Global Information Assurance Certification Paper

Windows 2003 Group Policy Security

GSEC Practical Assignment
Version 1.4b
Option 1

Fiona Law

May 31, 2004

Table of Contents

Introduction

With the massive number of worms, viruses, and attacks on nowadays enterprise systems, IT professionals and security administrators are searching for the best practices to manage and protect their systems in the most efficient and effective way. Enforcing group policy in a domain-based Windows environment has become a proactive approach to increase the level of security in network systems. Group Policy can also help to reduce administration workload and help desk costs within your organization.

This paper details how to configure and implement group policy in a Windows 2003 Server environment in making your network more secure and restrictive. It is important to understand what group policies are and what they actually do before you enforce the correct set of security policies onto your networks.

What are Group Policies?

Group policies are generally used by administrators to configure, control, and restrict user environment settings. Administrators create group policies to limit users in their organizations from performing certain tasks and to restrict specific functionalities such that network security can be tightened. Group policies can be applied at multiple levels such as sites, domains, and organizational units and you must link the Group Policy Object (GPO) to an Active Directory domain. There is close to a maximum of 1000 group policies that are applicable in a Windows 2003 environment.

Group Policy Settings

Group Policies can be generally categorized into a few main settings:

- Software settings – to control software deployment, applications can be run by users or computers
- Windows settings – to manage startup or shutdown scripts as well as to control security settings
    - Security settings – to manage account policies such as password policies and account lockout policies, event log and registry settings, audit policy, user rights assignments, and other security options
- Administrative templates – to manage user's environments and computer settings, such as configuring windows components, system, network, and printers

Group Policy Priorities

Please note that group policies are applied down from the highest level objects to the lowest level objects. The sequence of how group policies are processed is as follows:

1. Sites
2. Domains
3. Organization Units

By default, children objects are inherited from the policy of the parent objects. This means if a parent object has a specific group policy in place, it is cumulative and it applies to all the children objects below it. However, group policy can be blocked so that it cannot be overridden. In some cases, you may want to force some policies to never be overridden and not to inherit settings from a parent container. The default behavior of group policy can be modified using one of the following settings:

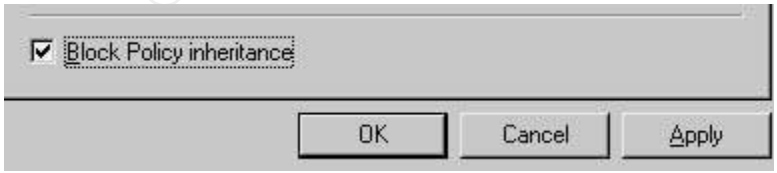
- Block Policy inheritance – It stops child objects inheriting policies from parent objects. It is set only on sites, domains, and organizational units, and not on individual GPOs.

- No Override – This prevents child objects from overriding policies set at higher levels.

Keep in mind that the No Override option takes precedence over the Block Inheritance option. This means that if a child object has Block Inheritance set but a group policy has No Override set on its parent container, then it will still get applied.

How to block inheritance:

1. Open Active Directory User and Computers.
2. Navigate to the object you wish to stop inheriting policies from its parent container
3. Right-click on it and go to 'Properties, select the "Group Policy" tab.
4. Check the "Block Policy inheritance' option
5. Click Apply then OK.



How to set No Override to a container object:

1. Open Active Directory Users and Computers.
2. Navigate to the object you wish it to never be overridden.
3. Right-click on it and go to 'Properties', select the "Group Policy" tab.
4. Click "Options", check the 'No Override' option.
5. Click OK, then click Apply and OK.

Group Policy Tools

In the earlier versions of Windows, administrators use the Active Directory Users and Computers MMC snap-in to create and administer group policies. However, with the latest version of Windows Server 2003, Microsoft has released a couple of free management tools which make it easer to work around Group Policies. These tools are downloadable by any organizations and they work not only in Windows 2003 Servers, but also in Windows 2000 environment and on any Windows XP workstations that belongs to a Windows 2000 Active Directory environment.

Group Policy Management Console

The Group Policy Management Console (GPMC) is a new tool available from Microsoft for using Group Policy in Windows Server 2003. It can be downloaded from http://www.microsoft.com/windowsserver2003/downloads/featurepacks (Fulton). It is designed for Windows Server 2003 rather than Windows 2000. Once you have it installed, you will find the application under Start>Programs>Administrative Tools, Group Policy Management option. As an alternative, you can also go to Start>Run, and type in gpmc.msc. It is a great tool that provides advanced functionality for planning, testing, deploying, and managing group policies on the Windows domain. In short, it makes it a whole lot easier for you to use and manage group policy.

