Centralized Identity and Access Management of Cross-Platform Systems and Applications with Active Directory and the Centrify Suite

The Centrify Suite is an integrated family of Active Directory-based auditing, access control and identity management solutions that secure your cross-platform environment and strengthen regulatory compliance initiatives.

ABSTRACT

The Centrify® Suite™ is an integrated family of Active Directory-based auditing, access control and identity management solutions that secure your cross-platform environment and strengthen regulatory compliance initiatives. Centrify DirectControl™ secures your non-Microsoft platforms using the same authentication and Group Policy services deployed for your Windows environment. Centrify DirectAuthorize™ centrally manages and enforces role-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems. Centrify DirectAudit™ delivers auditing, logging and real-time monitoring of user activity on your non-Microsoft systems. Built on a common architecture, the seamlessly integrated Centrify Suite of solutions helps you improve IT efficiency, strengthen regulatory compliance initiatives, and centrally secure your heterogeneous computing environment.

This white paper examines the compelling business and technical case for centralizing administration in Microsoft’s Active Directory, describes how the Centrify Suites integrated architecture enables you to extend Active Directory to your non-Microsoft platforms, and describes the Centrify Suite’s unique benefits.
Contents

Introduction ...................................................................................................... 1
  1.1 The Case for Extending Microsoft Active Directory to Non-Microsoft Environments .......................................................... 2
  1.2 The Fragmentation of Identity and Access Management within the Distributed Environment........................................... 2

2 Cross-Platform Identity and Access Management: A "Must Have" Solution. 4

3 The Centrify Suite........................................................................................ 7

4 Secure Access Control, Authentication and Cross-Platform Group Policy with Centrify DirectControl................................................................. 8
  4.1 Centrify DirectControl Management Tools.................................................. 12
     4.1.1 Centrify DirectControl Property Extensions ....................................... 12
     4.1.2 Centrify DirectControl Administrator Console ................................ 13
     4.1.3 Centrify DirectControl Web Administrator Console ......................... 14
     4.1.4 DirectControl Reporting Center ....................................................... 14
  4.2 DirectControl UNIX/Linux/Mac Architecture................................................ 15
     4.2.1 NSS Module ................................................................................. 16
     4.2.2 PAM Module ................................................................................. 17
     4.2.3 Kerberos Libraries, Software Development Kit and LDAP Proxy ........... 18
     4.2.4 Command-Line Interface Tools ....................................................... 18
     4.2.5 DirectControl Group Policy Architecture ........................................... 19
     4.2.6 NIS Server ................................................................................... 20
     4.2.7 DirectControl for Samba ................................................................. 21
     4.2.8 DirectControl for Databases and ERP Applications ......................... 21
     4.2.9 Apache and SPNEGO Modules......................................................... 21
     4.2.10 J2EE Modules ............................................................................... 22

5 UNIX Privilege Management with Centrify DirectAuthorize ....................... 22
  5.1 DirectAuthorize’s Key Features and Benefits .............................................. 22
  5.2 The DirectAuthorize Architecture ............................................................. 25

6 Detailed Auditing for UNIX and Linux with Centrify DirectAudit ............... 27
  6.1 DirectAudit’s Key Features and Benefits .................................................... 27
  6.2 The DirectAudit Architecture .................................................................... 28

7 Summary: Why the Centrify Approach Makes Sense................................ 28

8 How to Contact Centrify ............................................................................. 30
Introduction

The Centrify Suite is an integrated family of Active Directory-based auditing, access control and identity management solutions that secure your cross-platform environment and strengthen regulatory compliance initiatives. Centrify DirectControl secures your non-Microsoft platforms using the same authentication and Group Policy services deployed for your Windows environment. Centrify DirectAuthorize centrally manages and enforces role-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems. Centrify DirectAudit delivers auditing, logging and real-time monitoring of user activity on your non-Microsoft systems. Built on a common architecture, the seamlessly integrated Centrify Suite of solutions helps you improve IT efficiency, strengthen regulatory compliance initiatives, and centrally secure your heterogeneous computing environment.

Figure 1-1. Centrify enables you to create a secure, connected computing environment.

Centrify’s integration strategy emanates from three significant trends occurring within today’s IT organizations:

- The large installed base of Windows desktops and servers has driven the adoption of Active Directory and the wide deployment of Active Directory-enabled applications such as Microsoft Exchange.

- IT departments are managing increasingly heterogeneous environments as departmental or line-of-business systems are consolidated into a central IT organization for security, compliance, and cost-cutting reasons. Merger-and-acquisition activity also continues to present unpredictable integration challenges on tight deadlines. At the same time, identity and access management tools and practices have not kept pace with the growing diversity of platforms, particularly across the many emerging Linux vendors and distributions.
Companies are faced with a proliferation of identity stores, user accounts and passwords. This has led to higher administrative costs, increased security risks, challenges with meeting regulatory compliance requirements and a decrease in end-user satisfaction and productivity.

This white paper examines the compelling business and technical case for centralizing administration in Microsoft’s Active Directory, which is a robust, scalable and supported identity and access management infrastructure that the vast majority of enterprises have already deployed. It then introduces the solution architecture and benefits of the Centrify Suite, and describes how the Centrify Suite addresses one of the top issues facing IT organizations: how to build a secure, connected computing environment whose underlying components are comprised of disparate and heterogeneous systems, applications and databases that have been built without interoperability in mind.

1.1 The Case for Extending Microsoft Active Directory to Non-Microsoft Environments

In a typical IT environment, heterogeneity is the standard – not only as it relates to server operating systems running within an organization, but also as it relates to software applications and databases running on those servers. The reality is that mixed Windows, UNIX, Linux and Mac environments are a fact of life for almost all IT departments. And this will continue to be the case as both Linux and Windows continue to grow in the data center and Java- and web-based enterprise applications are deployed.

Not surprisingly, interoperability among these platforms is a key concern for IT managers. Organizations want heterogeneous servers and applications to “plug and play” so IT does not have to spend its time and budget acting as a systems integrator or having to manually (and expensively) administer an ever-growing number of systems and applications individually. In addition, organizations want to leverage existing investments as their budgets continue to force them to do more with less.

This need for interoperability within mixed Windows, UNIX, Linux, Mac, web, database and enterprise application platforms is probably most pronounced as it relates to identity and access management. Identity management is the set of processes and technologies involved in storing user information and granting rights based on authentication and authorization rules. Access management lets organizations deterministically grant users appropriate access to corporate resources – regardless of the platform that is being used.

