



# **Active Directory**

## **Administration & Security Challenges**

# Agenda

- **AD Challenges**
  - *Active Directory Pains*
  - *Administrator Questions*
- **Group Policy Management Challenges**
  - *Group Policy Pains*
  - *Administrator Questions*
- **Permissions Management Challenges**
  - *Permissions Management Pains*
  - *Administrator Questions*
- **NetIQ Solutions**
  - *Active Directory Pains : NetIQ Answers*
    - *Directory Resources Administrator : DRA*
    - *Directory Security Administrator : DSA*
  - *GPO Pains : NetIQ Answers*
    - *Group Policy Administrator : GPA*
  - *Permissions Management Pains : NetIQ Answers*
    - *File Security Administrator : FSA*
- **Questions**

# Active Directory Overview

## *What is the Active Directory?*

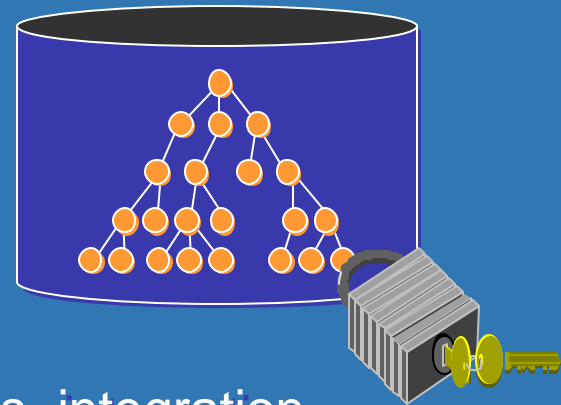
- **The Active Directory is...**
  - A special-purpose database
  - The place where user, group, computer and other information is stored
  - Allows rights to be assigned over users, groups, computers, and other resources
  - A replacement database for the SAM database that existed in previous versions of Windows NT



# Active Directory Overview

## *A Word About Active Directory*

- **Core component of the computing infrastructure**
  - Must be protected
- **Integrity is paramount**
  - Must be the “trusted source”
- **Complex**
  - Rich, robust structure
  - More objects, properties, relationships, integration
  - More administrative volume
- **Specialized ‘database’**
  - Needs an ‘application’ to manage it



# **Active Directory Overview**

## ***But Active Directory Brings New Management Challenges***

- **OU structure definition -> requires flexibility**
- **Volume -> requires delegation**
- **Delegation -> requires content management**
- **Content management -> requires timely, coherent integration through policies**
- **Complexity and newness -> requires understanding of what is going on**

# Active Directory Overview

## *Windows 2000 Security Administration Concerns*

- **Multiple security models**
  - Presents huge risk
  - Unified security administration is required
- **Delegation**
  - Windows 2000 - no roles, lack of un-delegate wizard, etc.
  - Flexible, granular delegation of permissions required
- **Content management**
  - Access control does not go far enough – can not enforce policies regarding information being placed in the directory
- **Reporting and auditing**
  - Need to be able to track “who did what to whom”, or “who did what to

# Active Directory Challenges

## Administrator Challenges [1/2]

- **Secure delegation of day-to-day account administration so that security policies are enforced, account escalation issues are avoided and audit trails are created**
  - Secure delegation
  - Account management auditing
  - Automation of repetitive activities
  - Enforce account policies

# Active Directory Challenges

## Administrator Challenges [2/2]

### ■ Windows 2000

- Native Tools are insufficient for security administration (i.e., no way to limit administrators and their permissions)
- Native tools provide limited auditing and logging capabilities
- Native tools require the use of multiple tools
- Directory structures are inflexible
- No way to secure the content of the Active Directory
- Lack of Automation on Administrative Transactions
- No unified or integrated administration of multiple data sources



# Active Directory Challenges

## Administrator Questions [1/2]

- How broadly are you able to delegate authority while still remaining secure?
- How do constrain the contexts in which administrators use their authority?
- Is everything being audited? Who is doing the logging?
- How many administrator accounts do you have? Who are they?
- Do you have administrators doing mundane tasks like password resetting?
- How are you preventing “directory pollution?”

# Active Directory Challenges Administrator Questions [2/2]

- Who owns the data? How do you know they will update the data correctly? Do you even know how your permissions are given out? Who has access to what?
- Can you create views of the directory that make sense to you? Are you fully satisfied with your Active Directory structure?
- How good are you at obeying company policies?
- How are you doing provisioning? Would you like to be able to automate complex multi-step business processes?

# Group Policy Management Challenges

- **If Group Policy is not managed prudently, risks can arise that may compromise the internal security of the enterprise**
  - Securely manage Group Policy change & release processes
  - Analyze implications of policy application on users & computers
  - Plan & perform policy backup & recovery processes

# Group Policy Management Administrator Challenges

- Difficult to predict which of 680+ Group Policy settings will be applied to a user or computer.
- Difficult to plan and test Group Policies.
- Difficult to migrate Group Policy Objects across domains in test and production environments.
- Difficult to search for Group Policy Objects using native tools.
- Difficult to backup and restore Group Policy Objects.
- Difficult to report on Group Policy settings in Windows 2000.
- Difficult to troubleshoot Group Policy Objects.

# Administrator Questions – GPO

## [1/5]

- How do you support security audits of Group Policy?
- Do you have a way to quickly view and analyze Resulting Sets of Policies when using Group Policy Objects?
- Do you have a way to search for Group policy Objects by name, or to easily search for Group Policy settings?
- Do you have a way to easily view and report on policy settings, or is this a manual process?
- How do you document what settings are in effect for each policy in a domain?
- Do you have a way of comparing current Group Policy Object settings with past settings to determine if there have been any changes?

# Administrator Questions – GPO

## [2/5]

- Do you have a way to back up and restore Group Policy Objects? Or if you have a problem with your Group Policy Objects, will you have to restore the entire Active Directory in order to restore your Group Policy Objects?
- Do you have a way to quickly restore Group Policy Objects that have been corrupted or inadvertently changed or deleted? Or will they have to be manually recreated?
- If a security Group Policy is inadvertently corrupted or deleted, do you have a way to quickly reapply the Group Policy before a security breach occurs?

# Administrator Questions – GPO

## [3/5]

- Have your end users ever been denied access to their business-critical applications due to problems with Group Policy?
- Can you quickly diagnose and fix Group Policy-related problems when they are submitted to the help desk?
- Do you have a way to perform remote diagnostics when users call with Group-Policy related questions?
- Has implementing Group Policy lowered or increased your desktop support costs?
- Are you looking for a way to automate Group Policy Object creation in order to save on administration costs?

