

WHITE PAPER
CENTRIFY CORP.
DECEMBER 2006

Integrating Centrifify DirectControl with Identity Management Systems

Centrifify DirectControl complements an organization's existing Identity Management Systems, and readily integrates with both Agent-based and Agentless architectures. Using DirectControl reduces the provisioning complexity associated with databases and web servers, and Centrifify's patent-pending Zone technology simplifies management of UNIX, Linux and Mac computers while at the same time strengthening access controls through centralized management.

ABSTRACT

This white paper provides detailed examples of how to integrate Centrifify™ DirectControl™ with commercial off-the-shelf Identity Management Systems. It demonstrates how to handle common Identity Management events such as hiring a new employee, managing an employee's membership in Active Directory groups, marriage and divorce, promoting or demoting an employee, detecting and preventing unauthorized access attempts, and termination. This white paper discusses how DirectControl can simplify provisioning tasks and strengthen security when used in an environment that includes LDAP-based systems, databases, and portal servers.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrifly Corporation.

Centrifly may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrifly, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Centrifly Corporation. All rights reserved.

Centrifly and DirectControl are trademarks of Centrifly Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

[WP-010-2006-12-27]

Contents

1	Integrating DirectControl with Identity Management Systems.....	1
1.1	Introduction	1
1.2	About Centrify DirectControl	1
1.3	Scenario	2
1.3.1	Organization	3
1.3.2	Current IT Architecture.....	3
1.4	Current Password Change Workflow	5
1.5	Current Role-Based Provisioning	6
1.5.1	Provisioning an Accountant	7
1.5.2	Provisioning an Auditor.....	9
2	Solution Architecture.....	12
2.1.1	Solution: IT Architecture.....	12
2.2	Solution: Password Change Workflow	14
2.2.1	Solution: Zone Architecture.....	15
2.3	Solution: Role-Based Provisioning	16
2.3.1	Solution: Provisioning an Accountant.....	17
2.3.2	Solution: Provisioning an Auditor	19
3	Identity Management Components.....	21
3.1	Connectors	21
3.1.1	Data Storage in Active Directory	22
3.2	Agents or Agentless.....	24
3.3	Passwords	25
3.4	Reporting	25
4	Identity Management Events.....	26
4.1	Employee	26
4.1.1	Hiring.....	26
4.1.2	Add User to Active Directory Groups.....	29
4.1.3	Promotion / Demotion	30
4.1.4	Change Active Directory Groups	32
4.1.5	Marriage / Divorce	33
4.1.6	Unauthorized Access Detection and Prevention	33
4.1.7	Termination	35

4.2 Mergers and Acquisitions.....	38
4.2.1 Initial Integration.....	39
4.2.2 Group Migration.....	41
4.2.3 User Migration.....	41
4.2.4 Consolidation.....	44
5 Identifying Initial Tasks.....	44
5.1 DirectControl Prerequisites.....	44
5.2 Identity Management System Prerequisites.....	44
5.3 Active Directory Setup.....	45
5.4 Zone Design.....	45
5.5 UNIX Deployment.....	45
5.6 Provisioning Integration.....	45
5.7 Conclusion.....	46
6 Related Publications.....	46
6.1 Product Documentation.....	46
6.2 White Papers.....	46
6.3 Video Chalktalks.....	46
7 How to Contact Centrify.....	47

1 Integrating DirectControl with Identity Management Systems

1.1 Introduction

When evaluating enterprise software solutions, IT organizations that have invested in Identity Management Systems must carefully examine the ease with which the new software can be integrated. Centrify™ DirectControl™ complements Identity Management Systems, and readily integrates with both Agent-based and Agentless architectures. Using DirectControl reduces the provisioning complexity associated with databases and web servers, and Centrify's patent-pending Zone technology simplifies management of UNIX, Linux and Mac computers. This white paper provides specific examples of how to integrate Centrify DirectControl with commercial off-the-shelf Identity Management Systems.

This document assumes a general knowledge of Identity Management Systems and a technical understanding of Centrify DirectControl.

This white paper focuses on commercial off-the-shelf Identity Management Systems. If your organization is using an internally developed Identity Management System or provisioning system, additional integration options exist. Please contact Centrify for further details.

1.2 About Centrify DirectControl

Centrify DirectControl's core feature is its ability to enable UNIX, Linux and Mac servers and workstations to participate in an Active Directory domain. The Centrify DirectControl Agent effectively turns the host system into an Active Directory client, enabling organizations to secure that system using the same authentication, access control and Group Policy services currently deployed for their Windows systems. Additional seamlessly integrated modules snap into the DirectControl Agent to provide services such as web single sign-on, strong authentication to database and ERP systems, and Samba integration. The DirectControl Management Tools include extensions to standard Microsoft management tools, an administration console, out-of-the-box reporting, and an account migration wizard.

With the Centrify DirectControl suite, organizations with diverse IT environments can leverage their investment in Active Directory to:

Move to a central directory with a single point of administration for user accounts and security policy. By centralizing user account management and security policy in Active Directory, organizations can improve IT efficiency and move toward a more secure, connected infrastructure for their heterogeneous environment. Using DirectControl they can eliminate redundant identity stores, provide administrators and end-users with a single sign-on account, standardize on a single set of tools and processes, and enforce enterprise wide security and configuration policies for their heterogeneous environment.

Use DirectControl Zones to provide secure, granular access control and delegated administration. Only DirectControl, with its patent-pending Zone technology, delivers the

granular access control that real-world enterprises need to securely manage their heterogeneous environments. Any logical collection of mixed UNIX, Linux or Mac systems can be segregated within Active Directory as a DirectControl Zone. Each Zone can have a unique set of users, a unique set of administrators, and a unique set of security policies.

Extend single sign-on to web applications, databases and ERP systems. Centrify delivers Active Directory-based web single sign-on for both intranet and extranet applications running on Apache and popular J2EE servers at a fraction of the cost of older point solutions. For intranets, DirectControl enables Active Directory-based web SSO via Kerberos and LDAP. For extranets, DirectControl leverages Microsoft Active Directory Federation Services (ADFS) to provide federated identity management for both business-to-business and business-to-customer web applications.

Simplify compliance with regulatory requirements. DirectControl greatly simplifies the administrative, reporting and auditing tasks brought on by Sarbanes-Oxley, PCI, HIPPA and other government and industry regulations by providing IT managers with a single point of administration from which to reliably manage user accounts, set access controls and enforce security policies. DirectControl Zones enable “need to know” access controls, and out-of-the-box reports verify who has access to what.

Deploy quickly without intrusive changes to existing infrastructure. DirectControl’s support for open standards and its unified architecture make it far easier to deploy than any other Active Directory-based solution. Certified for Windows 2003 Server, DirectControl does not require proprietary schema changes in order to store UNIX identity data or to enable advanced features.

1.3 Scenario

This white paper describes a fictional corporation named Illumi Clinics, which is using a generic Identity Management system and Centrify DirectControl. The root domain of this organization is stored as “illumclinics.com” in Active Directory. Per corporate policy, all employees at Illumi Clinics log in with their User Principal Name, such as “Larrie.Mixey@illumclinics.com”.

Over the course of this whitepaper, Illumi Clinics will hire a new employee named Larrie Mixey. Larrie will initially work in the Finance organization, and will later join in a special project team, led by the IT organization, to investigate wider deployment of DirectControl at Illumi Clinics.

A generic Identity Management system was selected for this white paper because DirectControl is fully interoperable with all Identity Management systems and servers that are capable of either calling COM/COM+/.NET objects or provisioning data over LDAP.

Centrify DirectControl was installed using all default options.

1.3.1 Organization

Illumi Clinics has its headquarters in Pittsburgh, Pennsylvania. It operates non-urgent care medical clinics within surrounding states. As a publicly traded company, it is subject to Sarbanes-Oxley regulations. Because it handles patient records, it is subject to HIPAA. It also accepts credit card payments at clinics, making it subject to the PCI standards promoted by the payment card industry.

Illumi Clinic's regional sales personnel carry laptops. Local clinics have desktops systems, from which personnel connect to web-based applications managed through the corporate data center. Illumi Clinics has a flat organizational structure consisting of the following departments:

- Engineering
- Finance
- Human Resources
- Marketing
- Sales

1.3.2 Current IT Architecture

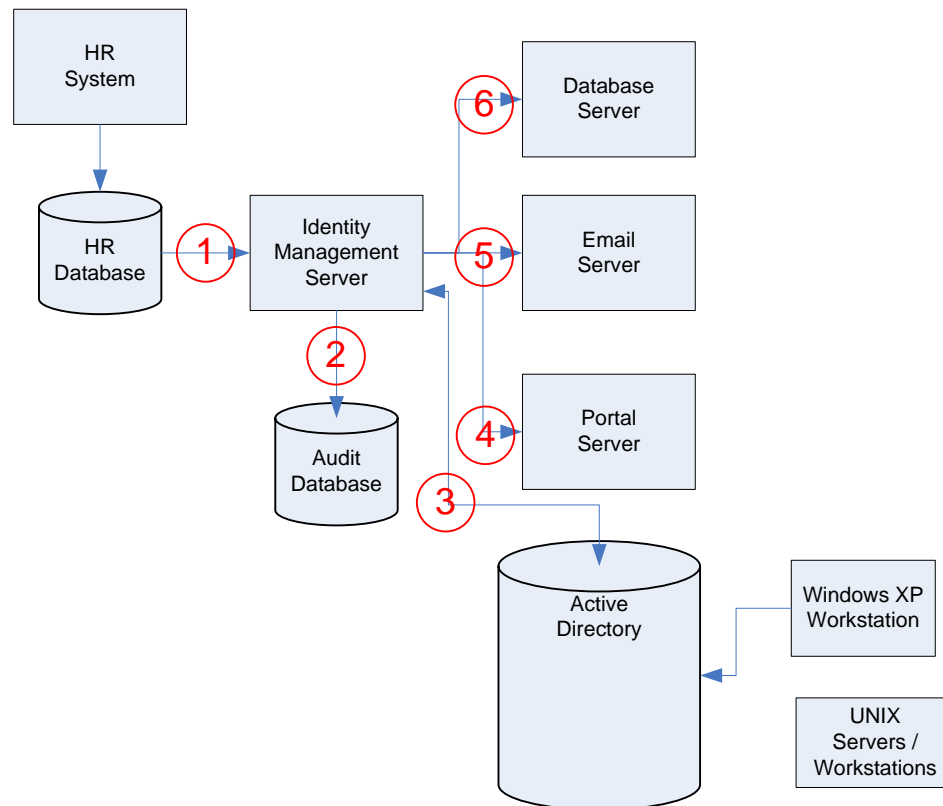


Figure 1-1

This figure illustrates the current IT architecture in use at Illumi Clinics. Specifically, this illustrates the state before deploying Centrify DirectControl. Figure 2-1 shows the state after deployment of Centrify DirectControl.

- The HR System is the authoritative repository of employee information at Illumi Clinics.
- The Identity Management Server runs on a Windows 2003 server cluster.
- The Database Server is Oracle 10g installed on Sun Solaris 9. Multiple applications on Windows and UNIX access applications on the database server.
- The Portal Server is running Apache 2.x with PHP on Red Hat Enterprise Linux 4. The Portal is a PHP application which uses basic authentication over HTTPS, and the Portal is used by local clinic staff to connect to business applications.
- The Email Server is Microsoft Exchange 2003 running on Windows Enterprise Server 2003 R2.
- The Active Directory server is a fully redundant cluster running on Windows Server 2003 Enterprise Edition R2.
- The UNIX servers / workstations include HP-UX 11.23, Sun Solaris 9 and 10 and Red Hat Enterprise Linux 3 and 4 computers.

Current Provisioning Workflow

The Identity Management system uses a set of rules to determine which servers to provision. These rules are largely based on data stored in the HR System. For purposes of this example, this workflow will describe provisioning all servers.

1. The HR System notifies the Identity Management Server that there is new data via a trigger. The Identity Management Server reads the new data.
2. The Identity Management Server writes transaction logs to the Audit Database.
3. The Identity Management Server provisions the Active Directory user and group objects via LDAP.
4. The Identity Management Server provisions a user account stored on the Portal Server in a plain text password file.
5. The Identity Management Server provisions the employee's Exchange mailbox.
6. The Identity Management Server provisions the employee's Oracle account via ODBC. This includes their password and GRANT statements permitting database access.

The UNIX servers and workstations are manually provisioned by system administrators using native platform tools.

1.4 Current Password Change Workflow

Per company policy, all employees at Illumi Clinics change their password using the Windows CTRL-ALT-DEL “change password” dialog. The Identity Management Server is responsible for password synchronization throughout Illumi Clinics.