One great feature of the GPMC tool is its backup functionality which allows you to export the Group Policy data to a file. Then you can import this file at a later time to a different location or use it for restoration. You can also use this tool to copy group policy from one place to another.

Resultant Set of Policies (RSoP) Tool

The Resultant Set of Policies tool is used by administrators for testing and planning before enforcing them on domain users and machines. With this powerful tool, administrators can actually benefit from the simulation of deployment to test out the results of the group policies and make any necessary changes before it gets implemented to the real domain.

The RSoP tool comes in two modes: the logging mode and the planning mode. When you are in the logging mode, it displays the actual policies for a specified computer or OU; whereas in the planning mode, it is a simulation of an effective GPO which will be in place. So it actually helps you to fully test out your group policy and its effects before you fully implement it in your domain.

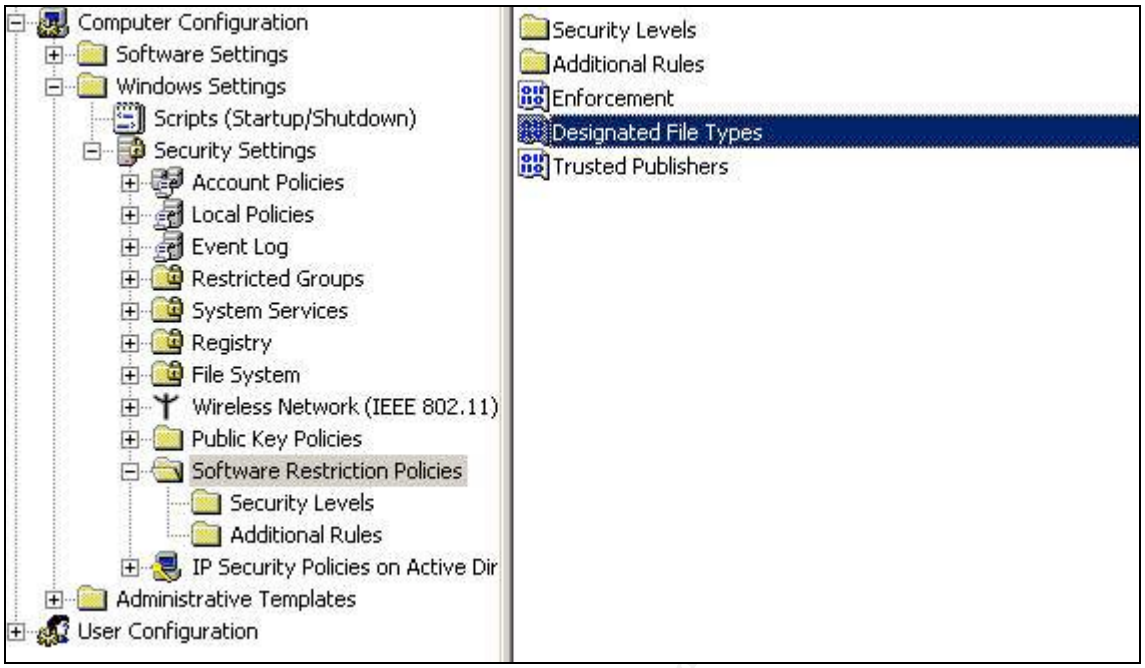
Group Policies

With almost 1000 individual group policy settings in Windows Server 2003, administrators may find it challenging to begin with configuring the different kinds of restrictions and security controls in their environment. In this paper, I will outline and detail a few significant group policy settings to give a guideline of the start of group policies implementation. Before I begin discussing some of the account policies and local polices, I would like to first introduce a new feature in Windows Server 2003 which is the software restriction policies and how it can greatly improve the level of security on your systems.

Software Restriction Policies

Many companies have set certain rules and policies to prohibit users from downloading and installing software onto their computers at work as this may lead to harmful results such as virus infection or hacker attacks. With the newly introduced software restriction policies in Windows Server 2003, it gives administrators more powerful control over software administration and it helps to strongly safeguard their systems.

Software restriction polices can be found under Windows Security>Security Settings. Under this policy, administrators can specify what applications can be installed and what cannot be installed. It can be machine-based or user-based.



