Group policy

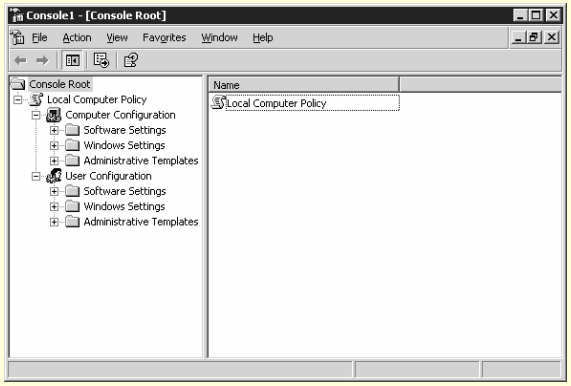
http://www.cs.vsb.cz/navrat

Jan Žák

Agenda

- Lokální X doménové politiky
- Computer X User
- Výhody
- Linky
- Delegování
- Tools
- Instalace SW
- Prostředí uživatelů

What Is Group Policy?



Processing Group Policy Objects

Group Policies are processed in the following order:

- Local computer Group Policy
- Group Policy objects linked to the site
- Group Policy objects linked to the domain
- Group Policy objects linked to the OU

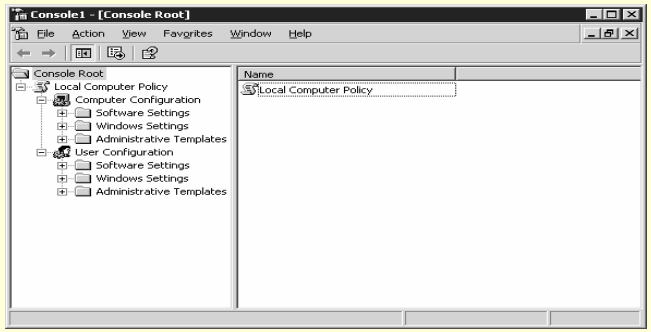
What Are User and Computer Configuration Settings?

- Group Policy settings for users control:
  - **Software settings**
  - **Windows settings**
  - **Security settings**
  - **Desktop settings**

- Group Policy settings for computers control:
  - **Software settings**
  - **Windows settings**
  - **Security settings**
  - **Operating system**

Local Computer Group Policy

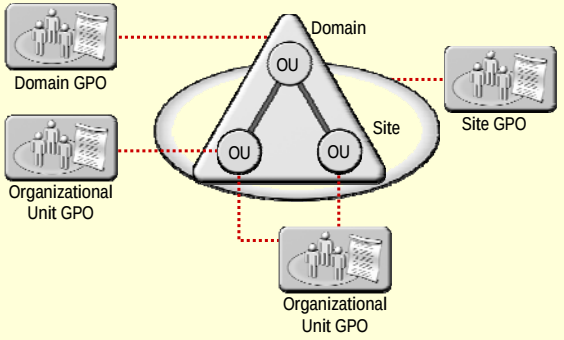
Local Group Policy Snap-in



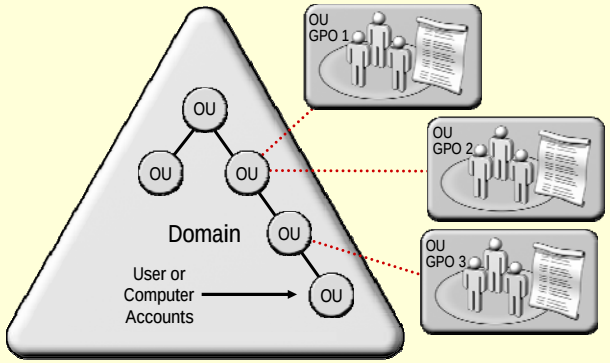
Tools Used to Manage GPOs

- Default Group Policy tools
  - Active Directory Users and Computers
  - Active Directory Sites and Services
  - Local Group Policy Custom Management Console
- Add-in tools
  - Group Policy Management Console (GPMC)

What Is a GPO Link?



