Identify. Simplify. Centrify.

Centrify™

Top Five Benefits of Using Windows Group Policy to Secure and Manage UNIX, Linux and Mac Systems

WHITE PAPER

CENTRIFY CORP.

MARCH 2008

By Jeremy Moskowitz & David McNeely

Centrify DirectControl's ability to extend Windows Group Policy to Linux, UNIX and Mac systems now points the way toward consolidated, centralized and consistent cross-platform policy enforcement.

ABSTRACT

Applying standardized security and configuration policies to enforce IT security requirements and meet government and industry regulations remains one of the most difficult challenges for organizations with large numbers of mixed Windows, Linux, UNIX and Mac computers. Since the release of Windows 2000, IT administrators have used Group Policy to globally distribute computer and user policies across their Windows environment. No single solution addresses the same need across all Linux vendors and distributions, and the same is true of UNIX vendors. Centrify DirectControl's ability to extend Windows Group Policy to Linux, UNIX and Mac systems now points the way toward consolidated, centralized and consistent cross-platform policy enforcement.

This white paper is for Linux, UNIX and Mac system administrators who are unfamiliar with Windows Group Policy and want to know what it can do for them, how it works, and what they can expect to accomplish with it. Windows administrators will benefit from understanding what types of Linux, UNIX and Mac security and configuration settings they can control using their familiar Windows Group Policy tools.

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

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

© 2008 Centrify Corporation. All rights reserved.

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

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

[WP018-2008-03-28]

Contents

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

About the Authors

Jeremy Moskowitz
Author, Instructor, Infrastructure Architect, Moskowitz, Inc.

Jeremy Moskowitz is one of less than a dozen Group Policy MVPs. He is the Chief Propeller-Head of Moskowitz, Inc. He is an independent consultant and trainer for Microsoft Windows and Linux technologies, specifically in the areas of Group Policy and Windows/Linux integration. He runs two community forums, www.GPanswers.com and www.WinLinAnswers.com, that answer tough questions about Windows Group Policy and Windows/Linux integration. Jeremy's books include *Windows and Linux Integration* and the upcoming companion books *Group Policy Fundamentals, Security, and Troubleshooting* and *Creating the Secure Managed Desktop: Group Policy, SoftGrid, and Microsoft Deployment and Management Tools* (due out in April 2008). Learn more about the new books at GPanswers.com/book.

David McNeely
Director of Product Management, Centrify Corporation

As Director of Product Management, David works with customers to drive the roadmap for Centrify's award-winning DirectControl solution. David was previously Technical Marketing Manager at ActivCard, where he launched the company's new Single Sign-On product. His 18-plus years of industry experience also include several roles at Netscape, including Director of Product Management for the Netscape Directory and Security product line.

Introduction

Applying standardized security and configuration policies to enforce IT security requirements and meet government and industry regulations remains one of the most difficult challenges for organizations with large numbers of mixed Windows, Linux, UNIX and Mac computers. Since the release of Windows 2000, IT administrators have used Group Policy to globally distribute computer and user policies across their Windows environment. No single solution addresses the same need across all Linux vendors and distributions, and the same is true of UNIX vendors. IT administrators can turn to third-party solutions that are typically based on setting up a separate policy server, or rely on in-house scripted solutions that are time-consuming to develop, test, and maintain. Apple’s Open Directory and WorkGroup Manager solutions enable IT to globally control Macs, but also require a separate server infrastructure and specialized skills to set up, manage and maintain.

Centrify DirectControl’s ability to extend Windows Group Policy to Linux, UNIX and Mac systems now points the way toward consolidated, centralized and consistent cross-platform policy enforcement. With Windows Group Policy you can configure and enforce policies that control sudoers and crontab files, define home directory setup,

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

enforce screensaver password locks, and apply hundreds of other configuration and security settings. For Mac systems, Centrify also delivers a variety of desktop lockdown policies to, for example, manage access to applications, system preferences and external media.

This white paper is for Linux, UNIX and Mac system administrators who are unfamiliar with Windows Group Policy and want to know what it can do for them, how it works, and what they can expect to accomplish with it. Windows administrators will benefit from understanding what types of Linux, UNIX and Mac security and configuration settings they can control using their familiar Windows Group Policy tools.

How Windows Group Policy Works – a Quick Introduction

By Jeremy Moskowitz
Group Policy MVP

Imagine if you had a way to reach out and touch every machine on your network. Imagine if you could send out specific changes to some of the machines, but prevent those changes from making it to other machines. Imagine if there was an easy way to specify that specific users received settings based on what their job description was, or were automatically deployed software based on precisely the functions they needed to do in the company.