# Administrator Questions – GPO

## [4/5]

- Some of our customers have reported that it may take a week or more to create and test each Group Policy they plan to implement in their environment. How does this compare to your experience with testing and deploying Group Policies?
- How often do you expect to have to change your Group Policy design?
- Do you have a way to model and test your Group Policy Objects and perform “what if” analyses prior to deploying them in a production environment?



# Administrator Questions – GPO [5/5]

- Do you have a way to configure Group Policy Objects once, and then easily replicate and apply them to other domains and forests? Or do you have to manually recreate them each time?
- How comfortable do you or your staff feel configuring Group Policy Objects? Are you in-house experts, or are you still dealing with a bit of a learning curve as you come up to speed on how Group Policy works in Windows 2000?
- Are you doing all of your Group Policy planning and deployment in-house, or consultants helping you implement Group Policy?

# Permissions Management Challenges

- Making sure that only the appropriate accounts have access to the appropriate areas of Active Directory is a critical issue for maintaining enterprise security
- If the wrong users have inappropriate access, the integrity and availability of directory information can be jeopardized significantly
  - Security policy implementation & auditing
  - Analysis & remediation
  - Administration

# Permissions Management Pains

## 1/2

- **Who has access to what?**
  - Do you know where the Everyone group still has full control?
  - Where's Waldo's permissions?
  - What level of access do users have?
- **Where do risks exist and how are you correcting permission problems?**
  - Identify areas that need to be locked down and take corrective action

# Permissions Management Pains

## 2/2

- **What if I make a mistake?**
  - Backup security settings in case you make mistakes
- **What's taking up all the space?**
  - What file types and in what proportions?

# Administrator Questions

## [1/4]

- **Do you know where the Everyone group still has full control?**
  - (Full control is the default security setting for Windows NT.)
- **Do you know to whom you have given what file permissions?**
  - Can you easily fix and correct it?
  - How fast can you report on it?
- **Can you quickly answer what users and groups have access to what files?**
- **Can you say your storage systems don't have any MP3 files on them?**

# Administrator Questions

## [2/4]

- **Are your auditors satisfied with your file and directory permission settings?**
  - Can they even figure out if they are satisfied?
- **Are you able to grant permissions at a very granular level?**
  - Example: Make sure that Bob has no more than read access across a 200GB volume.
  - Example: Give Fred the ability to grant no more than read access to members of the Atlanta group.
- **Can you get access to the files you are supposed to have access to or do incorrect security settings lock you out?**
- **Do you leave permission “open” to prevent access issues?**

# Administrator Questions

## [3/4]

- **Do you know how your disk systems are being used?**
  - What percentage is being used for graphics, presentations, MP3 files, and so on?
- **What do you want your expensive administrators to be doing?**
  - Are they caught up in firefights or are they doing systems management?
- **How many manual, repetitive tasks are your administrators doing in their efforts to keep track of the storage systems?**
  - How much control do the administrators have in the absence of strong reporting?

# Administrator Questions

## [4/4]

- **Are you able to easily capture data from all data sources to compile reports?**
  - How do you ensure the reports are complete and accurate?
- **Do you allocate NTFS5 disk quotas?**
  - How do you make sure disk quotas settings abide by company policy?





# NetIQ ANSWERS

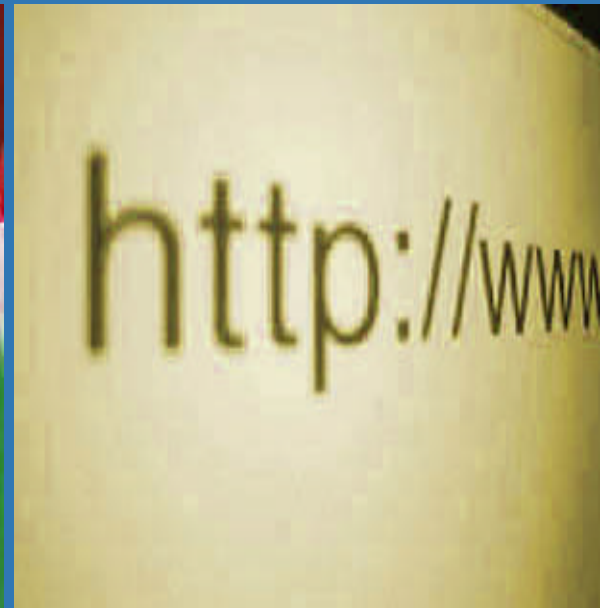
# NetIQ: Three Major Solution Areas



**Performance &  
Availability Management**



**Security Management  
& Administration**

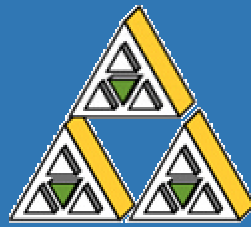





**Web Analytics &  
Management**

## NetIQ Provides

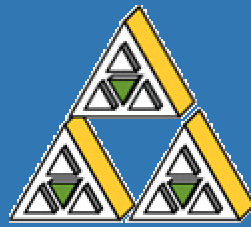
- Solutions for your three most critical infrastructure management needs
- Award winning best of breed products in each solution area
- Comprehensive platform Support – Windows, UNIX and Linux



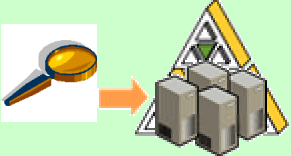
# Administer



PRODUIT	DESCRIPTION	PLATE-FORME
<b>Directory and Resource Administrator</b> 	Administration des comptes NT/2000 : audit, unifiée, simplifiée, automatisée et sécurisée l'administration des domaines NT4 et de l'Active Directory	Windows NT Windows 2000
<b>Exchange Administrator</b> 	Gestion centralisée des boîtes aux lettres Exchange intégrée à l'administration des utilisateurs Windows 2000	Windows NT Windows 2000 Exchange 5.5 Exchange 2000
<b>File &amp; Security Administrator</b> 	Administration centralisée de la gestion des fichiers et des comptes de service. Reporting complet et dynamique	Windows NT Windows 2000

# Administer



PRODUIT	DESCRIPTION	PLATE-FORME
<p>Group Policy Administrator</p> 	<p>Simplifie et optimise la gestion des Group Policy Objects, basée sur la solution FAZAM, leader du marché</p>	<p>Windows 2000 .net</p>
<p>Directory &amp; Security Administrator</p> 	<p>Gestion complète de la délégation et de la sécurité en environnement natif Windows 2000</p>	<p>Windows 2000</p>
<p>Configuration Assessor</p> 	<p>Audit et reporting complet pour les organisations Windows NT et Windows 2000 Active Directory.</p>	<p>Windows NT Windows 2000</p>



