Centralized Management for UNIX, Linux, Mac and Java with Active Directory and DirectControl

Centrify DirectControl delivers secure access control and centralized identity management by seamlessly integrating UNIX, Linux, Mac, J2EE and web platforms with Microsoft Active Directory.

ABSTRACT

Centrify™ DirectControl™ 3.0 enables a secure, connected computing environment by seamlessly integrating your UNIX, Linux, Mac, Java and web platforms with Microsoft Active Directory’s identity, access and policy management services. With its patent-pending Zone technology, Centrify delivers the only solution that does not require intrusive reconfiguration of existing systems and provides the granular administrative control needed to securely manage a diverse set of systems and applications. With DirectControl, you can now fully leverage your investment in Active Directory to significantly strengthen security, reduce infrastructure costs, streamline IT operations and better comply with regulatory requirements.

This white paper examines the compelling business and technical case for centralizing administration in Microsoft’s Active Directory, describes how DirectControl’s integrated architecture enables you to extend Active Directory to your UNIX, Linux and Apple Mac systems and applications, and describes DirectControl’s unique benefits.
Contents

Introduction ......................................................................................................................... 1
  1.1 The case for extending Microsoft Active Directory to non-Microsoft
environments .................................................................................................................. 1
  1.2 The balkanization of Access Control, Identity and Policy Management within the
distributed environment .............................................................................................. 2

2 Cross-Platform Secure Connected Computing: A “must have” solution ........ 4
  2.1 Alternatives for solving the Secure Connected Computing crisis ...................... 5

3 The Centrify DirectControl solution ................................................................. 7
  3.1 Extended Identity and Access Management with Centrify Zones ............. 8
  3.2 Centrify DirectControl Management Tools on Windows ...................... 10
    3.2.1 Centrify DirectControl property extensions ......................................... 10
    3.2.2 Centrify DirectControl Administrator Console .................................. 10
    3.2.3 Using the DirectControl Management Tools ...................................... 11
  3.3 DirectControl UNIX/Linux/Mac architecture .............................................. 12
    3.3.1 NSS module ..................................................................................... 13
    3.3.2 PAM module .................................................................................. 14
    3.3.3 Kerberos libraries and Software Development Kit .............................. 15
    3.3.4 Command line interface tools ......................................................... 16
    3.3.5 DirectControl Group Policy architecture ........................................ 16
    3.3.6 NIS Server .................................................................................... 17
    3.3.7 DirectControl for Samba ................................................................ 17
    3.3.8 Apache and SPNEGO modules ........................................................ 18
    3.3.9 J2EE modules ............................................................................... 18
  3.4 Support for Microsoft ADFS .............................................................................. 18

4 Summary .................................................................................................................... 19
  4.1 Core features and benefits ............................................................................. 19
  4.2 Why the Centrify approach makes sense ...................................................... 21

5 How to contact Centrify ....................................................................................... 22
Introduction

Centrify enables a secure, connected computing environment by seamlessly integrating your UNIX, Linux, Mac, Java and web platforms with Microsoft Active Directory’s identity, access and policy management services.

Centrify’s extension strategy grew 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.
- The use of Linux within the enterprise is growing even though there is a dearth of Linux identity and policy management tools.
- Companies are faced with a proliferation of identity systems, 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.

With its patent-pending Zone technology, Centrify delivers the only solution that does not require intrusive reconfiguration of existing systems and provides the granular administrative control needed to securely manage access to a diverse set of systems and applications.

This white paper introduces the solution architecture and benefits of Centrify DirectControl, and describes how DirectControl 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 and applications 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 running on those servers. The reality is that mixed Windows, Mac and UNIX/Linux environments are a fact of life for almost all IT organizations. 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, Java and web platforms is probably most pronounced as it relates to Access Control, Identity Management and Policy Management. Access Control allows organizations to deterministically grant users appropriate access to corporate resources – regardless of the platform that is being used. Identity Management is the set of processes and technologies involved in storing user information and granting rights based on authentication and authorization rules. Policy Management is a system for centrally defining policies for groups of systems and users and enforcing those policies in an automated way.

1.2 The balkanization of Access Control, Identity and Policy Management within the distributed environment

In the Windows environment, Microsoft provides a comprehensive Access Control, Identity and Policy Management solution through Active Directory. Numerous IT organizations have invested millions of dollars deploying Active Directory as a replacement for the 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 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 controlled 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, it is 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.