This idea is called "Policy-Based Management." I like to think of the idea as a way to "*get* something because you *are a part* of something." For instance, because Sally works in the Sales department, she gets access to the Sales applications. It sounds simple, and it is. But within that simplicity is a huge amount of power to give you fine-grained control over precisely who leverages what resources in your environment, how secure you want your systems to be, and how every person's user experience in the environment is shaped.

Microsoft's way to perform Policy-Based Management revolves around Active Directory and its policy-delivery mechanism called Group Policy. Some people get confused about Group Policy right away, because it's an unfortunately named technology. Group Policy doesn't apply directly to Active Directory groups. It applies to levels within Active Directory. Specifically, administrators can apply Group Policy to:

- Active Directory Sites
- Active Directory Domains
- Active Directory OUs and sub-OUs

Group Policy settings are stored in Group Policy Objects (GPOs) and they're "linked" to the Active Directory level you want them to apply to.

Group Policy is, by its very nature, a highly extendable technology – and it was always meant to be that way. For instance, you can extend both the native reach of what "categories" Group Policy covers, and also what platforms Group Policy will apply to.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The architecture is very simple: GPOs are stored in Active Directory and then simply "read" by a piece of software on the client computers called a CSE, or Client-Side-Extension. The CSE checks for changes within Active Directory every-so-often (by default at logon for users, at reboot for computers, as well as a background refresh of every 90 minutes with a random offset of up to an additional 30 minutes). Then the client simply processes these changes and the administrator's wish is applied.

By default there are 18 categories of items that are configurable in Group Policy. Many of them are security related, many are desktop look-and-feel related, and still others handle user experience details like where users should store files and which hardware is considered acceptable on the network. Again, these categories are extensible to third parties, and development to "do more with Group Policy" is encouraged by Microsoft. Most administrators seem happy with this too; it's a one-stop-shop place to make settings and configuration changes against a broad category of features.

Group Policy has two "halves": the user half and the computer half. Policies contained on the user side generally only affect user accounts. Likewise, policies contained on the computer side generally only affect computer accounts. In Figure 1 you can see the Group Policy Management Console, which handles the creation and linking of GPOs (amongst other things) and its corresponding Group Policy Object Editor in Figure 2, the main interface when editing GPOs themselves.

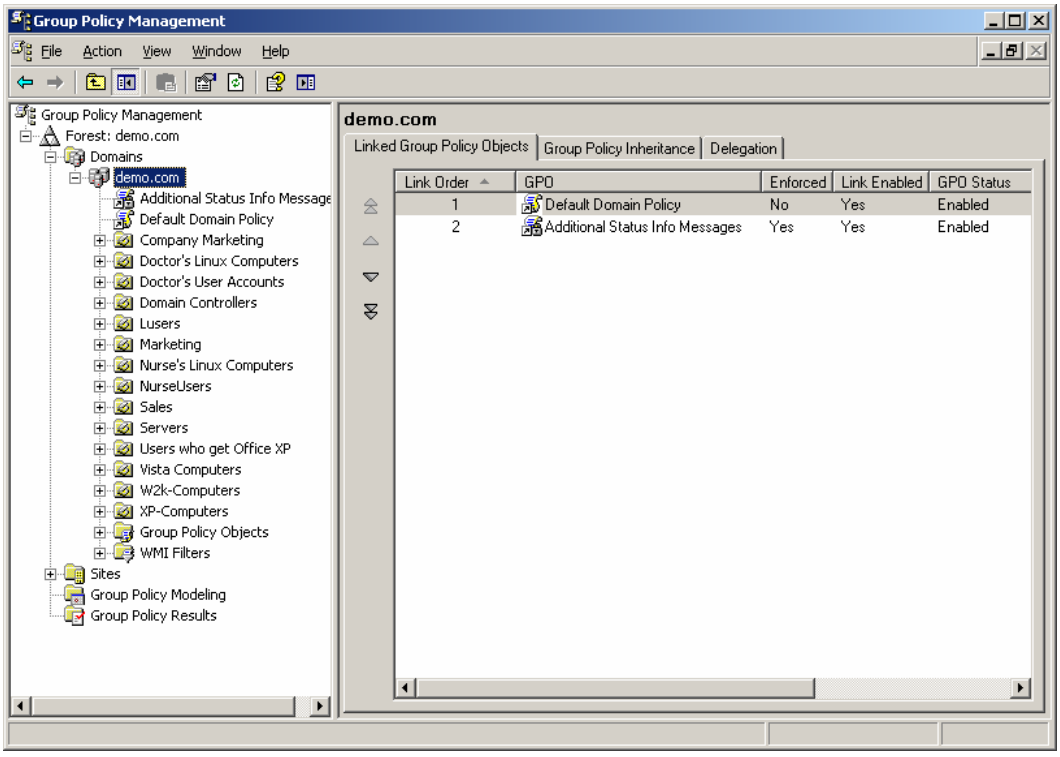

Figure 1. The Group Policy Management Console

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Group Policy has a lot of power. For instance, there are 2,400 possible settings contained within just one category (the Administrative Templates, which mainly deal with look-and-feel settings). But the best news is that you can be granular in your approach when applying settings to users and computers.

