DON'T REJOIN TO FIX: The trust relationship between this workstation and the primary domain failed

Apr 13, 2012

If you Google "the trust relationship between this workstation and the primary domain failed", you get plenty of information from support blogs and Microsoft articles; however, most of them ask you to rejoin your machine to the domain. That's not always possible.

##TL;DR You got this error and you can't simply unjoin and rejoin because the machine is a Certificate Authority. Run this command from PowerShell:

```
Reset-ComputerMachinePassword [-Credential ] [-Server ]
```

##What's the problem and how did I get here?

The underlying problem when you see this error is that the machine you are trying to access can no longer communicate securely with the Active Directory domain to which it is joined. The machine's private secret is not set to the same value store in the domain controller. You can think of this secret as a password but really it's some bits of cryptographic data called a Kerberos keytab stored in the local security authority. When you try to access this machine using a domain account, it fails to verify the Kerberos ticket you receive from Active Directory against the private secret that it stores locally. I think you can also come across this error if for some reason the system time on the machine is out of sync with the system time on the domain controller. This solution also fixes that problem.

##The standard fix This problem can be caused by various circumstances, but I most commonly run into it when I reset a virtual machine to a system snapshot that I made months or even years before. When the machine is reset, it is missing all of the automatic password changes that it executed against the domain controller during the intervening months. The password changes are required to maintain the security integrity of the domain.

Support blogs and Microsoft will generally tell you to rejoin the domain to restore the trust relationship. Another option they will give is to delete the computer object and recreate it without a password and rejoin.

Microsoft support article on the topic: http://support.microsoft.com/kb/162797 (http://support.microsoft.com/kb/162797)

I'm not a fan of any of these options. This seems heavy handed and sometimes they aren't even possible.

Recently, when I ran into this problem, the virtual machine that reset was an enterprise certificate authority joined to my test domain. Well, guess what, Microsoft will not allow you to rename or unjoin a computer that is a certificate authority—the button in the computer property page is greyed out. There may be another way to unjoin but I wasn't going to waste time on it when it isn't even necessary.

##UPDATE: An even better fix (IMO) **Just change your computer password using the Reset-**

ComputerMachinePassword cmdlet from Powershell v3!


```
Reset-ComputerMachinePassword [-Credential <PSCredential>] [-Server <String>]
```

I haven't looked at this problem for a while, but it seems to come up very often and there has been a lot of positive response. I wanted to point out an improvement (a more up-to-date method) that came from Lord_Arokh. Powershell v3 shipped with a cmdlet for resetting computer passwords. For those with Powershell skills, this is a much better option. Powershell v3 ships with the latest version of Windows and can be downloaded from Microsoft:

http://www.microsoft.com/en-us/download/details.aspx?id=34595 (http://www.microsoft.com/en-us/download/details.aspx?id=34595)

I noticed that on my Windows 8 install, I only received partial help when I issued the Get-Help Reset-ComputerMachinePassword command. You can fix this by opening Powershell with administrative rights and running Update-Help.

You can use the Get-Credential cmdlet for a secure way to generate a PSCredential, which can be stored in a variable and used in a script. You will want to generate a credential for an Active Directory user with sufficient rights to change the computer's password. The Server parameter is the domain controller to use when setting the machine account password.

Good Luck! Thanks for the update Lord_Arokh.

##A better fix

Just change your computer password using netdom.exe!

```
netdom.exe resetpwd /s:<server> /ud:<user> /pd:*

<server> = a domain controller in the joined domain

<user> = DOMAIN\User format with rights to change the computer password
```

Here are the full steps:

1. You need to be able to get onto the machine. I normally just log in with the local Administrator account by typing, ".\Administrator" in the logon window. I hope you remember the password. If you're creative and resourceful you can hack your way in without the password. Another option is to unplug the machine from the network and log in with domain user. You will be able to do disconnected authentication, but in the case of a reset machine, remember that you may have to use an old password. Your domain user's cached credential has the same problem as the machine's private secret.
2. You need to make sure you have netdom.exe. Where you get netdom.exe depends on what version of Windows you're running. Windows Server 2008 and Windows Server 2008 R2 ship with netdom.exe you just have to enable the Active Directory Domain Services role. On Windows Vista and Windows 7 you can get it from the Remote Server Administration Tools (RSAT). Google can help you get them. For other platforms see this link: http://technet.microsoft.com/en-us/library/ee649281(WS.10).aspx (http://technet.microsoft.com/en-us/library/ee649281(WS.10).aspx)
3. Extra steps if the machine is a domain controller. If the broken machine is a domain controller it is a little bit more complicated, but still possible to fix the problem. I haven't done this for a while, but I think this works:
    1. Turn off the Kerberos Key Distribution Center service. You can do this in the Services MMC

snap-in. Set the startup type to Manual. Reboot.
2. Remove the Kerberos ticket cache. A reboot will do this for you, or you can remove them using KerbTray.exe. You can get that tool here: http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&pid=17657 (http://www.microsoft.com/downloads/en/details.aspx?displaylang=en&id=17657)
3. Post change steps. Do these in conjunction with 5 below:
    - Turn the Kerberos Key Distribution Center Service back on before rebooting.
    - You should reboot the domain controller and then force replication in the Active Directory Sites and Services MMC snap-in.
4. Run netdom.exe to change the password. Open an administrative command prompt. On Windows platforms with UAC enabled, you will need to right-click on cmd.exe and select "run as Administrator". Type the following command: `netdom.exe resetpwd /s:<server> /ud:<user> /pd:*`
5. Reboot the machine.

Here is more information on netdom.exe: http://support.microsoft.com/kb/325850 (http://support.microsoft.com/kb/325850)

I hope this is helpful. This problem comes up every few months for me, so I wanted to document it for my own use. It is difficult to find when you just search for the error you get in the login window.