

Daily Active Directory Administration: Simplified, Streamlined – and Successful

*written by
Quest Software, Inc.*



© 2009 Quest Software, Inc. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

Quest, Quest Software, the Quest Software logo, AccessManager, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BusinessInsight, ChangeAuditor, DataFactory, DeployDirector, DirectoryAnalyzer, DirectoryTroubleshooter, DNS Analyzer, DSExpert, ERDisk, Foglight, GPOAdmin, iToken, I/Watch, Imceda, InLook, IntelliProfile, InTrust, Invirtus, I/Watch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogAdmin, MessageStats, Monosphere, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportAdmin, RestoreAdmin, SelfServiceAdmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL LiteSpeed, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer Pro, vPackager, vRanger, vRanger Pro, vSpotlight, vStream, vToad, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, Vizioncore vTraffic, Vizioncore vWorkflow, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

July, 2009

CONTENTS

- INTRODUCTION 1**
- ACTIVEROLES SERVER: MANAGEMENT FOR AD AND BEYOND..... 2**
 - OVERVIEW OF FEATURES 2
 - SEPARATION OF DUTIES 2
 - APPROVAL-BASED WORKFLOW 3
 - EXCHANGE RECIPIENT MANAGEMENT 3
 - COMPUTER MANAGEMENT 4
 - MORE CHOICES IN ADMINISTRATION 4
 - EXTENSIBILITY AND AUTOMATION 5
 - BUT WAIT, THERE’S MORE! 5
- CONCLUSION 7**
- ABOUT QUEST SOFTWARE, INC. 8**
 - CONTACTING QUEST SOFTWARE 8
 - CONTACTING QUEST SUPPORT 8

INTRODUCTION

There's no question that Windows Active Directory (AD) is a mission-critical part of the infrastructure. AD certainly gets plenty of attention when it comes to high-profile issues like security, compliance, auditing, and so forth—but what about all of the work you do managing AD on a day-to-day basis? Managing user accounts, controlling user access to resources, managing Exchange recipients and computer accounts—these are the things that occupy most of an administrator's time. However, there never seems to be much focus on making these tasks *simpler, as well as more streamlined and successful*.

Quest ActiveRoles Server (ARS) provides those capabilities: it makes AD administration more efficient, automated, consistent, powerful and faster.

ACTIVEROLES SERVER: MANAGEMENT FOR AD AND BEYOND

Let's face it: the day-to-day grind of managing Active Directory isn't very much fun. Creating and deprovisioning users, as well as reconfiguring permissions when someone changes jobs is very tedious. Moreover, these tasks are all prone to errors and inconsistencies. Typically, the "new guy" gets to do user management because the tasks are so boring—but the "new guy" may be the one most likely to make mistakes.

To make access and identity management easier, you want to:

- Improve efficiency by automating tedious, time-consuming, and repetitive tasks. For example, wouldn't it be great to be able to create "smart" groups that automatically add users based on pre-defined criteria?
- Save time and improve accuracy through advanced management features based on top-level, consistent policies. It would be very helpful to automate group management based on membership policies.

Overview of Features

Quest ActiveRoles Server (ARS) provides these capabilities and many more. You can:

- Grant group membership temporarily, revoking it after a specified time period
- Use top-level policies to pre-populate and enforce AD attributes
- Automatically add members to groups based on AD attributes (so sales people always wind up in the right AD sales groups, for example), and automatically remove members when they no longer meet the criteria
- Grant (or revoke) permissions to enterprise-wide resources easily by adding users to their assigned role—no more messing around with individual permissions dialog boxes

Just that last feature—the ability to automatically manage permissions in Exchange, AD, files, folders, and more—can save an immense amount of time and improve accuracy. Why should someone have to wade through dozens of permissions dialog boxes—isn't that the kind of tedious, mind-numbing task that computers are designed for? Compliance audits are faster and easier, and administrators can work on *projects*, not busywork.

Separation of Duties

In addition to automation, today's organizations are looking for separation of duties. This enables administrators to control access to specific resources without

abusing that control, covering their tracks, or violating organizational policies. ActiveRoles Server accomplishes this through a controlled administration model. ARS wraps a “firewall” around AD, controlling directory change through its own administrative roles and policies and enabling a least-privilege access model. This enables organizations to delegate control to specified roles and associated permissions.

Approval-based Workflow

ActiveRoles Server fits perfectly into organizations that are adopting change management frameworks like COBIT and ITIL by providing a customizable approval-based workflow for all changes to AD. No matter how changes are introduced to AD—a graphical console, a script, or a Windows PowerShell command—ARS workflow rules kick in and hold designated changes for review and approval.

Exchange Recipient Management

Today’s organizations rely on their messaging as the same way they do on their directory. And the tight integration between Exchange Server and AD means that any change to AD usually results in changes in Exchange, too.

ActiveRoles Server can help take the tedium out of Exchange management, and also keep the Exchange environment operating more efficiently:

- Not only will ARS automatically create new Exchange mailboxes for new users, it will automatically select a mailbox store, helping to balance Exchange workload across available servers.
- Similarly, when you remove a user, ARS will automatically de-provision the user’s Exchange mailbox, based on a centrally defined management policy.
- Role-based access control makes the delegation of mailbox and recipient management easier and more secure: you now safely and quickly can delegate these tasks to other administrators, without wading through permissions dialogs.
- You can easily assign and manage “send as” permissions from a convenient graphical user interface—not a permissions dialog box.
- ARS automates provisioning of Microsoft Office Live Communication Server, helping to further reduce management overhead.
- ARS can enforce data formats, such as unified communication phone numbers, based on top-level policies.
- ActiveRoles Self-Service Manager can provide users with self-service management of selected Exchange distribution lists. Users can subscribe and unsubscribe themselves from internal mailing lists, with no administrator intervention or help desk calls.

