

RE: Account Lockout Policy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-10/0053.html>

From: Laura A. Robinson (*larobins_at_bellatlantic.net*)

Date: 10/25/05

Date: Tue, 25 Oct 2005 13:16:43 -0400

To: "'Alexander Suhovey'" <asuhovey@mtu-net.ru>, 'Rasmus RÛnlev' <rr.it@cbs.dk>, <focus-ms@securi

Rasmus is mostly correct; he didn't say that the policy would be **linked** at the Domain Controllers OU, just that the domain password policy would apply to the domain controllers. There is one fly in the ointment, however— DCs that (for reasons unknown and probably nonsensical) were moved outside of the Domain Controllers OU will still use the password policy that is defined at the domain level.

Domain controllers have no SAM. They replicate the Active Directory database. The only place where one can apply password policies that will affect the AD database is at the domain (AD database) level. Password policies applied at ANY OU will affect the [LOCAL] SAM for any machines located in that OU. Therefore, if one were to do something even more nonsensical such as place member servers into the Domain Controllers OU, then were to link a password policy to the Domain Controllers OU, the member servers in that OU would apply that policy to their local SAM. Because, again, DCs have no local SAM (except for the one that is initialized only in Directory Services Restore Mode, and GP is not applied when booted into DSRM, anyway), DCs will still process and apply any policies linked to the OU(s) in which the DCs are located. However, the account policy section of such policies would be ignored because there is NO SAM to which they would apply.

I would encourage anybody for whom this is confusing to try out the scenarios I've outlined in a test lab. Move DCs around and you'll see that they still utilize the domain-level account settings, because, again, the DOMAIN is where their accounts are housed, regardless of the location of the domain controller object in AD. Then stick a member server into the Domain Controllers OU and link a policy defining account settings to that OU. The DCs will not apply it because they have no SAM "in" that OU, but the member servers will, because they now DO have a SAM "in" that OU.

Laura

> -----Original Message-----

> From: Alexander Suhovey [mailto:asuhovey@mtu-net.ru]

> Sent: Saturday, October 22, 2005 4:05 PM

> To: 'Rasmus RÛnlev'; focus-ms@securityfocus.com

SecurityFocus Microsoft: RE: Account Lockout Policy

> *Subject: RE: Account Lockout Policy*
>
> > -----Original Message-----
> > *From: Rasmus RÛnlev [mailto:rr.it@cbs.dk]*
> > *Sent: Friday, October 21, 2005 1:37 AM*
> > *To: focus-ms@securityfocus.com*
> > *Subject: Re: Account Lockout Policy*
> >
> > *Hi,*
> >
> > *[..]*
> > *It seems some of the responding*
> > *people are knee-jerk-reacting to "you can only put into*
> > *effect account*
> > *policy from the domain level". This is correct in so far*
> > *that "Domain*
> > *Policy" will be applied towards Domain Controllers, sitting in the*
> > *Domain Controllers OU.*
> >
> > *Not quite. Having DCs in GPO scope is not how it works for*
> > *domain account policies. If you create a GPO linked to Domain*
> > *Controllers OU, DCs will ignore account policies configured*
> > *in this GPO. Domain account policies must be configured only*
> > *at the root level of domain.*
> > *Here's a couple of quotes from [2]:*
> > *"Password policies, Kerberos, and some security options are*
> > *only merged from GPOs that are linked at the root level on*
> > *the domain. This is done to keep those settings synchronized*
> > *across all domain controllers in the domain."*
> >
> > *"For domain accounts, only one account policy is permitted*
> > *per domain. This account policy must be specified in the*
> > *Default Domain Policy GPO, or in a new GPO that is linked to*
> > *the root of the domain and has precedence over the Default*
> > *Domain Policy GPO. [...] A domain controller always gets the*
> > *account policy from a GPO linked to the domain, by default*
> > *from the Default Domain Policy GPO."*
> >
> >
> > *1. "Where does your client's security policy actually come from?"*
> > *http://searchwin2000.techtarget.com/tip/1,289483,sid1_gci11081*
> > *25,00.html*
> >
> > *2. "How Security Settings Extension Works"*
> > *<http://www.microsoft.com/technet/prodtechnol/windowsserver2003>*
> > */library/TechR*
> > *ef/824b4758-9430-4633-8d8f-3dad0f2bf839.msp*
> >
> > --
> > *Al*
> >

RE: Account Lockout Policy

SecurityFocus Microsoft: RE: Account Lockout Policy

>
>
>
>
>
>
>