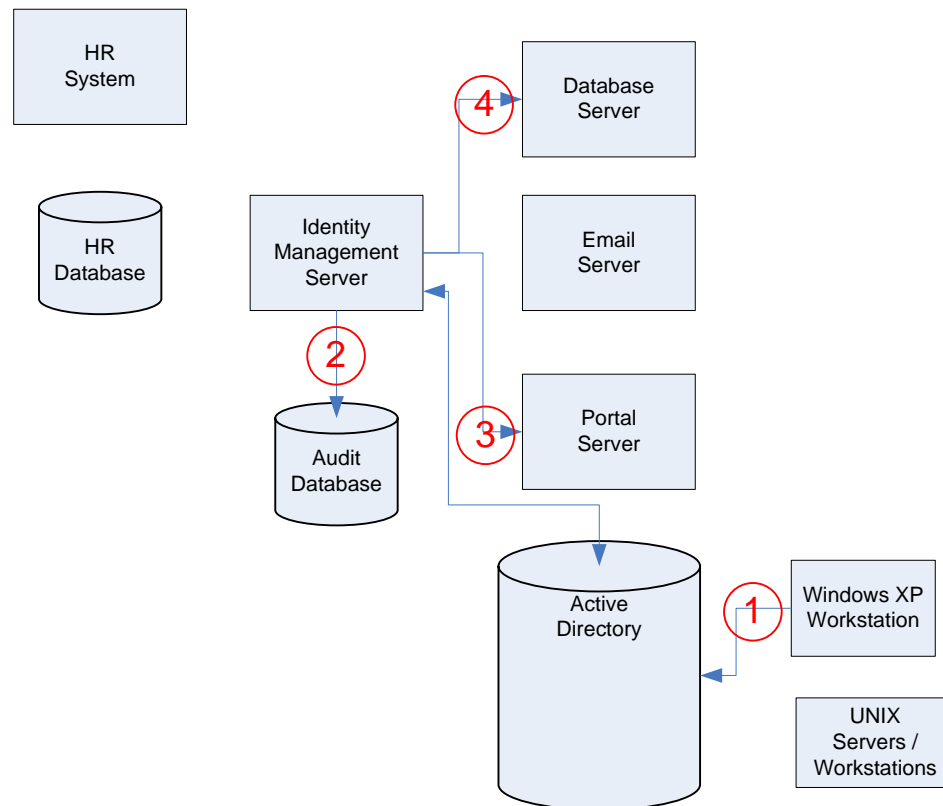


Figure 1-2

1. The employee changes their password from their Windows XP workstation.
2. The Identity Management Server writes a transaction log to the Audit Database.
3. The Identity Management Server writes the employee’s new password to the plain text password file on the Portal Server.
4. The Identity Management Server writes the employee’s new password to the Oracle Database via ODBC.

As part of the current company policy, employees are required to manually update their passwords on each of the different UNIX servers and workstations. This is a burden for administrative users, some of whom have access to over 100 different UNIX servers and workstations.

1.5 Current Role-Based Provisioning

The Identity Management Server in place at Illumi Clinics features role-based provisioning. Also known commonly as “rules-based provisioning” or “access management,” this feature automatically provisions employee accounts based on their job role as defined in the HR System. The employee’s role is thus used to control which systems the employee may access.

For example, two job roles defined at Illumi Clinics are those of accountant and auditor. Figure 1-3 shows the provisioning sequence for an accountant and Figure 1-4 shows the provisioning sequence for an auditor.

The Portal Server is configured to allow any valid user access to basic applications. However, the Financial Auditing Dashboard application has been configured to allow only members of the ‘finsec’ group (stored on the Apache server) access to the Dashboard application.

The UNIX servers and workstations are manually managed by a small team of UNIX system administrators. Auditors have access to all of the same UNIX accounting workstations as an accountant, as well as a specialized Auditing Server which stores compliance data.

1.5.1 Provisioning an Accountant

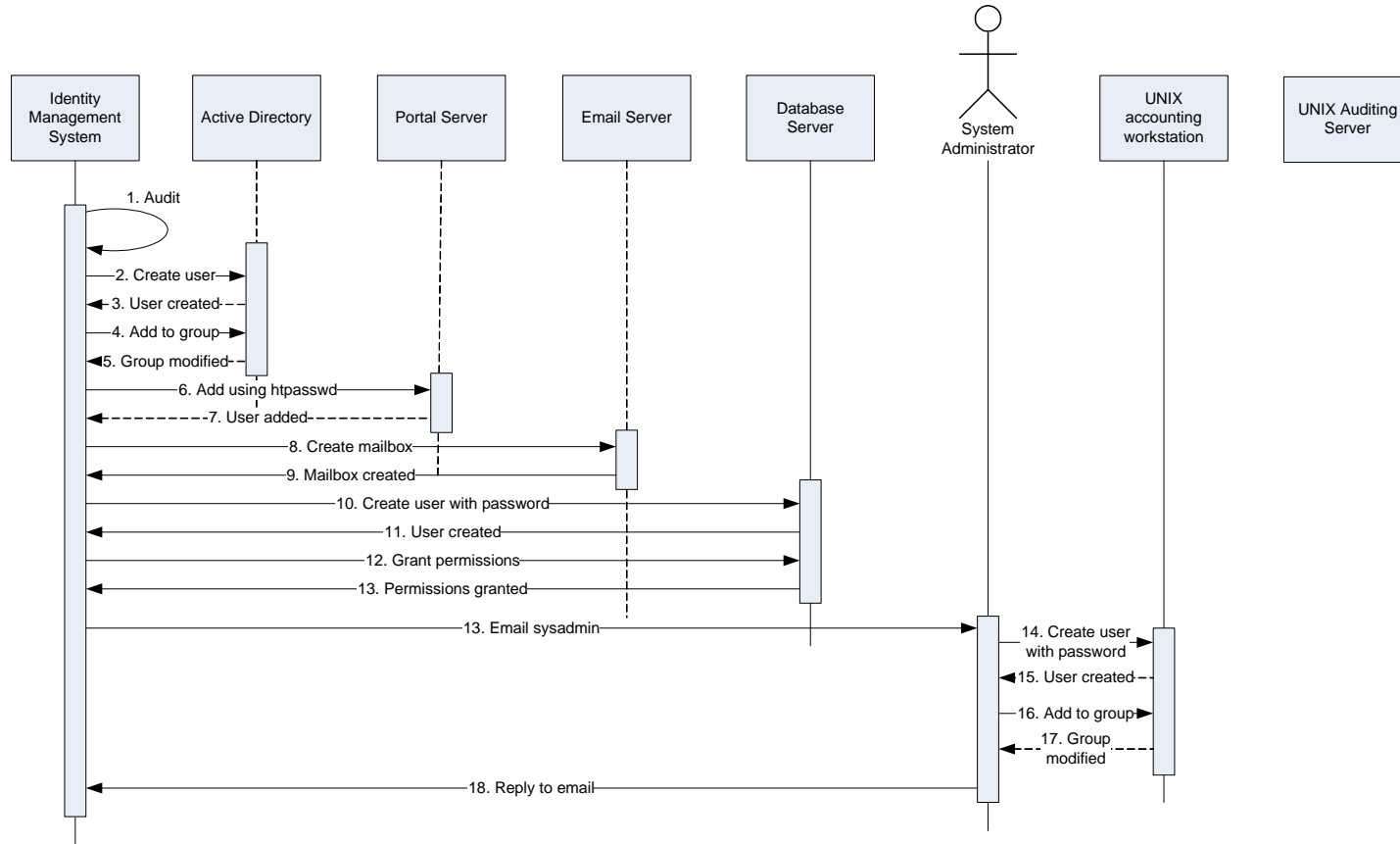


Figure 1-3

Sequence Description: Provisioning an Accountant

1. The Identity Management Server writes an audit record to the Audit Database.
2. The Identity Management Server creates an Active Directory user object for the new accountant; and,
3. The add operation succeeds.
4. The Identity Management Server adds the new Active Directory user object to an existing “Finance Users” Active Directory group; and,
5. The modify operation succeeds.
6. The Identity Management Server uses ‘htpasswd’ to create a new user account and a new password for the new accountant on the Apache server. Note that this password is maintained separately from the Active Directory password.
7. The operation succeeds.
8. The Identity Management Server allocates storage for the new accountant’s Exchange mailbox; and,
9. The mailbox is created.
10. The Identity Management Server creates a new Oracle user with a new password on the Oracle Database Server. Note that this password is also maintained separately from the Active Directory password; and,
11. The user is created on Oracle successfully.
12. The Identity Management Server uses SQL GRANT statements to set up the accountant’s permissions on the Oracle Database; and,
13. The GRANT statements succeed.
14. The Identity Management Server sends an email to the UNIX system administrator.
15. The system administrator remembers to check his email and creates a new UNIX user account for the new accountant, along with a new password. Note that this password, too, is maintained differently than the Active Directory password and is not part of the current password change process; and,
16. The add user operation succeeds and creates a home directory for the new accountant.
17. The system administrator adds the new accountant to the appropriate UNIX groups on the UNIX workstation; and,
18. The group files are successfully modified. Note that these group files may be inconsistent across UNIX computers.
19. The system administrator replies to the email from the Identity Management Server, indicating that the new accountant’s UNIX accounts were created successfully.

1.5.2 Provisioning an Auditor

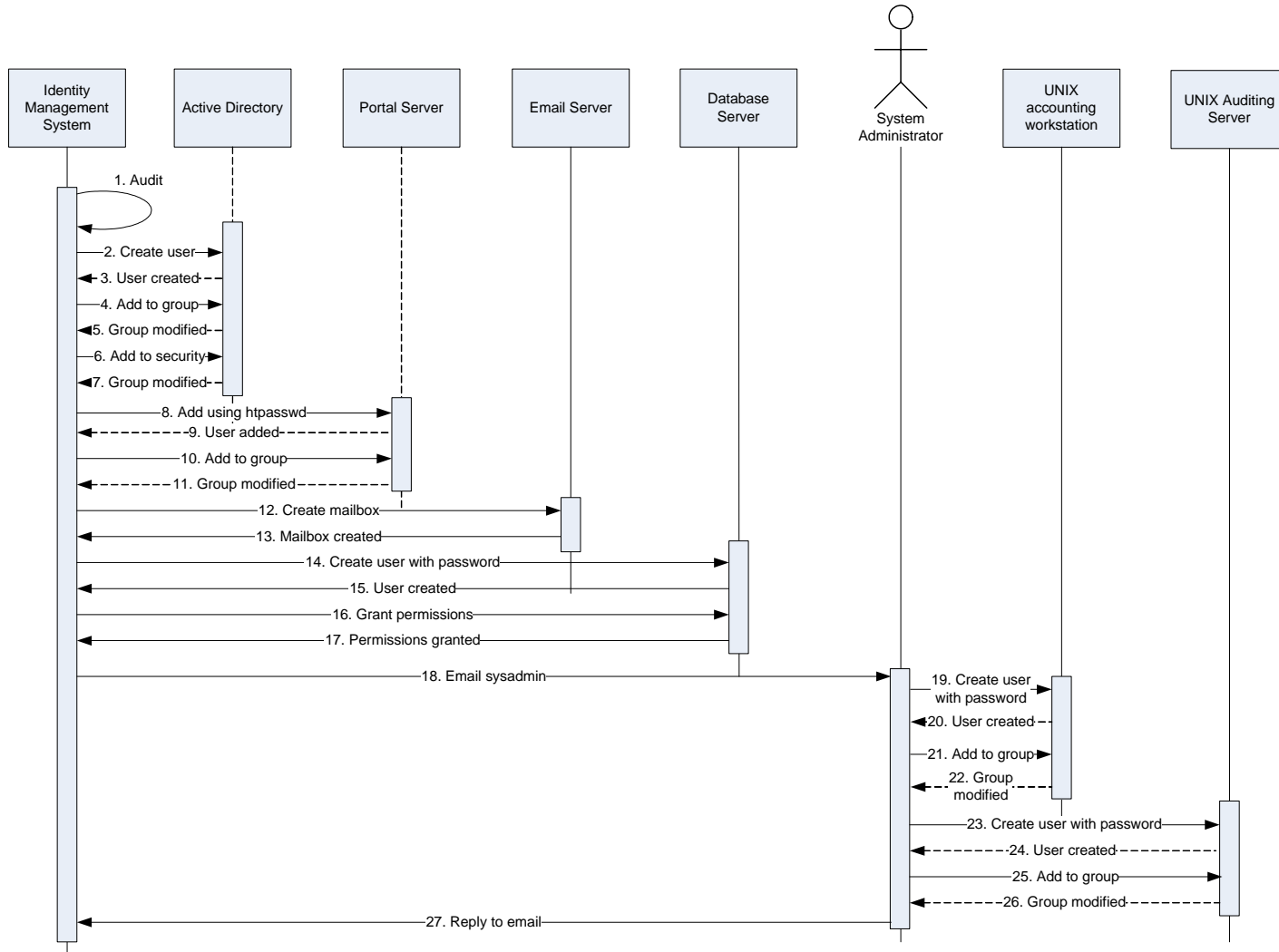


Figure 1-4

Sequence Description: Provisioning an Auditor

1. The Identity Management Server writes an audit record to the Audit Database.
2. The Identity Management Server creates an Active Directory user object for the new auditor; and,
3. The add operation succeeds.
4. The Identity Management Server adds the new Active Directory user object to an existing “Finance Users” Active Directory group; and,
5. The modify operation succeeds.
6. The Identity Management Server adds the new Active Directory user object to an existing “Finance Security” Active Directory group; and,
7. The modify operation succeeds.
8. The Identity Management Server uses ‘htpasswd’ to create a new user account and a new password for the new Auditor on the Apache server. Note that this password is maintained separately from the Active Directory password.
9. The operation succeeds.
10. The Identity Management Server adds the new user account to the Apache groups file, stored in /usr/local/apache/passwd/groups; and,
11. The groups file is saved.
12. The Identity Management Server allocates storage for the new auditor’s Exchange mailbox; and,
13. The mailbox is created.
14. The Identity Management Server creates a new Oracle user with a new password on the Oracle Database Server. Note that this password is also maintained separately from the Active Directory password; and,
15. The user is created on Oracle successfully.
16. The Identity Management Server uses SQL GRANT statements to set up the Auditor’s permissions on the Oracle Database; and,
17. The GRANT statements succeed.
18. The Identity Management Server sends an email to the UNIX system administrator.

