

Re: Account Lockout Policies

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2007-09/msg00012.html>

- *From:* Bogwitch <bogwitch@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 03 Sep 2007 14:05:09 +0100
-

Roger Abell [MVP] wrote:

[snip]

Slight flaw there. Imagine a user who last used the system just before the password change reminder. Let's assume 14 days. Now, that user will have an expired password in 14 days, not 30 days. Now remember that most users (IMO) won't change their password until they absolutely positively have to....

Well observed Bogwitch, and stated.
The solution to poster's is either being overlooked or it is even more deeply messy, as you show.

One's nightly process would need to track the age of first expiry of the pwd, disabling only upon an uninterrupted 16 days (per your example) in expired pwd state, so it is soluble. The use of this delay counter might even work with the need to adjust the "lockout" threshold and the pwd aging settings (age and prewarn) toward each other. But still, needing to persist info, being no longer a stateless simple script, raises the bar for the nightly's code.

Good catch; thanks.

Is there really no direct, reliable, way to determine accounts qualifying for the poster's scenario ?

The problem is the OP is looking for a technical solution that should be addressed by policy. Deleting user accounts after 30 days of inactivity allows a windows of opportunity of 30 days for an ex-user to re-use the network. The ex-user could have left the organisation in question and could have left under unfavourable circumstances. Allowing accounts to remain dormant for 30 days is simply not good business practice.

If a technical solution is unavoidable due to a lack of management buy-in, there are a few ways that it can be achieved.

Re: Account Lockout Policies

1. Extract login details from the security logs. Ascertain from those logs when users last logged in and add 30 days. This would be messy and cumbersome. ADGP will have to be configured to record the logins and it may be necessary to collect the security event log from multiple servers/ workstations. It will also introduce a risk of DOS if the device that has the latest logons is missed for any reason.

2. From the users logon script, touch a unique (to the user) file in a common area. If the file becomes older than 30 days, delete the account. Correct permissions will need to be set on the common area to prevent anyone from modifying the data contained therein.

There are utilities available that can identify files that are more than 30 days old.

3. Florian suggested using the last logon date from AD. While there are several utilities that will extract the relevant information I have had some issues with the scripts I have found that report some erroneous information back.

One flaw with the above examples: These will only detect a logon within the last 30 days. It is possible for a user to log on and lock their workstation every night. (Some won't even do that!) If they continue to do this for 30 days, the login will become 'stale' and will be listed by each of the above methods as ready for deletion.

Personally, I would try to get the administrative control in place first. If necessary, one of the other solutions could be implemented as a detective control.

Bogwitch.

--

Posted via a free Usenet account from <http://www.teranews.com>

.