1.2 The Fragmentation of Identity and Access Management within the Distributed Environment

In the Windows environment, Microsoft provides a comprehensive identity management solution through Active Directory. Numerous IT departments have invested millions of dollars deploying Active Directory as a replacement for their Windows NT 4.0 domain structure or as part of deployments of Windows XP and Microsoft Exchange 2003. In fact, according to a number of industry analysts, migration to Windows Server and the
deployment of Active Directory were among the top budgeted items for all of IT over the last few years. The ongoing rollout of Windows Server 2003 and now Windows 2008 is projected to be one of the top budgeted items moving forward.

The investment in Active Directory is so significant that The Gartner Group predicts that “by the end of 2010, at least 90 percent of midsize and large enterprises will have deployed Active Directory in their internal infrastructure.” Active Directory has become the default directory for a range of uses within the corporate network. For example, in many organizations all corporate users have Active Directory accounts to enable corporate email and control access to network resources such as printers and file shares. These factors clearly make Active Directory a strategic IT platform.

On the UNIX/Linux side, no single identity management solution enjoys anything like the pervasiveness of Active Directory within the Windows environment. IT organizations must deal with a plethora of identity stores deployed on UNIX/Linux platforms, including:

- Significant usage of locally managed /etc/passwd text files on individual systems.
- Heavy use of Sun’s outdated Network Information Service (NIS) and other legacy solutions such as Netscape’s Directory.
- Use of LDAP-based directories such as OpenLDAP.

While identity management solutions exist for Apple Mac networks, they represent yet another identity system for the IT staff to manage. Many of the key cross-platform integration features needed by administrators are lacking in the solutions that come from Microsoft and Apple.

Access control features are built into Active Directory and are heavily used to manage access to Windows resources. However, few solutions exist to expand access control to non-Windows environments. IT managers are often faced with implementing proprietary layered solutions that are costly and difficult to manage.

And as new Java and web applications are rolled out on platforms such as Apache, JBoss, Tomcat, IBM WebSphere and BEA WebLogic, developers are creating even more identity stores through the use of text files or database tables. Database platforms such as IBM’s DB2 and Informix, along with enterprise applications such as SAP, add yet another set of individual identity stores.
Thus, the fact is that in most organizations, identity and access management for UNIX, Linux and Mac systems, applications and databases is quite fragmented compared to Windows.

Figure 1-2. Balkanization of identity management in the distributed environment: one user, multiple accounts, multiple identity stores, and fragmented (or no) policy mechanisms.

2. Cross-Platform Identity and Access Management: A “Must Have” Solution

An obvious question is: Why haven’t organizations been able to standardize on one identity and access management solution? The answer lies in several obstacles:

- **Lack of interoperability.** Many identity stores and directory services simply do not operate with each other. Cross-platform access control is difficult to implement, especially if different authentication and authorization systems are used on each platform. Policy systems that are tied to identity stores tend to be tuned to individual operating systems rather than enterprise-wide policy.
Lack of platform support. Many leading solutions, such as Microsoft Active Directory, work only on a subset of platforms that an organization has deployed. And in the case of the Windows platform, an organization must deploy Active Directory. As the Gartner Group observes, “… there is no choice … if you deploy Windows 2000 or Windows 2003 Servers, you will deploy Active Directory.” However, Active Directory has historically only been used for Windows networks.

Lack of coordination. In some cases, groups that are isolated from one another in an organization install different server and application solutions. This can result in the deployment of multiple incompatible point solutions.

Lack of openness. Internal developers of new applications often don’t have the means to seamlessly interoperate with existing identity stores. When APIs do exist, developers have to spend significant effort developing complex integration capabilities that rely on meta-directories or synchronization. This leaves multiple identity stores intact, requiring continued resource-draining maintenance while adding yet another layer of complexity.

Lack of delegated administration capabilities. IT management may need to isolate the management of certain identity stores and assign privileged rights to certain administrators for a subset of the entire organization. If a centralized identity and access management system were to be used, the system would need to be flexible enough to accommodate delegated administration for well defined identity groups.

Many organizations are only now starting to come to grips with the hidden costs associated with the proliferation of identity systems. These costs include the following:

Increased IT administration costs. Given that Gartner Group estimates that 45% of all helpdesk calls are requests for password resets, an IT organization’s costs go up as the number of different identity stores increase. In addition, having to individually maintain multiple identity stores results in IT administrative processes that are time-consuming, redundant and error-prone as duplicate user ID data is keyed into multiple systems. Furthermore, this complexity makes it difficult, and thus expensive, to extend infrastructure to new business processes – so much so in extreme cases that it actually inhibits the company’s growth.

Significant impact on end-user productivity. According to Gartner Group, the average large organization has over 20 sources of identities, resulting in the average internal user having to remember more than five user names and passwords. This creates a scenario where end users have too many credentials to remember, and incredibly the average user spends over 16 minutes a day logging on. Multiple identity stores also lead to delays in provisioning new employees and fulfilling requests for changes to existing accounts.

Increased security risks. The greater the number of identity stores, the greater the likelihood of dormant and orphan accounts being misused to access sensitive information. In addition, numerous passwords (and password change policies) force
users to store passwords insecurely. Finally, the greater the number of identity stores, the greater the difficulty of implementing consistent security policies. Without a cross-platform access control solution, it is difficult to enforce a consistent set of access rights for every platform.

- **Increased difficulty in complying with regulatory requirements (such as PCI DSS, Sarbanes-Oxley, HIPAA and GLBA).** An increasing number of industry and governmental regulations require organizations to maintain strict control over business processes and, in particular, access to sensitive personal and financial information. With control and tracking of key business data and processes distributed among multiple identity systems, companies are resorting to awkward, time-consuming manual methods to consolidate the information needed to audit and report on their compliance. The inability to meet these regulatory requirements in a reliable and timely manner leaves many businesses critically exposed.

Clearly it may be difficult to move to a single identity and access management solution. For example, it may be impractical to integrate a mainframe identity system into a centralized environment. Still, a significant reduction of identity stores in the corporate network (such as providing a single, integrated solution for Windows, UNIX, Linux and Mac) can significantly improve end-user productivity, reduce operating costs, improve security and make it significantly easier to comply with regulatory requirements.

Faced with the issues discussed above, IT organizations have at least three choices to resolve this Identity and Access Management crisis.

**Do nothing and live with a balkanized environment**

The downside to this strategy is the potential costs and risks documented above. Yet, many organizations feel themselves forced into this situation given the lack of a solution that fits their budget and doesn’t require intrusive (and thus impractical) changes to existing systems or business practices.

**Try to implement an expensive and complex synchronization solution**

Many existing management solutions follow this approach. They leave the existing systems in place and install solutions that map and synchronize user information and access rights between the various incompatible systems. Often these mapping solutions are facilitated by a database that maintains the credential “links” between each system. The problems with this approach are numerous:

- Deployments of these solutions are very complex, frequently requiring a RDBMS to provide the data mapping.
- IT management is still left with the burdensome maintenance of duplicate records in multiple identity systems.
- In many cases, passwords or other sensitive data is being synchronized across the network in clear text.
These solutions often deliver lowest-common-denominator capabilities across identity systems. For example, they may just manage user names and passwords, leaving IT to look for yet another point solution for directory needs, access control or policy enforcement.

