



5 Challenges in Active Directory Management and How to Manage Them

Presented by:

Zubair Alexander

Microsoft MVP – Directory Services

Microsoft Certified Trainer



Agenda

- ▶ Active Directory General Limitations
- ▶ Password and User management
- ▶ Provisioning and deprovisioning – consistency through centralized management
- ▶ How to successfully perform granular restores of AD objects
- ▶ Active monitoring of managed and unmanaged changes
- ▶ Better management of security through delegation of roles

Active Directory Limitations

- ▶ Active Directory Users and Computers (ADUC) offers very limited management capabilities
- ▶ Creation and management of users and computers is cumbersome
- ▶ There's no easy way to customize user and computer objects
- ▶ Delegation of routine tasks to IT staff is difficult

Active Directory Limitations

- ▶ Active Directory lacks Web-based interface
- ▶ ADUC suffers from the limitations imposed by MMC
- ▶ Managing and resetting user passwords is a major pain point for IT departments
- ▶ Users must rely on IT to unlock their accounts
- ▶ Search functionality is limited

Active Directory Limitations

- ▶ Managing objects and security across domains and forests is not very easy
- ▶ Group Policy Management Console (GPMC) offers better management of GPOs but still lacks enhanced functionality (no quality reporting, rudimentary application of WMI filters, etc.)
- ▶ ADUC offers very limited customization

Active Directory Limitations

- ▶ Better management of permissions for Users and Groups is sorely missing in AD
- ▶ There is no single tool to centrally manage AD
- ▶ There is no built-in reporting capability included with ADUC
- ▶ NTDSUTIL, perhaps the most important tool in AD, is the most cumbersome AD tool and has no GUI version

Active Directory Limitations

- ▶ ADUC does not accommodate change management
- ▶ AD lacks change notifications and alerts
- ▶ Current AD versions lack a Recycle Bin feature
- ▶ There has been no significant improvement in ADUC in almost 10 years

NOTE: Windows Server 2008 R2 offers significant improvements over its predecessors but won't be released until 10/22/09 and is beyond the scope of this presentation.

5 Major Challenges in Active Directory Management

- ▶ Password and User management
- ▶ Provisioning and deprovisioning – consistency through centralized management
- ▶ How to successfully perform granular restores of AD objects
- ▶ Active monitoring of managed and unmanaged changes
- ▶ Better management of security through delegation of roles

Password Management Challenges

- ▶ According to researchers, up to 40% of all helpdesk calls can be related to password reset issues
- ▶ People have trouble remembering passwords so they use simple passwords, write them down, reuse old passwords, share them with friends, or forget their passwords

Password Management Challenges

- ▶ Users do not have the ability to reset their own forgotten passwords
- ▶ Users cannot unlock their own account
- ▶ People are told to remember complex passwords and then change them frequently
- ▶ Intruder lockout feature can be used as a denial of service (DoS) attack
- ▶ Built-in Administrator account cannot be locked out (unless you use PassProp.exe)

Provisioning and Deprovisioning

- ▶ Businesses have a need to provision and deprovision User accounts automatically
- ▶ Creation of multiple accounts requires scripting or third-party tools
- ▶ ADUC is not designed for automatic deprovisioning of User accounts
- ▶ MMCs are not an ideal solution to centralize all the Active Directory tools

Granular Restore of AD Objects

- ▶ AD is not designed to offer quick, granular restore of objects
- ▶ Restoration of AD objects is not only cumbersome, it requires shutting down the Domain Controller
- ▶ To restore individual objects you must go through numerous hoops
- ▶ In most cases, authoritative restores first require non-authoritative restores

Change Management Issues

- ▶ AD lacks active monitoring of managed and unmanaged changes
- ▶ Changes to GPOs cannot be easily monitored
- ▶ You can't automatically get notified if users are added to the Administrators group
- ▶ Management of changes to security groups is difficult

Delegation of Roles

- ▶ Large enterprises heavily rely on role-based security
- ▶ Delegation of roles functionality in AD is severely limited
- ▶ You can't create your own roles to better manage security
- ▶ There is no easy way to view delegated roles, or to find out who made what modifications and when

CionSystems AD Solutions

- ▶ CionSystems addresses AD limitations by offering the following solutions
 - Active Directory Manager
 - Active Directory Reporter
 - Active Directory Change Notifier
 - Active Directory Self-Service

CionSystems AD Solutions



- ▶ Active Directory Manager
 - Web-based interface
 - Supports Multiple domains
 - Reports available on demand or scheduled (e-mailed)
 - Roles-based delegation
 - Search & replace, search & compare functionality
 - Simplifies activities like resetting passwords, unlocking user accounts, changing contacts, etc.

