

Re: AD and Expired Password Checking and how to test?

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00054

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 1 Sep 2006 09:48:20 -0500
-

It is also easy and straightforward to handle this in .NET, as it too handles 64 bit numbers well. Ch. 10 of our book (free download from link below) demonstrates this clearly. It is really VBScript that suffers here and contributes to the inaccuracy of the results. Like Joe said, the exact date is set and known. There is no guesswork on the part of the directory itself. It is the tool you are using that is providing all the fuzziness.

Joe K.

--
Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

--
"Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx> wrote in message
news:e3Fhr%23XzGHA.2076@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Download my AdFind (<http://www.joeware.net/win/free/tools/adfind.htm>)

Then run the following command

```
adfind -sc u:username pwdlastset -tdcs
```

That will give you the exact time the password was set. Add the number of days for your expiration policy onto it and that is your exact expiration time. Note that it isn't just a day, it could be any time during the day.

AdFind isn't a script and deals with the 64 bit numbers natively and uses the Microsoft internal conversion routines so it will give you the exact time in the pwdLastSet (as well as any other int8 time attributes).

joe

--
Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition

Re: AD and Expired Password Checking and how to test?

www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

ohaya wrote:

Joe,

Actually, no, I'm not positive about the "real" expiration date/time. As I mentioned earlier, a number of VBs show 10/13/06, and at least one shows 10/11/06. But then again, I've tested after setting the system time to 10/10/06, and got the Invalid Credentials then too.

I guess that's really the point/question... how to find the "real" expiration date/time, since AD doesn't have it stored anywhere :(...

Jim

Joe Richards [MVP] wrote:

Are you positive on the date/time the account is supposed to be expiring. VBSCRIPT has issues dealing with 64 bit values and most of the scripts I have seen are *close* for the time but never actually correct.

--

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

ohaya wrote:

ohaya wrote:

Re: AD and Expired Password Checking and how to test?

Hi,

I have a sample VBScript program to check if a user's password has expired linked here:

<http://www.rlmueller.net/User%20Password%20Info.htm>

The program uses the value of the pwdLastSet attribute of the user and the maxPwdAge attribute of the domain. I have more info on handling Integer8 values like pwdLastSet and maxPwdAge linked here:

<http://www.rlmueller.net/Integer8Attributes.htm>

Richard,

I guess the thing that is really giving me a hard time is getting my code to detect that a password has expired when Windows thinks that it has expired.

Re: AD and Expired Password Checking and how to test?

I'll try to explain:

– I reset the password for a user, and the password expires on 10/13/06 @ ~03:55, according to various VBscripts that I tried (one said 10/11/06).

– I change the system date to 10/10/06, and try a bind, which fails. My program says that the password has not yet expired.

I guess that I've been assuming that bind failure is because Windows/AD thinks that the password has expired, but maybe there might be another reason why the binds would fail as I get "nearer" to the password expiration? FYI, when I ran an ldifde with a simple bind, the error I was getting was "INVALID CREDENTIALS".

I'm doing the bind using LDAP (i.e., using LDAP JDK). Is it possible that AD expires passwords for LDAP binds EARLIER than it expires something like an SSPI or Windows bind?

Jim

Hi,

I need to clarify what I said above: Actually, I am getting the "invalid credentials" prior to the password

Re: AD and Expired Password Checking and how to test?

expire date/time, even if
I do an SSPI bind. Is there any way to find
out why this might be
happening?

Thanks,
Jim