These solutions are very expensive to purchase, deploy and maintain, with even entry-level implementations often starting in the hundreds of thousands of dollars.

There are no avenues toward significant savings. If an organization has 30 identity systems, they would continue to maintain those 30 identity systems. Plus, the organization is saddled with the additional cost of purchasing and maintaining the synchronization solutions. In many cases, costs actually go up and complexity increases, leaving the potential benefits of this type of solution in question.

**Extend an existing identity store to replace as many existing identity stores as possible**

The goal would be to begin building a centralized directory system by selecting an identity system that has a proven track record and a clearly defined future direction, and leverage that single identity system to replace and/or consolidate existing identity systems over time.

The last option clearly makes the most business sense for solving the cross-platform identity management crisis. Consolidating and centralizing identity systems offers clear benefits in terms of productivity, cost savings, security and reporting. The hard question to answer has been: which identity store has the potential to fill this need?

Given that Active Directory is an inseparable part of the Windows environment, that most organizations already have Active Directory deployed, and that Microsoft is committed to applying significant resources to improving its features and scalability, it is the ideal candidate for assuming the role as an organization’s centralized identity system. Microsoft, however, focuses its efforts on the Windows platform and does not provide a comprehensive solution for servicing other platforms. Thus, organizations have been forced to use other identity stores for non-Microsoft platforms. Hence this third and most practical approach couldn’t be implemented – until now.

### 3 The Centrify Suite

The Centrify Suite is an integrated family of Active Directory-based auditing, access control and identity management solutions that secure your cross-platform environment and strengthen regulatory compliance initiatives. More than 600 enterprise customers, including over 38% of the Fortune 50, have selected the Centrify Suite for its quick-to-deploy and easy-to-manage approach for securing their heterogeneous computing environment.

The Centrify Suite is comprised of the following solutions:
• **Centrify DirectControl** — secures over 150+ flavors of UNIX, Linux and Mac using the same authentication and Group Policy services deployed for your Windows environment. DirectControl also provides Active Directory-based single sign-on solutions for popular web-based servers (e.g. Apache, WebLogic and WebSphere), databases (e.g. DB2) and enterprise applications (e.g. SAP);

• **Centrify DirectAuthorize** — centrally manages and enforces role-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems; and

• **Centrify DirectAudit** — delivers auditing, logging and real-time monitoring of user activity on your non-Microsoft systems.

Built on a common architecture, the seamlessly integrated Centrify Suite of solutions helps you improve IT efficiency, strengthen regulatory compliance initiatives, and centrally secure your heterogeneous computing environment.

The following sections of this whitepaper will drill down into the details of each product within the Centrify Suite.

4 Secure Access Control, Authentication and Cross-Platform Group Policy with Centrify DirectControl

Centrify DirectControl delivers secure access control and centralized identity management by seamlessly integrating your UNIX, Linux, Mac, web, database and enterprise application platforms with Microsoft Active Directory. DirectControl effectively turns a non-Microsoft system into an Active Directory client, enabling you to secure that system using the same authentication and Group Policy services currently deployed for your Windows systems. DirectControl is non-intrusive, easy to deploy and manage, and is the only solution that enables fine-grained access control through its unique Zone technology.
Figure 4-1. Centrify eliminates the need for multiple Identity and Access Management solutions in the distributed environment by consolidating management in Microsoft Active Directory: one user, one account, one directory, one policy mechanism.

DirectControl is comprised of two main architectural components that seamlessly integrate with your Active Directory infrastructure:

- On UNIX, Linux and Mac systems, a **DirectControl Agent** is installed on each server or workstation. The DirectControl Agent, which is natively compiled for each platform, effectively turns the host system into an Active Directory client, enabling you to secure that system using the same authentication, access control and Group Policy services currently deployed for your Windows systems. The Agent is not a single piece of code; rather, it is a central service that interacts with a set of seamlessly integrated modules that provide services such as web, database and SAP single sign-on and Samba integration. UNIX administrators have a comprehensive command-line interface for real-time or scripted interaction with Active Directory-held data.

- The **DirectControl Management Tools** enable both Windows and UNIX administrators to manage UNIX-specific data stored in Active Directory. The
Windows tools consist of a Microsoft Management Console (MMC) application for all administrative tasks and centralized reporting and license management. Property extensions to the Active Directory Users and Computers MMC are also provided, and DirectControl’s UNIX/Linux/Mac policies are fully integrated into the standard Group Policy Editor. A browser-based management console also provides cross-platform access to essential administrative tasks.

To better understand the overall DirectControl architecture from both a UNIX and Windows perspective, a further discussion of one of DirectControl’s core features — Zones — is warranted.

From an identity management perspective, it is very hard to ensure that UNIX/Linux/Mac UIDs are unique throughout the enterprise. This is especially true when user accounts are held in a variety of identity stores: NIS, /etc/passwd files or LDAP-based directories. If there is no way to map these multiple UNIX identities to a single Active Directory account, an organization will be forced to undergo a painful UID rationalization project before they can even began to add non-Windows systems into their Active Directory domains.

From a security and compliance perspective, it is neither desirable nor practical to allow all users in an enterprise to log on to all UNIX/Linux/Mac systems, which could be the net result if UNIX identities were simply imported together into Active Directory and UNIX-enabled. Organizations frequently need a way to create logical groups of non-Windows systems to preserve existing security boundaries.

To deal with these dual challenges, Centrify has developed the concept of Zones. Zones may be used as either a permanent solution for identity mapping, or as a technique for migrating users’ multiple identities into a single Active Directory account over time. It frequently happens that these separate identity stores represent security boundaries that must be preserved, so in addition to providing identity mapping they can also be used to control access to systems as well. However, even in scenarios when an organization has a single, consistent UID namespace across its enterprise, and thus there is no need to use Zones for identity management, Zones are still frequently employed for security and compliance reasons to provide granular access control for sensitive systems.
Zoning, as shown in the illustration above, works like this:

- Each managed UNIX/Linux/Mac system exists in a single Zone; its Zone name is part of its configuration. A Zone can contain any number of computers with a variety of operating systems. In many cases, a Zone consists of the identities formerly held in a separate identity store. However, IT administrators can choose to set up Zones by department, by geography, by function, by system type, or by any other business rules that make sense for their organization.

- A user (Joan Smith in Figure 4-2) is configured in Active Directory with her normal Windows information such as name, password, group membership and so on. In addition, the “Centrify Profile” that Centrify adds to her Active Directory account indicates which Zones she can access.

