QUEST SOFTWARE
Smart Systems Management

Active Directory Provisioning: More Efficient, More Secure… Wouldn't it Be Nice?

Written by
Don Jones
Concentrated Technology, LLC

WHITE PAPER

Quest Software, Inc.
Attn: Legal Department
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
E-mail: **legal@quest.com**

Trademarks

Contents

Abstract

Most organizations spend far too much time provisioning, de-provisioning, and re-provisioning users in Active Directory. The native tools are inefficient and time-consuming, and the manual processes they require introduce human error that compromises both the security and stability of the environment. In addition, many organizations have equally inefficient but completely separate processes for provisioning their non-Windows systems, adding to administrative overhead and introducing even more security risks.

This white paper explains the challenges of managing Active Directory provisioning using native tools, and the challenges of provisioning in a heterogeneous environment. It also describes the features and functionality that would be desirable in a comprehensive provisioning solution such as Quest One.

Introduction

Provisioning new users, re-provisioning existing users, and de-provisioning departing users —these are some of the biggest identity management challenges faced by today's organizations. However, these tasks can be difficult and time-consuming when using Microsoft Active Directory, a central component of many organizations' identity management infrastructure. Moreover, most of these organizations also have several non-Windows systems that also require provisioning, creating a completely separate and parallel set of identity management challenges.

The fact is that most organizations spend way too much time provisioning, de-provisioning, and re-provisioning Active Directory and their non-Windows systems. These processes are inefficient and time-consuming, and because they are entirely manual, they are subject to a great deal of human error that compromises both the security and stability of the environment. Wouldn't it be nice if Active Directory provisioning was faster, more efficient, and more secure? And wouldn't it be nice if those non-Windows systems could become part of the same faster, more efficient, and more secure identity management process?

The Provisioning Doldrums

Challenges of Native Tools

It's hard to find administrators who enjoy Active Directory provisioning. The native tools available in Windows are incredibly difficult to use and to automate. For example, simply granting permission on a file or folder to a user or group requires nearly a dozen mouse clicks and at least three dialog boxes!