There are three nodes where you can configure settings under software restriction policies: policy enforcement, designated file types, and trusted publishers. The enforcement setting allows you to do DLL checking when installing software, and also gives exceptions to local administrators to install software while restricting all other users. The designated file types allow you to restrict specific executable file types from being installed. Trusted publishers let you choose which software publishers you want to trust, once administrators have designated all the trusted publishers, the system will only allow applications from these trusted sources to be installed (Shinder).

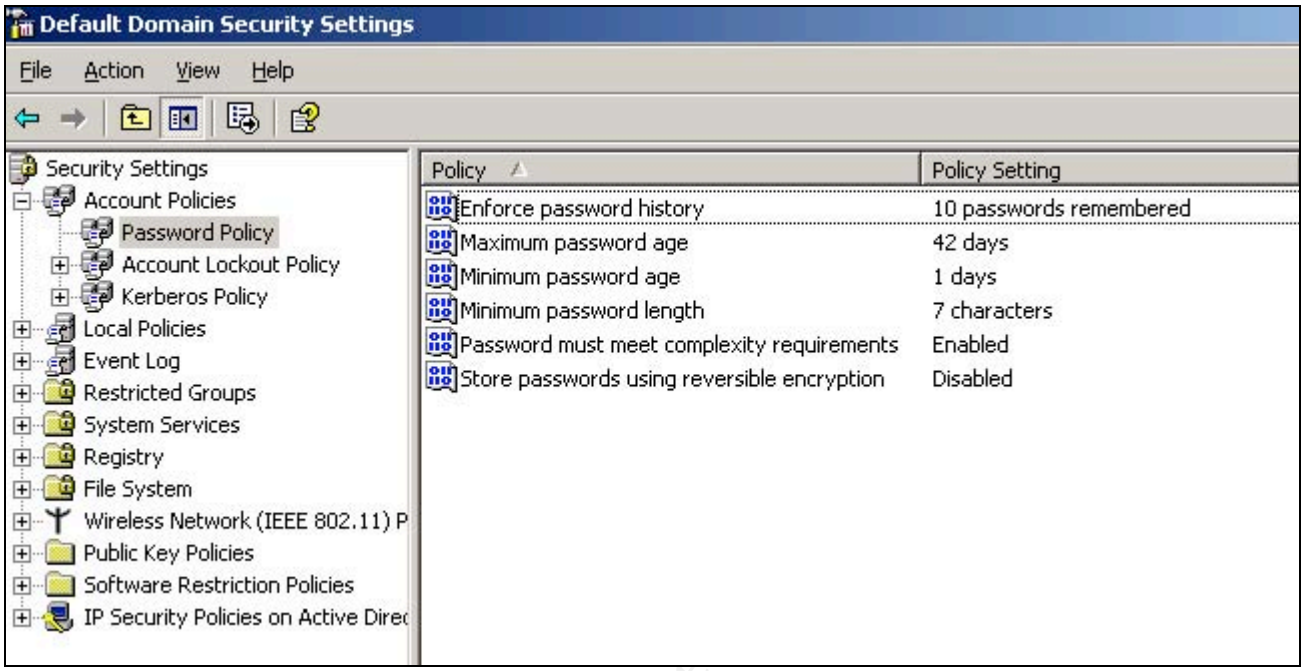
With a strong enforced software restriction policy in place, it will help administrators to take preventive measures against hackers and intruders from compromising your systems. It avoids the excessive and unnecessary downloads of games and unauthorized applications.

In Domain Security Policy, under Security Settings, you will find Account Polices and Local Policies which are generally more frequently used by administrators to set their restrictions on domain users.

Password Policy

Weak passwords tend to be one of the most common attack points and they can be easily cracked with dictionary attacks and default passwords. Therefore, it is very critical to have a strong password policy in place for every organization. You can configure password length, history, age, and complexity in password policies.

The following is an example of a strong password policy:



- *Password history* – 10 passwords remembered.
  Objective: It prevents users to reuse the last 10 passwords. This is to enhance security by ensuring that old passwords cannot be continually used.

- *Maximum password age* – 42 days
  Objective: It forces users to constantly change their passwords every 42 days, this is to ensure that passwords are changed often enough to maintain security.

- *Minimum password age* – 1 day
  Objective: It has to be less than the maximum password age. This has to be set at a value more than 0 to prevent users from repeatedly trying their passwords until they get to one of their old ones.

