Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Implementing Password Controls and Account Policies Using Windows 2000 Group Policy

Microsoft's Windows 2000 brought many changes to the way security is implemented in the Windows environment. Windows 2000 uses Active Directory to store and manage security information, and the security rules on a domain are enforced using Group Policy and Group Policy Objects. This paper will provide the reader with a high-level understanding of Group Policy, discuss some issues to consider when implementing Group Policy, and describe how strong password controls and secure account policies, as documented in the SANS ...

Copyright SANS Institute

Author Retains Full Rights

AD

Entrust < Let's Talk

Implementing Password Controls and Account Policies Using Windows 2000 Group Policy

Carlo Scannella
February 15, 2001

Introduction

Microsoft's Windows 2000 brought many changes to the way security is implemented in the Windows environment. Windows 2000 uses Active Directory to store and manage security information, and the security rules on a domain are enforced using Group Policy and Group Policy Objects. This paper will provide the reader with a high-level understanding of Group Policy, discuss some issues to consider when implementing Group Policy, and describe how strong password controls and secure account policies, as documented in the SANS Windows NT Security Step by Step, can be implemented in Windows 2000.

Active Directory and Group Policy Objects

Active Directory is Microsoft's implementation of a Directory Service. Active Directory (AD) uses a tree-like structure to store all the information about objects on the network. The AD holds accounts for the users, groups and computers within a domain, and this information is organized in "containers" called Organizational Units (OU's).

Group Policy Objects (GPO's) contain a set of "rules." These rules can be used to specify settings for software distribution, logon and logoff scripts, desktop look-and-feel, and more. From a security perspective, GPO's can be used to specify account and password settings, audit capabilities, screen saver settings, as well as settings for new Windows 2000 features such as IPSec and Certificates. GPO's can be applied to Windows 2000 sites, domains, or OU's.

How are the Active Directory and Group Policies related? The rules that govern the domain are set by creating Group Policy Objects and applying them to OU's. At the highest level, there is a Default Domain Policy GPO. This GPO is created when the first domain controller is installed, and contains domain-wide account policy settings. At each lower level OU, or "child OU," additional GPO's can be created and applied.

Windows 2000 organizes Group Policies into two broad categories - Computer Settings and User Settings. Under each of these categories, there are Software Settings, Windows Settings, and Administrative Templates. The important security settings for accounts can be found under Computer Settings - Windows Settings. This is where account policies, such as password length, password history, account lockout and Kerberos settings, can be implemented.

Issues to Consider When Implementing Group Policy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows 2000 Group Policies can be a complex matter, and there are many things to consider when implementing them. An introductory paper on the subject obviously cannot go into enough depth on this topic - here are just a few issues to consider:

- **Account Policies are domain-wide** - In the Domain GPO, the three categories of settings under Account Policies - Password Policies, Account Lockout and Kerberos Policies - are defined on a domain basis only. This is a very important consideration - GPO's for account settings defined for lower level OU's WILL NOT WORK for domain users. Settings at lower level OU's will take effect if users logon locally (i.e., using a local account) to a computer, but will not when logging on to the domain.
- **No Override and Block Inheritance Settings** - In Active Directory, policies defined at higher-level OU's are inherited, or "passed down," to child OU's. When creating a GPO at a lower level, a "Block Inheritance" setting can be activated, which will prevent policies from being passed down from the parent OU. Conversely, a "No Override" option can be set on a GPO at a parent OU, which FORCES its policies to be set at the lower level OU. It is easy to see how this can quickly complicate the administration of the domain, and how difficult it can be to troubleshoot problems with Group Policies. Microsoft recommends limiting the use of the No Override and Block Inheritance settings.
- **Policy Processing** - It is important to understand how Windows 2000 processes policies. Policies are processed in a hierarchy:

    1. Local GPO's - these policies are local to a computer, which can be set on any Windows 2000 computer, regardless of its participation in a domain
    2. GPO's applied to Sites
    3. GPO's applied to the Domain
    4. GPO's applied to OU's

    When policies are applied, they overwrite those previously applied. Considering the above order of precedence, policies applied at the local level will be overwritten by domain policies when joining the domain. Policies applied at the OU in which the user or computer is placed will be applied last (and therefore be implemented).