19. The system administrator remembers to check his email and creates a new UNIX user account for the new auditor, along with a new password. Note that this password, too, is maintained differently than the Active Directory password and is not part of the current password change process; and,
20. The add user operation succeeds and creates a home directory for the new auditor.
21. The system administrator adds the new auditor to the appropriate UNIX groups on the UNIX workstation; and,
22. The group files are successfully modified. Note that these group files may be inconsistent across UNIX computers.
23. The system administrator creates a new UNIX user account for the new auditor on the UNIX Auditing Server, along with a new password. Note that this password is also maintained differently than the Active Directory password and is not part of the current password change process; and,
24. The add user operation succeeds and creates a home directory for the new auditor.
25. The system administrator adds the new auditor to the appropriate UNIX groups on the UNIX Auditing Server; and,
26. The group files are successfully modified. Note that these group files may be inconsistent across UNIX computers.
27. The system administrator replies to the email from the Identity Management Server, indicating that the new auditor's UNIX accounts were created successfully.

2 Solution Architecture

This section describes the deployed solution at Illumi Clinics after DirectControl has been deployed. Specific focus is given to the changes to the Identity Management Server and affected network elements.

2.1.1 Solution: IT Architecture

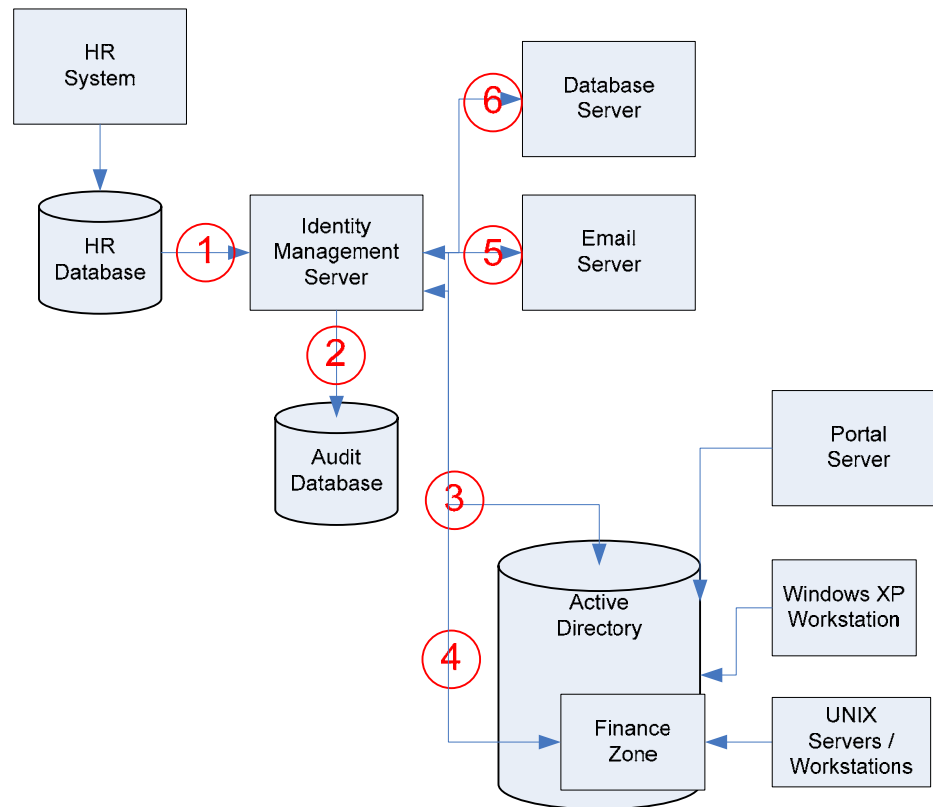


Figure 2-1

This figure illustrates the IT architecture in use at Illumi Clinics following deployment of Centrify DirectControl. For clarity, only the Finance Zone is shown but there are multiple Zones defined within Active Directory.

Solution: Provisioning Workflow

Italicized items have been modified as part of the deployment of DirectControl.

1. The HR System notifies the Identity Management Server that there is new data via a trigger. The Identity Management Server reads the new data.
2. The Identity Management Server writes transaction logs to the Audit Database. The Identity Management Server provisions the Active Directory Server user and group objects via LDAP.

3. *The Identity Management Server provisions the UNIX profiles for the Active Directory User via LDAP.*
4. The Identity Management Server provisions the employee's Exchange mailbox.
5. *The Identity Management Server provisions the employee's Oracle account via ODBC. This includes GRANT statements permitting database access.*

There have been additional benefits as a result of the successful deployment of DirectControl.

- User and group information on UNIX servers and workstations is no longer manually provisioned. This information is now stored in Active Directory.
- User information is no longer provisioned to the Portal. Centrify DirectControl for Apache uses Active Directory as a repository for user accounts.
- The employee's password is no longer stored in the Oracle Database Server.

2.2 Solution: Password Change Workflow

The password change workflow has been simplified as part of the successful deployment of DirectControl.

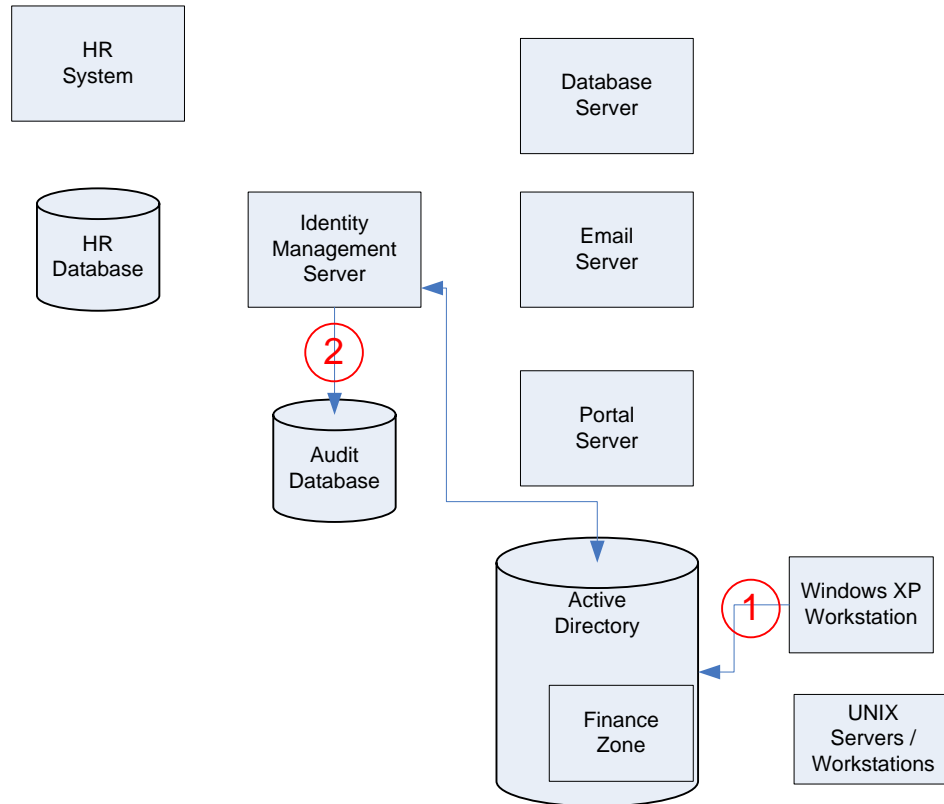


Figure 2-2

1. The employee changes their password from the Windows XP workstation.
2. The Identity Management Server writes a transaction log to the Audit Database. (This step is not optional due to strict compliance requirements at Illumi Clinics.)

The Portal Server, Database Server, and UNIX servers and workstations are all using Active Directory as the source of authentication and authorization data. Therefore, these network elements are no longer provisioned as part of a “password synchronization” process, as no synchronization is necessary.

In the future, the UNIX workstations, Linux computers or Mac OS X computers could also be used to change the user’s Active Directory password. However, this would require a change of company policy (requiring the use of CTRL-ALT-DEL on Windows XP to change passwords) at Illumi Clinics.

2.2.1 Solution: Zone Architecture

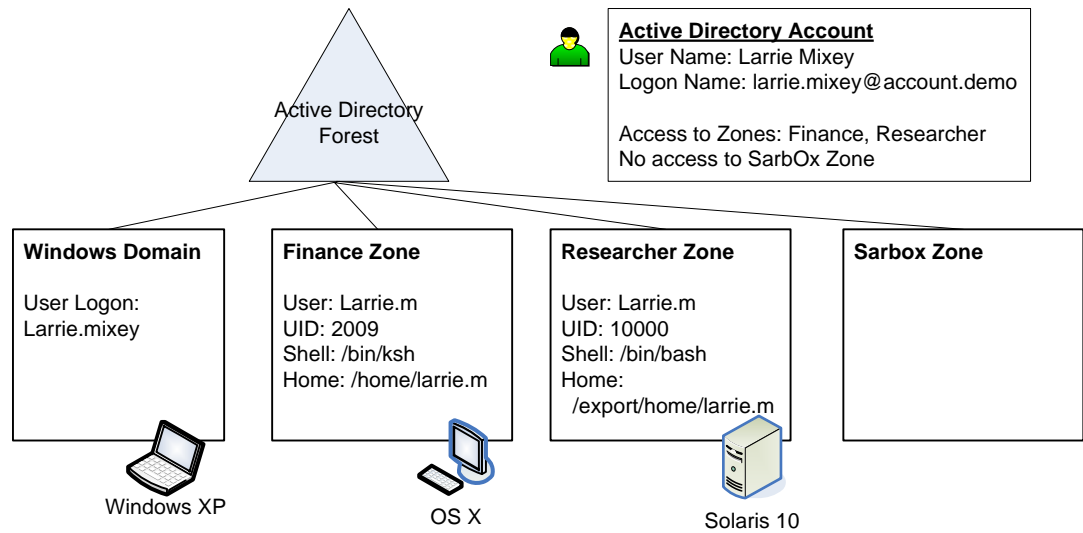


Figure 2-3

Illumi Clinics has defined multiple Zones within their Active Directory; this white paper focuses on just three Zones:

- Finance: a Zone primarily used by financial analysts, actuaries, comptrollers, and executives within the Finance department. This is a mixed Zone with Mac OS X workstations and Red Hat Enterprise Linux servers. The default Active Directory group for this Zone is:

```
cn=finance users, ou=finance, dc=illumi clinics, dc=com
```
- Researcher: a test Zone, composed primarily of Solaris servers, which is owned by the Engineering department but accessed by personnel in other departments. The default Active Directory Group for this Zone is:

```
cn=engineering users, ou=engineering, dc=illumi clinics, dc=com.
```
- Sarbox: a Zone designed to ensure compliance with Sarbanes-Oxley requirements. Access is limited to designated personnel. The default Active Directory Group for this Zone is:

```
ou=finance security, ou=finance, dc=illumi clinics, dc=com.
```

2.3 Solution: Role-Based Provisioning

The Identity Management Server in place at Illumi Clinics features role-based provisioning. Also known commonly as rules-based provisioning or access management, this feature automatically provisions employee accounts based on their job role as defined in the HR System. The employee's role is thus used to control which systems the employee may access.

For example, two job roles defined at Illumi Clinics are those of accountant and auditor. Figure 2-4 shows the updated provisioning sequence for an accountant and Figure 2-5 shows the updated provisioning sequence for an auditor.