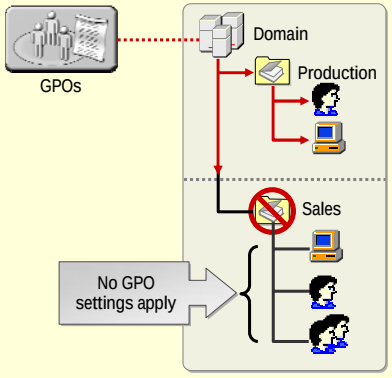
How Group Policy Settings Are Inherited in Active Directory



Attributes of a GPO Link

- Enforced
  - Take precedence over other GPO settings
- Link Enabled or Disabled
  - Links can be disabled for troubleshooting
- Deleted
  - Links can be deleted without deleting the GPO
- Multiple Links
  - When there are multiple GPOs linked to a container there is an order of precedence

Blocking the Inheritance of a GPO

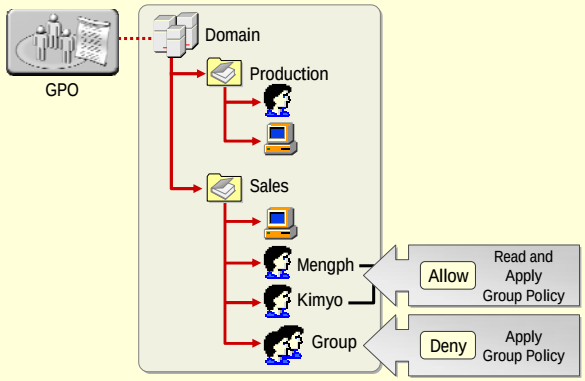


What Happens When GPOs Conflict

How conflicts are resolved:

When Group Policy settings in the Active Directory hierarchy conflict, the settings for the child container GPO apply

Filtering the Deployment of a GPO

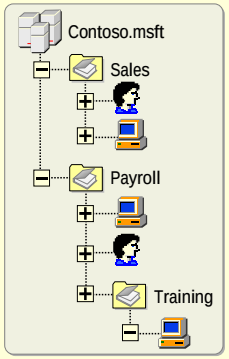


Modifying Group Policy Inheritance

Requirements

- Set up GPOs with the following requirements
  - Antivirus protection
  - Office suite
  - An accounting application

How do you set up your GPOs?



Why Use Group Policy?

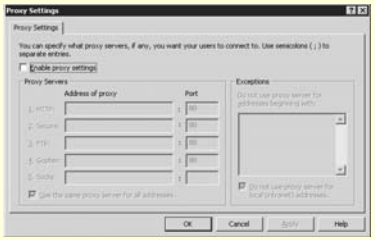
Use Group Policy to:

- Manage users and computers
- Deploy software
- Enforce security settings
- Enforce a consistent desktop environment
- Enforce loopback processing

What Are Enabled and Disabled Group Policy Settings?

Enable / Disable

Multivalued settings



What Are Group Policy Script Settings?

Group Policy script settings can be used to assign:

- For computers
  - Startup scripts
  - Shutdown scripts
- For users
  - Logon scripts
  - Logoff scripts

Why Use Group Policy Scripts?

Group Policy scripts can:

- Perform tasks that cannot be done through other Group Policy settings
- Clean desktops and return computers to their original state
- Provide a secure environment by clearing temp folders and page files

Restricting Group Membership

Group Policy can control group membership:

- For any group on a local computer
- For any group in Active Directory

What is a Software Restriction Policy?

- A policy-driven mechanism that identifies and controls software on a client computer
- A mechanism restricting software installation and viruses
- A component with two parts:
  - A default rule with two options:
    - Unrestricted
    - Disallowed
  - Exceptions to the default rule

Software Restriction Rules

Hash Rule
- Use to employ MD5 or SHA1 hash of a file to confirm identity
- Use to allow or prohibit a certain version of a file from being run

Certificate Rule
- Checks for digital signature on application
- Use when you want to restrict Win32 applications and ActiveX content

Path Rule
- Use when restricting the path of a file
- Use when multiple files exist for the same application
- Essential when SRPs are strict

Internet Zone Rule
- Controls how Internet Zones can be accessed
- Use in high-security environments to control access to Web applications

What Is Folder Redirection?