# Directory and Resource Administrator

# What does DRA Do ?

- **Secure distributed administration of NT4 and Windows 2000 from a single product**
  - Password resets
  - Account unlocks
  - Group membership modifications
  - Account creations
  - Resource administration
- **Automation**
- **Policy enforcement**
- **Auditing**
- **Web Console for helpdesk & delegated administrators**

The screenshot displays the NetIQ Administration console interface. On the left, a tree view shows the hierarchy of objects under 'My ActiveViews', including 'All my managed objects', 'DRA-ExA EvalGuide (Reg): Cent', and 'AD and domain explorer (peterdx01)'. The main pane shows an 'ActiveView' for 'Accounting-DG' with a table of objects:

Object Name	Type	Description
Accounting-DG	Group	Description of: Accounting-DG_0008
Accounting-DL	Group	Description of: Accounting-DL_0008
Accounting-DU	Group	Description of: Accounting-DU_0008
Accounting-SG	Group	Description of: Accounting-SG_0008
Accounting-SL	Group	Description of: Accounting-SL_0008
Accounting-SU	Group	Description of: Accounting-SU_0008

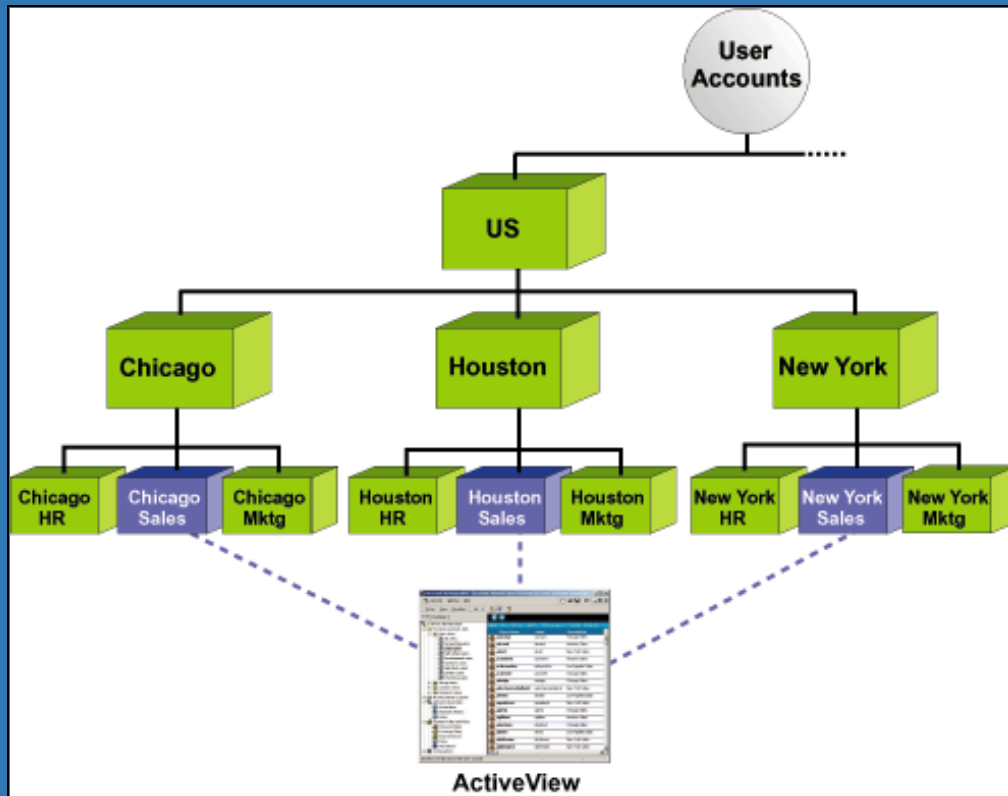
Below the table, a 'Web Console' window is visible, showing the 'webconsole' interface for 'NETIQCDRP' domain. The console includes navigation links for 'User Tasks', 'Group Tasks', 'Mailbox Tasks', and 'Reports', along with a search function and a 'Change Managed Domain' button. The footer of the web console displays the NetIQ logo and the slogan 'Work Smarter.' with a copyright notice for 1995-2011.



# Two Environments to Secure One Integrated Solution: DRA

- **DRA: Seamless security administration for :**
  - Windows NT 4 domains
  - Windows 2000 domains (Active Directory)
  - Microsoft Exchange Server 5.5 and Exchange 2000 mailboxes (with NetIQ Exchange Administrator)
  - Resources (connected users, open files, printer queues, services, shares)
  - Member server and workstation SAMs

# Flexible, Unified Security Model for Windows NT 4.0 and Windows 2000



## DRA's Advanced Delegation

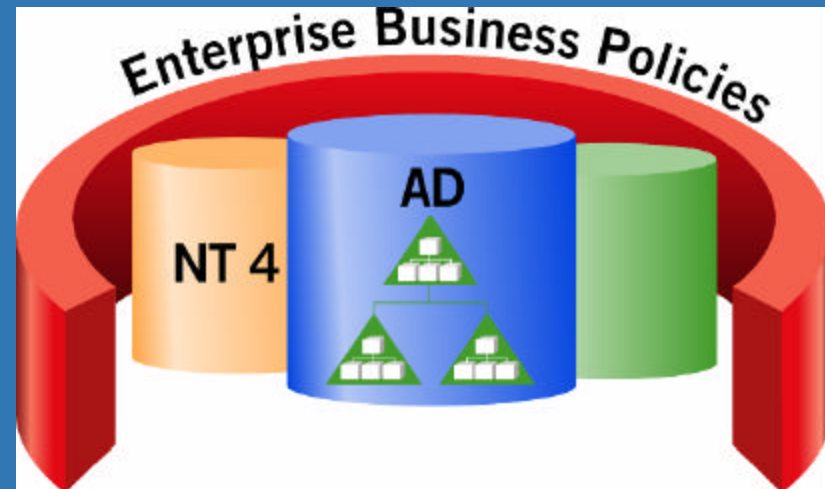
- “ActiveViews”
  - Logical “virtual OUs” that can cross OU boundaries –domains, trees, and forests
  - Tied to automation, policy enforcement, and reporting
- “Assistant Admins”
  - Role-based delegation of permissions
  - Tied to ActiveViews

Reduce the number of user accounts with Admin permissions, safely distribute administration, and control data content ownership throughout your organization.