- For each Zone, Joan’s UNIX profile in Active Directory stores account information specific to that Zone: UNIX user name, user ID, shell, and home directory for example. Thus, a single Active Directory account can be mapped to any number of UNIX identities.

- Joan can only log on to computers in the Zones to which she has been granted access.

- As Figure 4-2 illustrates, Joan authenticates through her Active Directory credentials regardless of which system she logs on to. The Zones are part of the same Active Directory domain where Joan’s account exists.

Each Zone can have its own set of administrators, each with specific privileges within the Zone. For example, one administrator might have rights to create new user accounts in “Zone A” while another administrator might have no rights in “Zone A” and only rights to change user access for “Zone B”. Administrators for one Zone do not have rights in other Zones, unless those rights have been assigned. This added security feature means
not only can users and computers be compartmentalized into logical secure groups, but the administrators who manage those systems can also be segregated. For many companies, the ability to finely control the elevated privileges for administrators is essential for maintaining appropriate levels of confidentiality and for complying with regulatory controls that call for separation of duties. For example, it would not be appropriate for the administrator of the company’s web site to also have the ability to create user accounts or to change user access rights for the company’s payroll server. This unique capability of delegated administration for each Zone is indispensable for any large real-world enterprise.

DirectControl automatically sets up a default Zone and populates it correctly as managed systems are added to Active Directory. Additional Zones can be set up and used based on the identity management and access control needs of the organization.

The following sections describe the Windows-based Management Tools and the UNIX/Linux/Mac solution architecture in more detail.

4.1 Centrify DirectControl Management Tools

The DirectControl Management Tools consist of the Centrify DirectControl property extensions for the Active Directory Users and Computers MMC, the DirectControl Administrator Console, and the DirectControl Web Administrator Console.

The Windows-based DirectControl property extensions and Administrator Console are the only software you need to install in your Windows environment in order to deploy DirectControl. You are not required to install software on your Windows domain controllers. Nor does the Centrify DirectControl Windows installation require modifications to your Active Directory schema. As UNIX, Linux and Mac computers join your Active Directory domain and you enable users for access to these systems, DirectControl provides the option of unobtrusively storing its data in an Active Directory program data container using a standardized method. Or, you can choose to use the Microsoft-supplied Active Directory schema extensions that are provided by Microsoft Services for UNIX (SFU) or Microsoft Windows Server 2003 R2. DirectControl is the only solution that offers these multiple deployment options based on the needs of your organization.

4.1.1 Centrify DirectControl Property Extensions
The Centrify DirectControl property extensions for the Active Directory Users and Computers MMC enable you to manage access to UNIX/Linux/Mac systems from within the native Active Directory interface. UNIX properties are displayed within the Centrify Profile tabs as you use Active Directory Users and Computers to set user, group, or computer properties.

![DirectControl property extensions for Active Directory Users and Computers.

4.1.2 Centrify DirectControl Administrator Console

The **Centrify DirectControl Administrator Console** provides a management view of UNIX-enabled users, groups and computers. You can use it to:

- Centrally manage all your UNIX, Linux and Mac systems.
- Create logical groups of computers, called DirectControl Zones, and assign users access to systems based on Zones.
- Assign detailed access rights for administrators in each Zone.
- Manage NIS Server settings for each Zone.
- Set password and other policies.
- Run access rights and other reports.
- Import account information from NIS and text files into Active Directory.
- Manage licensing.
4.1.3 Centrify DirectControl Web Administrator Console

UNIX administrators in particular may not have easy access to Windows-based administrative tools. Roving administrators also need a way to quickly perform some management tasks from systems where they may be logged in. DirectControl is the only cross-platform integration solution to deliver a browser-based administrator console.

4.1.4 DirectControl Reporting Center

DirectControl’s built-for-compliance architecture makes reporting a central, integrated feature. Available from within the DirectControl Administrator Console, the Reporting Center enables IT administrators, security managers, and compliance auditors to run reports that show which users can access a given computer and which computers a given user can access. Other reports show the UNIX properties for users and computers, Zone membership, group membership, delegated administrators and their rights, license details, and more.
4.2 DirectControl UNIX/Linux/Mac Architecture

The heart of DirectControl on the UNIX/Linux/Mac platform is the DirectControl Agent (adclient) and the service library that exposes its functionality to all other components. The DirectControl Agent runs as a daemon on the managed system. The daemon generates all LDAP and Kerberos traffic between the UNIX system and Active Directory. The DirectControl Agent is responsible for:

- Enabling an administrator to join a UNIX/Linux/Mac computer to an Active Directory domain through a command-line interface on the managed system. The rules and steps for joining a domain are the same as for a Windows system. Once a UNIX system has been joined to the Active Directory domain, it is visible as a standard computer object in the Active Directory Users and Computers console.
- Locating the relevant domain controllers based on the Active Directory forest and site topology.
- Maintaining time synchronization with Active Directory.
- Enabling a Kerberos environment so that existing Kerberos applications will work seamlessly with Active Directory.
- Caching responses from Active Directory information queries.
- Storing user credentials so that users can log on in disconnected mode.
- Providing all of the authentication and directory look-up services needed by higher-level components and applications.
- Resetting the password on its machine account at regular intervals.
Enabling logons using users’ Active Directory credentials. Logging on in this context means connecting to the UNIX/Linux/Mac shell through a logon, telnet, ssh, graphical desktop, or connecting to web applications through a web browser.

Validating that the user has appropriate permissions to log into the UNIX machine based on policies, group memberships and Zone memberships.

Determining a user’s full group membership (including nested groups) the first time the user logs on.

Allowing users to manage their Active Directory passwords from UNIX/Linux/Mac systems.

Validating privileged account logins centrally from Active Directory if needed.

In addition, Group Policy services are enabled for the UNIX client. The DirectControl NIS server is available to direct NIS requests from UNIX clients to Active Directory. Services are available to allow Samba integration with DirectControl. Other modules to tie Java and web-based applications, databases and ERP applications into Active Directory are also included.

The following sections describe each service module in more detail.

4.2.1 NSS Module

The Name Service Switch (NSS) module provides a database of names (users, groups, computers) to many parts of a UNIX system. The two classic NSS systems are the module that uses files (such as /etc/password and /etc/group) and the one that uses NIS.
The DirectControl NSS module provides an equivalent service by reading its data from Active Directory using LDAP. The module is tightly integrated with the rest of DirectControl for policy, security and performance reasons.

The DirectControl Agent will be busy a large amount of time answering NSS requests to list users, list groups, map UIDs to users, etc. To ensure requests are answered quickly, and to ensure DirectControl does not swamp Active Directory domain controllers with lookup requests, the DirectControl Agent maintains a cache of responses.