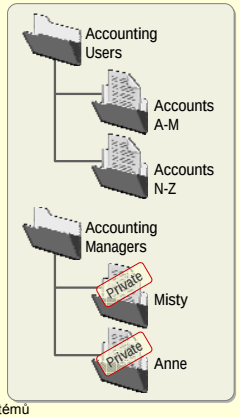
Folder Redirection allows:
- Redirection to folders on the local computer or on a network drive
- Folders on a server appear as if they are located on the local drive

Folders That Can Be Redirected

- My Documents
- Application Data
- Desktop
- Start Menu

Settings That Configure Folder Redirection

- Use basic Folder Redirection for common files and limited-access files
- With advanced Folder Redirection, the server hosting the folder location is based on group membership



Security Considerations for Configuring Folder Redirection

- NTFS permissions for Folder Redirection root folder
- Shared folder permissions for Folder Redirection root folder
- NTFS permissions for each user's redirected folder

What Are gpupdate and gpresult?

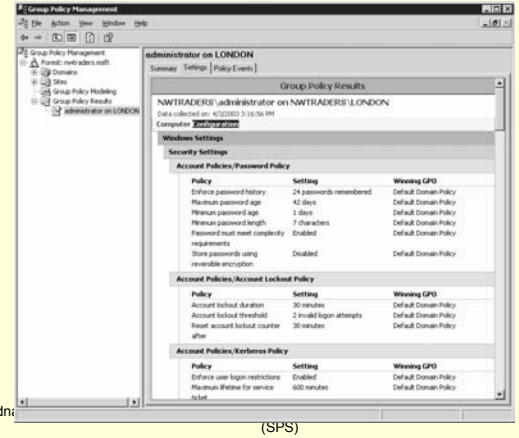
Use **gpupdate** to:

- Manually refresh updated Group Policy settings
- Force the refresh of all Group Policy settings
- Force a reboot or logoff if required to refresh the settings

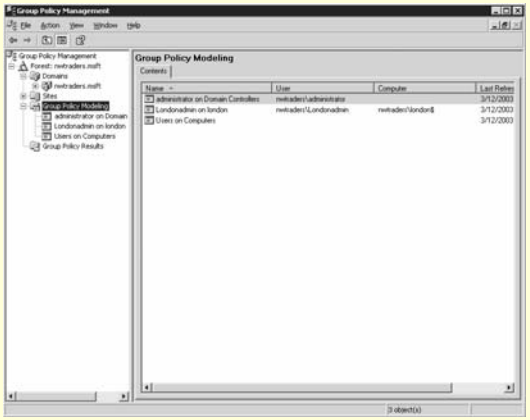
Use **gpresult** to:

- Display the resulting set of policies for a user or computer
- Redirect the resulting set of policies information to a file

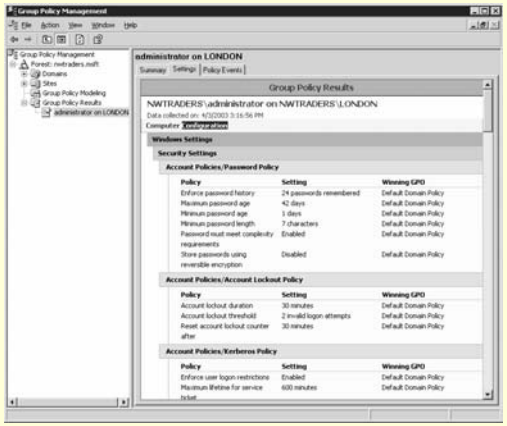
What Is Group Policy Reporting?



What Is Group Policy Modeling?