# DRA – Key Features

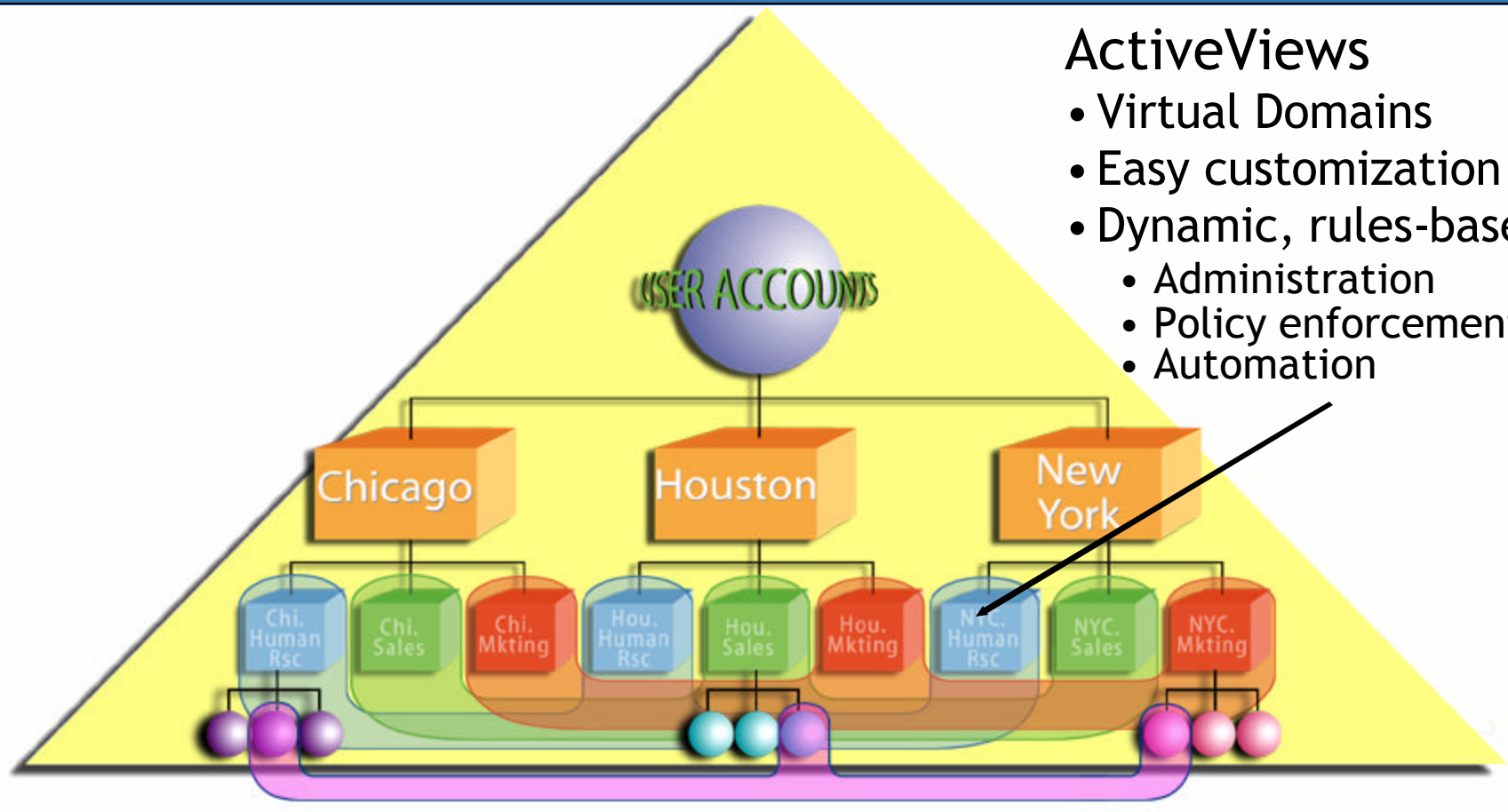
- **ActiveViews**
  - Custom views of directory data
- **Policy enforcement**
- **Virtual Property Objects**
  - Simple directory extensibility
- **Workflow Automation**
- **Audience focused interfaces**
  - Web, MMC, ADSI, COM
- **Safe, distributed self-administration**
- **Mixed-mode management**
- **Administrative ‘power tools’**
- **Reporting, Analysis & auditing**



# ActiveViews

## Exploit and Extend Active Directory

### Windows 2000 Domain



### ActiveViews

- Virtual Domains
- Easy customization of AD
- Dynamic, rules-based, for:
  - Administration
  - Policy enforcement
  - Automation

# Key Benefits – DRA [1/2]

- **Windows NT 4.0**
  - Enables safe, secure, distributed administration
  - Allows granular delegation of permissions
  - Allows you to set and enforce policies for data integrity and consistency
  - Extensive, rich reporting and logging of all actions
  - Unified administration of users, groups, mailboxes, etc through single tool
  - Allows you to automate tasks and workflows through out-of-the-box and custom automation
  - Enables you to seamlessly join and administer data from multiple sources
  - ActiveViews enable seamless administration of data across multiple sources
  - Helps prepare/ease the transition to Active Directory, investment carries forward during the migration to Windows 2000
- **Windows NT 4.0 -> Windows 2000 Transition**
  - Same UI's and same toolset - no retraining required
  - All policies, automation, administrative ActiveViews, etc defined in NT 4.0 carry forward to Windows 2000.

# Key Benefits – DRA [2/2]

## ■ Windows 2000

- Improves security
  - By allowing IT to limit the number of administrators and their privileges
  - By providing dual key security and a user account recycle bin
  - Through extensive logging and comprehensive reporting
- Unified administration of users, groups, mailboxes, etc through single GUI
- ActiveViews allow you to organize directories the way you want to view them. They enable you to seamlessly join data from multiple sources
- Secures the content of the Active Directory by
  - Enforcing administrative policies,
  - Safely distributing data content ownership throughout the organization
  - Integrating policy and automation with directory updates
- AD modifications can be unified through policies and automation
- Provides out-of-the-box and custom automation capabilities
- Provides easy integration of AD with other databases, directories and critical administrative data.