Group Policy has several nuanced abilities to ensure that only the people who you want to get policies, will get policies.

One ability is called Group Filtering. Even though GPOs can only be linked to Active Directory Sites, Active Directory Domains, or Active Directory OUs, administrators can filter GPOs to these targets based on what Active Directory groups the users or computers are in (as long as they're also part of the targeted Active Directory Site, Active Directory Domain or Active Directory OU).

Another more complex scenario involves the ability to deploy user-only settings to a specific computer. This is called "Loopback" policy processing. The upshot is that anyone who logs on to a specific machine gets exactly the same settings. This can make short work of ensuring that one group of computers is used exactly the same way by anyone who logs on.

Group Policy is a very powerful mechanism and one which shouldn't be underestimated. The work you do within Group Policy has the potential to affect many hundreds or thousands of machines and users. But with that power comes incredible control. Be sure to learn how to use it to your fullest extent possible, so you're leveraging the Active Directory and client investment you already have.

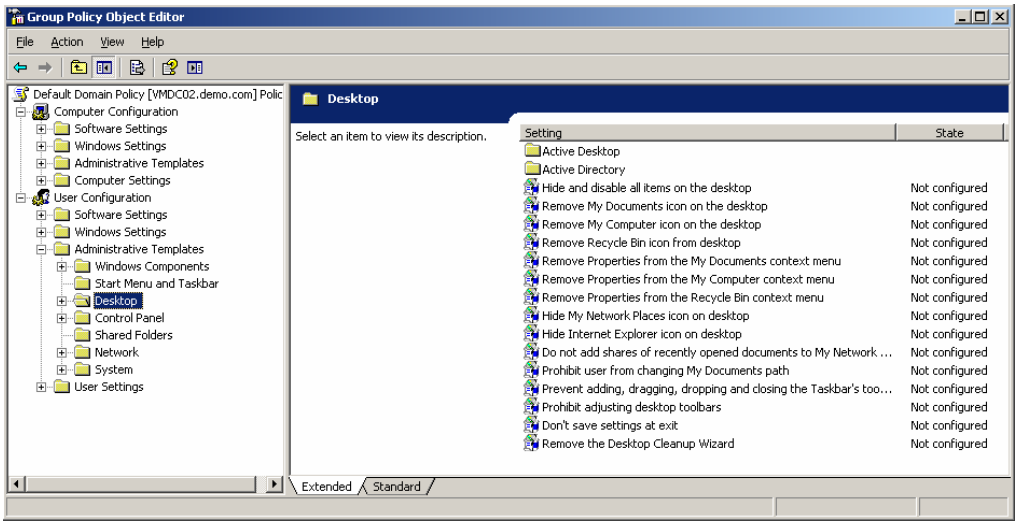

Figure 2. The Group Policy Object Editor

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

How Centrify DirectControl Implements Group Policy

By David McNeely
Director of Product Management, Centrify

Centrify DirectControl enables you to replace your existing practices for bulk configuration of Linux, UNIX and Mac systems with secure, centralized distribution of policies via Windows Group Policy. Before we get into the mechanics, however, let's do a quick review of Centrify DirectControl itself.

Centrify DirectControl's core feature is its ability to enable UNIX, Linux and Mac servers and workstations to participate in an Active Directory domain. DirectControl provides natively compiled software agents for all popular Linux, UNIX and Mac systems. This Agent 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. Additional seamlessly integrated modules snap into the DirectControl Agent to provide services such as web and database single sign-on and Samba integration. DirectControl also includes native management tools to suit administrators in all IT departments: standard Windows-based tools, a web-based administrator console, and a comprehensive UNIX command-line interface. Implementing DirectControl does not require schema changes to your Active Directory or additional software on domain controllers, and is certified for both Windows 2003 and Windows 2008. For a deeper look at DirectControl, request the Centrify white paper, Implementing Detailed User-Level Auditing of UNIX and Linux Systems Using Centrify DirectAudit.

As you read in Jeremy's section, "How Windows Group Policy Works − a Quick Introduction," Windows Group Policy works by setting user and computer registry keys on Windows computers. Since almost all of a Windows system is configured through registry settings, this is a very straightforward way to enforce almost any policy. However, in the non-Microsoft world there is no equivalent to the Windows registry. Computer and user settings are held in text-based configuration files stored in the /etc directory.

