

RE: Finding Domain Service Running Every 12 Hours

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2008-10/msg00049.html>

- *From:* Smurfman <smurfman@xxxxxxxxxxxxxxxx>
 - *Date:* Wed, 1 Oct 2008 11:32:08 -0700
-

Thank you David.

The Audit Policy was already in effect, we use a network log collection tool to analyze and collect event logs and so forth, so we already had this turned on.

I ran the LockoutStatus tool, and from my PC I could only get results for the one DC not the other, which was weird – so I installed the tool on the DC in question and ran it again. The result is that I can see both DC's. SERVER #1 shows a Last Bad Pwd of 10/01/2008 12:06:02 PM (so today) and the other DC SERVER #2 shows Last Bad Pwd of 06/23/2008 01:25:08 PM (so it appears that it is unrelated to my second DC). Both show no Bad Pwd Counts, and both show Not Locked – which is what I would expect for a Domain Admin account.

To make sure the two were still talking properly for Active Directory, I decided to reset the Domain Admin account password to be the same of course, and the password change timestamp was exactly the same on the LockOut Status tool.

Regarding Step 5 – There are no passwords cached on the server in question. Using the command you gave me.

STEP 6 – I downloaded and ran the Aloinfo command and looked at the file it created, I searched for the user account, and there no matches

Please advise. My log analysis tool shows me everything that is taking place at the time the account reports locked out, including processes and object access and so forth, perhaps if you give me an email I could privately send you the log to see what you think? I have it in pdf and crystal format.

Thanks
J

"David Shen [MSFT]" wrote:

RE: Finding Domain Service Running Every 12 Hours

Hello customer,

Thanks for posting here.

According to the description, you want to find out a way to record the domain admin account logon event to investigate on the account lockout event at the specific time 12:06 am and 12:06 pm. If I have any misunderstanding, please feel free to let me know.

Analysis and Suggestion:

=====
Based on the research, we can enable the Audit Policy settings in the Default Domain policy on the domain level to record the account logon events.

Steps:

1. To enable the Auditing policy settings, in the Group Policy MMC, double-click Computer Configuration, double-click Windows Settings, double-click Security Settings, double-click Local Policies, double-click Audit Policy, and then double-click Audit account logon events, check the "Define these policy settings", Select "Success" and "Failure".
2. Run "gpupdate /force" to make the policy take into effect.
3. After we set the Auditing policy, please wait until account lockouts occur. When the account lockout occurs, we can retrieve both the Security event log and the System event log for all of the computers that are involved with the account lockout. This includes the PDC emulator operations master, the authenticating domain controller, and all of the client computers that have user sessions for the locked-out user.
4. To determine the domain controllers that are involved with the lockout, we can run the LockoutStatus.exe. By using this tool, you can gather and displays information about the specified user account including the domain admin's account from all the domain controllers in the domain. In addition, the tool displays the user's badPwdCount value on each domain controller. The domain controllers that have a badPwdCount value that reflects the bad password threshold setting for the domain are the domain controllers that are involved in the lockout. These domain controllers always include the PDC emulator operations master.

Download Account Lockout Status (LockoutStatus.exe)

<http://www.microsoft.com/downloads/details.aspx?FamilyID=d1a5ed1d-cd55-4829-a189-99515b0e90f7&DisplayLang=en>

5. Once we confirm the problematic computer, we can perform further research to locate the root cause. Actually, there are many possible causes for bad password, such as cached password, schedule task, mapped drives, services, etc. Please remove the previous password cache which may be used

RE: Finding Domain Service Running Every 12 Hours

by some applications and therefore cause the account lockout problem.

Troubleshooting steps:

- 1) Click Start, click Run, type "control userpasswords2" (without the quotation marks), and then click OK.
 - 2) Click the Advanced tab.
 - 3) Click the "Manage Password" button.
 - 4) Check to see if these domain account's passwords are cached. If so, remove them.
 - 5) Check if the problem has been resolved now.
6. Also besides checking services, we also need check scheduled task, mapped drivers running with the credentials of the problematic user account:

Please download the Account Lockout and Management Tools:

Account Lockout and Management Tools

<http://www.microsoft.com/downloads/details.aspx?familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e&displaylang=en>

Please Note: Aloinfo.exe included in the above package helps display all local services and the account used to start them.

Please logon the problematic client computer as the Local Administrator and run the following command:

```
Aloinfo.exe /stored >C:\CachedAcc.txt
```

Then check the C:\CachedAcc.txt file. If there is any application or service is running as the problematic user account, please disable it and then check whether the problem occurs.

For more information, please refer to the following link:

Troubleshooting Account Lockout

<http://technet.microsoft.com/en-us/library/cc773155.aspx>

Hope the information can be helpful.

David Shen

Microsoft Online Partner Support