# DRA's Secure Role-Based Administration

- **Allows organizations to safely delegate permissions**
  - Can assign permissions to “assistant administrators” (e.g., Help Desk Admin)
  - Roles can be saved and reutilized
- **Limits views for “Assistant administrators”**
  - Only see objects that are relevant to their duties
- **Provides detailed Audit trail by logging every action**
  - Allows you to see if tasks were success or failure
  - Tracks which attributes were changed by any Assistant Admin role
- **Reduces intrusions through role-based administration**
  - For example, Help Desk person looks at the entire directory to obtain information on infrastructure security settings
- **Enables customers to implement “dual-key” security**
  - For particularly sensitive tasks
  - Takes two assistant administrators to complete an action

# DRA's Built-in Content Control Policies

- **DRA helps you decrease your security exposure**
  - Provides the ability to control the context in which an action may be taken
  - **Includes built-in policy enforcement capabilities:**
    - Naming conventions for objects like computers, groups, and user accounts
    - Limits on how many members a group may have
    - Maintains unique user account names across multiple domains
    - Maintains unique user principal names
    - Prevents the proliferation of administrator access privileges
    - Controls the types of groups that can be created
    - Enforces creation of home directory for each new user account
    - Enforces creation of Exchange mailbox for each new user account
    - Enforces that only specific values can be specified for properties
    - Enforces that the value entered for a property conforms to a specific format
    - Enforces password strength

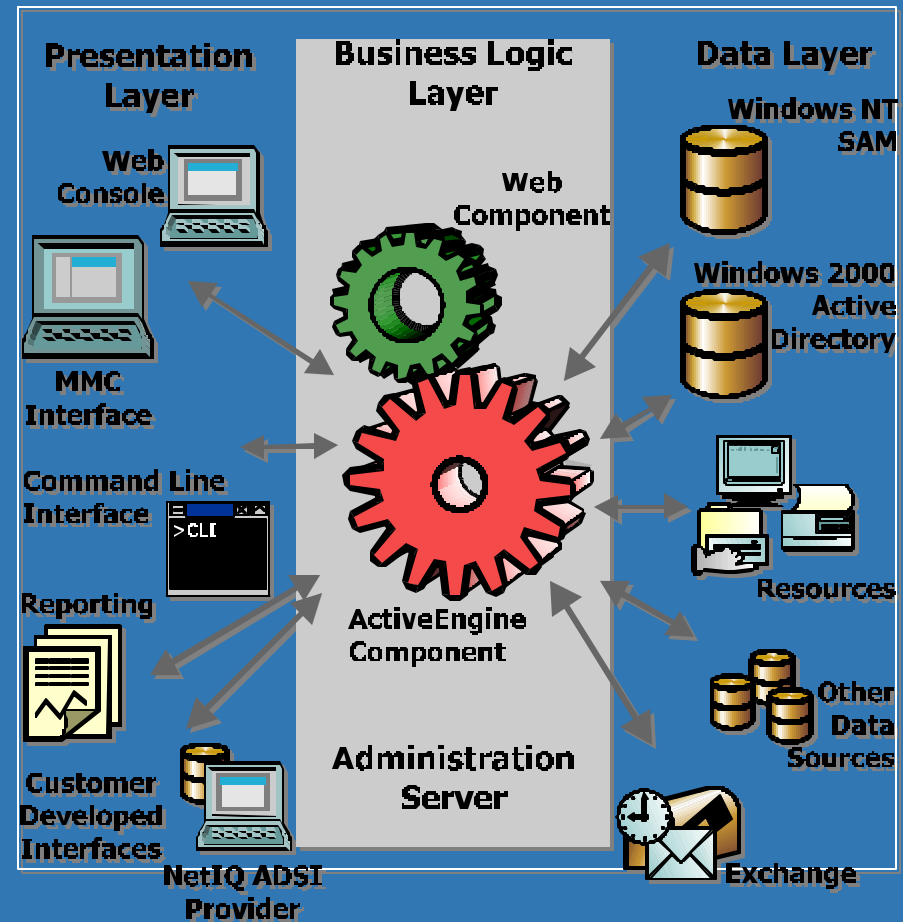


# DRA's Comprehensive Reporting & Auditing

- **More than 75 built-in reports,**
  - Includes more than 17 change activity reports
  - Reports on all ActiveView delegations of authority
  - Provides detailed data suitable for audits
- **Detailed audit logging that cannot be turned down or off**
  - Auditing of all transactions against the directory when they occur
- **Makes it easy to answer the following kind of questions:**
  - Whose passwords can Bob change?
  - What groups can Sarah alter the membership of?
  - In which OUs can the New York Help Desk create users?
  - Over which objects does Barney have some write power?
  - Who changed the CEO's password and when?
  - Who tried unsuccessfully to add themselves to the Domain Admins group?

# DRA's Open and Secure Architecture

- **3-tier architecture means security is maintained at the middle-tier as opposed to vulnerable 2-tier models**
- **Open transaction model exploits AD, COM and ADSI**
  - Exposes an ADSI provider to write to other applications enabled for Active Directory, letting you take advantage of content control policies.
  - Trigger-based automation that can cause changes outside the directory whenever the directory is changed







# Directory Security Administrator

# What does DSA do ?

## ACL Visualization

- Display entire domain contents (as rights dictate)
- View permissions at a glance
- Filter permissions
- View inheritance

## ACL Manipulation

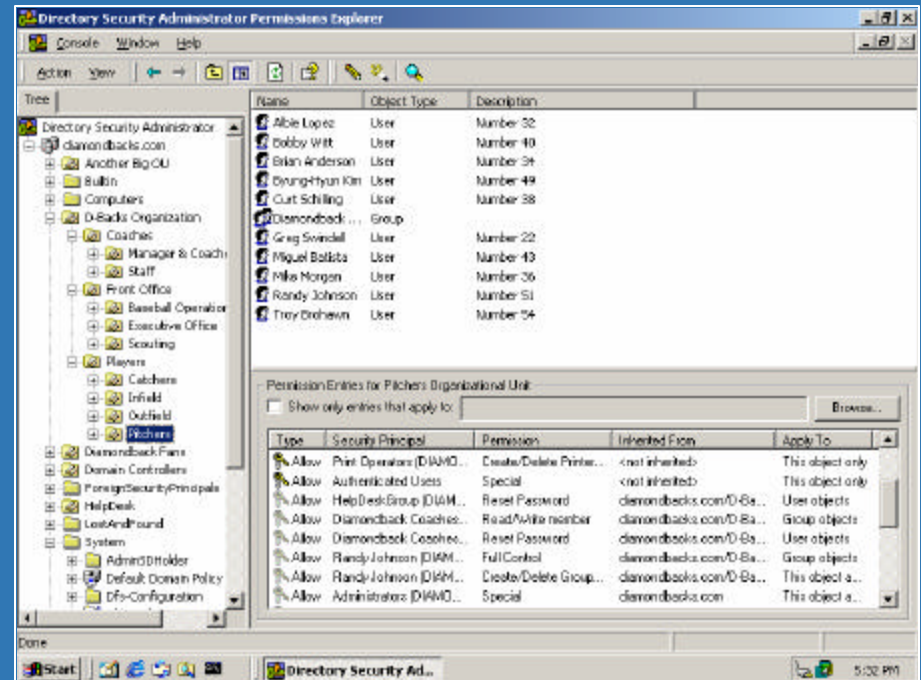
- Launch native ACL Editor from any object/container
- Launch native Delegation of Control Wizard from any object/container
- Launch AD Security Search

## Launchable from ADU&C

Quickly search for where in AD permissions have been granted to users, groups or machines

Easily visualize and make changes to the AD security model

Determine exactly what permissions have been granted to any given account and where those permissions came from (i.e. were they explicitly granted or inherited?)