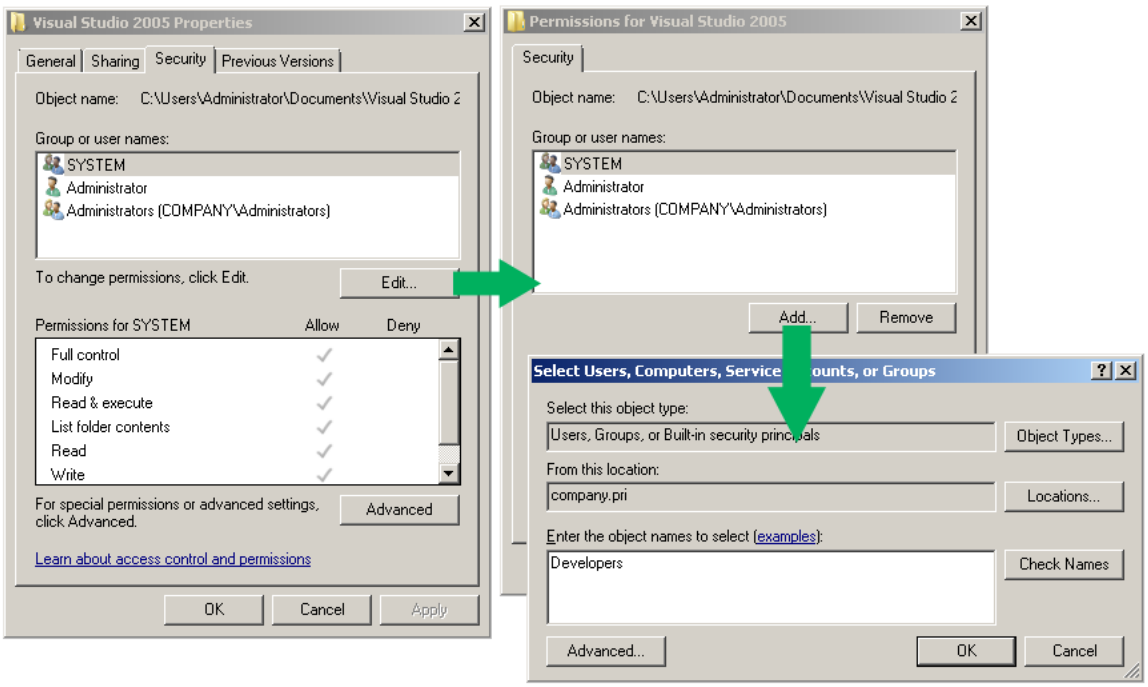

Figure 1. Granting permissions in Active Directory requires multiple steps.

It's even more difficult to inventory user permissions, because Windows doesn't natively provide any central place to store them. Windows also doesn't collect historical permissions, making it impossible to determine who *has had* permissions to a particular resource in the past. It is difficult to accurately map users to their job roles using native tools, making it challenging to determine which resources a user *should* have access to. When new users join the organization or change roles, permission assignment and re-assignment is often a matter of guesswork. Users frequently don't have the permissions they need, creating workload for your help desk. And often they have permissions to resources they *don't* need; this may cause security problems and audit failures. Of course, this assumes the auditors can even figure out what resources your users actually have permission to.

A final problem is that the native Windows tools force you to pretty much rely on the integrity and attention to detail of your administrators to implement your organization's security policy. There's no top-level, policy-based enforcement of security—meaning administrators can do pretty much anything they want to when it comes time to assign permissions.

It would be nice if you could:

- Accurately assign permissions to job roles, rather than individual users or Windows user groups
- Simply place users in the correct job roles to grant and remove permissions to resources
- Track both current and historical permissions in a central location, enabling faster and easier audits and security management

- Enforce your security decisions through a top-level policy

We Don't Live in a Homogeneous World

Does your organization include any Mac, Linux, or Unix computers? What about enterprise applications and legacy systems? Managing resource permissions on those systems is usually *completely* manual, involving an entire additional layer of user accounts, directories, and so forth. There's no true native integration between Active Directory and these non-Windows systems, so users typically have to remember multiple accounts and passwords, and administrators have to learn and execute entirely different patterns for managing permissions and provisioning accounts.

Think about it. When a new user arrives in the organization, someone in your IT department has to create an Active Directory user account, assign it to various user groups, and manage permissions on countless files, folders, databases, shared folders, and more. Someone else has to create accounts on Unix servers, and another person may have to assign permissions on Mac, Linux, and Unix computers, as well as dozens of applications. When multiple administrators are required to manually perform multiple tasks, it's time consuming and error prone.

Even worse, what happens when a user *leaves* your organization? Will your administrators remember *each and every* account that has to be disabled and de-provisioned? You'd better hope so, because if not, you're leaving a back door open for that user to exploit any way they wish. Maybe their next employer could benefit from access to some of your organization's intellectual property?

It would be nice if you could:

- Provision users *once* in Active Directory, and have that automatically extend to non-Windows systems
- De-provision users automatically across the entire enterprise
- Offer your users a single user name and password to use across Mac, Unix, Linux, and Windows systems as well as many applications

Too Many Directories

Most companies have more than one directory, even if you don't always think of some of those things as "directories." For example, you probably have some kind of Human Resources database where user information lives; why not use that to drive your provisioning process, first to Active Directory and from there to drive your Mac, Unix, and Linux provisioning?

Are you using Novell eDirectory? Sun One Directory Server? A directory that supports SPML? Maybe you have an application-specific user database contained in an Oracle or SQL Server database? SharePoint Server? Google Apps? Every one of these directories and databases is *yet another* thing an administrator has to spend time on when provisioning, re-provisioning, or de-provisioning users—as well as *another* place for simple human error to degrade the stability and security of your environment.

Maybe you already *have* an existing identity provisioning framework, such as a metadirectory or identity lifecycle manager, but want to use it to also drive the assignment and removal of resource access permissions. That would truly help automate the entire provisioning process!

