Domain Security Policy Application

(Wednesday, 24 November 2004) - Contributed by Paul Williams

Many Active Directory administrators are often asking questions about the password polices in their domains. Questions such as:

- Why does password and Kerberos policy need to be applied at the domain level?
- Why can't this be applied at the OU level?
- Is it possible to have different password policies applied to different objects in a single domain?

The answers to these questions are answered in this article.

Domain Controllers process account policies differently to computers (workstations, member servers). Computers process the account policy configured in the closest GPO. The settings that are applied, either from the closest GPO, or possibly another GPO higher up the hierarchy with the No Override/ Enforced setting configured, applies only to that computer. This means that the only user accounts affected by this policy are those stored on that computer. Those stored in the computers SAM.

Domain Controllers do not apply policy in the same way. Domain Controllers read (apply) account policy from the Domain Naming Context. This behaviour is by design. Any given Domain Controller is an exact replica of all other Domain Controllers in the domain. As Domain Controllers are responsible for user and computer logons, all domain controllers must have the same policy. It would not be sensible to have Domain Controllers applying account policy in the same way as computers, as that would mean that some Domain Controllers might have a less secure policy than others. Therefore they must not process the policy linked to the OU in which they reside, as they might not all reside in that OU.

Note. It is recommended that all Domain Controllers are not moved from the default OU - Default Domain Controllers. However, it is possible to move them or indeed apply different policies to them.

The most common account policies are password settings policies. The password settings are defined with the attributes:

- maxPwdAge
- minPwdAge
- minPwdLength
- pwdHistoryLength
- pwdProperties

These attributes are what are authorative for the domain. However, there is a little more to the process than the Group Policy Client Side Extension (CSE) of any Domain Controller simply applying these values. This isn't what happens. The Domain Controller that holds the Primary Domain Controller Emulator (PDCe) FSMO role is the only Domain Controller that actually applies the password policies from these attributes. The PDCe runs a thread (SCE) that applies the policy object linked to the domain. This sets the attributes of the domain NC, which are then replicated normally to the other DCs.

Security Configuration Editor (SCE) is a "pseudo-service" that runs within services.exe and is responsible for applying security templates (INF file, for example, DCUP.INF). Among other things it applies the password policy GPO settings to the Active Directory (domain NC) via LDAP. SCE is implemented as a Group Policy extension module. SCE only processes account policy linked at the domain level. The thread within SCE that applies the policies to the PDCe lies dormant if the DC isn't the PDCe. Password policy configured anywhere else is not processed by SCE, which means that it will only apply to the local SAM of any computer accounts within scope.

Summary

Q. Why does password and Kerberos policy need to be applied at the domain level?

Because the SCE service running on the PDCe applies this policy by reading the values in the highest GPO linked to the domain and writing those values to their attributes of the domainDNS object for that domain. This change is then replicated normally to all other Domain Controllers. Modifying these values on Domain Controllers other than the PDCe will see these values overwritten by the PDCe the next time Group Policy is applies - by default, every five minutes.

Q. Why can't this be applied at the OU level?

These policies can be applied at any level within the domain. However the settings will only apply to computer accounts. Domain Controllers only use the policy linked to the domain.

The reason that these policies cannot be applied at the OU level is a design decision. This decision was probably to ensure consistency. If Domain Controllers were to apply policy from their nearest OU, there is the possibility that some Domain Controllers would have different settings than others (in the case where Domain Controllers have been moved to different OUs). This would be a grave security error.

Q. Is it possible to have different password policies applied to different objects in a single domain?

Yes and no. Natively (with the default tools available in Active Directory) the answer is no. Some third party software developers have developed software that will allow stronger policies for select computers.

TIP. Microsoft is investigating allowing stronger passwords for selected users and computers. However at this time it is not know whether this work will be ready for Longhorn.

Author: Paul Williams
Date: 25-07-2004
Version: 1.2.1

Last updated: 25-10-2005
Last updated by: Paul Williams