Tight AD-Exchange integration lets ActiveRoles Server streamline and simplify management. Administrators focus on *human beings* and *job roles*, rather than on users, mailboxes, mailing lists, and permissions.

Computer Management

Managing users isn't the only thing that consumes administrator time in AD. Managing computers creates its own fair share of overhead, starting with computer deployment, which often requires administrator intervention to manage domain computer accounts. You then need to add managing service accounts, local shares and printers and much more. And many organizations simply write off local users and groups as entirely unmanageable. Who wants to roam from computer to computer, checking the membership of the local Administrators group?

ActiveRoles Server helps with the most tedious and difficult computer management tasks. It enables you to:

- Easily manage local service log-on accounts, passwords, and more.
- Start and stop services, too, all from a central location
- Manage local shares, printers, and device settings across the enterprise, all from a central location
- Manage local user and group accounts—again, all from a central location

Centralization means that you can manage a hundred computers as easily as you manage only one.

Best of all, these tasks—many of which may be performed by someone other than the AD administration group—can be easily and safely delegated to anyone in the organization. You can even delegate control over specific services, by service name, for the most granular administrative scenarios possible.

More Choices in Administration

Windows comes with one basic tool for day-to-day management tasks: Active Directory Users and Computers (ADUC). While ADUC certainly won't let administrators perform any task they don't have permissions for, most organizations aren't wild about widely distributing ADUC to folks who have been delegated few AD management permissions.

Therefore, ARS not only makes it easy to granularly delegate almost any kind of administrative task, it also gives delegates the appropriate user interface to perform their tasks. There's no need to ramp up their access rights "full domain admin" level.

- The ARS snap-in to the Microsoft Management Console (MMC) is a top-level, super-powerful interface that provides access to users, groups, computers, and Exchange management.

- Dedicated web consoles bring administrative capabilities to a broad range of delegates, and are accessible to anyone who has a Web browser.
- Web consoles include interfaces designed specifically for different target audiences: administrators, help desk, and even end-user self-service.
- Web consoles simplify day-to-day tasks by focusing on specific tasks, reducing administrative costs and skill requirements.
- Web consoles are configured with point-and-click simplicity to help meet your specific needs.
- Web consoles are built on the latest Microsoft ASP.NET technology for great performance and sharp-looking user interfaces.

ActiveRoles Server helps provide the right tool for every job to the right users within your organization, from top-level domain administrators all the way down to end users who need self-service functionality.

Extensibility and Automation

As good as ActiveRoles Server is, Quest knows that we can't anticipate every single administrative scenario that every customer might have. Rather than simply ignoring unusual or niche requirements, ARS enables them through powerful scripting and shell interfaces.

ARS supports Active Directory Services Interface (ADSI) scripting (in languages like VBScript) that is subject to ARS rules, roles, and reporting. In other words, you can keep using your existing AD management scripts (or create new ones) and be assured that ARS is properly using those scripts behind the scenes. ARS even includes a software development kit (SDK) that helps expose its own interfaces to scripters and programmers.

Organizations adopting Microsoft's Windows PowerShell management shell will be delighted to find a full set of cmdlets for both ARS and AD, so you can use powerful one-line commands and scripts to automate their management. All cmdlet actions are subject to ARS rules, roles, and workflow-based approvals. These cmdlets can even enable AD administrative automation in environments that don't have ARS installed.

ARS also supports a standards-based Web service interface, providing yet another way for third-party or in-house developers to connect to, and work with, ARS.

But Wait, There's More!

ActiveRoles Server has many more capabilities to make AD and access management simpler and more streamlined. These include:

- Data integrity rules, which ensure that AD attributes always contain data that's valid for your organization
- Management of non-Windows accounts within AD

- Support for multiple AD forests and for Active Directory Lightweight Directory Services (AD LDS) management
- Virtual directory attributes

ARS is designed with administrators in mind, as well as security and compliance. ARS makes AD administration easier and more efficient, while also keeping your infrastructure secure and helping you achieve legislative or industry compliance.

CONCLUSION

ActiveRoles Server simplifies establishing and standardizing access controls in the Windows environment. It can reliably delegate administrative control and provides users with exactly the control that they need -- nothing more, nothing less.

ARS enables a least-privilege access model by defining roles with associated permissions and rules that are strictly enforced by a unique administrative service that acts as a firewall around Active Directory (AD).

ARS offers automated provisioning, rule enforcement, separation of duties, self-service group attestation, centralized reporting, and approval workflow. Together these provide an evolutionary security and compliance solution for Active Directory that extends beyond simple auditing and reporting.

ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 100,000 customers worldwide meet higher expectations for enterprise IT. Quest also provides customers with client management through its ScriptLogic subsidiary and server virtualization management through its Vizioncore subsidiary. Quest Software can be found in offices around the globe and at www.quest.com.

Contacting Quest Software

Phone: 949.754.8000 (United States and Canada)
Email: info@quest.com
Mail: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site: www.quest.com

Please refer to our Web site for regional and international office information.

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 <http://support.quest.com>

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the **Global Support Guide** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: [http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)