# AD Security Search

- Search the entire domain or sub-OUs
- Search any security principal
- Exclude or include inherited permissions
- Exclude or include group memberships
- Take action on search results:
  - Edit ACLs of resultant objects directly
  - Launch native Delegation of Control Wizard from any object/container
- Launchable from ADU&C
- Command-line scriptable
- Export results to CSV

The screenshot shows the 'Directory Security Administrator Search' window. The search criteria are: 'Search diamondbacks.com for objects where Diamondback Pitchers (DIAMONDBACKS\Diamondback Pitchers) has permission excluding inherited permissions and including all group memberships'. The search results table is as follows:

Name	Object Type	Location	Permissions Summary
Front Office	Organizational Unit	diamondbacks.com/D-Backs Organization	Modify Owner
Diamondback Pitchers	Group	diamondbacks.com/D-Backs Organization/PL...	Special
Domain Controllers	Organizational Unit	diamondbacks.com/	Full Control
HelpDesk	Organizational Unit	diamondbacks.com/	Read/Write member, Reset Passw...

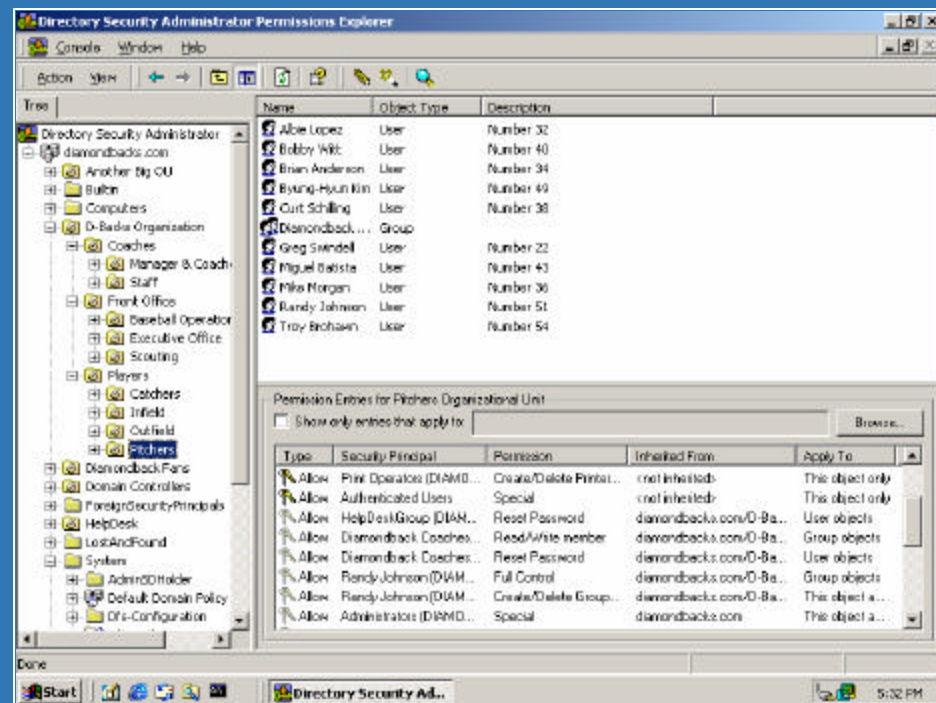
Below the results, the 'Permission Entries for HelpDesk Organizational Unit' are shown for the 'Diamondback Pitchers (DIAMONDBACKS\Diamondback Pitchers)' group. The table is as follows:

Type	Security Principal	Permission	Inherited From	Apply To
Allow	Diamondback Pitchers (DIAMONDBACKS\Diamondb...	Read/Write member	<not inherited>	Group objects
Allow	Diamondback Pitchers (DIAMONDBACKS\Diamondb...	Reset Password	<not inherited>	User objects

4 items found

# Permissions Explorer

- **ACL Visualization**
  - Display entire domain contents (as rights dictate)
  - View permissions at a glance
  - Filter permissions
  - View inheritance
- **ACL Manipulation**
  - Launch native ACL Editor from any object/container
  - Launch native Delegation of Control Wizard from any object/container
  - Launch AD Security Search
- **Launchable from ADU&C**