To deliver Active Directory's Group Policy capabilities in a Linux, UNIX or Mac computer, DirectControl creates a configuration file that represents a "virtual registry" of the policies that apply to either the computer itself or the users who have logged into the system. A DirectControl mapper program knows how to apply a policy setting by updating the relevant configuration file. On Macintosh systems, DirectControl updates the plist file for the application associated with the particular virtual registry setting and presents the appropriate MCX settings to the operating system for the user logging in.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Just as on a Windows system, the DirectControl Agent loads the required policy settings during any of the following events:

- **System startup.** When the DirectControl Agent starts up (usually when the system boots up), it updates the computer's virtual registry.
- **User log on.** When a user logs on, the DirectControl Agent creates or updates the user's virtual registry settings.
- **On-demand update.** IT administrators can interactively use the adgpupdate command to force the DirectControl Agent to immediately update the user and computer virtual registries.
- **Periodic refresh interval.** The DirectControl Agent will also refresh the virtual registry on a periodic basis according to the Group Policy refresh interval setting in the domain policy.

The loading of policy is asynchronous (this is equivalent to the behavior in recent Windows versions). The loaded settings are stored on the local computer for disconnected operation. Once the virtual registry has been updated through one of the events described above, then either the appropriate mapper program is activated to update or create the configuration file or, on the Mac, the plist file or the appropriate MCX setting.

Centrify includes an extensive set of out-of-the-box policies that are tailored to Linux, UNIX and Mac security and configuration management. 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. See Appendix A for a complete list of policies included with all versions of DirectControl, and see Appendix B for a list of Mac-specific policies.

DirectControl Group Policies are fully integrated with the standard Group Policy Object editor. Because Sudo policies are such a common and powerful way to manage user permissions, Centrify has added advanced editing features to make it easier to create and manage them, as shown in Figure 3.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

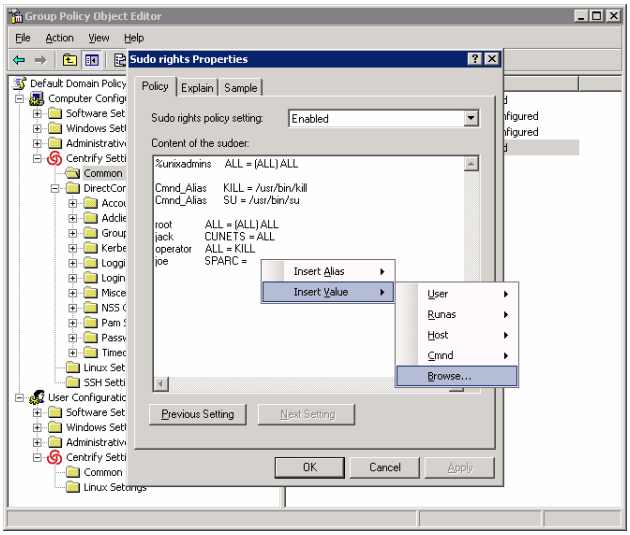

Figure 3. Free-form editing, a syntax checker, and the ability to insert all standard commands and Active Directory object names make it easy to manage Sudo Group Policies for fine-grained privilege management.

For added flexibility, you can also create your own custom policies. On Linux and UNIX systems, you can use standard Perl scripting to create your own mapping programs that update relevant configuration files which correspond to your own Administrative Templates within the Group Policy Object Editor.

Top 5 Benefits of Using Group Policy to Secure and Manage UNIX, Linux and Mac Systems

Linux, UNIX and Mac system administrators all know that, in theory, securing and configuring their systems is just a matter of editing text files that usually reside within the /etc directory on each computer. In large enterprises, however, manually updating configuration files becomes impractical, and scripted distribution-and-update solutions quickly become convoluted as the scripts attempt to cover a bewildering set of conditions for dealing with failover, refresh periods, platform-specific differences in settings, and more. Policy servers attempt to provide some of this capability but may cover only a subset of platforms, and they represent yet another infrastructure to maintain and monitor.

The Windows Group Policy infrastructure has proven reliable, scaleable and robust through many years of enterprise usage. With the DirectControl Agent for UNIX, Linux and Mac systems, Centrify has replicated the Group Policy engine found in Windows systems. This Group Policy engine is an integral part of the Agent's unified architecture; there are no separate licensing fees to pay, and nothing else to install and configure either on the target systems or your domain controllers. While using the Group Policy feature is purely optional, we have found that, once they understand how Windows Group Policy works, many Linux, UNIX and Mac administrators see compelling benefits to leveraging it across the rest of their enterprise.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Here are the top five benefits that mean the most to our customers.

1. Security. Store and deploy policies from Active Directory.

Centrify DirectControl enables you to store policies securely within the Active Directory system volume (sysvol) and to deploy them from a single, central location. Like Windows policies, Linux, UNIX and Mac policies are communicated over an encrypted and authenticated connection between Active Directory and the target system.