4.2.2 PAM Module

The DirectControl Pluggable Authentication Module (PAM) enables applications (ftpd, telnetd, login, Apache, etc.) to authenticate users using their Active Directory user name and password. The DirectControl PAM module provides the following features:

- The module issues a request asking the application to prompt for a password.
- If the password has expired, the module asks the user to change the password and, through the DirectControl daemon, forwards the change to Active Directory.
- It will verify that the user has permission to log on to this system based on policy settings.
- It will optionally auto provision the user by creating his or her local home directory.

It may also be useful to have Active Directory control the root account passwords. However, it does not make sense to simply have a user name of “root” in Active Directory. Since all root users on all UNIX systems are called root, it would mean that a root user for “webserver1” would be a root user for all servers in Active Directory. Instead, DirectControl uses PAM settings to map root on a given system to some other user name for the purpose of password validation. This remapped user name could be unique to that system or shared among a set of machines. So for example, the settings for all machines in a web farm could specify that the PAM module authenticate root logins with the Active Directory user name of “root_webfarm”. A major benefit of this approach is root passwords are securely stored centrally in Active Directory. For example, if the root password needed to be changed for all the machines in the web farm, only one password change would be required for the “root_webfarm” user in Active Directory instead of manually changing passwords on every machine.

The PAM module is the main gatekeeper to the UNIX system. Most of its behavior is driven by policy. The policy can be specified locally, through Active Directory using Group Policy, or a combination of both. Things that can be specified via policy:

- Which users and groups are permitted to log on.
- When they are allowed to log on.
Applications with which they can log on (for example, it might permit them to authenticate through Apache but not `telnet`).

Whether disconnected mode is allowed (that is, whether they can log on when they are unplugged from the network) and, if so, how long the offline credentials should be trusted.

Control over which users can obtain elevated privileges using commands such as `sudo`.

Note that different policies will apply to different PAM users. For example, the list of users who can log on and get a shell prompt is probably different from those who can log on to a CRM application running in Apache.

### 4.2.3 Kerberos Libraries, Software Development Kit and LDAP Proxy

The DirectControl Software Development Kit (SDK) includes a full set of standard Kerberos libraries and APIs. Users can run Kerberos-enabled applications (such as `telnet` or `ftp`) and directly leverage their Kerberos-based Active Directory credentials resulting in a secure, single sign-on (SSO) experience. As a convenience for customers, Centrify has a resource center (http://www.centrify.com/resources/application_notes.asp) that describes our precompiled binaries and documentation for a number of popular Open Source applications such as OpenSSH, PuTTY and `telnet`. These applications have been enhanced to work with Active Directory credentials by using the DirectControl libraries.

Developers can also use the DirectControl libraries to Kerberos-enable existing applications – making them more secure and easier to use. There are also LDAP APIs and an LDAP Proxy to enable searching and retrieving information stored in Active Directory. Support is included for C/C++, Java, Perl, PHP and Python interfaces.

### 4.2.4 Command-Line Interface Tools

DirectControl provides a comprehensive set of command-line interface (CLI) tools that UNIX administrators can use interactively or via scripts. Here are some of the tasks you can perform using these interfaces:

- Join a computer to a domain or leave a domain.
- Query user and group data in Active Directory and create, modify or delete users and groups.
- Change user passwords.
- Display real and effective UID/GIDs for current or specified users.
- Display machine status, dump or check cache files, and force a reload of the Centrify configuration file.
4.2.5 DirectControl Group Policy Architecture

Windows Group Policy works by forcibly setting user and computer registry keys. Since almost all of a Windows system is configured through registry settings, this is a very natural and simple way to enforce almost any policy.

In the UNIX world, there is no equivalent to the Windows registry. The de-facto standard for configuration is ASCII text files. To deliver Active Directory’s Group Policy capabilities in a UNIX environment, DirectControl creates a “virtual registry” by mapping the registry settings that Group Policy would create to entries in various system files. For each configurable application, DirectControl provides a specific mapper that knows what needs to be set in the configuration file for that application.

Centrify includes an extensive set of out-of-the-box Group Policies that are tailored to UNIX, Linux and Mac security and configuration management – more than any other cross-platform solution. It is the only solution to provide both user and computer policies, along with advanced features such as filtering and loopback processing. These policies can be used to copy syslog or other configuration files to target systems and to globally manage logon settings, PAM settings, password prompts, timeout settings, Kerberos settings, NSS overrides, password caching, LDAP settings, user/group maps, crontab settings, firewall configuration, graphical desktop properties, sudo permissions, DirectControl Agent settings, and a growing list of other settings that are suitable for being centrally managed. In addition, DirectControl is the only solution that enables you to globally control ssh usage policy with Group Policy, and it provides the most extensive set of Mac-specific policies available, including desktop lockdown policies that, for example, globally manage system preferences, require a password to unlock a screensaver, enable/disable the ability to install software or to save data to external media, or block access to specific applications.

A good example of the value of enforced policy can be seen with the administration of the sudoers file. This file defines who can run privileged programs on a Linux system. If the configuration of this file is not strictly controlled across every system in your organization, then security is not only compromised on an individual system but also potentially compromised across your organization. DirectControl’s Group Policy capability ensures that your systems are secured in a consistent, enforced manner.
Free-form editing, a syntax checker, and the ability to insert all standard commands and Active Directory object names make it easy to manage Sudo Group Policies for fine-grained privilege management.

DirectControl Group Policies are fully integrated with the standard Group Policy Object editor. For added flexibility, you can also create your own custom policies. On the UNIX systems, you can use standard Perl scripting to create your own mapping programs that update relevant configuration files.

4.2.6 NIS Server

The DirectControl software on UNIX includes a pseudo NIS server. This component runs as a daemon and is designed to service clients and applications that require NIS and expect a service on the defined NIS network ports. This NIS service is fully integrated with the `adclient` daemon and vectors all NIS-related requests to Active Directory via DirectControl. All NIS maps are now stored and managed centrally in Active Directory, enabling full replacement of existing NIS servers with a secure, centralized Active Directory-integrated solution.

These maps are associated with the Zone where the service is running so it is possible to service multiple virtual NIS domains from a single Active Directory domain. The NIS server can service requests both locally and from other computers devices on the network, including legacy systems that have not been joined to Active Directory. For example, a network attached storage (NAS) device may be “hardwired” to only work with NIS. By configuring the NAS device to use the DirectControl NIS service, this device can now use Active Directory as its central server for validating users. In this way, systems that need specific NIS functionality e.g. `automount` map information, can continue to function but now are serviced through the centralized Active Directory system rather than a separate NIS service infrastructure.
4.2.7 DirectControl for Samba

Samba is a popular Open Source technology for setting up a UNIX or Linux system as a file server for Windows clients. Since Samba is most often used with Windows clients, it makes sense to tightly integrate Samba with the Active Directory security model. DirectControl for Samba addresses this need through an identity mapping module that plugs into Samba. This module redirects all user information queries to Active Directory so that information is stored centrally as opposed to locally on each Samba server. In addition, Samba uses the Kerberos single sign-on capabilities that are provided by DirectControl. The DirectControl for Samba solution also includes scripts to assist with configuring Samba, documentation and pre-compiled Samba binaries for supported UNIX/Linux platforms.

