

Re: OU group policy and how to use ldapsearch to find GPO settings

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-03/msg00229.html

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Thu, 16 Mar 2006 22:37:43 -0700
-

First question:

There is only one set of Account policies that are applied to all accounts of the domain. Setting Account policies at an OU level effects those policy settings for the machine local account of computers in those OUs.

Second question:

Not sure I understand what you are after, or what you mean by the new group policy. Your ldap search (a little reckless with the wildcard) is showing your attributes of the domain object you named. GPOs are stored partly in AD and partly in the filesystem (SYSVOL).

—

Roger Abell
Microsoft MVP (Windows Server : Security)

"emily1997" <emily1997@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:E9C5349C-8DC5-4CA9-92CD-0E3E4C812869@xxxxxxxxxxxxxxxxxxxx

Hi, I am from the UNIX world. I have an environment that my HP-UX unix machine is configured with a Windows 2003 server(single domain). Users in ADS can logon to my unix box via pam_kerberos.

If I configure the account lockout policy in the default domain policy, say:

Account lockout duration: 30 min
Account lockout threshold: 5 invalid logon attempts
Reset account lockout counter after: 30 min

Then an ADS user try to logon to the unix box with an invalid password for 5 times, this user's account will be locked out for 30 minutes. I verified that this works as expected.

Now, I crated an ou=test_ou, and added a new group policy linked to this OU,
and I set the accout lockout policy in this new GPO as following:
Account lockout duration: 3 min

Re: OU group policy and how to use ldapsearch to find GPO settings

Account lockout threshold: 2 invalid logon attempts
Reset account lockout counter after: 3 min

then I should expect that a user under ou=test_ou should be locked out if this user entered bad password twice in a row at logon time. But it didn't work this way. This new group policy somehow didn't get applied to this user. So does anyone know why it didn't work?

The second question I have is: I can use ldapsearch command to find out the settings for the default domain policy. For example, I can do the following:

```
./ldapsearch -s base -h HOST -p PORT -D administrator@xxxxxxx -w  
PASSWORD -b  
"DC=test, DC=com" "objectclass=*" | grep -i lockout  
lockoutDuration: -18000000000  
lockOutObservationWindow: -18000000000  
lockoutThreshold: 5
```

How can I use ldapsearch command to find out the settings for the new group policy?

Thanks in advance for your help.