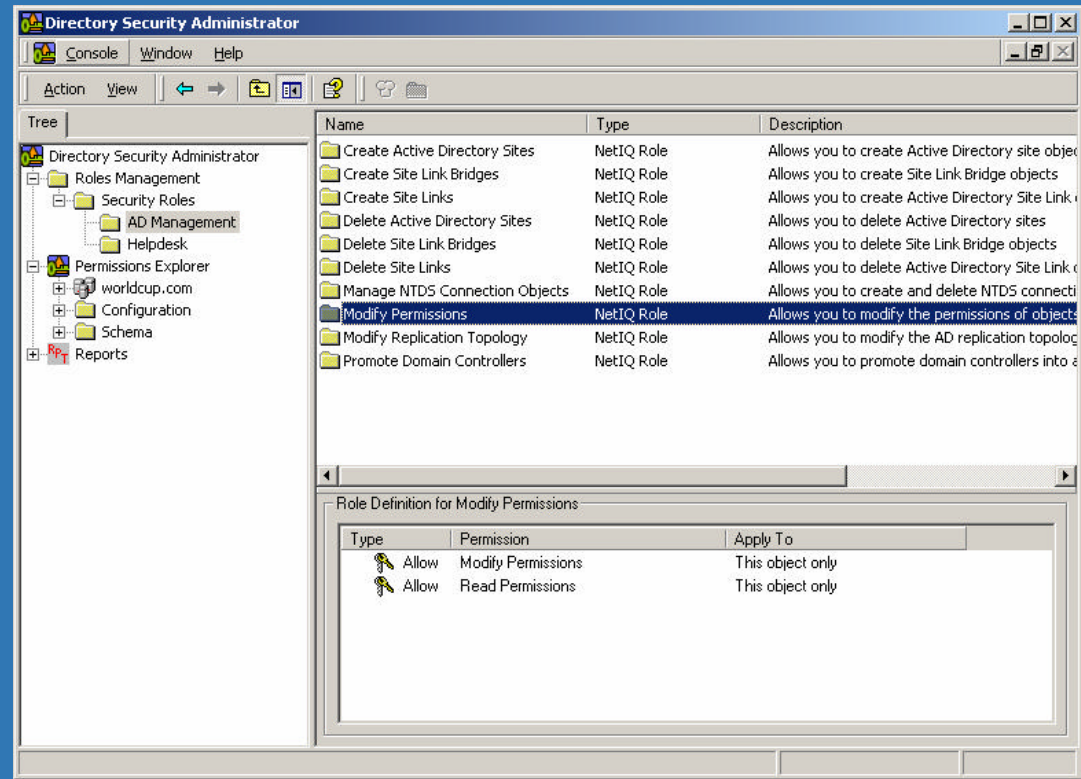


# Resultant Permissions Analysis

- **Select individual objects or containers**
- **Filter out all ACL entries except for specific security principals**
  - Displays what permissions have been granted/denied
  - Where permissions originated (explicitly granted or inherited)
  - Where permissions apply

# Role-Based Security

- Local or forest-mode
- Role management
  - Creation/deletion
  - Cloning
  - Application/revocation
  - Visualization
  - Import/export
- Role security
- Tracking
- AD UI integration







# Group Policy Administrator

# What is Group Policy Administrator ?

## ■ NetIQ Group Policy Administrator

- Improves the security of your Windows environment by simplifying the use of Active Directory Group Policy.
- Provides a single console for managing Active Directory Group Policy
- Gives Active Directory systems and security administrators the ability to:
  - Determine Resultant Set of Policies (RSOP)
  - Backup and restore Group Policy Objects (GPOs)
  - Report and search for Group Policy Object settings
  - Replicate Group Policy Objects across domains and forests
  - Perform auditing and remote diagnostics of Group Policies



# What does GPA do ?

- Provides a single console for managing Active Directory Group Policy
- Gives Active Directory systems and security administrators the ability to:
  - Report on Group Policy Object (GPO) settings
  - Backup and restore Group Policy Objects
  - Replicate Group Policy Objects across domains and forests
  - Determine Resultant Set of Policies (RSOP)
  - Perform remote diagnostics and auditing of Group Policies
  - Search for Group Policy Object settings
  - Delegate administration of GPOs

The screenshot displays the Group Policy Administrator console. The left pane shows a tree view with 'Policy Planning & Analysis [winchem.W2KAD.local]' selected. The right pane shows the 'AD Links' and 'Security Filters' sections. The 'Restricted IE' GPO is selected, showing its GUID and state. Below, the 'User settings' and 'Computer settings' are listed with their respective values and revision information.

AD Object	Type	Block Inheritance	Link Options
Domain Controllers	OU	False	None

Account	Receive	Parse	Edit
Domain Admins (W2KAD\Domain Admins)		Allow	Allow
Enterprise Admins (W2KAD\Enterprise Admins)		Allow	Allow
CREATOR OWNER		Allow	Allow
SYSTEM		Allow	Allow
Authenticated Users	Allow	Allow	

Name:	Restricted IE
GUID:	{A1BE2CD3-89DF-4690-8D7D-D587BA8CD229}
State:	Valid GPO

Settings	Value	Revisions
User settings:	Enabled	0 (Computer), 1 (User)
Computer settings:	Enabled	Created: 2/14/2002 2:19:54PM
Loopback processing:	Not configured	Modified: 2/20/2002 12:49:06AM

AD Object	Type	Block Inheritance	Link Options
Migrated	OU	False	None
W2KAD	domain	False	None

# Key Benefits – GPA [1/2]

- **Improves the security of your Windows environment**
  - By simplifying the use of Group Policy, GPA makes your Windows environment more secure.
- **Audits your policies**
  - Reporting capabilities allow you to document exactly what Group Policy Object settings are in place.
  - Compare them to past reports and determine whether there have been any changes.
  - Use Resultant Set of Policy features to audit that the policies in place are performing as desired and eliminate any security holes that are identified.
- **Maintains the security of your Group Policy environment**
  - If Group Policy Objects are changed inadvertently or maliciously, the security of your environment could be at risk.
  - The backup and restore capabilities ensure that your policies are properly enforced.

# Key Benefits – GPA [2/2]

- **Reduces the risk of error when configuring Group Policy Objects in other domains and forests**
  - By leveraging the GPO replication capabilities, you can configure Group Policy Object settings once, and then replicate and apply them to multiple other Group Policy Objects in other domains, and even other forests.
  - Guarantees that your Group Policy Object settings are configured correctly, and reduces the risk of missing or mis-configuring a setting.
- **Simplifies Group Policy management**
  - Makes it simple and easy to manage Group Policies in a policy-centric way from a single console
  - Reducing the likelihood of error and the security exposure that these errors may introduce
  - GPA's RSoP capability also reduces the process of manual RSoP generation from days/hours to seconds.
- **Lowers total cost of ownership**

# Features – GPA [1/4]

- **Ensure compliance with corporate security policies**
  - If a security Group Policy is inadvertently corrupted or deleted, quickly reapply the security Group Policy before a security breach occurs.
- **Fully leverage Windows 2000, Windows XP and Active Directory investments**
  - Implement the Group Policy capabilities available with Windows 2000, Windows XP and the Active Directory and maximize investments in Windows technology.
- **Improve IT service levels and responsiveness**
  - Quickly diagnose and fix Group Policy-related problems users submit to the help desk.

# Features – GPA [2/4]

- **Reduce downtime**
  - Ensure users are not denied access to their business-critical applications due to problems with Group Policy application.
- **Reduce total cost of ownership and increase user productivity by effectively applying Group Policies at the desktop**
  - Lost productivity is frequently attributed to user errors, such as modifying system configuration files and rendering the computer unworkable, or to complexity, such as the availability of non-essential applications and features on the desktop.
  - With Group Policy, administrators can create managed desktop environments tailored to users' job responsibilities and level of experience with computers.