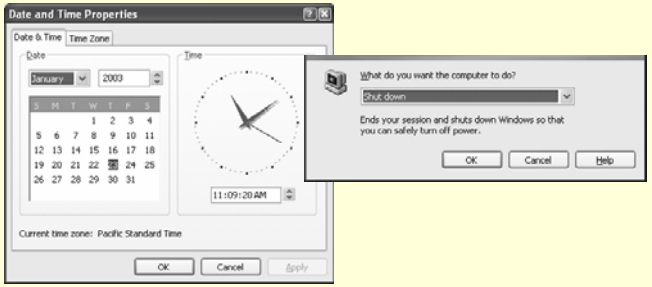


What Are Group Policy Results?



What Are User Rights?

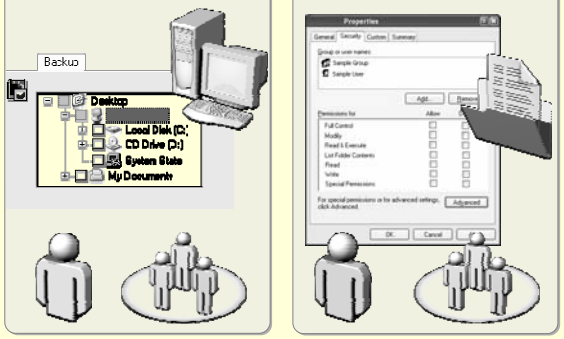
Examples of User Rights



User Rights vs. Permissions

User Rights:
Actions on System

Permissions:
Actions on Object



User Rights Assigned to Built-In Groups

Built-in local groups:

- Administrators
- Backup Operators
- Power Users
- Remote Desktop Users
- Users

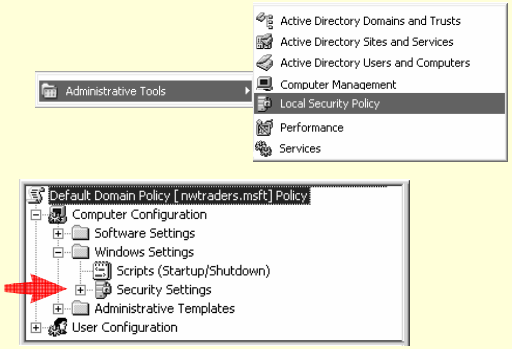
Groups in Users container:

- Domain Admins
- Enterprise Admins

Groups in Builtin container:

- Account Operators
- Administrators
- Backup Operators
- Pre–Windows 2000 Compatible Access
- Print Operators
- Server Operators

What Is a Security Policy?



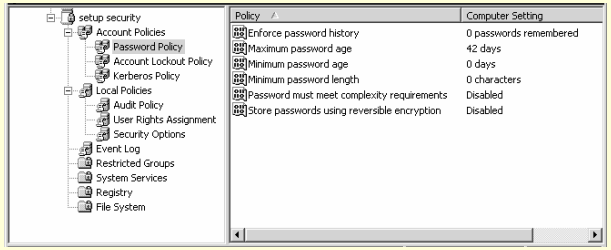
What Are Security Templates?

Template	Description
Setup security.inf	**Default security settings**
DC security.inf	**Default security settings for a domain controller**
Compatws.inf	**Modifies permissions and registry settings for application compatibility**
Securedc.inf and Securews.inf	**Enhances security settings**
Hisecdc.inf and Hisecws.inf	**Increases the restrictions on security settings**
Rootsec.inf	**Specifies permissions for the root of the system drive**
IESacls.inf	**Configures auditing and permissions on registry keys of Internet Explorer**

What Are Security Template Settings?