- *Minimum password length* – 7 characters
  Objective: It is recommended to set a value of 7 or more to avoid short passwords from being used.

- *Password must meet complexity requirements* – enabled
  Objective: It strengthens the integrity of your passwords by forcing your passwords to contain at least three characters from the following:
  - English upper case characters (A...Z)
  - English lower case characters (a….z)
  - Based 10 digits (0…9)
  - Nonalphanumeric (For example: !,@,#,$,%)

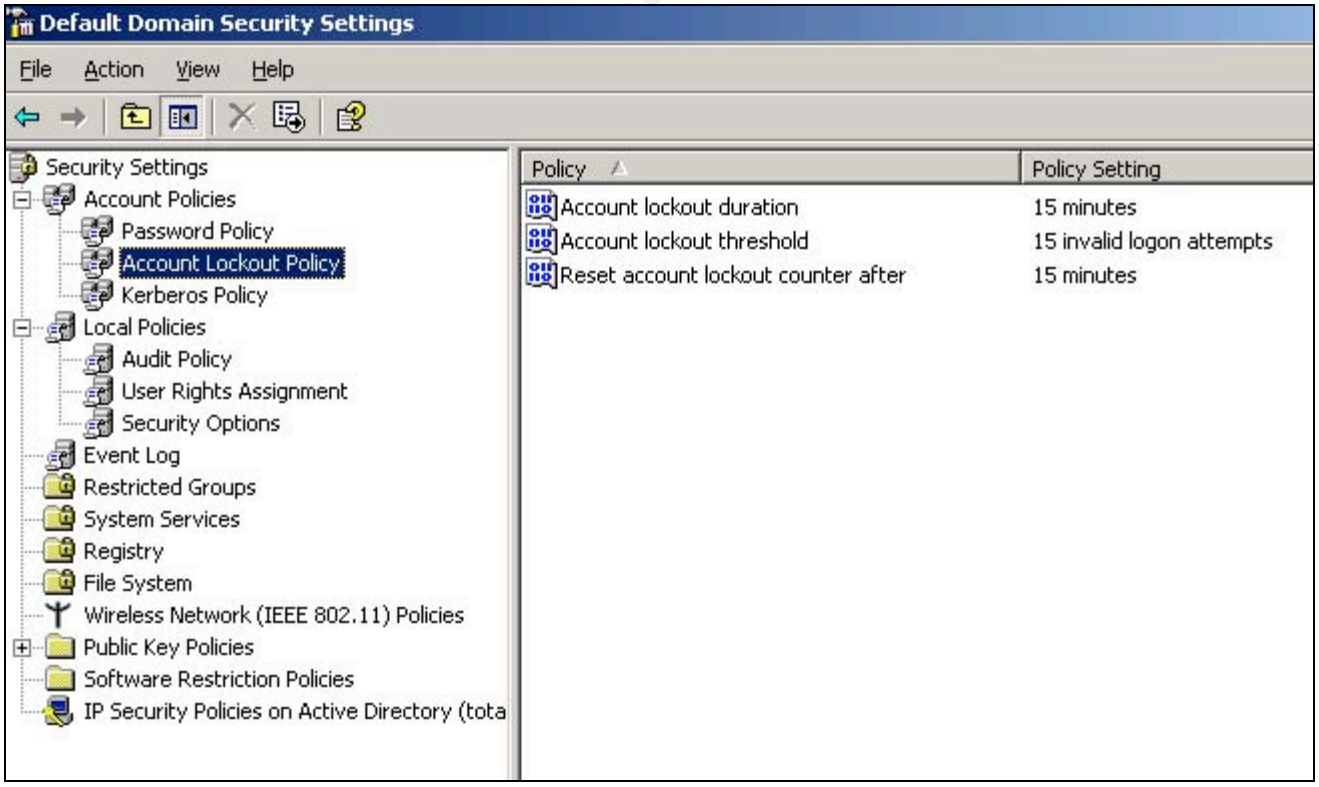
Account Lockout Policy

The importance of having an account lockout policy in place is to help prevent continuous brute-force password-cracking attempts. It locks the accounts after a certain number of failed attempts.

Account lockout duration – 15 minutes
Objective: The lockout durations should be set at a reasonable level to make password cracking attempts difficult.

Account lockout threshold
Objective: This value determines the number of failed logon attempts before a user account gets locked out. Generally, administrators allow enough failed attempts for typo or forgotten passwords.