2. Consistency & Reliability. Apply policies consistently across your enterprise

In a highly distributed cross-platform environment, ensuring that the same policy is distributed to every machine, on every platform, in an automated and reliable fashion is a complex and thus illusive goal. Even if you do manage such a feat, maintaining the resulting patchwork of solutions for all platforms is painful, as is the reporting your organization may need in order to meet IT security and/or compliance requirements.

Linux, UNIX and Mac systems that have been joined to Active Directory using DirectControl will be able to take full advantage of your existing Active Directory domain controller infrastructure. The DirectControl Agent uses the same logic for finding and communicating with domain controllers as Windows systems do, immediately and easily delivering fault tolerance and failover that previously was so hard to achieve.

While no one expects that a Windows policy for, say, restricting application use to a set of pre-approved programs, can be applied as-is to a non-Microsoft system, you now have a structured interface from which to manage and deploy such policies. For every corporate security policy, you can now work within a standard interface to set up analogous Windows, UNIX/Linux and Mac policies. For example, your Windows policy for restricting the use of Windows Media Center can have an analog in a Mac policy to restrict the use of iTunes.

In addition, because policies are stored and distributed centrally from Active Directory, you now also have an automated and reliable way to deploy new and updated policies to heterogeneous systems throughout your environment.

3. Delegated Administration. Specify who can apply policies to sets of systems, and what privileges they have

In many Linux, UNIX or Mac environments, for convenience system administrators are often given access to privileged accounts or elevated privileges so they can log in to a computer they manage, even if all they need to do is make simple changes, such as updating a config file. This gives them access to a much larger number of systems or access to data that they should not have because of their job's role, frustrating IT security and compliance efforts to limit access to sensitive systems to those with a "need to

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

know." It also means that sys admins, once logged in even on a system that they manage, have more privileges than they need to do their jobs.

With DirectControl you can leverage Active Directory's delegation model to authorize system administrators to apply policies only to the computers they manage. You can also use DirectControl Zones to organize non-Windows systems into logical groups (for example, by business function, geography or system type), enabling even finer-grained control. For example, a sys admin may have the ability to grant or deny end-user access to computers in both the QA Zone and Engineering Zone, but have the ability to link Group Policies only to computers in the QA Zone.

The right to apply Group Policy can be granted to administrators without giving them broader administrative privileges on their systems. Group Policy management itself can also be delegated. For example, you can give some system administrators the right to create or modify Group Policies, while others only have the right to link existing policies to computers.

4. IT Efficiency: Reduce IT infrastructure costs and streamline administration with standardized tools and automated provisioning

Standardizing on a single Active Directory-centric policy engine enables IT departments to significantly reduce the amount of time spent managing and distributing policies. A single policy, once written, can be applied to one computer or a thousand, and changes made to a policy get distributed out automatically to affected systems.

One particularly powerful benefit is the "automatic provisioning" of policies on new systems. Once DirectControl is installed on Linux, UNIX or Mac system and that system is joined to Active Directory, the policies in force for the computer's OU are automatically deployed, saving IT additional steps and also ensuring consistency.

All DirectControl-supplied policies for Linux, UNIX and Mac systems can be managed using standard Windows tools such as the Group Policy Object Editor. Thus IT departments can streamline operations by using their current Active Directory tools and processes for enterprisewide policy management. IT productivity can be enhanced because administrators need to be trained on only one set of tools, and they can manage many basic security settings without deep domain knowledge of, say, sudo or of Mac desktop configuration.

5. Auditing. Enhance compliance reporting with a global view of policy settings

IT security administrators and compliance auditors can now see, from a single administrative interface, what policies are applied to what systems. You can also leverage existing reporting tools to simplify security reporting and auditing of policies.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Top 5 'Must-Have' Group Policy Features that DirectControl Delivers

Supporting Group Policy means more than just enabling administrators to copy files across the network. To get the full benefit of Active Directory's policy engine, you need a solution that fully leverages its power and flexibility.

Centrify DirectControl's feature set has been shaped by our experience working with hundreds of customers in industries where security and compliance are the key drivers for consolidating identity management within Active Directory. These include customers in the retail, banking/finance, pharmaceutical, and healthcare industries who rely on Linux and UNIX servers for business-critical services, as well as publishing and educational institutions that rely on Mac desktops to keep their workforce productive. Here are the features that have made a difference with these customers.

1. Support for both user and computer policies

In most IT organizations, it is not uncommon for system administrators or even end-users to have different roles – and therefore need different configurations or security settings – as they roam from one system to another. Windows Group Policy provides fine-grained control over policy enforcement with the ability to assign policies to either computers or to users. DirectControl extends this same ability to Linux, UNIX and Mac systems.