4.2.8 DirectControl for Databases and ERP Applications

DirectControl supports strong Kerberos-based Active Directory authentication for databases such as IBM’s DB2 and Informix, and for enterprise applications such as SAP. While many of these platforms offer some type of Kerberos support, setting up and administering the Kerberos service to talk with Active Directory securely and reliably can be a complex task on non-Microsoft platforms. With the DirectControl Agent installed, the host platform becomes Active Directory-aware and can take advantage of DirectControl services – such as automatic updates of Keytab files and Keytab versioning, automatic time synchronization with Active Directory, local caching for disconnected mode, and dynamic DNS support – that greatly simplifies initial configuration and provides a much higher degree of maintainability and reliability. With databases such as IBM DB2, Centrify also delivers a DirectControl module that provides additional benefits such as the ability to implement single sign-on and leverage Active Directory-based group management. And its module for SAP has been certified by SAP.

4.2.9 Apache and SPNEGO Modules

DirectControl includes support for the popular Apache web server. This allows Apache applications to use Active Directory as the identity system for user information, group-based access control and password validation. There is also support for SPNEGO in the Apache and J2EE modules. SPNEGO is the mechanism that Microsoft’s Internet Explorer uses to silently and securely pass the client’s user identity to a web application hosted on Microsoft’s IIS web server. By allowing application servers on UNIX to support the same mechanism, the end-user experience is greatly enhanced. For example, if a user uses Internet Explorer to navigate to the internal CRM application running on a UNIX-based Apache system, they are no longer required to enter a user name and password. Instead, the DirectControl SPNEGO module on the Apache web server silently validates the user and obtains the required log-on information from Active Directory.
4.2.10 **J2EE Modules**

DirectControl provides the ability to authenticate and perform access control for Java/J2EE applications. DirectControl includes support for Tomcat, JBoss, WebSphere, and WebLogic. For example, the JAAS module is a general purpose module for “logging on” a user in the Java world (this is very similar to a PAM module; in fact, the JAAS authentication scheme is modeled on PAM). It can operate in one of two ways:

- **Silent.** In this mode, the user is not prompted for a user name or password. Instead, the module queries the underlying platform to determine who this user is and to set up the credentials for later use.

- **Prompted.** In this mode, the JAAS module asks the application to prompt the user for a user name and password. It then validates this data and stores the credentials for later use.

The JAAS configuration file provided by DirectControl is used to specify which mode to use.

Although Sun provides a Kerberos implementation in J2EE 1.4, it does not work well in an Active Directory environment. In fact, DirectControl provides an implementation running on top of the DirectControl Agent on UNIX and also supports popular web applications running on Windows. From the application’s view point, it sees standard interfaces and is not aware of the underlying platform (unless it specifically needs to).

DirectControl support for Apache and J2EE also includes support for Microsoft Active Directory Federation Service (ADFS).

5 **UNIX Privilege Management with Centrify DirectAuthorize**

Centrify DirectAuthorize centrally manages and enforces role-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems. According to Gartner, UNIX and Linux systems inherently lack a scalable and simple model for administrative delegation, and organizations that give too many users root permission run unnecessary security risks and will invariably fail audits. By controlling how users access systems and what they can do, DirectAuthorize enables organizations to lock down sensitive systems and eliminate uncontrolled use of root accounts and passwords.

5.1 **DirectAuthorize’s Key Features and Benefits**

With DirectAuthorize you can:

- Meet regulatory compliance requirements with a centralized, role-based model for fine-grained delegation of administrative rights on UNIX and Linux systems.
- Secure your UNIX and Linux infrastructure by eliminating the need to share the passwords of root or super-user accounts with privileged access

- Leverage your existing Active Directory infrastructure for role-based entitlement management without the need to deploy additional servers or infrastructure

- Replace sudo or other complex, script-driven products with a modern, role-based solution that extends beyond controlling privileged commands

- Deploy a highly available solution for privilege management that works well in a networked environment and does not require changes to your UNIX systems

Let’s expand on each in more detail below.

Meet regulatory compliance requirements with a centralized, role-based model for fine-grained delegation of administrative rights on UNIX and Linux systems

Government and industry regulatory compliance requirements such as SOX, PCI, HIPAA, GLBA and FISMA dictate that organizations establish individual accountability for actions taken on any system holding critical information. Instead of multiple administrators sharing a root or privileged account, they should each log in as themselves, and only then gain privileges based on their role within the organization. Yet, UNIX personnel — such as system administrators, DBAs, backup operators and help desk staff — have a genuine need for increased privileges to accomplish even narrowly focused administrative tasks such as performing backups. But as Gartner points out, unlike the Windows platform, UNIX lacks a “simple and scalable model for administrative delegation.” (Gartner Research Report ID# G00130427 ) Gartner further notes that “the larger and more complex the organization, the greater the number of people who will sometimes need privileged access, increasing the likelihood of mistakes and deliberate attacks.” Such practices are “likely to draw the attention of the external audit.”

Centrify DirectControl facilitates compliance by enabling each user to log in to a UNIX or Linux system as themselves using their Active Directory credentials, drawing a line of accountability back to a centrally managed enterprise identity. DirectControl’s patent-pending Zone feature provides the first level of granular access control by restricting who can log in to which set of systems. DirectAuthorize provides further granular access control by controlling how these authorized users access that system, and when. It can also control what actions they can perform once on a given system.

DirectAuthorize meets compliance-driven requirements for “least access” management by allowing organizations to centrally define logical roles (backup operator, DBA, web developer, application administrator, etc.) that carry with them the specific rights needed to perform duties within that role. Roles also define times when a user can log in to a system; for example, a backup operator role might allow access to systems on Wednesdays and Fridays between the hours of 5:00 p.m. and 9:00 p.m. You can also assign roles to users for specific time periods; for example, you could assign a system
administrator role to a contractor with a start date of Monday, August 4th, and an expiration date of Friday, August 29th.

Rights describe both access methods and privileges. Rights specify how users within a role can connect to systems (FTP, Telnet, SSH, etc.). Rights can also specify permitted commands and the accounts they will run under (such as the ability to create files on a system without knowing the password to a privileged account that would normally be required). You can use DirectAuthorize to give users additional rights that they would not normally have, or you can use the unique Restricted Environment feature to limit users to a “whitelist” of specific commands.