# Features – GPA [3/4]

- Create and manage Group Policies quickly, easily, and securely
- Quickly understand what policies have been/will be applied to a user when the user logs on to a machine
- View Group Policy in the Active Directory from a policy-centric perspective
- Easily create Group Policy Objects in one domain and replicate them to other domains and forests
- Easily back up and restore Group Policies independently from the Active Directory

# Features – GPA [4/4]

- Create standard Group Policy templates to leverage as a base when building new Group Policy Objects
- Easily search and find specific settings within the context of a Group Policy Object in order to set, modify, or remove settings
- Audit and report on Group Policy Object settings throughout the forest
- Remotely diagnose and troubleshoot Group Policy application





# **File Security Administrator**

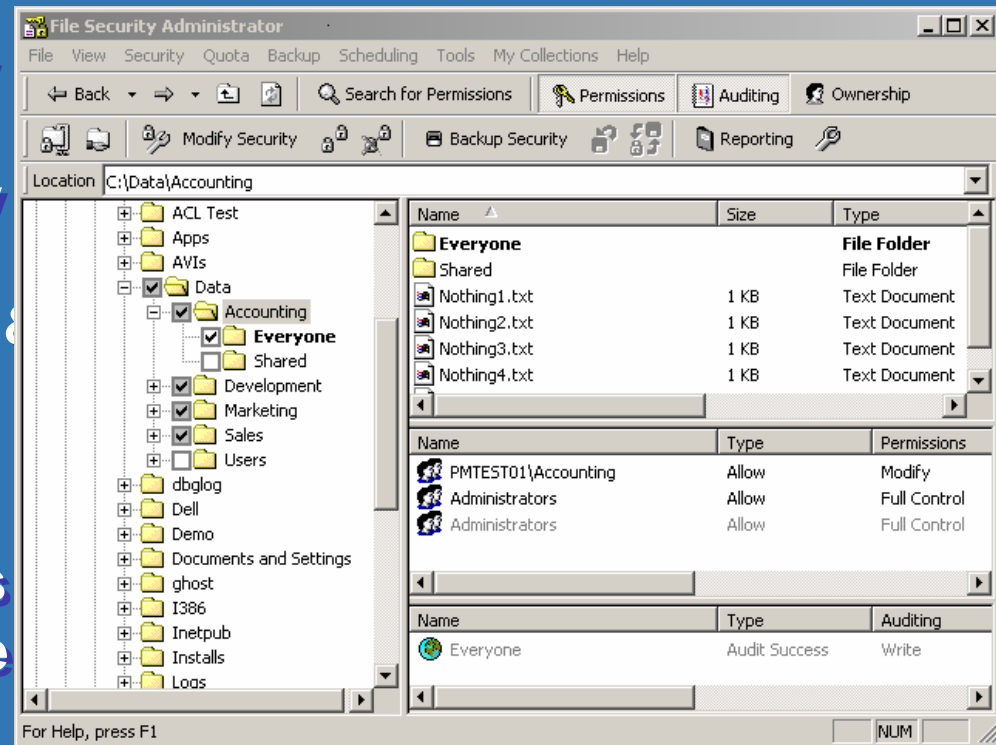


# What is File Security Administrator?

- **A complete file security management and reporting solution for your Windows NT and Windows 2000 environment**
  - The product's straight-forward interface and extensive, flexible reporting features simplify tasks such as determining who can access your file system, eliminating and preventing enterprise security holes and reporting on storage utilization.
  - Its ActiveReporting feature allows you to pinpoint the exact locations where you need to take corrective action.
- **File Security Administrator is a key component of the NetIQ Administration Suite**

# What does FSA do ?

- Search for file system permissions granted to user accounts
- Automate file security policy enforcement
- File system security backup & restore
- Analyze changes since last security backup
- Report on storage resources
- Manage cross-server service accounts
- File system auditing



# Key Benefits of FSA

- **Eliminates storage security risks**
  - Find where the “Everyone” group still has full control
- **Automates file permissions backup and restore**
  - Prevent having to spend time “rebuilding” permissions
- **Reduces costs and simplifies file system management**
  - Give a sales manager’s assistant the ability to give other people read access to sales related data

# Key Benefits of FSA (cont)

- **Provides extensive, rich reporting**
  - Find out how many MP3 and AVI files are on your network and wasting space
- **Enables storage capacity planning**
  - Find those files that haven't been access is over a year or all the MP3 files on your network and deleted them
- **Scales massively for enterprise-wide operations**
  - Get file and security information from 100's or 1,000's of servers
- **Facilitates service account management**
  - Get rid of your service account security holes

# Features – FSA [1/4]

- **View permissions at a glance**
  - Save time by quickly showing the current permissions on any file, directory, or share in tree control like Explorer
- **Searching for permissions**
  - Quickly search for where accounts have access and display the results
  - You can also do a search and replace of permissions
- **Summarized reporting**
  - Provides ability to drill down and get additional details and take action where needed.
  - Example: The reporting tool can find all .MP3 files. From the list of returned objects, the user can then select a set of objects and then take action upon them through the GUI, such as deleting them.

# Features – FSA [2/4]

- Easily backup and restore or compare file security descriptors.
- Modify, copy, replace or set file, directory and share permissions, audit settings, and ownership.
- Compare current security to a backup copy.
- Enables modification of file security
  - Allows precise changes that won't disrupt the rest of the security model.
- Ability to schedule most operations to be repeated as needed or to run during off-hours.
- Share creation, deletion, permission management, and reporting.

# Features – FSA [3/4]

- **Delegation of control over the Windows file system**
  - Control who can grant what level of access where and over what users without having to make those users local administrators.
- **Service account password management tool**
  - Update service account passwords across multiple machines en masse
- **My Collections**
  - Provide logical group of objects across multiple locations so they can be managed as one.
  - Allows for tasks like backing up settings and searching for permission across multiple directories and across many systems at once.



# Features – FSA [4/4]

- **Enterprise-scale reporting**
  - On file systems, computer hardware, service account, and TCP/IP settings, as well as file types (.doc, .MP3, etc.).
- **Over 30 built-in reports**
  - On file security, file attributes, quotas, shares, and hardware information
- **Management of NTFS 5 quotas with policy enforcement**
  - (who can set a quota within what limits)

# FSA Usage Examples

- Gather nightly reports on what the Everyone group has access to
- Locate, move and delete files that haven't been accessed in over a year
- Apply incremental permission changes across 100's of servers
- Gather data on unused groups for domain clean-up
- Update service account passwords for in-house and off-the-shelf applications
- Delegate out to data owners the ability to grant, deny and report on access to their data