The Portal Server has been DirectControl-enabled using the Apache Module and is configured to allow any valid Active Directory user access to basic applications. However, the Financial Auditing Dashboard application has been configured (in an `.htaccess` file) to allow only members of the Finance Security Active Directory group access to the Dashboard application, as follows:

```
Require group "illumi clinics.com/finance/finance security"
```

The UNIX accounting workstations and the UNIX Auditing Server are members of the Finance Zone. All Active Directory Users with UNIX profiles in the Finance Zone may access the UNIX accounting workstations. However, the UNIX Auditing Server has been configured (in `centrifydc.conf`) to only allow members of the Finance Security Active Directory group access, as follows:

```
pam.allow.groups: "illumi clinics.com/finance/finance security"
```

Benefits of this Solution

1. One password stored in Active Directory, regardless of the resource being accessed.
2. Centralized, consistent, real-time provisioning across the enterprise.
3. Simplified provisioning of web applications and UNIX computers.
4. Simplified, centralized authorization for web applications and UNIX computers. Adding an Active Directory user to an Active Directory group can grant additional privileges to users which require no additional configuration.
5. Increased Oracle Database security by removing weak passwords in favor of Kerberos.

2.3.1 Solution: Provisioning an Accountant

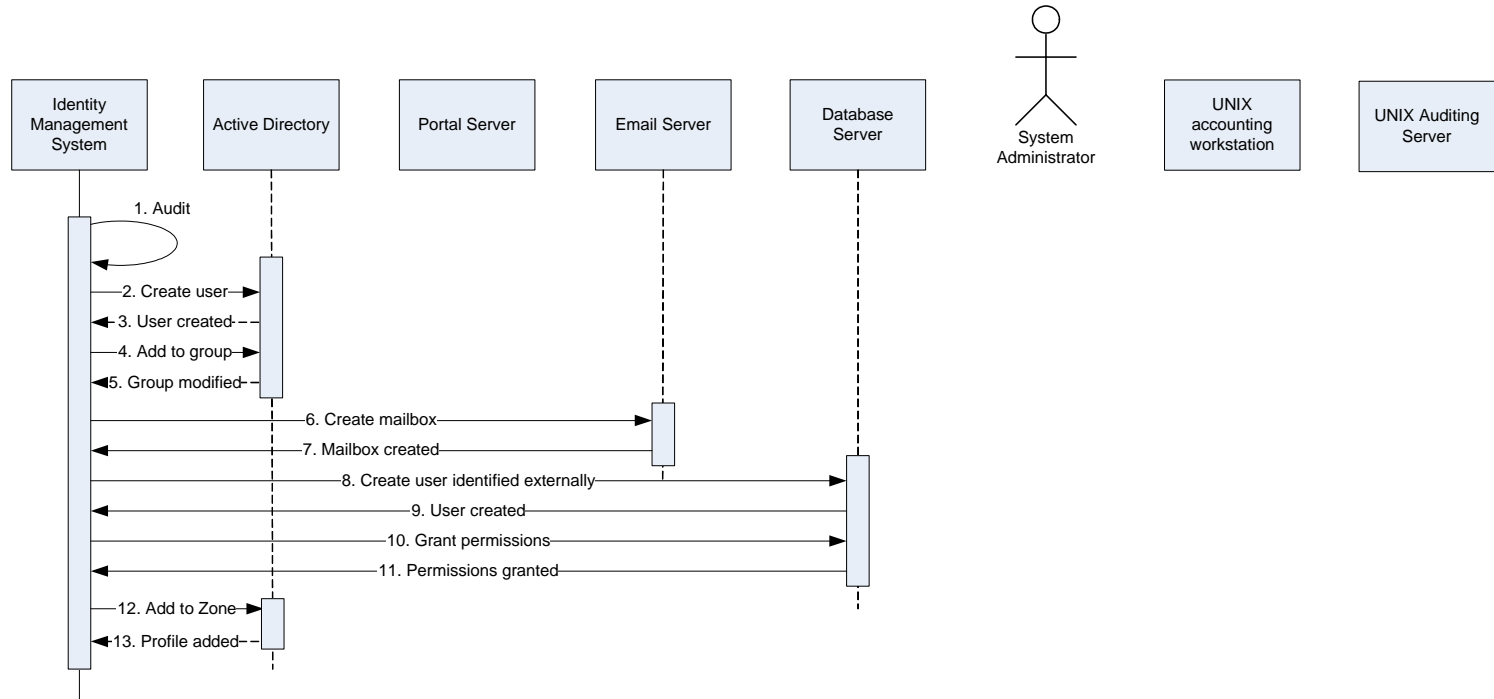


Figure 2-4

Sequence Description: Provisioning an Accountant

1. The Identity Management Server writes an audit record to the Audit Database.
2. The Identity Management Server creates an Active Directory user object for the new accountant; and,
3. The add operation succeeds.
4. The Identity Management Server adds the new Active Directory user object to an existing Finance Users Active Directory group; and,
5. The modify operation succeeds.
6. The Identity Management Server allocates storage for the new accountant's Exchange mailbox; and,
7. The mailbox is created.
8. The Identity Management Server creates a new Oracle user without a password on the Oracle Database Server. Rather, the new accountant user is identified externally by their Kerberos ticket from Active Directory; and,
9. The user is created on Oracle successfully.
10. The Identity Management Server uses SQL GRANT statements to set up the accountant's permissions on the Oracle Database; and,
11. The GRANT statements succeed.
12. The Identity Management Server adds the new accountant's Active Directory user object to the Finance Zone; and,
13. The UNIX profile is created.

2.3.2 Solution: Provisioning an Auditor

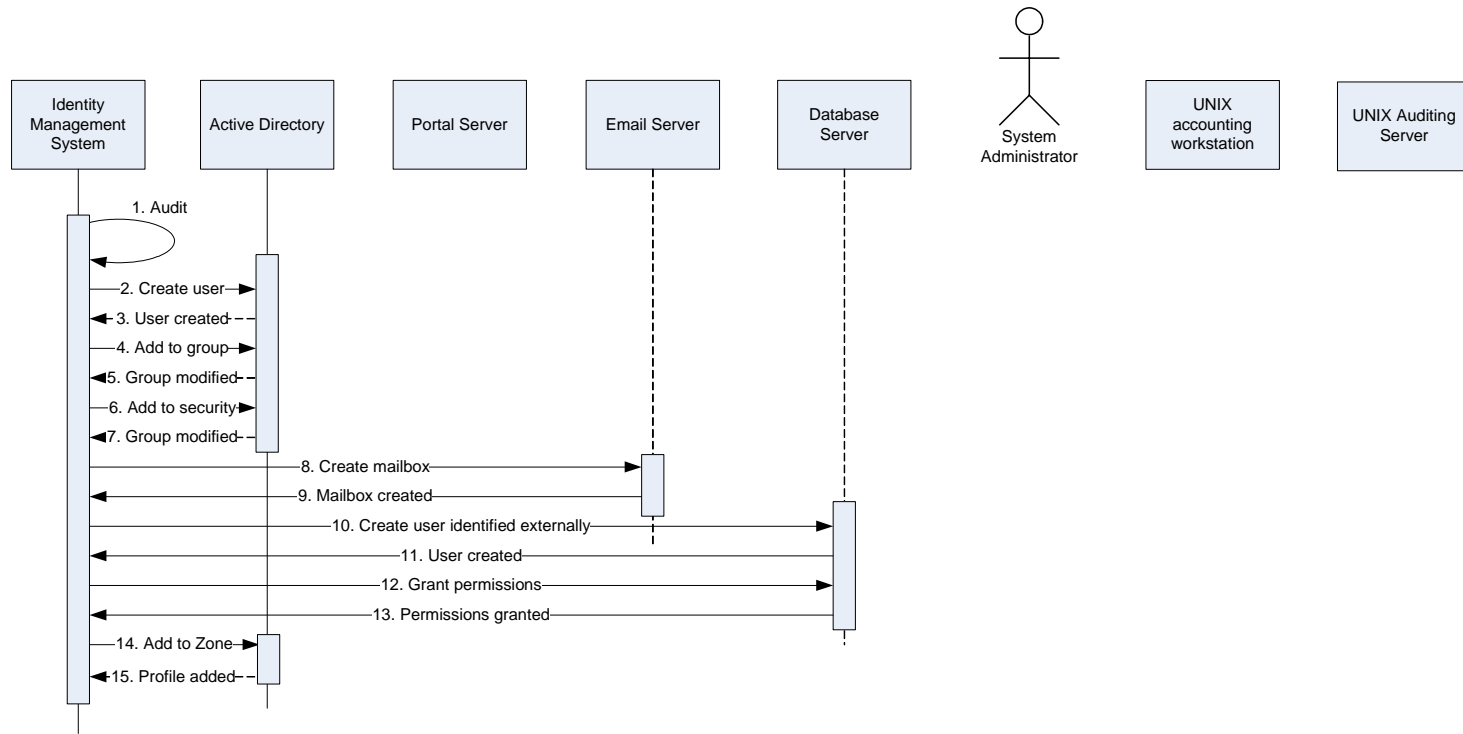


Figure 2-5

Sequence Description: Provisioning an Auditor

1. The Identity Management Server writes an audit record to the Audit Database.
2. The Identity Management Server creates an Active Directory user object for the new auditor; and,
3. The add operation succeeds.
4. The Identity Management Server adds the new Active Directory user object to the existing Finance Users Active Directory group; and,
5. The modify operation succeeds.
6. The Identity Management Server adds the new Active Directory user object to an existing Finance Security Active Directory group; and,
7. The modify operation succeeds.
8. The Identity Management Server allocates storage for the new auditor's Exchange mailbox; and,
9. The mailbox is created.
10. The Identity Management Server creates a new Oracle user without a password on the Oracle Database Server. Rather, the new Auditor is identified externally by their Kerberos ticket; and,
11. The user is created on Oracle successfully.
12. The Identity Management Server uses SQL GRANT statements to set up the auditor's permissions on the Oracle Database; and,
13. The GRANT statements succeed.
14. The Identity Management Server adds the new auditor's Active Directory User object to the Finance Zone; and,
15. The UNIX profile is created.

3 Identity Management Components

3.1 Connectors

The majority of commercial off-the-shelf Identity Management Systems use external connectors to provision data in other systems within an organization. These connectors may be native code built directly into the Identity Management System, they may be third-party components that extend the system, or they may be customized source code (either as scripts or as binaries). Connectors typically exist for provisioning mainframes, databases, operating environments, directory servers, and major applications.

In order to integrate Centrify DirectControl with an Identity Management System, one of the following requirements must be met:

- The Identity Management System must be able to call either .NET or COM objects as part of a connector; or,
- The Identity Management System must provide an LDAP connector that can bind to Active Directory.

It is highly recommended to use the DirectControl Software Developer's Kit (SDK) to build connectors using the COM/.NET objects. These objects are maintained by Centrify and effectively future-proof your Identity Management System from future modifications to Zone structures, user and group structures, and other operational changes. Alternatively, the majority of common Identity Management Systems provide native LDAP connectors which are compatible with Active Directory.

All examples in this white paper provide two formats for a given transaction:

- VBScript, for those Identity Management Systems which can call COM/.NET objects.
- LDIF, for those Identity Management Systems with an LDAP connector. The LDIF shows both the necessary transaction type (`changetype:`) as well as the attributes and example values.

3.1.1 Data Storage in Active Directory

There are three possible Zone types that may be defined within Active Directory:

- Standard
- Standard RFC-2307
- Services for UNIX

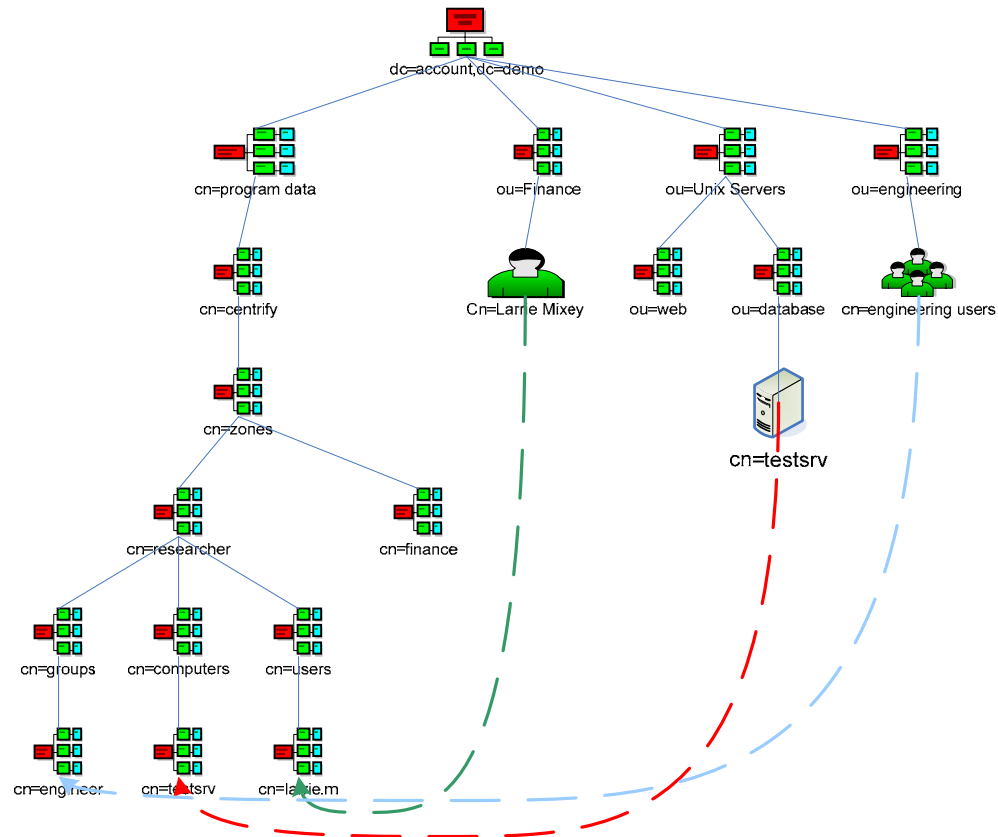


Figure 3-1

The diagram shows the logical layout of a Standard Zone or a RFC-2307 Standard Zone in Active Directory. A Zone is a separate branch of the directory. The top-level branch is an Active Directory container with the same name as the Zone; the Zone attributes are stored in attributes of this container. Below this there are several sub-containers:

- Users: this contains the users of the Zone
- Groups: this contains the groups in the Zone
- Computers: this contains the computers in the Zone.