Implementing Account and Password Policies using Group Policy

The SANS Windows NT Step by Step describes how to implement security on an NT 4.0 server. Phase 4 of this document demonstrates how strong password controls and secure accounts policies are implemented. Using the Step by Step as a guide, the following will describe how the same controls can be implemented in Windows 2000.

Creating new user accounts - Users are created in Windows 2000 using an MMC snap-in called Active Directory Users and Computers. As in Windows NT User Manager, the administrator can enable "User must change password at next logon," and disable "Password never expires" when creating new user accounts.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Setting account and password policies - To implement the settings as described in the SANS document, the Domain Group Policy Object must be modified. In the Active Directory Users and Computers snap-in, right-clicking on the domain and selecting Properties, Group Policy and Edit will launch the Group Policy Editor. Navigating to Computer - Windows - Security - Account Policies - Password Policies will allow the following account settings to be modified:

- Maximum Password Age
- Minimum Password Age
- Minimum Password Length
- Enforce Password History (equivalent to "Password Uniqueness" in the Step by Step)
- Password Must Meet Complexity Requirements - this must be enabled if a password filter (such as PASSFILT.DLL) is used to enforce complex password requirements
- Store Password Using Reversible Encryption - This should be DISABLED so that passwords remain encrypted!

Navigating to Computer - Windows - Security - Account Policies - Account Lockout Policies will allow the following account settings to be modified:

- Account Lockout Duration - this sets the amount of time, in minutes, that an account remains locked out. If administrators must reset locked accounts, this should be set to 0.
- Account Lockout Threshold - this sets the number of failed logon attempts before an account is locked out
- Reset Account Lockout Counter After - this value establishes a waiting period before resetting the account lockout counter. This setting forces a user, presumably an unauthorized user, to wait before another logon attempt can be made.

Additional Group Policy Settings

In addition to those previously discussed, there are a great deal of security settings that can be enabled using Group Policy. Many of these can be found by using the Group Policy Editor and navigating to Computer - Windows - Security - Local Policies. There are three categories of policies that can be set. The first is Audit Policy - audit can be enabled for many events, including logon and logoff, account management and policy changes. The second category is User Rights Assignment. In this section, an administrator can enforce rules on users and groups, such as "deny logon locally," "add workstations to a domain," and "log on as a service." Finally, the Security Options section provides a "catch-all" for many settings, such as "do not display last user name in logon screen," automatically logging off users when sessions expire, and setting the logon message text.

Conclusion

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows 2000 Group Policy is a complex subject. This paper has attempted to provide a high-level introduction to the subject, and bring to light some important considerations surrounding the implementation of Group Policies. In addition, the paper has provided some examples of how security can be implemented in Windows 2000. To learn more about the subject, the reader is encouraged to review the references provided, as well as get some hands-on experience with the Windows 2000 operating system.

References

Full Armor. "FAZAM 2000 - Managing Policies in the Enterprise." http://www.fullarmor.com/solutions/group/whitepaper.cfm (6 Feb, 2001).

Lowe-Norris, Alistair G. "Profiles and Group Policy Primer." Windows 2000 Active Directory. January 2000. http://www.oreilly.com/catalog/win2000ads/chapter/ch08.html (6 Feb. 2001).

McLean, Ian. "Windows 2000 Security Little Black Book." The Coriolis Group, 2000.

Microsoft. "Windows 2000 Group Policy." 26 July, 2000. http://www.microsoft.com/windows2000/library/howitworks/management/grouppolwp.asp (6 Feb. 2001).

The SANS Institute. "SANS Windows NT Step by Step." Version 2.15. 30 July, 1999.

Stanek, William R. "Microsoft Windows 2000 Administrator's Pocket Consultant.w" Microsoft Press, 2000.

© SANS Institute 2003, Author retains full rights

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**