With DirectAuthorize, organizations can meet regulatory compliance requirements by locking down access to sensitive systems and eliminating uncontrolled use of root and service accounts and passwords.

Secure your UNIX and Linux infrastructure by eliminating the need to share the passwords of root or super-user accounts with privileged access.

As Gartner notes, organizations “should look to implement delegation when more than three people have access to the root password.” Yet unfortunately, given that UNIX systems often require multiple IT staff to have administrative privileges to perform a variety of daily functions, Gartner has found that many larger organizations will have as many as 50-plus people who know and have access to the root password. Given the power that root access has, “such a situation is a disaster waiting to happen” notes Garter.

DirectAuthorize addresses this security challenge by controlling how users can access the UNIX system and what they can do, as well as by eliminating a user’s need to use the root account which in turn allows the root account to be locked down. In addition, DirectAuthorize can delegate rights to run specific commands with elevated privileges where authorized. This means that DirectAuthorize can ensure that root and other privileged account’s password is never revealed, making your environment even more secure and compliant.

Leverage your existing Active Directory infrastructure for role-based entitlement management without the need to deploy additional servers or infrastructure

DirectAuthorize is a seamlessly integrated component that leverages the scalable and robust DirectControl architecture. It enables you to centrally manage how users access DirectControl-managed computers and the operations they can perform on them. Like DirectControl, DirectAuthorize is tightly integrated into Active Directory, which means you do not need to deploy, test and manage additional servers or infrastructure to use DirectAuthorize. DirectAuthorize stores its role and rights data in Active Directory Authorization Manager’s existing rights-based logical model and data storage schema found in Windows 2003 and above. This means no Active Directory schema extensions are required to install and use DirectAuthorize. You can manage DirectAuthorize from within the Centrify Console, or you can leverage Authorization Manager (AzMan) APIs to access DirectAuthorize’s roles and rights data. With its use of a modern LDAP
directory to centrally store and manage authorization data, and its ability to leverage an existing Active Directory infrastructure, DirectAuthorize represents next-generation technology compared to older, proprietary solutions that require separate servers and infrastructure to operate.

**Replace sudo or other complex, script-driven products with a modern, role-based solution that extends beyond controlling privileged commands**

DirectAuthorize provides an easy-to-use framework to simplify granting users rights to services and applications by allowing organizations to centrally define logical roles (backup operator, DBA, web developer, application administrator, etc.) that carry with them the specific rights — and only the rights — needed to perform duties within a role. DirectAuthorize’s modern, role-based approach to UNIX privilege management has been designed with compliance in mind, delivering a solution that is both easier to administer and more robust compared to older products with complex and proprietary scripting languages that can only approximate the rich modeling available via Active Directory. In addition, DirectAuthorize’s unique Restricted Environment feature and its ability to control users’ access to systems via PAM-enabled interfaces go well beyond the capabilities of older legacy products.

**Deploy a highly available solution for privilege management that works well in a networked environment and does not require changes to your UNIX and Linux systems**

Like DirectControl and DirectAudit, DirectAuthorize provides a local caching mechanism that enforces authorization and privilege management even if a system cannot temporarily talk to the network. And also like DirectControl and DirectAudit, DirectAuthorize is non-intrusive and does not require any changes to the underlying UNIX operating system. By contrast, older products can only work if there is a constant network connection and require proprietary changes to the underlying UNIX kernel.

### 5.2 The DirectAuthorize Architecture

DirectAuthorize, a seamlessly integrated component of the Centrify Suite, leverages the scalable and robust DirectControl architecture, which joins UNIX, Linux and Mac systems to Active Directory and enables non-Windows identities to be centrally managed within Active Directory. DirectAuthorize meets compliance-driven requirements for “least access” management by allowing organizations to centrally define logical **roles** (backup operator, DBA, web developer, application administrator, etc.) that carry with them the specific **rights** needed to perform duties within a role. Rights describe both access methods and privileges, specifically:

- **PAM (Pluggable Authentication Module) Access** rights identify the specific PAM-enabled interfaces and applications the user can access, such as FTP, Telnet, SSH, or Informix.
Privileged Commands: These commands identify specific commands that the user can run and whether those commands can be run under the user’s own account or as another account. On the UNIX and Linux systems, these privileged commands are run via the command line “dzdo,” which operates similarly to and replaces “sudo.” The dzdo command acquires its policy from Active Directory only, and this is cached for offline enforcement.

Restricted Environments: These environments provide strictly controlled access to a defined subset of commands in a DirectAuthorize shell (sash). In effect, this grants users access to whitelisted applications only, and automatically grants privilege execution where authorized.

Roles: Roles are defined for a Centrify Zone, which is a logical collection of DirectControl-managed systems. Active Directory users or groups can be assigned to one or more roles. A role assignment can apply to all computers in a Zone, or to a specific computer. For example, in the Engineering Zone, the user Chris could be assigned the system administrator role for all computers, and also be assigned a DBA role for a single database server. Thus, roles are a flexible and scalable method for defining users’ access methods and privileges for a specific set of systems.

Effectiveness: Roles can be active and available for use during specific hours of the day or days of the week. For example, you can specify that a backup operator role is available only on Wednesdays and Fridays between the hours of 5:00 p.m. and 9:00 p.m. Users and groups in that role are allowed to perform the operations associated with the role during the days and times you have defined.

Duration: An individual user or group role assignment can be given an effective starting date and time, an expiration date and time, or both. For example, if the user Jane needs to be a database administrator temporarily for four weeks in August, you can assign this user to the database administrator role with a start date of Monday, August 4th, and an expiration date of Friday, August 29th. Or, a patch role might be assigned to user Fred for a short time while he works on a trouble ticket.

Integration: Like DirectControl, DirectAuthorize is tightly integrated into Active Directory, meaning no additional servers or infrastructure is required to run DirectAuthorize. DirectAuthorize stores its role and rights data securely in Active Directory Authorization Manager’s existing rights-based logical model and data storage schema found in Windows 2003 and above. This means no Active Directory schema extensions are required to install and use DirectAuthorize, and you can leverage the pre-existing Authorization Manager (AzMan) APIs to access DirectAuthorize’s roles and rights data.

User Interface: The DirectAuthorize user interface is integrated with the DirectControl Administrator’s Console. The DirectAuthorize rights enforcers are integrated into the DirectControl Agent. And unlike other solutions, DirectAuthorize requires no UNIX kernel changes or system reboots.
Detailed Auditing for UNIX and Linux with Centrify DirectAudit

Centrify DirectAudit helps you comply with regulatory requirements, perform in-depth troubleshooting, and protect against insider threats for your UNIX and Linux systems. DirectAudit’s detailed logging strengthens your compliance reporting and helps you spot suspicious activity by showing which users accessed what systems, what commands they executed, and what changes they made to key files and data. With DirectAudit you can also perform immediate, in-depth troubleshooting by replaying and reporting on user activity that may have contributed to system failures. And its real-time monitoring of current user sessions enables you to spot suspicious activity.