Reset account lockout counter after
Objective: This value sets the reset time after a failed logon attempt.

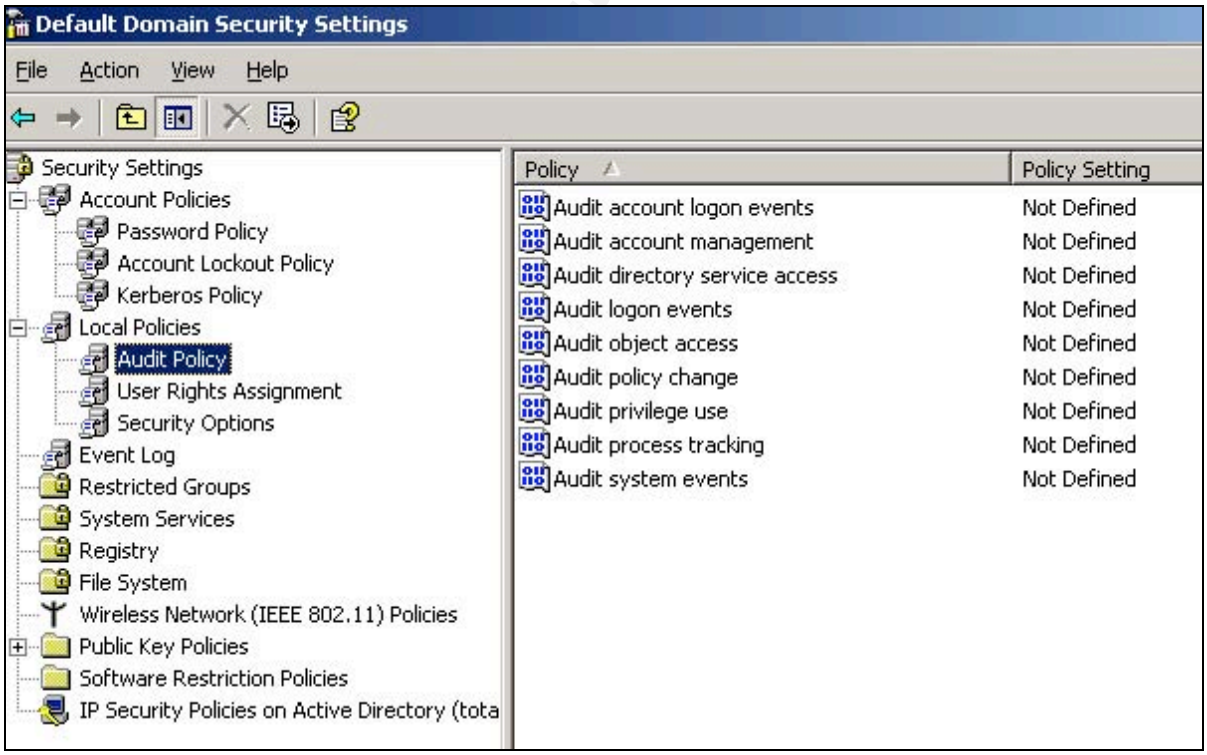


Audit Policy

A good audit policy can be very useful for administrators to track what is going on with your system, such as who is trying to logon, which files have been deleted and so forth. Generating and logging the correct information can save you a lot of time in troubleshooting history events.

You can choose to audit a numerous of events as shown below. However, administrators should consider carefully what they should be auditing to best meet the needs of their organization and what kind of information would be valuable to them. Over-auditing can end up wasting your hard disk space and human resources in reviewing the event logs. Therefore, think carefully before you configure an audit policy to avoid the unnecessary overheads.

In this section, I will focus on a few audit policies that are more commonly used by administrators such as the account logon events, account management, and object access. Once these policies have been enabled, administrators will get a clear picture of where their security level stays and what specific events or users they need to monitor closely to tighten their security control.



Audit account logon events

Enabling the account logon events policy will log an event every time a user connects to the server across the network. It gives administrators a good idea who is on your system or who is trying to get onto your system. You can specify whether you want to audit only successful or failed logons, or both. Logging failure logons will help you determine who is trying gain unauthorized access to your system.

Audit account management

Events that you can configure in account management policy include:

- When a user account or group is created, modified, or deleted
- When a user account is renamed, enabled, or disabled
- When a password is created or changed

Audit logon events

Auditing logon events will allow you to keep track of users logging on and off, and when they are making connections to the machine. Events are generated when logon takes places, whereas account logon events are generated when the account makes a connection.