It would be nice if you could:

- Drive provisioning activity in *all* of your directories and databases from a single source like Active Directory
- Drive Active Directory itself based on information in external directories or databases
- Maintain two-way synchronization of identities between various directories and databases
- Connect identity management and access management activities in a single, consolidated process

Yes, It Would Be Nice

It would be nice to have an environment that featured automated, enforced, cross-platform and cross-application provisioning. The capabilities you need can be summarized into three essential pillars of functionality:

- **Extend Active Directory to non-Windows systems running Mac OS X, Unix, or Linux.** Give your users a single identity, driven from and controlled by your central Active Directory infrastructure. New accounts are created automatically, and de-provisioned accounts are automatically de-activated across the entire enterprise. Users get a single user name and password, helping to make their jobs easier and lowering your help desk's workload.
- Enable Active Directory to synchronize with external databases and directories, including SharePoint Server, line-of-business applications, and many more, using add-on connectors. Every system on almost any modern operating system can now enjoy two-way identity synchronization. Best of all, identity provisioning can be used to drive automated access management.
- **Automate Active Directory-based provisioning and administration**. Users are assigned to job roles that map directly to their organizational responsibilities, ensuring that they always have the right permissions to the right resources— nothing more and nothing less. They are happier because they can get to the resources they need to do their jobs; administrators are happier because everything is automated, minimizing the need for tedious, manual button-clicking.

If you top it off with customized high-level security policies that control who can do what within your environment, administrators no longer manage permissions directly on resources; they use an abstracted interface that is largely automated and related to user job roles. Both current and historical permissions are tracked and can be used to generate auditing reports quickly and on demand. Your security policies are enforced automatically, ensuring that administrator mistakes or maliciousness never create a security issue in the environment.

Wouldn't it be nice if all these capabilities really existed?

Welcome to Quest One

Here's the good news - those capabilities *do* exist, and you can quickly and easily add them to your environment *today*.

The Quest One Identity Solution from Quest Software brings you capabilities that are not only nice to have—they're *great.* You get three basic pillars of a consolidated, automated identity and access management process:

- **A cross-platform identity for your users;** Active Directory provisioning is extended to non-Windows systems, and users only have one user name and password to remember.
- **Identity synchronization for Active Directory and beyond, including numerous external databases and directories;** everything is connected to access management for completely automated provisioning.
- **Automated provisioning, administration, and access management for Active Directory and beyond;** you can automatically provision users and groups, enforce access permissions through top-level policies, and eliminate unregulated access to resources.

Because administrators have a more automated, secure, and efficient process, Quest One helps you do more with less. Your environment becomes more uniform because identities are automatically synchronized. Best of all, your environment remains more stable and secure, thanks to automation, reduction of human error, and top-level policies and workflow. Even your help desk benefits from a lower workload associated with identity management and access permissions.

To learn more, visit http://www.quest.com/identity-management/provisioning.aspx.

About the Author

Don Jones is a co-founder of Concentrated Technology (ConcentratedTech.com), a Microsoft Most Valuable Professional Award recipient, and the author of more than thirty books on information technology. His consulting practice specializes in making the connection between technology and business, helping businesses realize more value from their IT investment, and helping IT align more closely to business needs and values. Don has been an IT journalist for more than eight years, and is currently a Contributing Editor for Microsoft TechNet Magazine. He is also a sought-after speaker at industry conferences and symposia, including Connections conferences, Microsoft TechEd, TechMentor Events, and others.

About Quest Software, Inc.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit **www.quest.com** for more information.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)
If you are located outside North America, you can find your local office information on our Web site.

E-MAIL **sales@quest.com**

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

WEB SITE **www.quest.com**

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at **https://support.quest.com**.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.

QUEST SOFTWARE
Smart Systems Management

5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com
If you are located outside North America, you can find your local office information on our Web site

WPW_ADProv_Jones_US_MJ-20100324