6.1 DirectAudit’s Key Features and Benefits

Some of DirectAudit’s key features and benefits include:

- **Enhance compliance with regulatory requirements.** Practically every industry and government compliance regulation (including SOX, PCI, HIPAA, FISMA, and GLBA) requires comprehensive logging and audit trails of user activity, especially on business-critical and sensitive systems. DirectAudit meets these needs by capturing detailed user session information – who logged into what systems, what commands they executed, what changes they made to key files and data. DirectAudit’s flexible querying and reporting features enhance your ability to document compliance and provide robust tools for identifying and investigating potential security breeches. With DirectAudit you can now answer questions such as:
  
  o Who has logged onto our UNIX servers running our ERP apps over the last month, and what did they do?
  
  o What was that recently fired systems administer doing on our systems last week?
  
  o Has anyone been editing these key system files, or typing any suspicious commands?

- **Perform in-depth troubleshooting and configuration reporting.** From DirectAudit’s central console you can quickly locate and replay user activity that may have contributed to a system outage. DirectAudit captures detailed session activity – both keystrokes and session output – so you can diagnose immediate problems or report on and document configuration and other changes. With DirectAudit you can now answer questions such as:

  o Over the last few hours, did anyone do anything to this system that just went down?

  o Did anybody change the Oracle config file on sol-ora-4 yesterday?
Did Operations actually apply that required patch on all 10 of our web servers over the weekend?

What steps did that consultant take to fix the problem on our file server?

- **Protect against insider threats and monitor real-time user activity.** DirectAudit lets you centrally view who is currently accessing all of your distributed UNIX and Linux systems and immediately drill down to see what they are doing. This real-time monitoring helps you proactively spot insider threats and gives you global visibility into activity across your organization. With DirectAudit you can now answer questions such as:

  o Who is logged on to our HR database server, and what are they doing?
  
  o Is anyone currently logged on to those development systems that we need to restart?

### 6.2 The DirectAudit Architecture

Centrify DirectAudit’s next-generation, enterprise-scale architecture was designed to be highly scalable, secure and reliable. It consists of four components. The low overhead DirectControl Agent transparently gathers comprehensive user session activity and communicates it in an encrypted, compressed format to a DirectAudit Collector Service. These load-balanced Collector Services in turn forward session data to the central DirectAudit Repository running on a Microsoft SQL Server database. The DirectAudit Console gives you a centralized view of every user session on every audited UNIX and Linux system across your enterprise. With a simple right-click you can replay any user session to see what commands were executed, what changes were made to key files and data, and what system output appeared. You can also perform full-text searches to find, for example, all instances of a password command across all sessions.

### 7 Summary: Why the Centrify Approach Makes Sense

Centrify’s approach of extending Active Directory to your UNIX, Linux, Mac, web and database platforms is a fundamentally good approach for the following reasons:

- **Active Directory has emerged as a powerful, scalable platform that is built for the enterprise.** Active Directory is built on two open, enterprise-ready foundations — LDAP for directory management and Kerberos for secure authentication across the network. It is a highly scalable platform and integrates well not only with business-critical applications such as email, but also with key infrastructure components (DNS, certificate services, firewall/proxy/VPN, Radius, etc.). Active Directory is a proven and established technology supported by Microsoft – the world’s largest software manufacturer.
- **Group Policy provides integrated bulk configuration and security policy management.** Active Directory extends identity and access management to provide powerful tools that, with the Centrify Suite, you can now use to configure UNIX/Linux/Mac systems as well. You finally also have the ability to enforce consistent enterprise-wide security policies, which is key to strengthening security generally and also complying with regulatory requirements.

- **Active Directory is a permanent, integral part of your Windows infrastructure upon which you can build a sustainable business plan.** Active Directory is the foundation upon which Windows Server 2003, Windows XP and future Windows versions are built. It is a known quantity and is typically already part of your IT plan and budget for the future. On the UNIX/Linux/Mac side, you must sort through a cacophony of point products that provide half measures and result in continual integration projects. The Centrify Suite now steps forward to demonstrate how you can build a rational business plan that points the way toward true reduction in expenses and streamlining of your IT environment.

- **You can leverage your already significant investment in Active Directory.** If you have implemented Active Directory, you have already invested substantially in software, migrating accounts, and training your IT staff. Through the Centrify Suite you now have a single, centralized tool – the Active Directory interface – to administer Windows, UNIX, Linux and Mac systems and control access to Java/web applications, databases, and ERP applications. Why spend even more money trying to deploy and maintain a separate costly, complex fragmented infrastructure and training users on different user interfaces when you already have a comprehensive, enterprise-class directory that can deliver even more functionality? With the Centrify Suite, you can leverage what you have already deployed, enabling you to do a lot more with a lot less.

For some organizations, consolidating identity and access management in Active Directory may be hard to initially accept because of the widespread view that Active Directory is limited to the Windows platform. But now Centrify provides a flexible, cost-effective way to incrementally extend Active Directory on a system-by-system basis. This stands in clear contrast to the all-or-nothing approach required by existing Identity Management vendors who deliver complex synchronization solutions. The dream of significantly reducing the plethora of identity stores has become a reality. And Centrify offers the only solution whose Active Directory-based authentication, authorization and auditing capabilities for cross-platform environments are built on a single, integrated architecture and delivered as a comprehensive suite.

The bottom line is that, with Centrify, you can now fully leverage your investment in Active Directory to address regulatory compliance, strengthen security, and enhance IT and end-user efficiency and productivity.
### How to Contact Centrify

<table>
<thead>
<tr>
<th>Region</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>North America (And All Locations Outside EMEA)</strong></td>
<td></td>
</tr>
<tr>
<td>Centrify Corporation</td>
<td>444 Castro St., Suite 1100</td>
</tr>
<tr>
<td>Mountain View, CA 94041</td>
<td>United States</td>
</tr>
<tr>
<td>Sales:</td>
<td>+1 (650) 961-1100</td>
</tr>
<tr>
<td>Enquiries:</td>
<td><a href="mailto:info@centrify.com">info@centrify.com</a></td>
</tr>
<tr>
<td>Web site:</td>
<td><a href="http://www.centrify.com">www.centrify.com</a></td>
</tr>
</tbody>
</table>

| **Europe, Middle East, Africa (EMEA)** |                |
| Centrify EMEA                     | Asmec Centre    |
| Merlin House                      | Brunel Road     |
| Theale, Berkshire, RG7 4AB        | United Kingdom  |
| Sales:                            | +44 1189 026580 |

© 2004-2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.