Audit object access

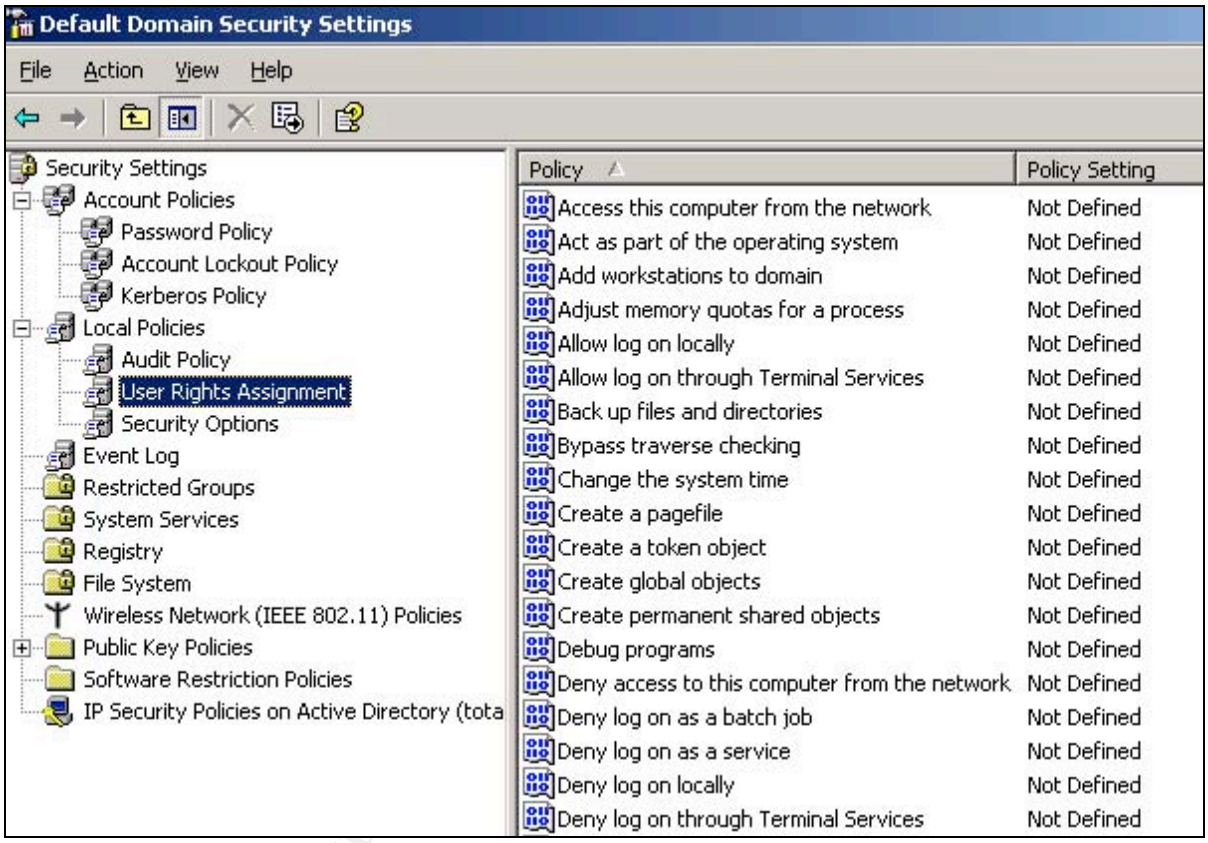
Auditing object access will help you track down who is accessing and modifying your files, folders, printers, registry keys, and so forth. This is helpful for administrators to determine who is trying to gain access to unauthorized areas on your systems. For instance, if only the finance group is allowed to access the HR and accounting data folders and all other users are being restricted, when someone who does not have the permissions to these directories try to access them, a failure event will be generated.

Audit policy change

Auditing policy changes is a good way to log events when there are changes made to your audit policies, password policies, or user rights assignment policies. At times, administrators might need to document the dates when new policies take effect.

User Rights Assignment

These settings help to determine actions that a user can perform on a system, such as shutting down the system, changing the system time, loading drivers, and others. You can control every aspect of security here by restricting what a user can do and cannot do. As always, you want to give the least amount of privilege to the users to limit their rights on your systems.