The situation is even worse for enterprise-class Policy Management for UNIX, Linux and Mac systems. Solutions are either incomplete and only focused on a limited set of platforms, or they are require a large investment for a non-integrated point product. In both these cases, the solutions are incompatible with Windows-based Group Policy and therefore require major resources to set up and maintain in order to provide consistency across multiple platforms.

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. The fact is that in most organizations, Access Control, Identity and Policy Management for UNIX/Linux/Mac systems and applications is quite balkanized compared to Windows.

Figure 1-1. Balkanization of Identity Management in the distributed environment: one user, multiple accounts, multiple identity stores.
Cross-Platform Secure Connected Computing: A “must have” solution

An obvious question is: Why haven’t organizations been able to standardize on one access control, identity and policy 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 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 policy 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 Meta 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 Meta 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 and policy 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 meeting regulatory compliance requirements (such as Sarbanes-Oxley, HIPAA, GLBA). An increasing number of 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 access, identity and policy solution. For example, it may be impractical to integrate a mainframe identity system into a centralized environment. Still, a significant reduction of identity, access and policy systems 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 meet regulatory requirements.

2.1 Alternatives for solving the Secure Connected Computing crisis

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

By using a central directory system, the goal would be to select 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.

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 UNIX, Linux and Mac systems and Java/web applications. Hence this third and most practical approach couldn’t be implemented – until now.

3 The Centrify DirectControl solution

Centrify DirectControl delivers secure access control and centralized identity and policy management by seamlessly integrating UNIX, Linux, Mac, J2EE and web platforms with Microsoft Active Directory. With DirectControl, organizations can improve IT efficiency, better comply with regulatory requirements, and move toward a more secure, connected infrastructure for their heterogeneous computing environment. DirectControl is non-intrusive, easy to deploy and manage, and is the only solution that enables fine-grained access control, reporting and auditing through its unique Zone technology.

![Diagram showing Centrify DirectControl integration with Active Directory](image)

**Figure 3-1.** Centrify eliminates the need for multiple Access Control, Identity and Policy Management solutions in the distributed environment by consolidating management in Microsoft Active Directory: one user, one account, one directory, one policy.

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

- On the UNIX/Linux/Mac platform, a **DirectControl Agent** is installed on each server or workstation. The DirectControl Agent is not a single piece of code; rather, it is a central service that interacts with a suite of underlying service modules.
Different modules are installed and activated depending on the features that are required for a particular system. The Agent allows an administrator to join the UNIX computer to an Active Directory domain as is done with Windows machines. The Agent also determines which DirectControl-enabled users can log in to the system or access applications using their Active Directory credentials. Optional services are included to route NIS and other infrastructure requests to Active Directory.

- On the Windows platform, the DirectControl Management Tools are installed on one or more Windows computers in the domain. These tools are comprised of a Microsoft Management Console (MMC) application and property extensions to the Active Directory Users and Computers MMC. IT administrators use the DirectControl Windows management tools to configure users, group and computer properties and control access to non-Microsoft systems and applications. These tools also allow administrators to report on the properties and rights for users, groups and computing resources.

3.1 Extended Identity and Access Management with Centrify Zones

One of the core features that warrants further discussion is Centrify’s innovative Zone technology. It is neither desirable nor practical to allow all users in an enterprise to log on to all UNIX/Linux/Mac systems. In addition, it is very hard to ensure that UNIX/Linux/Mac UIDs are unique throughout the enterprise. This is especially true when user accounts held in NIS, /etc/passwd files or LDAP-based directories are migrated to Active Directory. To deal with this, Centrify has developed the concept of Zones. DirectControl Zones are similar to NIS domains and sub-domains (but the term “domain” already has a specific meaning in Active Directory).

![Figure 3-2. An example of Zoning.](image-url)
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 user (Joan Smith in Figure 3-2) 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 3-2 illustrates, Joan authenticates through Active Directory 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. For example, it would not be appropriate for the administrator of the company’s web site to also have the ability 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 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.
3.2 Centrify DirectControl Management Tools on Windows

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

3.2.1 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.

Figure 3-3. DirectControl property extensions for Active Directory Users and Computers.

3.2.2 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/Mac systems.
- Create groups of computers, called Centrify Zones, so that you can assign access to systems based on Centrify 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.

Figure 3-4. DirectControl Administrator Console.