In each case, the object in the sub-containers are serviceConnectionPoint (SCP) objects. They contain the DirectControl-extended data for each type of object (user, group, and computer). There

are links from the SCP object back to the parent objects (shown as dotted lines). These are maintained in the ParentLink pseudo-attribute (stored in the Keywords attribute) which stores the objectSID attribute value of the parent Active Directory object.

- The user and group are shown in the same OU, but this is not a requirement.
- The Zone tree does not need to be in the same domain as the user or the computers.
- The separation of the Zone data into a separate tree is what allows the delegation of administration; the UNIX data for each Zone is separate from the other Zones and form the base Active Directory objects for the users and groups.
- A user and a group can be associated with many Zones.

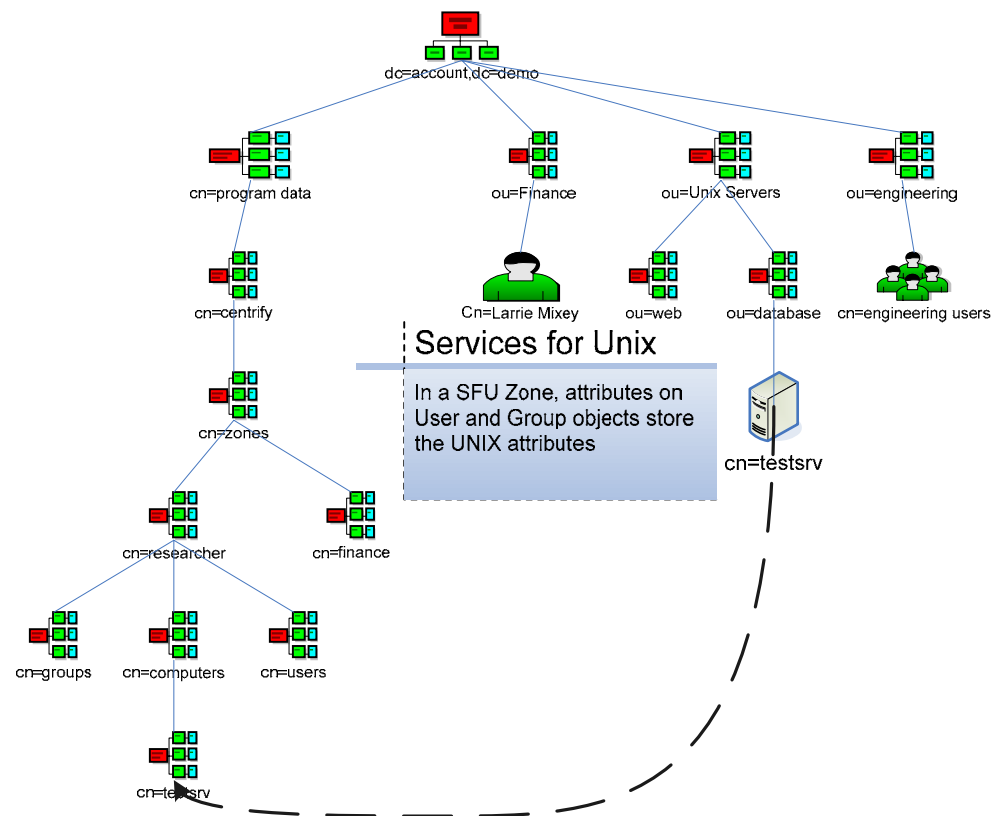


Figure 3-2

In a Services for UNIX Zone, UNIX attributes are stored as part of the individual Active Directory user and group objects. A user may only be associated with one SFU Zone. For example, Larrie Mixey's record would be extended with the following attributes (assuming the SFU name is 'research'):

```
uid: larrie.m
msSFU30Ni sDomain: research
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/larrie.m
loginShell: /bin/bash
```

3.2 Agents or Agentless

All major Identity Management Systems use one of two primary architectures for provisioning data on remote network elements:

Agents: Agent-based Identity Management Systems use executable processes running on the remote network element. These elements receive commands from the Identity Management Server and perform tasks on the remote network element; for example, a web server agent could provision user information on a web server.

Agentless: Agentless Identity Management Systems use native network protocols to connect to and provision remote network elements. For example, most Identity Management Systems can provision LDAP servers natively.

The Centrify DirectControl solution is primarily an Agent-based solution, and the deployment at Illumi Clinics is typical and illustrative of this architecture.

Active Directory is the sole source of authentication and authorization data using DirectControl. The Centrify DirectControl Agent is installed on UNIX and Linux computers. The deployment at Illumi Clinics uses the DirectControl Agent for HP-UX 11.23, Sun Solaris 9 and 10, and Red Hat Enterprise Linux 3 and 4.

The Centrify Software Developer's Kit (SDK) for Windows must be installed on Windows if it is to be used for provisioning; refer to section 3.1 for further details. However, no software is required nor recommended to execute on Windows Domain Controllers.

If an agentless architecture is required, the optional Centrify DirectControl NIS Service can be installed and UNIX and Linux computers can be configured to use NIS for authentication. This NIS authentication cannot be extended to database servers or web servers.

The Centrify DirectControl Module must be installed on the Apache web server, as well as the DirectControl Agent for Apache. Similarly, both the DirectControl Agent and the DirectControl Module for Oracle must be installed on the Oracle Database Server.

3.3 Passwords

Centrify DirectControl is *not* a password synchronization solution. DirectControl centralizes authentication and authorization data in Active Directory. DirectControl also removes insecure, weak password-based authentication and replaces it with secure Kerberos v5-based authentication. Refer to section 2.2 for further details.

3.4 Reporting

The Centrify DirectControl Administrator Console for Windows provides the following customizable reports:

- Users Report
- Groups Report
- Computer Report
- Zones Report
- Application Report
- User Account Report
- Computer Access Report
- Delegation Report

All data is stored in Active Directory. Many common Identity Management Systems can report on data stored in a LDAP server, and as such, additional integration with your Identity Management System's existing reports is possible.

4 Identity Management Events

4.1 Employee

This section describes commonly handled events by Identity Management Systems.

The Identity Management Server at Illumi Clinics defines all personnel who work at Illumi Clinics as employees. This basic definition is further extended by roles such as Actuary, Engineer, Compliance Officer, Executive, and so on. These roles define not only which servers are provisioned by the Identity Management Server but also what data is provisioned. For example, an Engineer and an Actuary have different job activities and as such would have access to different databases on the Oracle Database Server.

Note: These examples focus solely on the necessary provisioning operations so that DirectControl will be integrated with the Identity Management Server. As such, events such as the creation of Active Directory user and group objects, specific GRANT statements for databases and stored procedures, provisioning of the Exchange mailbox, and so on are outside the scope of this document. All examples show four ways of provisioning the UNIX profile in Active Directory:

1. Using COM/.NET objects: if the DirectControl SDK is being used by the Identity Management Server

Using LDAP: these are separated by Zone type and are shown as LDIF with correct line breaks and hyphenation

2. Standard Zone
3. Services for UNIX Zone
4. RFC 2307 Zone

Additionally, all pertinent examples show database provisioning commands for Oracle.

4.1.1 Hiring

Add to Zones

This example shows how to provision a UNIX profile for a new employee in the Researcher Zone, and how to create an Oracle account for the new employee.

On Monday, Illumi Clinics hired a new employee named Larrie Mixey. Larrie, an actuary from Bethel Park, PA, has ten years experience as an actuary, and was previously a software tester. Illumi Clinics has recently completed a complex Sarbanes-Oxley compliance project and is currently working on an industry-specific compliance project which will also use DirectControl. During his hiring process, Larrie was selected to work on the research project to determine if DirectControl will also be suitable for the industry-specific research project.

Larrie's manager worked with the Human Resources department to get his electronic files created in the HR System. Larrie's manager then worked with the Engineering department to allow Larrie to work on the research project, and this was also added to the HR System.

The Identity Management Server received the notification from the HR System and provisioned the following items:

1. An Active Directory user object, which is a member of the Finance Users Active Directory group.
2. UNIX profiles for Larrie in the Finance and Researcher Zones.
3. A new Exchange mailbox.
4. A new Oracle Database account, with access granted to several databases.

No data was provisioned to the Portal Server as it uses Active Directory for user authentication.

1. Using COM / .NET Objects

```
Set obj RootDSE = GetObject("LDAP://rootDSE")
set obj Container = GetObject("LDAP://cn=zones, CN=Centrify, CN=Program Data, " &
obj RootDSE. Get("defaultNamingContext"))
strContainerDN = obj Container. get("DistinguishedName")
set ci ms = CreateObject("Centrify.DirectControl.Cims")
Set obj User = ci ms. GetUserByPath("CN=Larrie
Mickey, OU=Finance, Dc=Illumiclinics, dc=com")
Set obj Zone = ci ms. GetZoneByPath("cn=researcher, " & strContainerDN)
set obj UserUnixProfiles = obj User. UnixProfiles
set obj UserUnixProfile = obj UserUnixProfiles. Find(obj Zone)
If obj UserUnixProfile is nothing Then
    set obj DefaultGroup = obj Zone. DefaultGroup
    lngGID = obj DefaultGroup. gid
    lngUID = obj Zone. nextAvailableUID
    strShell = obj Zone. defaultShell
    strHome = obj Zone. defaultHomeDirectory
    set obj UserUnixProfile = obj User. AddUnixProfile(obj Zone, lngUID,
"larrie.m", strShell, strHome, lngGID, False)
    obj UserUnixProfile. UnixEnabled = True
    obj User. Commit
end If
```

Using LDAP

2. Standard Zone

```
dn: CN=larrie.m, CN=Users, CN=Researcher, CN=Zones, CN=Centrify, CN=Program
Data, Dc=Illumiclinics, dc=com
changetype: add
objectclass: top
objectclass: leaf
objectclass: connectonPoint
objectclass: serviceConnectonPoint
cn: larrie.m
displayname: $CimsUserVersion2
showlnAdvancedViewOnly: TRUE
name: larrie.m
```

```

keywords: uid: 10000
keywords: home: /home/larrie.m
keywords: foreign: False
keywords: gid: 10000
keywords: unix_enabled: True
keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2120
keywords: shell: /bin/bash
managedBy: CN=Larrie Mikey, OU=Finance, Dc=illumini cs, dc=com
objectCategory: CN=Service-Connection-Point, CN=Schema, CN=Configuration, Dc=illumini cs, dc=com

```

3. Services for UNIX (SFU) Zone

```

dn: CN=Larrie Mikey, OU=Finance, Dc=illumini cs, dc=com
changetype: modify
add: uid
uid: larrie.m
-
add: msSFU30NisDomain
msSFU30NisDomain: research
-
add: uidNumber
uidNumber: 10000
-
add: gidNumber
gidNumber: 10000
-
add: unixHomeDirectory
unixHomeDirectory: /home/larrie.m
-
add: loginShell
loginShell: /bin/bash

```

4. RFC 2307 Zone

```

dn: CN=larrie.m, CN=Users, CN=Researcher, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illumini cs, dc=com
changetype: add
objectClass: top
objectClass: posixAccount
objectClass: leaf
objectClass: connectionPoint
objectClass: serviceConnectionPoint
cn: larrie.m
displayName: $CimsUserVersion3
showAdvancedViewOnly: TRUE
name: larrie.m
keywords: foreign: False
keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2120
keywords: unix_enabled: True
managedBy: CN=Larrie Mikey, OU=Finance, Dc=illumini cs, dc=com
objectCategory: CN=Service-Connection-Point, CN=Schema, CN=Configuration, Dc=illumini cs, dc=com
uid: larrie.m
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/larrie.m
loginShell: /bin/bash

```

Oracle

```
create user "LARRIE.MI XEY@ILLUMI CLINI CS.COM" identi fied external ly;
grant connect, resource to "LARRIE.MI XEY@ILLUMI CLINI CS.COM";
```

4.1.2 Add User to Active Directory Groups

This example shows how to create a UNIX profile for an Active Directory group.