Security Template: Setup Security

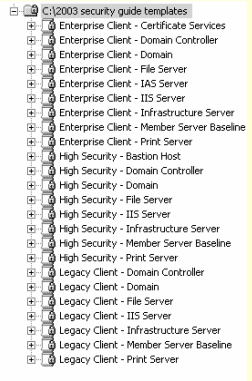
Sample Settings



Windows Server 2003 Security Guide Templates

The Windows Server 2003 Security Guide provides:

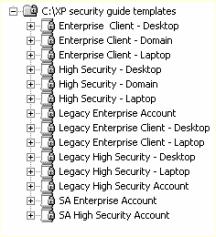
- Security documents and checklists
- Sample scripts
- Security templates for:
  - Legacy Clients
  - Enterprise Clients
  - High Security



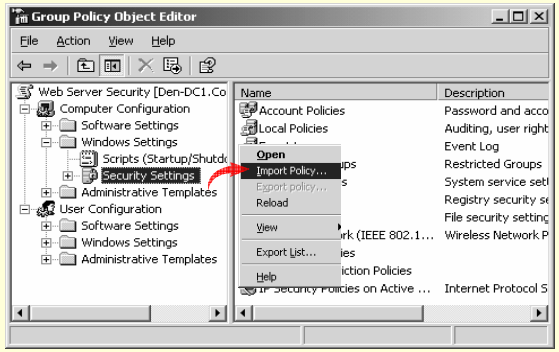
Windows XP Security Guide Templates

The Windows XP Security Guide provides:

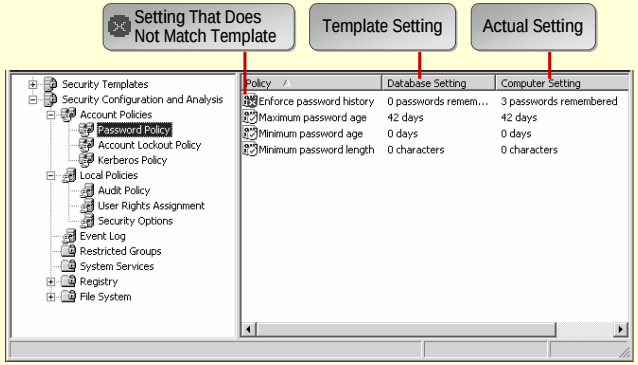
- Security documents and checklists
- Sample scripts
- Administrative templates
- Security templates for:
  - Enterprise Clients
  - High Security
  - Legacy Clients



Ways to Deploy Security Templates



What Is the Security Configuration and Analysis Tool?



What Is Auditing?

- Auditing tracks user and operating system activities and records selected events in security logs

What occurred? | Who did it? | When?

What was the result?

- Enable auditing to:
  - Create a baseline
  - Detect threats and attacks
  - Determine damages
  - Prevent further damage
- Audit access to objects, management of accounts, and users logging on and logging off

What Is an Audit Policy?

- An audit policy determines the security events that will be reported to the network administrator
- Set up an audit policy to:
  - Track success or failure of events
  - Minimize unauthorized use of resources
  - Maintain a record of activity
- Security events are stored in security logs

Types of Events to Audit

- Account Logon
- Account Management
- Directory Service Access
- Logon
- Object Access
- Policy Change
- Privilege Use
- Process Tracking
- System

Guidelines for Planning an Audit Policy

- Determine the computers to set up auditing on
- Determine which events to audit
- Determine whether to audit success or failure events
- Determine whether to track trends
- Review security logs frequently

Best Practices for Configuring Auditing

- Audit success events in the directory service access category
- Audit success events in the object access category
- Audit success and failure events in the system category
- Audit success and failure events in the policy change category on domain controllers
- Audit success and failure events in the account management category
- Audit success events in the logon category
- Audit success events in the account logon category on domain controllers

Types of Log Files

The following logs are available in Event Viewer:

- Application
- Security
- System
- Directory service
- File Replication service

Common Security Events

Logon	Event description
Event ID 528	**Successful logon**
Event ID 529	**Unsuccessful logon attempt**
Event ID 539	**Attempts to log on to a locked out account**
Security Log	Event description
Event ID 517	**Security log cleared**
Shutdown	Event description
Event ID 513	**System is shut down**

Tasks Associated with Managing the Security Log Files