3.2.3 Using the DirectControl Management Tools

With either the Centrify DirectControl property extensions or the Centrify DirectControl Administrator Console, you can enable DirectControl-managed UNIX/Linux/Mac systems to authenticate users through Active Directory. You can enable two types of access:

- Log on to the UNIX shell through telnet, ssh, graphical desktop, etc. (which is enabled by default when you join the computer to Active Directory), and/or
- Log on to Java and web-based applications running on the computer. You can authorize access individually for each type of web server running on that computer – Apache, JBoss, Tomcat, IBM WebSphere or BEA WebLogic.
The Centrify DirectControl Management Tools 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/Mac users and computers join your Active Directory domain, the Centrify DirectControl Agent unobtrusively stores its data in an Active Directory Program Data container using a standardized method. Centrify DirectControl also works seamlessly and unobtrusively with Active Directory if you have previously installed Microsoft Services for UNIX (SFU), which applies its own schema changes to Active Directory. DirectControl also works with Microsoft’s new UNIX schema extensions that have been included in Windows Server 2003 R2.

3.3 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.

Figure 3-5. Core DirectControl UNIX architecture.

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 into Active Directory are also included.

The following sections describe each service module in more detail.

### 3.3.1 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.

3.3.2 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 is also 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.

### 3.3.3 Kerberos libraries and Software Development Kit

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) where customers can download 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 to enable searching and retrieving information stored in Active Directory. Support is included for C/C++, Java, Perl, PHP and Python interfaces. These APIs give developers the ability to programmatically accomplish tasks such as:

- Authenticating users.
- Checking user authorization.
- Looking up objects in Active Directory.
- Creating, modifying and deleting users.
- Changing passwords.

These capabilities are useful in many scenarios:

- Enhancing server-based applications to perform role-based authorization.
- Creating systems administration scripts.
- Allowing applications to perform custom authentication requests through Active Directory.
3.3.4 Command line interface tools

DirectControl provides a robust set of command line interface (CLI) tools. Here are some of the tasks you can perform using these interfaces:

- Join a machine to a domain.
- Leave a domain.
- Change a user password.
- Create a new user in Active Directory.
- Delete a user in Active Directory.
- Display machine status.

3.3.5 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.

The DirectControl Agent will at various times load the Group Policy settings into its virtual registry. This load is triggered by:

- **System startup.** When the DirectControl daemon starts up (usually when the system boots up), it sets the machine registry.
- **User log on.** When a user logs on, the DirectControl Agent loads the user’s settings.
- **Signal or time out.** The DirectControl Agent can be signaled to reload. It will also refresh the registry on a periodic basis.

The loading of policy is asynchronous (this is equivalent to the behavior in recent Windows versions). The loaded settings are stored on the local machine for disconnected operation.

Centrify includes a unique set of Active Directory Group Policies that are specific to UNIX, Linux and Mac platforms. These policies can be applied to users or systems, as appropriate. DirectControl includes more Group Policy objects than any other solution including objects to 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 and a growing list of other settings that are suitable for being centrally managed. Group Policies can also be used to assist with the configuration management of the DirectControl Agent.

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. Centrify’s Group Policy module ensures that your systems are secured in a consistent, enforced manner.

For added flexibility, you can also create your own custom administrative templates. On the UNIX systems, you can use standard Perl scripting to create your own mapping programs that update relevant configuration files.

### 3.3.6 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. 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 machines on the network. 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.

### 3.3.7 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.
3.3.8 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.

3.3.9 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).

3.4 Support for Microsoft ADFS

Microsoft Active Directory Federation Services (ADFS) is a new component in Microsoft Windows Server 2003 R2 that provides single sign-on services for web-based applications. Using their Active Directory credentials, users can access multiple web applications over the life of a single online session. ADFS accomplishes this by securely
sharing digital identity and entitlement rights or “claims” across security and enterprise boundaries.

Before ADFS was available, Active Directory authentication was typically used to provide an SSO experience for Windows clients and applications within the organization’s security or enterprise boundaries. ADFS extends this functionality to Internet-facing applications beyond the organization’s enterprise boundaries. This allows customers, partners, and suppliers to have a similar SSO user experience when they access the organization’s secure web-based applications. Furthermore, federation servers can be deployed in multiple organizations to facilitate business-to-business (B2B) federated transactions between partner organizations.

Centrify solution for Active Directory Federation Services is the first solution that extends Microsoft’s federated identity management services to web-based applications running on non-Microsoft platforms. With the Centrify solution, you can use Microsoft ADFS to provide secure, federated identity management for applications hosted on Apache and popular J2EE web servers, including IBM WebSphere, BEA WebLogic, JBoss and Tomcat.