In this section, I will discuss a number of the user rights assignment settings and how vulnerable they can be to your system.

Allow log on locally

You should only grant the allow log on locally right to administrators. Any account with this right will have access to the computers system and not restricting this privilege could result in unauthorized users performing destructive activities on your system.

Allow log on through Terminal Services

Allowing a user to log on through terminal services means that the user can log on to the computer anywhere remotely by using a remote desktop connection.

Make sure you restrict this privilege to the proper users and groups to avoid any unauthorized access to your system.

Shut down the system

The right to shut down the system should be restrictive to domain administrators only. Shutting down the system basically means all functions and processes will be terminated and that could stop your business from running.

Log on as a service

This can be a powerful privilege which allows accounts to launch services on the network. It should be limited to administrators who need to install and configure services on your systems to have this log on as a service right.

Enhancing Security with Group Policy

Aside from the above few mentioned policy settings, there are many more group policy object settings in Windows 2003 that you can configure and apply for your domain, such as folder direction, event log settings, control panel access, system access etc. It is critical for administrators to understand what is important and what is vulnerable to your networks such that you can design and implement the right sets of security policies to maximize your security measures within your organization.

There are also other tools that Microsoft provides for doing group policy such as the security templates. You select the template that best fits your environment and security needs for implementation. You can configure settings such as account policies, passwords policies, and other local policies etc in these templates which can then be imported into your active directory objects. Different organizational units may have different level of security and restrictions.

It is also a good idea to turn off anonymous enumeration of SAM accounts and to rename the administrator and guest accounts on all your Windows machines to address some of the known vulnerabilities. You can configure these settings under the GPO's Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options node (Mar-Elia).

Conclusion

Deploying group policies is an effective proactive approach to enforce security in your network environment. A good group policy will help administrators establish a security baseline for network systems. It not only reduces overhead administration, it also helps IT administrators manage their secured networks easier. Group policies should always be reviewed and revised in a timely manner by various authorities to ensure that they can meet your up-to-date security needs and address your network security concerns.

Besides implementing a good group policy in your organization, you also need to identify other security essentials and components to tighten your network security, such as installing a good strong firewall system, educating your users, having anti-spam and anti-virus protection in place, setting up an intrusion detection system and network traffic monitoring system, applying content filtering, being aware of physical security breaches and so forth. All these parameters help to contribute to the establishment of a strong secure network and to overcome today's security challenges.

References

"Introduction to Group Policy in Windows Server 2003." April 2003. Microsoft TechNet. Microsoft. 12 May 2004. http://www.microsoft.com/windowsserver2003/techinfo/overview/gpintro.mspx

"Introducing the Group Policy Management Console." 7 April, 2003. Microsoft Windows Server 2003. Microsoft. 12 May 2004. http://www.microsoft.com/windowsserver2003/gpmc/gpmcintro.mspx

Rudich, Joe. "Group Policy Changes in Windows Server 2003." October 2003. Windows & .NET Magazine. 15 May 2004. http://www.winnetmag.com/WindowsSecurity/Article/ArticleID/39987/39987.html

Fulton, Scott. " Windows Server Guide - Active Directory." 21 April, 2004. InformIT Reference Guide. 12 May 2004. http://www.informit.com/guides/content.asp?g=windowsserver&seqNum=29

Mar-Elia, Darren. "GPO Security." October, 2003. Windows & .NET Magazine. 21 May 2004. http://www.winnetmag.com/articles/print.cfm?articleID=40044

"Windows 2003 – Group Policy Overview." 8 May 2004. http://www.computerperformance.co.uk/w2k3/W2K3_group_policy.htm

"Chapter 4 - User Rights Assignments - Threats and Countermeasures Guide." Microsoft TechNet. Microsoft. 17 May 2004. http://www.microsoft.com/technet/security/topics/hardsys/tcg/tcgch04.mspx

Shinder, Deb. "How Windows Server 2003 Software Restriction Policies Improve Security." Apr 30, 2003. WindowsSecurity.com. 21 May 2004 http://www.windowsecurity.com/articles/windows_2003_restriction_policies_security.html

Ruston, Neil, and Laura Hunter. Designing Security for a Windows Server 2003 Network. Syngress. 1 Feb, 2004.

Savill, John. "John Savill's FAQ for Windows." 27 July, 2000. Windows & .NET Magazine. 15 May 2004.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor