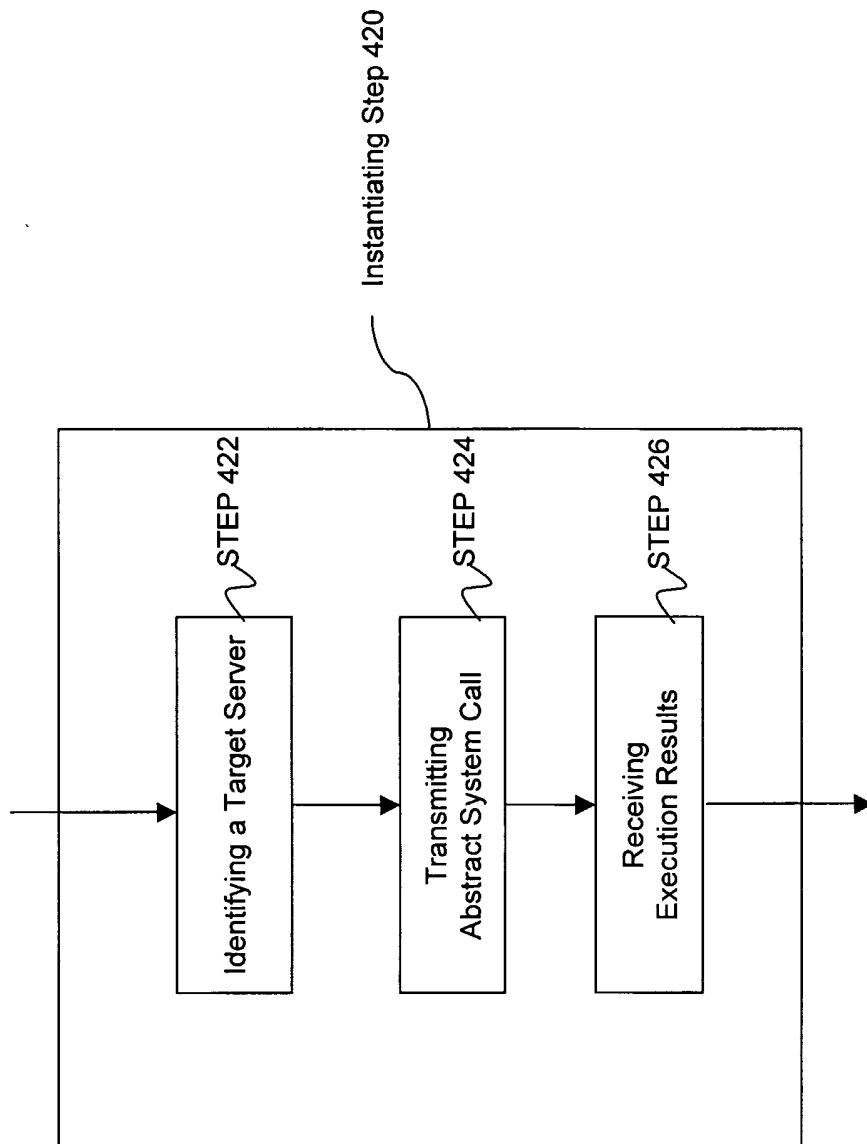
**FIG. 2**



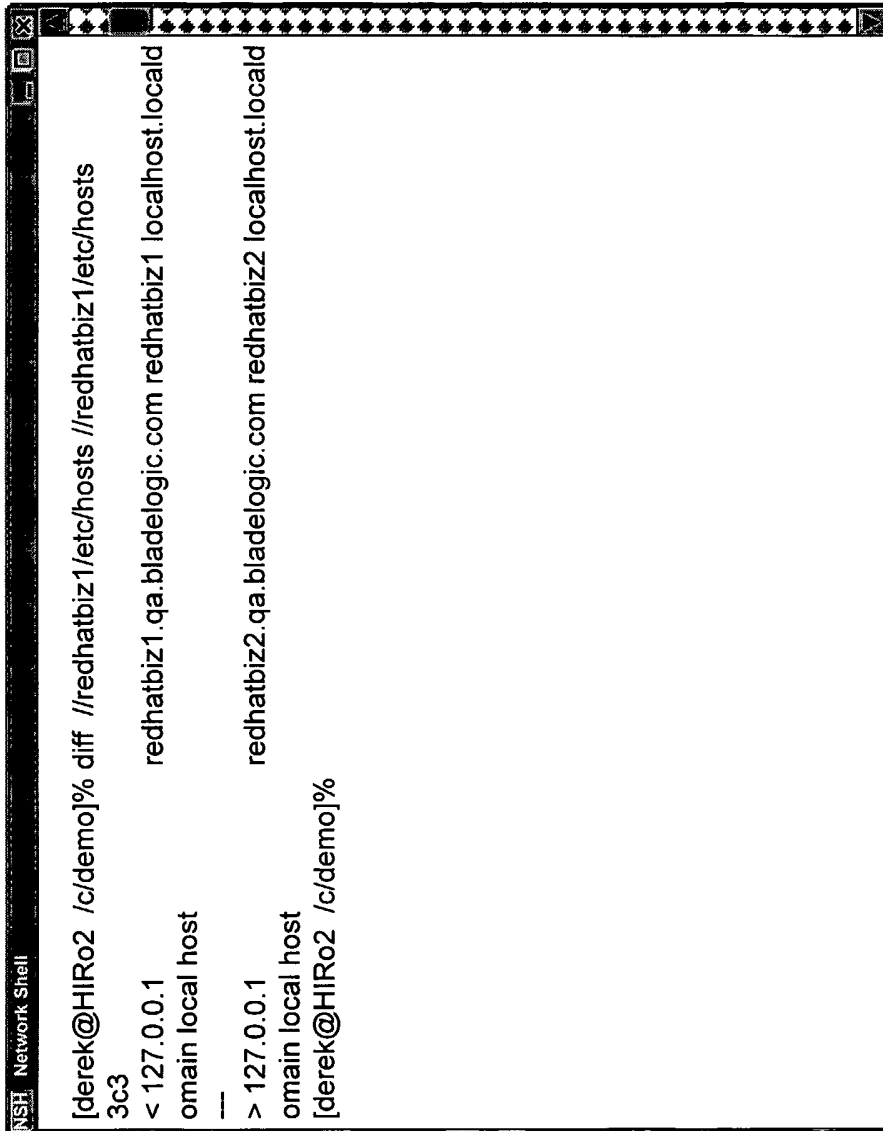
**FIG. 3**



**FIG. 4**

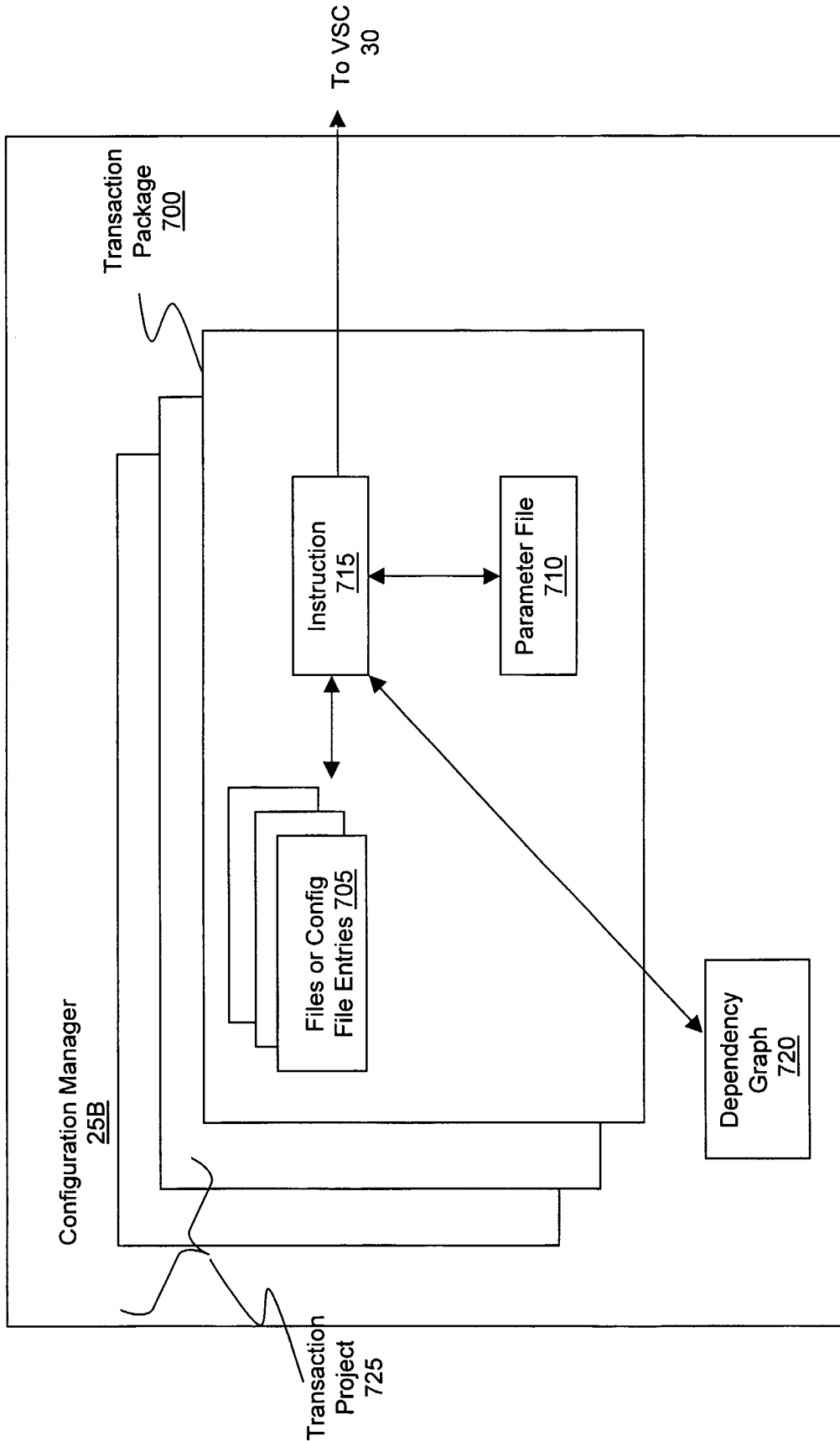


**FIG. 5**

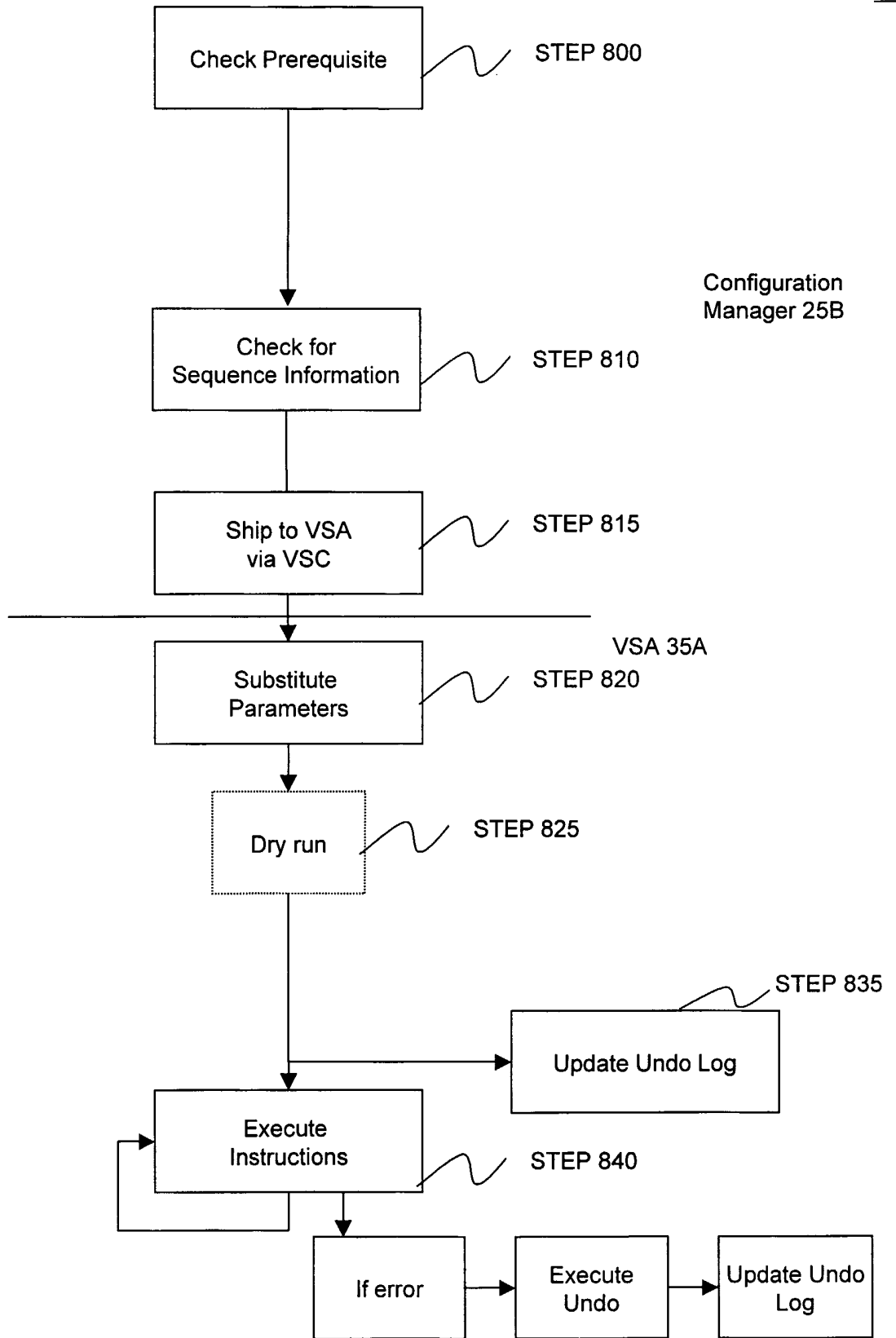


```
NSH Network Shell
[derek@HIRo2 /c/demo]% diff //redhatbiz1/etc/hosts //redhatbiz1/etc/hosts
3c3
< 127.0.0.1          redhatbiz1.qa.bladelogic.com redhatbiz1 localhost.locald
   omain local host
_
> 127.0.0.1          redhatbiz2.qa.bladelogic.com redhatbiz2 localhost.locald
   omain local host
[derek@HIRo2 /c/demo]%
```

**FIG. 6**

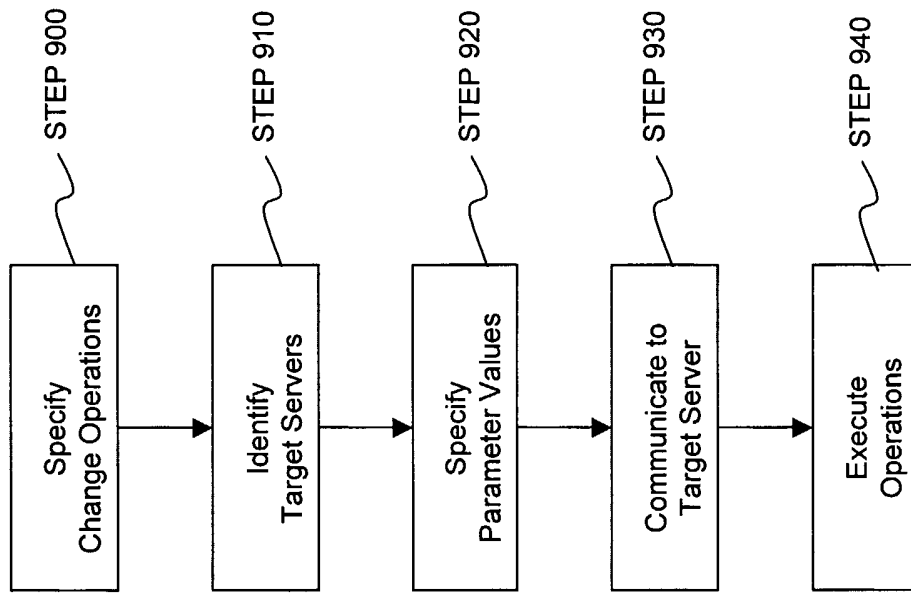


**FIG. 7**

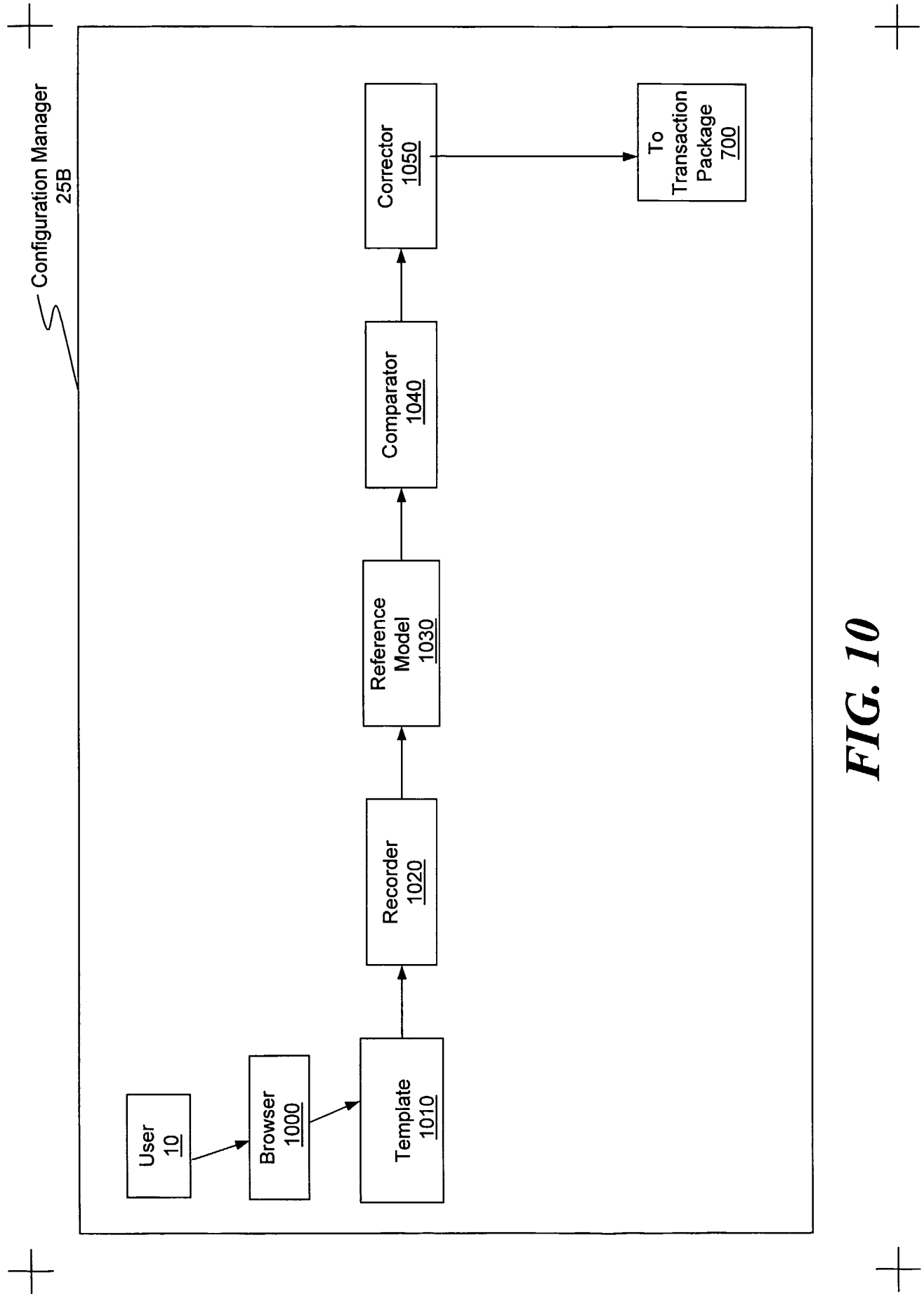


**FIG. 8**

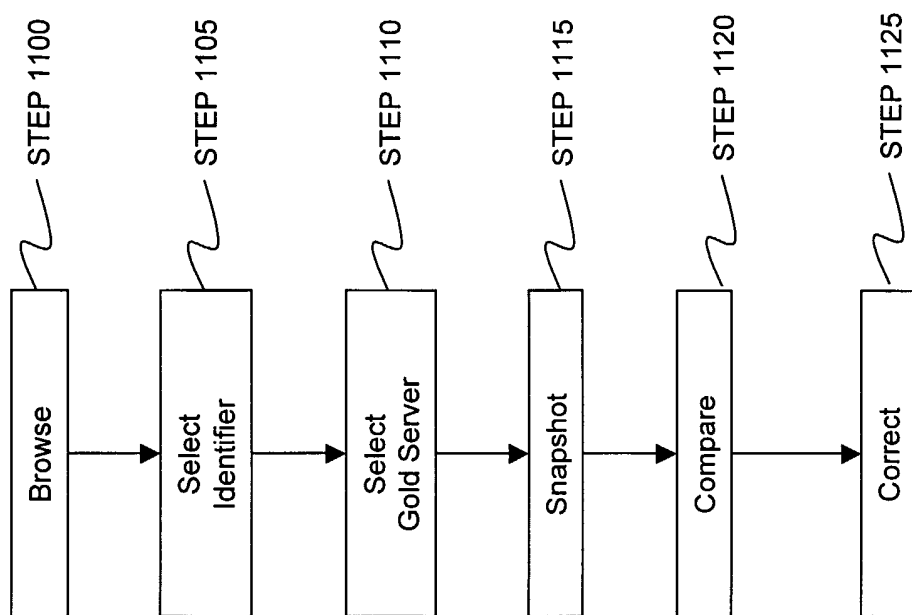




**FIG. 9**

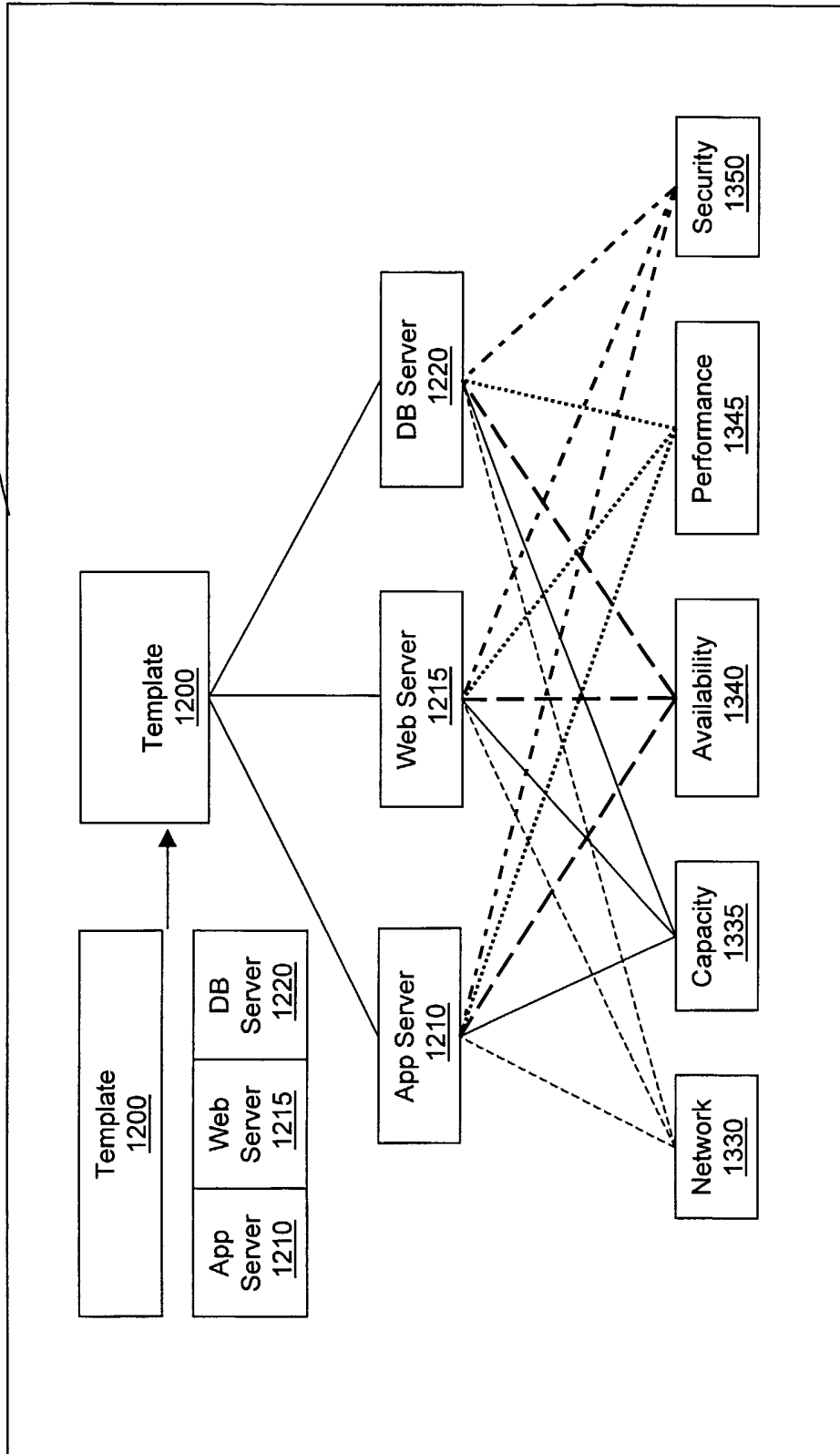


**FIG. 10**

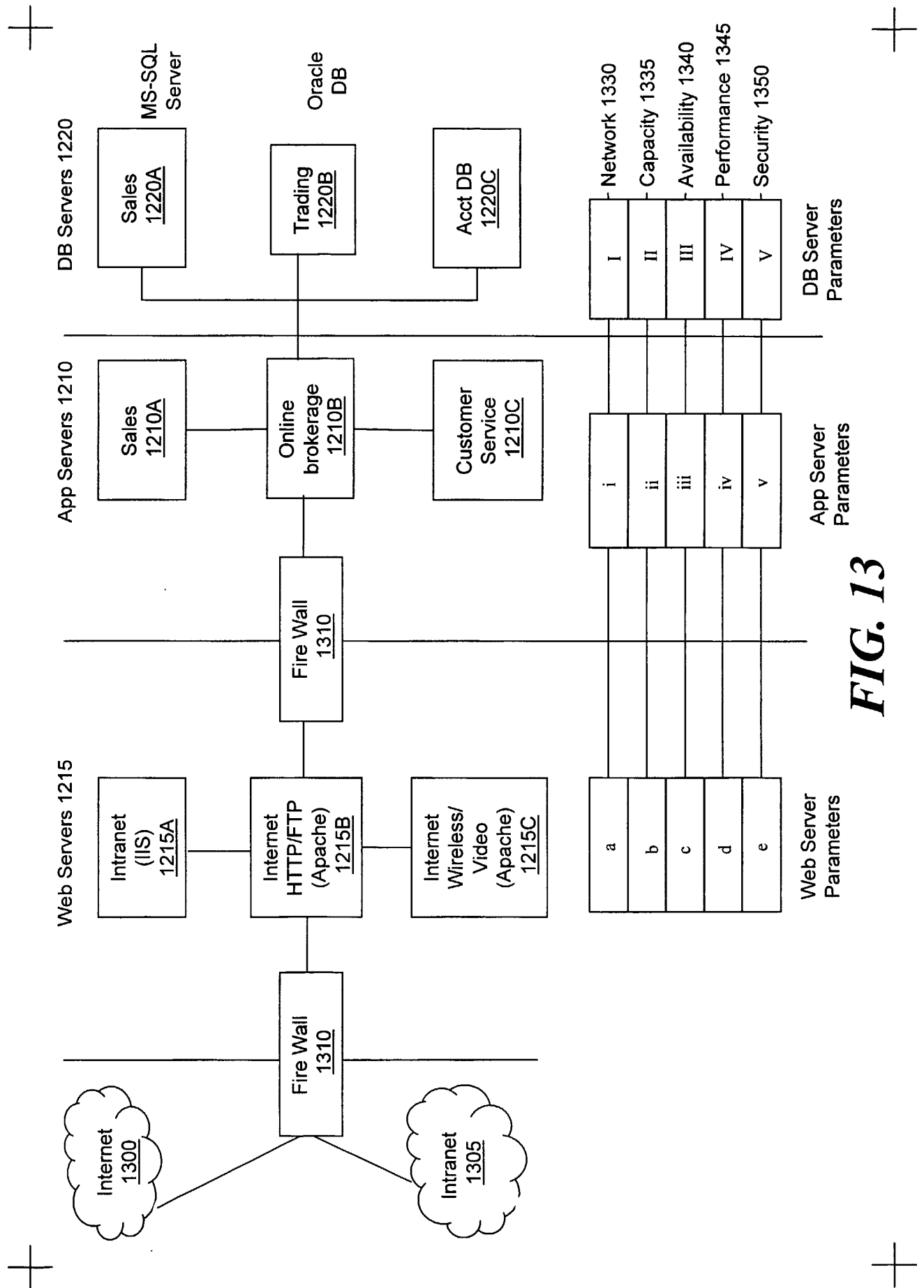


**FIG. 11**

Configuration Manager  
25B



**FIG. 12**



**FIG. 13**

1400

BladeLogic Configuration Manager  
File Edit View Actions Tools Help

Servers Depots

- Eastern Division
  - corellia
  - kessel
  - redhatter1
  - redhatter2
  - sun1
  - sun2
- File System
- Packages
- Patches
- System Info
  - win2kest1
  - win2kest2
  - win2kest4
- Western Division

Name	Description
108569-02	SUNWwpsr
108806-07	SUNWm64, SUNWm64w, SUNWm64x
108609-01	SUNWdialh
108652-15	SUNWwmt, SUNWwmpit, SUNWwmpix, SUNWwvinc, SUNWwmma
108714-02	SUNWdibas, SUNWdibax
108723-01	SUNWcst, SUNWcaix
108725-02	SUNWcsu, SUNWcsr, SUNWcarx, SUNWcsu, SUNWhea
108727-04	SUNWcst, SUNWcarx, SUNWhea
108808-02	SUNWqfed, SUNWqfedx, SUNWqfedu
108808-10	SUNWman
108820-01	SUNWcsb, SUNWcsi
108823-01	SUNWesu
108825-01	SUNWcsu
108827-04	SUNWcsb, SUNWcsi
108835-01	SUNWdidst
108869-02	SUNWmibil, SUNWsasnm, SUNWsadmi, SUNWsadmx, SUNWs
108874-01	SUNWcarx, SUNWcar
108875-07	SUNWcsu, SUNWcsr, SUNWcsk, SUNWcsi, SUNWcar, SUNWs
108887-01	SUNWwmmn

Contents of Patches (Number of entities: 186)

1420

1440

1450

1460

1410

1430

FIG. 14