Cedar Pirl, the engineering manager at Illumi Clinics, has defined the basic UNIX group of the Researcher Zone to be engineer. This group corresponds to the Engineering Users Active Directory group. Larrie, the new actuary from Finance, isn't a member of the Engineering Users group, and he's the first volunteer from the Finance department. So that the file permissions are correct, Cedar wants there to be a 'finance' UNIX group defined in the Researcher Zone. Larrie's primary UNIX group will still be 'engineer'.

This step would only need to be performed once. Larrie is already a member of the Finance Users Active Directory group, and all that needs to be done is for that group to be defined in the Researcher Zone.

1. Using COM / .NET Objects

```
Set obj RootDSE = GetObj ect("LDAP://rootDSE")
set obj Contai ner = GetObj ect("LDAP://cn=zones, CN=Centri fy, CN=Program Data, " &
obj RootDSE. Get("defaul tNami ngContext"))
strContai nerDN = obj Contai ner. get("Di sti ngui shedName")
set ci ms = CreateObj ect("Centri fy. Di rectControl . Ci ms")
Set obj Group = ci ms. GetGroupByPath("CN=Fi nance
Users, OU=Fi nance, Dc=i l l u m i c l i n i c s, dc=com")
Set obj Zone = ci ms. GetZoneByPath("cn=researcher" & ", " & strContai nerDN)
set obj GroupUni xProfi les = obj Group. Uni xProfi les
set obj GroupUni xProfi le = obj GroupUni xProfi les. Fi nd(obj Zone)
If obj GroupUni xProfi le is nothi ng then
    set obj GroupUni xProfi le = obj Group. AddUni xProfi le(obj Zone, "5000", "fi nance")
    obj Group. Commi t
    obj GroupUni xProfi le. Commi t
    Wscri pt. Echo "Added group"
end If
```

Using LDAP

2. Standard Zone

```
dn: CN=fi nance, CN=Groups, CN=Researcher, CN=Zones, CN=Centri fy, CN=Program
Data, Dc=i l l u m i c l i n i c s, dc=com
changetype: add
obj ectCl ass: top
obj ectCl ass: leaf
obj ectCl ass: connecti onPoi nt
obj ectCl ass: servi ceConnecti onPoi nt
cn: fi nance
di spl ayName: $Ci msGroupVersi on2
showI nAdvancedVi ewOnl y: TRUE
name: fi nance
keywords: gi d: 5000
keywords: forei gn: Fal se
```

keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2125
 managedBy: CN=Finance Users, OU=Finance, Dc=illuminics, dc=com
 objectCategory: CN=Service-Connection-Point, CN=Schema, CN=Configuration, Dc=illuminics, dc=com

3. Services for UNIX (SFU) Zone

dn: CN=Finance Users, OU=Finance, Dc=illuminics, dc=com
 changetype: modify
 add: msSFU30Ni sDomain
 msSFU30Ni sDomain: research
 -
 add: gidNumber
 gidNumber: 5000

4. RFC 2307 Zone

dn: CN=Finance, CN=Groups, CN=Researcher, CN=Zones, CN=Centrify, CN=Program
 Data, Dc=illuminics, dc=com
 changetype: add
 objectClass: top
 objectClass: posixGroup
 objectClass: leaf
 objectClass: connectionPoint
 objectClass: serviceConnectionPoint
 cn: finance
 displayName: \$CimsGroupVersion3
 showAdvancedViewOnly: TRUE
 name: finance
 keywords: foreign: False
 keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2125
 managedBy: CN=Finance Users, OU=Finance, Dc=illuminics, dc=com
 objectCategory: CN=Service-Connection-Point, CN=Schema, CN=Configuration, Dc=illuminics, dc=com
 gidNumber: 5000

Oracle

Active Directory group membership does not affect Larrie's Oracle account, so there is no provisioning transaction required.

4.1.3 Promotion / Demotion

Change Zones

This example shows how to modify a user's UNIX profiles.

Two months later, Larrie received a letter of commendation from Cedar for his great work on the research project, which was wrapping up. As a result of this and his strong work as an actuary, Larrie's manager promotes him to work on Sarbanes-Oxley compliance projects. This information was entered into the HR Database.

When the Identity Management Server receives the change notification, it will remove Larrie's UNIX profile from the Researcher Zone and add a profile to the Sarbox Zone. Additionally,

Larrie's Active Directory group membership will be modified to include the Finance Security group; see 4.1.4 for details.

1. Using COM / .NET Objects

```
Set objRootDSE = GetObject("LDAP://rootDSE")
set objContainer = GetObject("LDAP://cn=zones, CN=Centrify, CN=Program Data, " &
objRootDSE.Get("defaultNamingContext"))
strContainerDN = objContainer.get("DistinguishedName")
set cims = CreateObject("Centrify.DirectControl.Cims")
Set objUser = cims.GetUserByPath("CN=Larrie
Mikhey, OU=Finance, Dc=illumini cs, dc=com")
Set objZone = cims.GetZoneByPath("cn=researcher, " & strContainerDN)
set objUserUnixProfiles = objUser.UnixProfiles
set objUserUnixProfile = objUserUnixProfiles.Find(objZone)
objUser.RemoveUnixProfile objZone
objUser.Commit
Set objZone = cims.GetZoneByPath("cn=sarbox, " & strContainerDN)
If objUserUnixProfile is nothing Then
    set objDefaultGroup = objZone.DefaultGroup
    lngGID = objDefaultGroup.gid
    lngUID = objZone.nextAvailableUID
    strShell = objZone.defaultShell
    strHome = objZone.defaultHomeDirectory
    set objUserUnixProfile = objUser.AddUnixProfile(objZone, lngUID,
"larrie.m", strShell, strHome, lngGID, False)
    objUserUnixProfile.UnixEnabled = True
    objUser.Commit
end If
```

Using LDAP

2. Standard Zone

```
dn: CN=Larrie.m, CN=Users, CN=researcher, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illumini cs, dc=com
changetype: delete
```

```
dn: CN=Larrie.m, CN=Users, CN=sarbox, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illumini cs, dc=com
changetype: add
objectClass: top
objectClass: leaf
objectClass: connectionPoint
objectClass: serviceConnectionPoint
cn: Larrie.m
displayName: $CimsUserVersion2
showAdvancedViewOnly: TRUE
name: Larrie.m
keywords: uid: 10000
keywords: home: /home/Larrie.m
keywords: foreign: False
keywords: gid: 10000
keywords: unix_enabled: True
keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2120
keywords: shell: /bin/bash
managedBy: CN=Larrie Mikhey, OU=Finance, Dc=illumini cs, dc=com
objectCategory: CN=Service-Connection-
Point, CN=Schema, CN=Configuration, Dc=illumini cs, dc=com
```

3. Services for UNIX (SFU) Zone

Note: this requires the ‘research’ SFU NIS domain and ‘researcher’ Zone to be removed from Active Directory and a new ‘Sarbox’ SFU NIS domain to be created in its place. Services for UNIX has a limitation of a single Zone within a given domain.

```
dn: CN=Larrie Mikey,OU=Finance,Dc=illumincs,dc=com
changetype: modify
replace: msSFU30NISDomain
msSFU30NISDomain: sarbox
```

4. RFC 2307 Zone

```
dn: CN=Larrie.m,CN=Users,CN=researcher,CN=Zones,CN=Centrify,CN=Program
Data,Dc=illumincs,dc=com
changetype: delete
```

```
dn: CN=Larrie.m,CN=Users,CN=sarbox,CN=Zones,CN=Centrify,CN=Program
Data,Dc=illumincs,dc=com
changetype: add
objectClass: top
objectClass: posixAccount
objectClass: leaf
objectClass: connectionPoint
objectClass: serviceConnectionPoint
cn: Larrie.m
displayName: $CimsUserVersion3
showAdvancedViewOnly: TRUE
name: Larrie.m
keywords: foreign: False
keywords: parentLink: S-1-5-21-2297767280-3401545478-3115491676-2120
keywords: unix_enabled: True
managedBy: CN=Larrie Mikey,OU=Finance,Dc=illumincs,dc=com
objectCategory: CN=Service-Connection-
Point,CN=Schema,CN=Configuration,Dc=illumincs,dc=com
uid: Larrie.m
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/Larrie.m
loginShell: /bin/bash
```

Oracle

Larrie’s Oracle user account was not changed as a result of this promotion. While his database access may have changed, these are additional GRANT statements and are not within the scope of this white paper.

4.1.4 Change Active Directory Groups

This example shows how to add an Active Directory user to an Active Directory group and is a continuation of section 4.1.3. As the Finance Security group is already defined in Active Directory and has a UNIX profile in the Sarbox Zone, very little needs to be done.

1. Using COM / .NET Objects

```
set objGroup = GetObject("LDAP://cn=finance
security,ou=finance,dc=illumclinics,dc=com")
objGroup.Add("LDAP://cn=Larrie Mixey,ou=finance,dc=illumclinics,dc=com")
```

Using LDAP

2. Standard Zone

```
dn: cn=finance security,ou=finance,dc=illumclinics,dc=com
changetype: modify
add: member
member: cn=Larrie Mixey,ou=finance,dc=illumclinics,dc=com
```

Services for UNIX (SFU) Zone or RFC 2307 Zone

These are identical to the Standard Zone example.

Oracle

Larrie's Oracle user account was not changed as a result of this group change.

4.1.5 Marriage / Divorce

This example shows the effect of a surname change.

Several months go by at Illumi Clinics and Larrie gets married to an engineer named Alyssia Osteen. Alyssia changes her last name to Mixey, and the HR System is updated. This renames Alyssia's Active Directory user object to Alyssia Mixey, and her new User Principal Name is Alyssia.Mixey@illumclinics.com.

As the company policy at Illumi Clinics is for users to log in using their User Principal Name, there is no further change required for the UNIX systems or the Apache web server.

Oracle

Per Oracle's recommendations, Illumi Clinics re-creates user accounts upon a rename. This only shows how to recreate the user account; there are additional GRANT statements for access to tables, stored procedures, etc.

```
drop user "ALYSSIA.OSTEEN@ILLUMICLINICS.COM" cascade;
create user "ALYSSIA.MIXEY@ILLUMICLINICS.COM" identified externally;
grant connect, resource to "ALYSSIA.MIXEY@ILLUMICLINICS.COM";
```

4.1.6 Unauthorized Access Detection and Prevention

This example describes how to detect and prevent unauthorized access.

An Active Directory administrator leaves his Windows XP workstation unlocked and walks away for an hour-long meeting. During that hour, Larrie Mixey uses the workstation to create a UNIX

profile for himself in the Engineering Zone. This would normally give Larrie access to all engineering UNIX servers and workstations. Larrie then closes the windows and moves the mouse back to where he'd found it, thinking that he had covered his tracks.

Centrify DirectControl prevents unauthorized access by limiting those UNIX computers that an employee may access. DirectControl's Zone technology controls authorization; if an employee does not have access to a Zone, they may not access the UNIX computers in that Zone.

DirectControl also provides Group Policies for finer-grained allow/deny criteria based on Active Directory users or Active Directory group membership. This allows individuals or all computers within a Zone to require (for example) membership in a specific Active Directory group in order to access the UNIX computer. Additional Group Policies control the use of sudo, which restricts both the use of the root account as well as those commands which are available. In the previous example, the engineering UNIX servers that contained new product designs were configured to deny anyone who is not a member of the "Engineering Design" Active Directory group.

Additionally, some Identity Management Systems provide native facilities for monitoring or preventing changes to Active Directory. If your Identity Management System does not include a method of detecting or preventing unauthorized changes to Active Directory, a third-party tool such as NetPro ChangeAuditor 3.0 for Active Directory can be used. The goals are to verifiably establish:

- Who made the change
- What the change was, including new and previous values
- When the change was made
- Where the change was made
- Why the change was made

Recommendations on Monitoring Active Directory

Standard Zone or 2307 Zone

These Zone types store UNIX user profiles as ServiceConnectionPoint objects under the Users container in each Zone. Monitor the creation, deletion, and modification of these objects.

Services for UNIX Zone

This Zone type stores UNIX profiles on individual Active Directory user and group objects. Monitor the following attributes on user objects:

```
ui d:  
msSFU30Ni sDomai n:  
ui dNumber:  
gi dNumber:  
uni xHomeDi rectory:  
l ogi nShel l :
```

Oracle

The Oracle Database Server provides a number of reporting and management facilities. Monitor the use of CREATE USER statements, particularly those that specify “identified externally.” Additionally, monitor GRANT statements closely.