In a non-Windows environment, a user-specific policy (for example, a sudoers entry enabling a specific user to execute a commands as root) would need to be propagated to every system where that user might potentially log in; using Windows Group Policy, this policy can be stored and distributed centrally. The Group Policy engine on a DirectControl-managed system is able to determine the correct policies to retrieve during system startup and user login using the same hierarchical inheritance rules that a Windows system uses. The same user could be given root permissions on all computers in one organizational unit (OU), and that permission would follow him as he logged into different systems within that OU, but he would not have the same permission when logging into computers in another OU. If that permission was withdrawn, in a non-Windows environment that would require touching the sudoers file on every machine where the user might have been given that permission, a practice that can be slow and error-prone. With Group Policy, the policy would take effect the next time the user tried to log into any system in the OU (or an update could be pushed out manually on demand).

2. Support for advanced features – filtering and loopback processing

Two other key features to look for are filtering and loopback processing. Filtering (sometimes called security filtering) enables you to selectively apply a policy to individual computers or users. For example, within a department of 25 HR people you may have only five who need access to a particular personnel application. Using filtering you could apply a policy that enables access to that application to just those five members

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

within the HR department. Without filtering, you can get that level of granularity only by creating nested OUs or multiple policies, adding needless complexity.

Loopback processing also provides flexibility in large organizations with roaming users. In most cases, policies are applied based on where the user's account lives within Active Directory. However, sometimes a policy – such as mapping to the nearest printer – needs to be based on the location of the computer. Loopback processing enables you to apply policies based on what computer the user logs into.

In both cases, these features have been designed to replicate the behavior that Windows administrators expect of Group Policy. Support for these features is a sign of a mature and comprehensive solution.

3. Wide array of out-of-the-box policies

Centrify DirectControl comes with 225+ out-of-the-box policies so you don't have to do all the work researching, writing and testing configuration settings. These policies cover a broad range of tasks that go beyond the basics like controlling sudo, copying syslogs and other files. For example, recognizing that Linux and UNIX administration heavily rely on SSH, Centrify delivers a comprehensive set of policies for configuring who can connect to a system using SSH and what they can do once connected. See Appendix A on page 14 for a list of included policies. With comprehensive functionality also comes the need for comprehensive documentation, which Centrify delivers with a 150+ page *Centrify DirectControl Group Policy Guide*.

4. Desktop lockdown policies optimized for specific platforms, particularly the Mac

Configuring and securing a server and a desktop are significantly different tasks. Mac systems in particular are more commonly deployed as desktops, and performing tasks such as locking down applications, controlling software updates, preventing access to external disks, and configuring desktop look-and-feel require policies written for that purpose and for that platform. Centrify delivers the only solution with a comprehensive set of out-of-the-box Mac desktop policies so that you're not forced to create and test them yourself. See Appendix B for a list of policy settings you can control with DirectControl for Mac OS X. The comprehensive *Centrify DirectControl Administrator's Guide for Mac OS X* provides complete instructions on creating and deploying Mac policies.

5. Integrated architecture for Active Directory authentication, access control and Group Policy services

Especially in the case of server-class computers, Centrify recognizes that enterprises need to minimize the footprint and overhead of the services running on them and limit the impact of software deployments and updates. Just at the Group Policy engine is an

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

integral part of a Windows system, the Group Policy feature was designed from the start as an integral part of DirectControl's unified Agent architecture; there are no separate licensing, installation, configuration or server components required.

Summary

The Group Policy feature that is built in to the DirectControl Agent provides organizations with a consistent and reliable policy engine for their cross-platform environment. Their Linux, UNIX and Mac systems can now be managed using the same infrastructure, tools and processes current deployed for their Windows systems.

- Policies are centrally and securely stored in Active Directory, and securely transmitted over an authenticated and encrypted connection to clients.
- The clients know how to communicate with the existing Active Directory domain controller infrastructure, providing reliable, fault-tolerant delivery of policies.
- Active Directory's rich delegated administration model enables IT departments to grant system administrators some control over policy enforcement without giving them elevated privileges.
- Consistent policies can be developed, maintained, and reported on from a single set of tools. IT and security managers now have a global view of computer and user policies across the enterprise.
- New systems can be automatically provisioned with policies upon joining the Active Directory domain.
- IT departments can streamline their infrastructure and processes by eliminating redundant policy server deployments and time-consuming in-house scripting solutions in favor of a single set of tools on which IT personnel can be trained.