CionSystems AD Solutions

▶ Active Directory Reporter

- Web-based interface
- Fully customizable dashboard
- Extensive built-in library with more than 200 standard reports
- Save reports in CVS, DOC, HTML, XLS and LIDF formats
- No scripting knowledge required
- Excellent for regulatory compliance
- Reports can be configured for automatic delivery



CionSystems AD Solutions



▶ Active Directory Reporter

- Out-of-the-box available reports

- Active Directory User Reports
- Active Directory Logon Reports
- Active Directory Password Reports
- Active Directory Computer Reports
- Active Directory Site Reports
- Active Directory Replication Reports
- Active Directory OU Reports
- Active Directory Group Reports
- Active Directory Security Reports
- Active Directory Exchange Reports
- Active Directory GPO Reports
- Active Directory File & Printer Reports
- Active Directory Policy Reports
- Active Directory Terminal Server Reports
- Active Directory Schema Reports
- Active Directory Trust reports

CionSystems AD Solutions

- ▶ Active Directory Change Notifier
 - Get alerts when changes are made to the objects on your domain
 - E-mails are received in real-time
 - Filtering based on containers and type of change



CionSystems AD Solutions

- ▶ Active Directory Self-Service
 - Web-based solution
 - Help end users make account changes securely
 - Allows users to reset their own password and unlock their account by answering pre-configured questions
 - Administrators can give controlled access so users can update their personal contact details
 - All changes made by users are tracked
 - Generate comprehensive reports



CionSystems AD Solutions

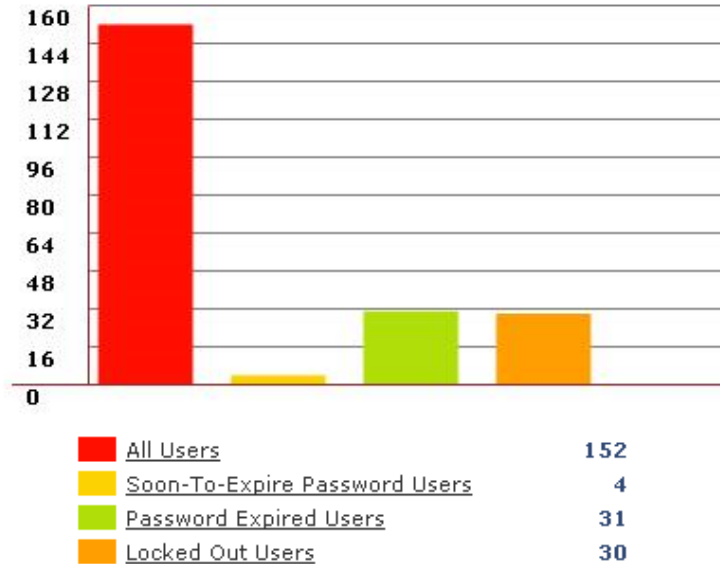
▶ Active Directory Self-Service

Dashboard | User Policy Settings | General Settings | Domain Settings | Reports | User Enroll Settings | Schedule Policy Settings

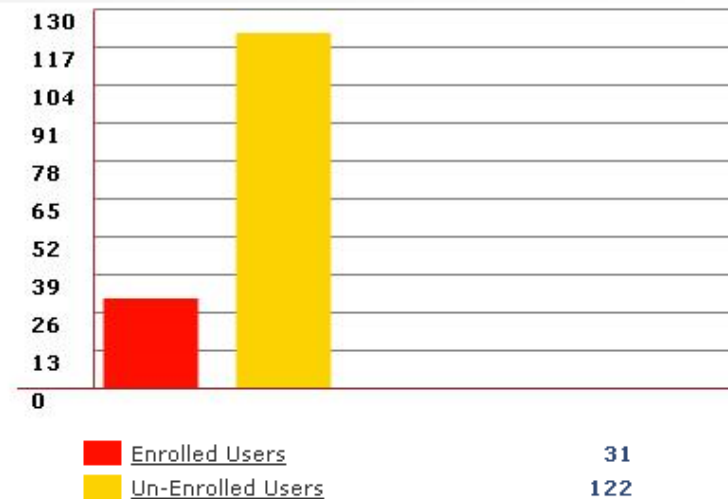
Dashboard

cion-demo.com

AD Reports



Audit Reports



CionSystems AD Solutions

- ▶ CionSystems products now include:
 - Temporary User Management
 - Create/Enable AND disable/delete users at scheduled times
 - Approval Process
 - User creation goes through an approval process (policy driven)
 - Temporary Group Membership Support
 - Schedule adding and removing Users and Groups
 - Delete Users
 - Deleted users are archived

References

- ▶ [Cleaning Up After AD](#)
- ▶ [Additional Account Info Tab for Users Properties](#)
- ▶ [Searching Active Directory Objects](#)
- ▶ [Lighten Up the Group Policy Load](#)

CionSystems, Inc.

- ▶ CionSystems home page:
<http://cionsystems.com>
- ▶ Products:
<http://www.cionsystems.com/products.php>
- ▶ Contact e-mail:
Webinar@CionSystems.com

SeattlePro Enterprises

- ▶ On-Site Training & Consulting Services:
<http://www.seattlepro.com/services.htm>
- ▶ Training Specials:
http://www.seattlepro.com/specials/training_specials.htm
- ▶ Contact Information:
<http://www.seattlepro.com/contact.htm>

Questions and Answers

Thank You!