4.1.7 Termination

Disable Active Directory Account

This example shows two possible ways of handling the termination of an employee. Preventing access to systems and the deletion of the former employee’s accounts is discussed.

Larrie’s unauthorized access to the UNIX servers where the new product designs were stored was thwarted by the group membership requirement, and then detected by the Identity Management Server’s auditing feature. Illumi Clinics has a strict policy regarding unauthorized computer access and fired Larrie. Upon employee termination, Illumi Clinics has a two-phase process:

1. Disable the user’s Active Directory account. Because all computing resources (except the Exchange server) are using DirectControl, this disables the former employee’s access to the Portal, the Oracle Database Server, and all UNIX computers. Exchange Server uses Active Directory as well, thus disabling access to the former employee’s email. Another employee is assigned ownership of the former employee’s files; in this example, Cedar Pirl will take ownership of Larrie’s files.
2. After one year, Illumi Clinics deletes the former employee’s Active Directory account.

1. Using COM / .NET Objects

```
set obj User = GetObject("LDAP://cn=Larrie mikey,ou=finance,dc=illumi clinics,dc=com")
obj User.AccountDisabled = TRUE
obj User.SetInfo
```

Using LDAP

Standard Zone, 2307 Zone, SFU Zone

This involves adding the number “2” to the existing userAccountControl attribute value. For example, if Larrie’s userAccountControl value were 66048 when the account was enabled, disabling the account would involve setting userAccountControl to 66050.

```
dn: cn=Larrie mikey,ou=finance,dc=illumi clinics,dc=com
changetype: modify
replace: userAccountControl
userAccountControl: 66050
```

File Ownership

This example focuses on UNIX file ownership when a UNIX profile has been disabled or deleted from a Zone. This example does not cover Windows file ownership.

A UNIX user may have multiple files and directories stored across multiple UNIX systems. This can be true even in the case of shared home directory or fileserver. In the event of an employee suspension or termination, it is typically necessary to give ownership of those files to another employee. Historically this has been a challenge on UNIX-based systems because it involves reviewing and modifying the file permissions or ownership of an indeterminate number of files.

Centrify DirectControl includes a utility, `adfi xid`, which reduces the difficulties associated with massive file permission operations. `adfi xid` is a program which is installed on individual UNIX systems and must be executed on each affected UNIX system. This utility permits mapping a user defined on the local UNIX host to a user defined in the Zone.

Follow these steps on each UNIX system to change the UNIX file ownership for all of Larrie's files to Cedar:

1. Create a mapping file to map Larrie's files to Cedar:

```
larrie.m cedar. pi
```

2. Using the editor of your choice, add a temporary account for Larrie in the `/etc/passwd` file:

```
larrie.m:x:10000:10000:Larrie Mikey:/home/larrie.m:/bin/bash
```

3. Run `adfi xid` in preview mode to preview the file system changes. The default behavior is preview mode, and note that the root file system was selected.

```
# adfi xid -u usermap.txt -V /
1 user-id conflict was found.
Local UID   Zone UID   User
-----
10000      10005     larrie.m/cedar.pi
No group-id conflicts were found.
```

4. Run `adfi xid` in commit mode and write the output to a file.

```
# adfi xid -u usermap.txt -V --commit --report output.txt /
adfi xid report - domain illumilincs.com
Date: Wed Oct 4 10:44:36 2006
Orig UID   New UID   Orig GID  New GID   File
-----
10000      10005     10000     10000     /home/larrie.m
10000      10005     10000     10000     /home/larrie.m/.kde
10000      10005     10000     10000     /home/larrie.m/.kde/Autostart
10000      10005     10000     10000     /home/larrie.m/.kde/Autostart/.directory
10000      10005     10000     10000     /home/larrie.m/.emacs
10000      10005     10000     10000     /home/larrie.m/.bash_logout
10000      10005     10000     10000     /home/larrie.m/.bash_profile
10000      10005     10000     10000     /home/larrie.m/.bashrc
10000      10005     10000     10000     /home/larrie.m/.gtkrc
10000      10005     10000     10000     /home/larrie.m/.k5login
10000      10005     10000     10000     /home/larrie.m/.bash_history
10000      10005     10000     10000     /home/larrie.m/Test Rich Text.rtf
10000      10005     10000     10000     /home/larrie.m/Test WordPad.doc
10000      10005     10000     10000     /home/larrie.m/Text Document.txt
10000      10005     10000     10000     /home/larrie.m/My UNIX Files
```

5. Remove larrie.m from /etc/passwd
6. At this point, Cedar now has access to the files which were previously owned by Larrie.

Deleting User Data from Active Directory

All of Larrie's UNIX profiles must be deleted along with his Active Directory user object. ADSI doesn't natively handle recursive deletes, unlike the Active Directory Users and Computers user interface.

1. Using COM / .NET Objects

```
Set obj RootDSE = GetObject("LDAP://rootDSE")
set obj Container = GetObject("LDAP://cn=zones, CN=Centrify, CN=Program Data, " &
obj RootDSE.Get("defaultNamingContext"))
set obj Parent = GetObject("LDAP://ou=finance, dc=illumination, dc=com")
strContainerDN = obj Container.get("DistinguishedName")
set cims = CreateObject("Centrify.DirectControl.Cims")
Set obj User = cims.GetUserByPath("CN=Larrie
Mixey, OU=finance, Dc=illumination, dc=com")
set obj UserUnixProfiles = obj User.UnixProfiles
For Each obj UserUnixProfile In obj User.UnixProfiles
    Set obj Zone = obj UserUnixProfile.Zone
    obj User.RemoveUnixProfile obj Zone
    obj User.Commit
Next
obj Parent.delete "user", "cn=Larrie Mixey"
```

Using LDAP

2. Standard Zone

```
dn: cn=larrie mixey, ou=finance, dc=illumination, dc=com
changetype: delete
```

```
dn: CN=larrie.m, CN=Users, CN=finance, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illumination, dc=com
changetype: delete
```

3. Services for UNIX (SFU) Zone

```
dn: cn=larrie mixey, ou=finance, dc=illumination, dc=com
changetype: delete
```

4. RFC 2307 Zone

```
dn: cn=larrie mixey, ou=finance, dc=illumination, dc=com
changetype: delete
```

```
dn: CN=larrie.m, CN=Users, CN=finance, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illumination, dc=com
changetype: delete
```

4.2 Mergers and Acquisitions

This section describes mergers and acquisitions, which are less-common events handled by Identity Management Servers.

Illumi Clinics purchased a privately held marketing firm, Greenmedia, based in Akron, Ohio. Greenmedia has an Active Directory 2003 forest, a small number of users, a number of Mac OS X desktop and laptop computers, and does not have Centrify DirectControl installed on any computers in their organization. Greenmedia had a small in-house user provisioning system that will be decommissioned in favor of the Identity Management Server at Illumi Clinics.

The engineering team at Illumi Clinics proposed the following acquisition strategy for integrating the users and groups from Greenmedia:

1. **Initial Integration:** Create a cross-forest trust between Illumi Clinics and Greenmedia. Next, create UNIX user profiles for selected Greenmedia personnel. These UNIX profiles will use the Marketing Zone (owned by Illumi Clinics) but Active Directory user objects for Greenmedia personnel will remain on the Greenmedia Active Directory servers.
2. **Group migration:** Using the Active Directory Migration Tool from Microsoft, migrate Active Directory Groups from Greenmedia to Illumi Clinics.
3. **User migration:** Next, use the Active Directory Migration Tool to migrate Active Directory Users from Greenmedia to Illumi Clinics.
4. **Consolidation:** Decommission Greenmedia hardware and software.

General recommendation: While it is possible to create UNIX profiles for selected Greenmedia personnel in advance of Active Directory user migration, this strategy has some limitations. These are discussed in full in section 4.2.3.

Note: These examples focus solely on the necessary provisioning operations so that DirectControl will be integrated with the Identity Management Server at Illumi Clinics. As such, events such as the creation of a two-way cross-forest trust, creation of Active Directory user and group objects, specific GRANT statements for databases and stored procedures, provisioning of the Exchange mailbox and so on are outside the scope of this document. All examples show four ways of provisioning the UNIX profile in Active Directory:

- Using COM/.NET objects: if the DirectControl SDK is being used by the Identity Management Server.
- Using LDAP: these examples are separated by Zone type (Standard, 2307, and Services for UNIX) and are shown as LDIF with correct line breaks and hyphenation.

4.2.1 Initial Integration

Preparation: The DNS servers at Illumi Clinics should be configured to forward queries for Greenmedia to the Greenmedia servers, and vice-versa. A two-way cross-forest trust must be created between Illumi Clinics and Greenmedia.

Adding UNIX Profiles for Active Directory Users from the Foreign Domain

This example shows how to add an Active Directory user from another Forest to a Zone.

Felix Hobbs, a marketing manager at Greenmedia, needs access to the Illumi Clinics Marketing Zone. The Marketing Zone contains several Oracle databases, an Apache webserver, and a number of OS X servers and workstations. The Marketing Zone MUST be either a Standard Zone or an RFC 2307 Zone; Active Directory does not support adding foreign users to Services for UNIX Zones.

The Apache web server in the Marketing Zone does not require additional provisioning or changes. The two-way cross-forest trust allows the Active Directory users from Greenmedia to automatically authenticate with their Kerberos credentials.

1. Using COM / .NET Objects

This is identical to the code shown in section 4.1.1; the only substantial change is the Distinguished Name of the Active Directory User object. In this case, the User object is stored on the Greenmedia Active Directory.

```
Set objRootDSE = GetObject("LDAP://rootDSE")
set objContainer = GetObject("LDAP://cn=zones, CN=Centrify, CN=Program Data, " &
objRootDSE.Get("defaultNamingContext"))
strContainerDN = objContainer.get("DistinguishedName")
set cims = CreateObject("Centrify.DirectControl.Cims")
Set objUser = cims.GetUserByPath("cn=Felix Hobbs, cn=Users, dc=Greenmedia, dc=Demo")
Set objZone = cims.GetZoneByPath("cn=Marketing, " & strContainerDN)
set objUserUnixProfiles = objUser.UnixProfiles
set objUserUnixProfile = objUserUnixProfiles.Find(objZone)
If objUserUnixProfile is nothing Then
    set objDefaultGroup = objZone.DefaultGroup
    lngGID = objDefaultGroup.gid
    lngUID = objZone.nextAvailableUID
    strShell = objZone.defaultShell
    strHome = objZone.defaultHomeDirectory
    set objUserUnixProfile = objUser.AddUnixProfile(objZone, lngUID,
"felix.ho", strShell, strHome, lngGID, False)
    objUserUnixProfile.UnixEnabled = True
    objUser.Commit
end If
```

Using LDAP

Using LDAP with foreign users introduces two substantial changes:

1. The managedBy attribute value is no longer used.
2. The Keywords attribute must now include "foreign: True".

2. Standard Zone

```
dn: CN=felix.ho, CN=Users, CN=Marketing, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illuminiacs, dc=com
changetype: add
objectClass: top
objectClass: leaf
objectClass: connectionPoint
objectClass: serviceConnectionPoint
cn: felix.ho
displayName: $CmsUserVersion2
showAdvancedViewOnly: TRUE
name: felix.ho
keywords: foreign: True
keywords: gid: 10000
keywords: unix_enabled: True
keywords: parentLink: S-1-5-21-445832693-776724510-3784369607-1106
keywords: uid: 10001
keywords: shell: /bin/bash
keywords: home: /home/felix.ho
objectCategory: CN=Service-Connection-
Point, CN=Schema, CN=Configuration, Dc=illuminiacs, dc=com
```

3. Services for UNIX (SFU) Zone

Services for UNIX Zones do not support foreign Active Directory user objects. The Active Directory user object for Felix Hobbs is stored in Greenmedia, and the Marketing Zone is stored in Illumi Clinics. This would be possible after the Active Directory User object for Felix Hobbs is migrated to Illumi Clinics.

4. RFC 2307 Zone

```
dn: CN=felix.ho, CN=Users, CN=Marketing, CN=Zones, CN=Centrify, CN=Program
Data, Dc=illuminiacs, dc=com
changetype: add
objectClass: top
objectClass: posixAccount
objectClass: leaf
objectClass: connectionPoint
objectClass: serviceConnectionPoint
cn: felix.ho
displayName: $CmsUserVersion3
showAdvancedViewOnly: TRUE
name: felix.ho
keywords: foreign: True
keywords: parentLink: S-1-5-21-445832693-776724510-3784369607-1106
keywords: unix_enabled: True
objectCategory: CN=Service-Connection-
Point, CN=Schema, CN=Configuration, Dc=illuminiacs, dc=com
uid: felix.ho
uidNumber: 10001
gidNumber: 10000
unixHomeDirectory: /home/felix.ho
loginShell: /bin/bash
```

Oracle

```
create user "FELIX.HOBBS@GREENMEDIA.NET" identified externally;
grant connect, resource to "GREENMEDIA.NET"
```

4.2.2 Group Migration

This example discusses Active Directory group migration from a source domain to a target domain.

The Marketing Active Directory group is the first group to be migrated per the engineering plan of record. Under the new business plan, Marketing will be a function of the Sales team at Illumi Clinics.

Using the Active Directory Migration Tool from Microsoft, the Marketing group from Greenmedia can be automatically migrated to Illumi Clinics, and the location moved to the Sales organizational unit in Active Directory. Group membership, however, was planned for a later phase and thus group members were not migrated.

Following the group migration, the new Active Directory group exists as CN=Marketing, OU=Sales, DC=IllumiClinics, dc=com. Because this is a regular Active Directory group, it can be added to the Marketing Zone using the same code (SDK code or LDIF) as in section 4.1.2 of this document.

4.2.3 User Migration

This example discusses Active Directory User migration from a source domain to a target domain.

As part of the acquisition deal, the staff of Greenmedia will become employees of Illumi Clinics. The Illumi Clinics HR Database is the system of record for the Identity Management Server in use at Illumi Clinics. The Identity Management Server at Illumi Clinics uses the Active Directory Migration Tool to migrate Active Directory user objects which must then be linked to records in the HR System. This is to preserve each user's former group membership, permissions, and other attributes.

The Active Directory Migration Tool allows selection of users from Greenmedia to be migrated to Illumi Clinics. As part of this migration, old Greenmedia Active Directory user objects will be disabled. The new Active Directory user objects will have new User Principal Name attributes; instead of Felix.Hobbs@Greenmedia.net, the UPN will become Felix.Hobbs@IllumiClinics.com. Finally, the Active Directory Migration Tool automatically generates new SIDs for the migrated Active Directory User objects and has the option to retain the SID history, which effectively preserves a user's permissions on the legacy Greenmedia Windows-based systems.

The requirement of Active Directory to generate a new objectSID value is the key limitation for those foreign users who had UNIX profiles created before their accounts were migrated. DirectControl uses the objectSID to link one or more UNIX profiles to a single Active Directory User object.

For example, Felix Hobbs had a UNIX profile created in the Marketing Zone at IllumiClinics.com. Felix Hobbs' Active Directory User object is then migrated from Greenmedia.net to IllumiClinics.com, and his Active Directory user object (at Greenmedia) is disabled. This

effectively will prevent Felix Hobbs from logging in on any Windows or UNIX computers as “Felix.Hobbs@Greenmedia.net”, because his Active Directory user object has been disabled.

Thus, when migrating Active Directory users, it is recommended to follow these steps:

1. Migrate the Active Directory user object, selecting appropriate options.
2. For each UNIX profile associated with the old Active Directory user object:
 - a. Copy all of the values (such as home directory, user name, user ID, group ID, and shell).
 - b. Delete the UNIX profile.
 - c. Create a new UNIX profile associated with the new Active Directory user object, using the previous values from the old UNIX profile.
3. Notify the user to login using their new UPN (or username, per corporate policy).

Note: this only affects migrated users who previously had UNIX profiles.

1. Using COM / .NET objects

This code finds all UNIX profiles associated with the old Greenmedia Active Directory User object and migrates them to the IllumiClinics.com Active Directory User object.

```

Set objRootDSE = GetObject("LDAP://rootDSE")
set objContainer = GetObject("LDAP://cn=zones, CN=Centrify, CN=Program Data, " &
objRootDSE.Get("defaultNamingContext"))
strContainerDN = objContainer.get("DistinguishedName")
set cims = CreateObject("Centrify.DirectoryControl.Cims")
Set objOldUser = cims.GetUserByPath("cn=Felix
Hobbs, cn=Users, dc=Greenmedia, dc=Demo")
Set objNewUser = cims.GetUserByPath("CN=Felix
Hobbs, OU=Sales, Dc=IllumiClinics, dc=com")
set objNewUserUnixProfiles = objNewUser.UnixProfiles
set objOldUserUnixProfiles = objOldUser.UnixProfiles
For Each objOldUserUnixProfile In objOldUser.UnixProfiles
    Set objZone = objOldUserUnixProfile.Zone
    lngUID = objOldUserUnixProfile.UID
    lngGID = objOldUserUnixProfile.GID
    strHome = objOldUserUnixProfile.HomeDirectory
    strName = objOldUserUnixProfile.Name
    strShell = objOldUserUnixProfile.Shell
    objOldUser.RemoveUnixProfile objZone
    objOldUser.Commit
    set objNewUserUnixProfile = objNewUser.AddUnixProfile(objZone,
lngUID, strName, strShell, strHome, lngGID, False)
    objNewUserUnixProfile.UnixEnabled = True
    objNewUser.Commit
Next

```

Using LDAP

2. Standard Zone

```
dn: CN=fel i x. ho, CN=Users, CN=marketi ng, CN=Zones, CN=Centri fy, CN=Program
Data, Dc=i l l umi cl i ni cs, dc=com
changetype: del ete
```

```
dn: CN=fel i x. ho, CN=Users, CN=marketi ng, CN=Zones, CN=Centri fy, CN=Program
Data, Dc=i l l umi cl i ni cs, dc=com
changetype: add
obj ectCl ass: top
obj ectCl ass: l eaf
obj ectCl ass: connecti onPoi nt
obj ectCl ass: servi ceConnecti onPoi nt
cn: fel i x. ho
di spl ayName: $Ci msUserVersi on2
showl nAdvancedVi ewOnl y: TRUE
name: fel i x. ho
keywords: ui d: 10001
keywords: home: /home/fel i x. ho
keywords: forei gn: Fal se
keywords: gi d: 10000
keywords: uni x_enabl ed: True
keywords: parentLi nk: S-1-5-21-2297767280-3401545478-3115491676-2120
keywords: shel l : /bi n/bash
managedBy: CN=Fel i x Hobbs, OU=Sal es, Dc=i l l umi cl i ni cs, dc=com
obj ectCategory: CN=Servi ce-Connecti on-
Poi nt, CN=Schema, CN=Confi gurati on, Dc=i l l umi cl i ni cs, dc=com
```

3. Services for UNIX (SFU) Zone

Services for UNIX Zones do not support foreign Active Directory user objects. Therefore, Felix Hobbs could not have a SFU Zone created before his Active Directory user object was migrated.

4. RFC 2307 Zone

```
dn: CN=fel i x. ho, CN=Users, CN=marketi ng, CN=Zones, CN=Centri fy, CN=Program
Data, Dc=i l l umi cl i ni cs, dc=com
changetype: del ete
```

```
dn: CN=fel i x. ho, CN=Users, CN=marketi ng, CN=Zones, CN=Centri fy, CN=Program
Data, Dc=i l l umi cl i ni cs, dc=com
changetype: add
obj ectCl ass: top
obj ectCl ass: posi xAccount
obj ectCl ass: l eaf
obj ectCl ass: connecti onPoi nt
obj ectCl ass: servi ceConnecti onPoi nt
cn: fel i x. ho
di spl ayName: $Ci msUserVersi on3
showl nAdvancedVi ewOnl y: TRUE
name: fel i x. ho
keywords: forei gn: Fal se
keywords: parentLi nk: S-1-5-21-2297767280-3401545478-3115491676-2121
keywords: uni x_enabl ed: True
managedBy: CN=Fel i x Hobbs, OU=Sal es, Dc=i l l umi cl i ni cs, dc=com
obj ectCategory: CN=Servi ce-Connecti on-
Poi nt, CN=Schema, CN=Confi gurati on, Dc=i l l umi cl i ni cs, dc=com
ui d: fel i x. ho
```

```
uidNumber: 10000
gidNumber: 10000
unixHomeDirectory: /home/felix.ho
loginShell: /bin/bash
```

4.2.4 Consolidation

The consolidation phase of mergers and acquisitions traditionally involves decommissioning old systems and software. From a DirectControl perspective, this can be performed after all Active Directory user and group objects have been migrated from Greenmedia.net to IllumiClinics.com, and appropriate UNIX user profiles in Zones have been created in IllumiClinics.com.

5 Identifying Initial Tasks

This chapter identifies and discusses some of the initial tasks to start integrating Centrify DirectControl with your existing Identity Management System.

5.1 DirectControl Prerequisites

Before deploying Centrify DirectControl, the following network elements should exist in your environment:

- Active Directory, such as Windows 2000, Windows 2003, and Windows 2003 R2
- UNIX, Linux, or Mac computers, such as Mac OS X, Debian Linux, HP-UX, AIX, SUSE Linux Enterprise, Red Hat Enterprise Linux, Red Hat Fedora Core, SGI IRIX, Sun Solaris, and VMware ESX Server.
- Web applications or web servers, such as Apache, Apache Tomcat, BEA WebLogic, IBM WebSphere, and JBoss.
- Databases and ERP applications, such as IBM DB2, Oracle, SAP Enterprise and SAP NetWeaver
- The full list of supported versions is available online at <http://www.centrify.com/platforms>.

5.2 Identity Management System Prerequisites

Centrify DirectControl easily integrates with most off-the-shelf Identity Management Systems. One of the following requirements must be met:

- The Identity Management System must be able to call either .NET or COM objects as part of a connector; or,
- The Identity Management System must provide an LDAP connector which can bind to Active Directory.

It is highly recommended to use the DirectControl Software Developer's Kit (SDK) to build connectors using the COM/.NET objects.

5.3 Active Directory Setup

The first task is to install Centrif y DirectControl in the Windows environment. This requires permissions to add UNIX-specific data to Active Directory, typically stored in `cn=Centri fy, cn=Program Data, dc=your, dc=domai n, dc=here`. This is not a schema extension – rather, it is a set of LDAP containers and class store objects that are used as part of the DirectControl Zone technology.

5.4 Zone Design

At least one Zone must be created in Active Directory before UNIX computers can be joined to Active Directory. Zone design is a complex and challenging subject covered in depth in the Centrif y DirectControl documentation and Centrif y DirectControl training. Generally speaking, Zone design requires the following steps:

1. Identifying existing UNIX identity stores (such as `/etc/passwd` files, NIS domains, legacy LDAP servers, etc).
2. Surveying the users and groups defined across those identity stores to find UID/GID collisions.
3. Grouping the UNIX computers by function, by geography, or by one of many other criteria into Zones, while minimizing UID/GID collisions.

5.5 UNIX Deployment

While many deployment strategies exist, the best practice is to install the DirectControl Agent on all UNIX computers. Each computer will join a Zone in the Active Directory domain. However, locally defined user accounts will continue to work until they are migrated to Active Directory. If DirectControl for Databases or DirectControl for Web Applications is being deployed, it should also be deployed at this time.

5.6 Provisioning Integration

Using either the DirectControl Software Developer's Kit or the LDIF in this white paper, integrate your Identity Management System with DirectControl.

For any except the smallest user base, it is recommended to provision users in small, logical groups – everyone who works in a quadrant of a floor, or an office branch, or a factory, etc. Once each user's UNIX profile has been provisioned into appropriate Zones, use the `adrm local` utility to remove the user's local profile from each UNIX computer.

5.7 Conclusion

These initial high-level tasks must be performed or verified in order to integrate your Identity Management System with Centrify DirectControl. Once this solution is deployed, the administrative tasks will primarily involve adding new services or servers as required, as well as routine maintenance on existing services and servers.

6 Related Publications

The publications listed in this section are recommended for a more in-depth discussion of the subjects covered in this white paper. All publications are available from Centrify.

6.1 Product Documentation

These publications are available at <http://www.centrify.com/resources/documentation.asp>

- Centrify DirectControl Quick Start
- Administrator's Guide
- Centrify DirectControl Authentication Guide for Apache

6.2 White Papers

These publications are available at <http://www.centrify.com/directcontrol/whitepapers.asp>

- Centralized Identity and Policy Management for Windows, Linux, UNIX, Mac and Java with Active Directory and DirectControl
- Active Directory and DirectControl
- Centrify's Solution for Migrating UNIX Directories to Active Directory

6.3 Video Chalktalks

These require an active Internet connection and a web browser with a Flash plugin, and are available at http://www.centrify.com/resources/video_chalktalk_library.asp

- DirectControl's Architecture
- Single Sign-On for Web Applications
- Migrating UNIX Identities to Active Directory

7 How to Contact Centrifly

North America
(And All Locations Outside EMEA)

Centrifly Corporation
444 Castro St., Suite 1100
Mountain View, CA 94041
United States

Sales: +1 (650) 961-1100

Enquiries: info@centrifly.com

Web site: www.centrifly.com

Europe, Middle East, Africa
(EMEA)

Centrifly EMEA
Asmec Centre
Merlin House
Brunel Road
Theale, Berkshire, RG7 4AB
United Kingdom

Sales: +44 1189 026580