Centrify DirectControl delivers a robust, mature solution for extending Windows Group Policy to Linux, UNIX and Mac systems. The Group Policy feature is an integrated part of the DirectControl agent, with no additional components to license, deploy or maintain on either the client computers or domain controllers. DirectControl delivers an extensive array of both computer and user policies, including desktop lockdown policies for Mac OS X, and support for advanced features such as filtering and loopback processing. IT administrators can be quickly productive with DirectControl's enhanced Group Policy Object Editor tools and extensive documentation.

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

How to Contact Centrify

North America
(And All Locations Outside EMEA)

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

Sales: +1 (650) 961-1100

Enquiries: info@centrify.com
Web site: www.centrify.com

Europe, Middle East, Africa
(EMEA)

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

Sales: +44 1189 026580

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Appendix A. Out-of-the-Box Policies Included with DirectControl

Computer Policies
Computer Configuration categories and policies
Common UNIX Settings
Configuring file copy from SYSVOL
Configuring sudo rights
Configuring crontab entries by group policy
Configuring commands to run by group policy
User's Initial Group ID
User's Initial Group ID
Logging
General Audit Logging Facility
Adclient Audit Logging Facility
NIS Audit Logging Facility
Log Message Queue Size
PAM
UID Conflict Resolution
User Name Conflict Message
UID Conflict Message
User Name and UID Conflict Message
Create K5Login
Create Home Directory
Creating Home Directory Message
Home Directory Permissions
Login
Login Controls
Allow localhost users
Users to Ignore
Groups to Ignore
Minimum User ID
Minimum Group ID
Split Large Group Membership
Password prompts
Login Password Prompt
Change Password Required Text
Change Password Notification Text
Password Expiry Approaching Text
Change Password Prompt for Old Password
Change Password Prompt for New Password

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Change Password Prompt for Confirm New Password
Change Password Old Password Incorrect Error Message
Change Password New Passwords Mismatch Error Message
Change Password Empty Password Error Message
Change Password Policy Violation Error Message
Change Lockout Error Message
Account Expired Error Message
Account Disabled Error Message
Workstation Denied Error Message
Active Directory Inaccessible Message
adpasswd Change Password Disallowed Message
adpasswd Permission Denied Message
adpasswd Account Locked Message
adpasswd Invalid User or Password Message

Network and cache settings

LDAP Connect Timeout
LDAP Response Timeout
LDAP Search Timeout
Maximum Server Connection Attempts
LDAP Cross-Forest Search
Idle Client Timeout
UDP Timeout
LDAP Trust Timeout
LRPC Response Timeout
LRPC2 Receive Timeout
LRPC2 Send Timeout
Object Expiration Time
GC Expiration Time
User Object Expiration Time
Group Object Expiration Time
Cache Negative Lifetime
DNS Cache Size
DNS Cache Timeout
DNS UDP Buffer Size
DNS Force TCP
DNS Server Rotation
Domain DNS Refresh Interval

Kerberos settings

Manage Kerberos Configuration
Forwardable Tickets
Configuration Update Interval
Password Change Interval

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Credential Renewal Interval

Generate Kerberos Version Numbers for Windows 2000

Use DNS to Lookup KDC

Use DNS to Lookup Realms

Group policy settings

Group Policy Machine Mapper List

Group Policy User Mapper List

Group Policy Mapper Execution Timeout

Total Group Policy Mappers Execution Timeout

NSS overrides

NSS password overrides

NSS group overrides

Account prevalidation

Users Enabled For Prevalidation

Allowed Groups For Prevalidation

Denied Users For Prevalidation

Denied Groups For Prevalidation

Prevalidation Update Interval

Prevalidation Service Name

Adclient Settings

Check Interval

Warn Level

Client Minimum Threads

Client Maximum Threads

Cache Encryption

Cache Encryption Type

Cache Cleanup Interval

Force Salt Force Lookup Password from KDC

Configure /etc/nsswitch.conf (Solaris, HPUX, Linux)

Configure /etc/{pam.conf,pam.d} (Solaris, HPUX, Linux, OS/X)

Configure /etc/security/methods (AIX)

Configure /etc/security/user (AIX)

Configure Directory Services (Apple OS/X)

Disable nscd group and passwd caching (Solaris, Linux)

Disable pwgrd (HPUX)

Password caching

Password caching

LDAP fetch count

LDAP fetch count

Merge Local Group Membership

Merge Local Group Membership

Direct Control 2.x Compatible

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Direct Control 2.x Compatible

User mapping

User mapping

Linux Settings

Basic firewall settings

Enforce screen locking

SSH Settings

Banner path

Maximum client alive count

Client alive interval

Deny Groups

Deny Users

Allow Groups

Allow Users

GSSAPI Authentication

GSSAPI Key Exchange

Login Grace Time

Log Level

PermitRootLogin

PAM Authentication

User Policies

User Configuration categories and policies

Common UNIX Settings

Configuring crontab entries by group policy

Configuring commands to run by group policy

Linux Settings

Enforce screen locking

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Appendix B. Out-of-the-Box Mac Desktop Lockdown Policies Included with DirectControl for Mac OS X