By having secure identity solutions for both internal intranet applications and external extranet applications, Centrify provides the most options for secure web application integration for non-Windows platforms working with Active Directory.

4 Summary

4.1 Core features and benefits

As you have seen from the detail product description in the prior section, Centrify DirectControl’s core feature is its ability to enable UNIX, Linux and Mac servers and workstations to participate seamlessly in an Active Directory domain, establishing Active Directory as your single point of administration and security policy enforcement for your heterogeneous environment. Centralizing user account management in Active Directory also eliminates common security exposures, such as the existence of orphan accounts and the proliferation of usernames and passwords that end users need to remember. Other features and associated benefits for DirectControl include:

- **Secure access to critical systems using DirectControl Zones.** DirectControl’s unique Zone technology is the only solution that provides the granular, enterprise-class access controls needed to manage a diverse environment. With DirectControl, any logical grouping of mixed UNIX, Linux or Mac systems can be segregated within Active Directory as a Centrify Zone. Each Zone can have a unique set of users, a unique set of administrators, and a unique set of security policies. DirectControl’s out-of-the-box reports can confirm for auditors who has access to which systems. For most customers, the DirectControl Zones capability for advanced access control is the “must have” feature that enables them to meet SOX and other security requirements.
• **Deliver web single sign-on at a fraction of the cost of more complex point products.** 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. The Centrify solution extends ADFS to Apache, WebLogic, WebSphere and JBoss applications that are running not only on non-Microsoft servers such as Red Hat and Solaris but also on Windows servers. The combination of ADFS plus DirectControl 3 provides a complete federated identity management solution without the need to deploy any additional federated identity software.

• **Deploy a unified, standards-based solution without intrusive changes to Active Directory.** DirectControl does not install any software on domain controllers, nor does it require any changes to the Active Directory schema to store UNIX identity data. DirectControl supports RFC 2307 via the Active Directory schema that Microsoft introduced with Windows Server 2003 R2. IT managers can take advantage of DirectControl’s ability to map multiple UNIX identities to a given Active Directory account, and can use straightforward ADSI and LDAP searches to access the UNIX data that DirectControl stores in Active Directory — without introducing any proprietary schema modifications. In addition, DirectControl’s unified architecture delivers identity management, access control and policy enforcement through an all-in-one Agent, making it the easiest Active Directory-based solution to deploy and manage.

• **Adopt a comprehensive solution with the industry’s broadest support for systems, applications and third-party tools.** DirectControl provides a single solution for more than 50 operating system versions, including not only Solaris, Red Hat, AIX, HP-UX (including Trusted Mode) and SUSE, but also Mac OS X, VMware and Debian. This includes support for an extensive array of both 32- and 64-bit systems. DirectControl also supports the most popular J2EE and web application servers: Apache, JBoss/Tomcat, WebLogic and WebSphere. DirectControl is also unique in providing robust integrated support for the Open Source Samba file server. In addition, the Centrify Resource Center delivers the industry’s broadest set of free downloads of Open Source tools such as OpenSSH and PuTTY that have been enhanced to work seamlessly with Active Directory via DirectControl.
4.2 Why the Centrify approach makes sense

Centrify’s approach of extending Active Directory to UNIX/Linux/Mac systems and Java/web applications is a fundamentally good approach for the following reasons:

- **Active Directory has emerged as a powerful, scaleable 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 Centrify DirectControl, 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. Centrify DirectControl now steps forward to demonstrate how you can build a rational business plan that points the way toward true reduction in expenses and streamlining your IT environment.

- **You can leverage your already significant investment Active Directory.** If you have implemented Active Directory, you have already invested substantially in software, migrating accounts, and training your IT staff. Through DirectControl you now have a single, centralized tool – the Active Directory interface – to administer Windows, UNIX, Linux and Mac systems and Java/web 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 DirectControl, 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 policy 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.

The bottom line is with Centrify, you can now fully leverage your investment in Active Directory to significantly strengthen security, reduce infrastructure costs, streamline IT operations, and better comply with regulatory requirements.

5

How to contact Centrify

Centrify Corporation
444 Castro St., Suite 1100
Mountain View, CA 94041

U.S. Sales Office: +1 (650) 961-1100
Enquiries: info@centrify.com
Web site: www.centrify.com