Computer Policies
Remote Management
Enable ARD administrator group
Enable ARD report group
Enable ARD management group
Enable ARD interactive group
Services
Enable Personal File Sharing
Enable Windows Sharing
Enable Personal Web Sharing
Enable Remote Login
Enable FTP Access
Enable Apple Remote Desktop
Enable Remote Apple Events
Enable Printer Sharing
Enable Xgrid
Network
Adjust list of searched domains 3
Configure Proxies
Exclude simple hostnames
Use Passive FTP Mode (PASV)
Enable Proxies
Bypass proxy settings for these Hosts & Domains
Enable FTP Proxy
Enable Web Proxy (HTTP)
Enable Secure Web Proxy (HTTPS)
Enable Streaming Proxy (RTSP)
Enable SOCKS Proxy
Enable Gopher Proxy
Configure Proxies using a PAC file
Firewall
Enable Firewall
Enable iChat
Enable iPhoto Sharing
Enable iTunes Music Sharing
Enable Network Time
Block UDP Traffic

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Enable Firewall Logging

Enable Stealth Mode

Internet Sharing

Disallow all Internet Sharing 3

Security

Disable automatic login 3

Require password to unlock each secure system preference

Log out after number minutes of inactivity 3

Use secure virtual memory

Accounts

Login Window Settings

Energy Saver

Put the computer to sleep

Put the display to sleep

Put the hard disk(s) to sleep when possible

Wake when the modem detects a ring

Wake for Ethernet network administrator access

Allow power button to sleep the computer

Restart automatically after a power failure

Software Update Settings

Automatically download and install software updates

Specify Software Update server

User Policies

Application Access Settings

Permit/prohibit access to applications

Permit/prohibit access to applications: Applications

Permit/prohibit access to applications: Utilities

Permit/prohibit access to applications: Server

Permit/prohibit access to applications: Apple Script

Permit/prohibit access to applications: Miscellaneous

Permit/prohibit access to the user-specific applications

Desktop Settings

Start Screen Saver

Dock Settings

Adjust the Dock's icon size

Adjust the Dock's magnified icon size

Adjust the Dock's position on screen

Adjust the effect shown when minimizing the Dock

Animate opening applications

Automatically hide and show the Dock

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Lock Dock Display
Place Applications in Dock
Place Documents and Folders in Dock
Merge with user's Dock
Add other folders to Dock

Media Access Settings

Permit/prohibit access: CDs & CD-ROMs
Permit/prohibit access: DVDs
Permit/prohibit access: Recordable Discs
Permit/prohibit access: Internal Disks
Permit/prohibit access: External Disks
Eject all removable media at logout

Mobility Synchronization Settings

Enable/disable Synchronization
Synchronization Rules: Login & Logout Sync
Enable/disable login & logout synchronization rules
Adjust list of items synchronized at login and logout

Skip these items

Skip items: Starts With
Skip items: Ends With
Skip items: Name Contains
Skip items: Name is
Skip items: Full Path
Skip items: Partial Path

Synchronization Rules: Background Sync

Enable/disable background synchronization rules
Adjust list of items synchronized in the background
Skip items: Starts With
Skip items: Ends With
Skip items: Name Contains
Skip items: Name is
Skip items: Full Path
Skip items: Partial Path

Synchronization Rules: Options

Manually/automatically synchronize background folders

Scripts (Login/Logout)

Login
Logout

Security Settings

Require password to wake this computer from sleep or screen saver

System Preferences Settings

Limit items shown in System Preferences

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

- **Enable System Preferences Pane: Personal**
  - Enable Appearance
  - Enable Dashboard & ExposeE
  - Enable Desktop & Screen Saver
  - Enable Dock
  - Enable International
  - Enable Security
  - Enable Spotlight
- **Enable System Preferences Pane: Hardware**
  - Enable Bluetooth
  - Enable CDs & DVDs
  - Enable Displays
  - Enable Energy Saver
  - Enable Keyboard & Mouse
  - Enable Print & FAX
  - Enable Sound
- **Enable System Preferences Pane: Internet & Network**
  - Enable .Mac
  - Enable Network
  - Enable QuickTime
  - Enable Sharing
- **Enable System Preferences Pane: System**
  - Enable Accounts
  - Enable Date & Time
  - Enable Software Update
  - Enable Speech
  - Enable Startup Disk
  - Enable Universal Access
  - Enable Ink
  - Enable Classic
- **Enable System Preferences Pane: Other**
  - Enable Other Preferences Panes

© 2008 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.