Repairing Broken Trust Relationship Between Workstation and AD Domain

https://woshub.com/repair-trust-relationship-workstation-with-ad-domain/

In this article we'll show how to fix a broken trust relationship between a workstation and an Active Directory domain when a user cannot logon to their domain computer. Let's consider the root cause of the problem and easy way to repair trust between a computer and a domain controller over a secure channel without rebooting the computer and domain rejoining.

Contents:

The Trust Relationship Between This Workstation and the Primary

Domain Failed.

The problem manifests itself when a user tries to logon to the workstation or member server using domain credentials and the following error occurs after entering the password:

```
The trust relationship between this workstation and the primary domain failed.
```

windows 10 domain user logon error: The trust relationship between this workstation and the primar

The error may also look like this:

```
The security database on the server does not have a computer account for this workstation trust relationship.
```

The security database on the server does not have a computer account for this workstation trust rel

Machine (Computer) Account Password in the Active Directory Domain

When a computer is joined to an Active Directory domain, a separate computer account is created for it. Like users, each computer has its password to authenticate the computer in the domain and establish a trusted connection with the domain controller. However, unlike user passwords, computer passwords are set and changed automatically.

Here are some important things about computer account passwords in AD:

- Computer passwords in AD must be changed regularly (once in 30 days by default).
  Tip. You can configure the maximum computer password age using the **Domain member: Maximum machine account password age** policy located under Computer Configuration-> Windows Settings-> Security Settings-> Local Policies-> Security Options. A computer password lifetime may last from 0 to 999 days (30 days by default);
  group policy parameter - Domain member: Maximum machine account password age
- Unlike user passwords, a computer password cannot expire. The password change is initiated by the computer, not the domain controller. A computer password is not subject to the domain password policy;

Even if a computer has been turned off for 30 days or more, you can turn it on, and it will be authenticated on your DC with its old password. Then the local **Netlogon** service will change the computer password in its local database (the password is stored in the registry `HKLM\SECURITY\Policy\Secrets\$machine.ACC`) and then it will update the computer account password in Active Directory.

- A computer password is change on the nearest DC, the changes are not sent to the domain controller with the PDC emulator FSMO role (i. e., if a computer has changed its password on one DC, it won't be able to authenticate on another DC till AD changes are replicated).

If the hash of the password that the computer sends to the domain controller doesn't match the computer account password in AD database, the computer cannot establish a secure connection with the DC and returns trusted connection errors.

Why the problem occurs:

1. A computer has been restored from an old restore point or a snapshot (in case of a virtual machine) created earlier than the computer password was changed in AD. If you roll the computer back to its previous state, it will try to authenticate on the DC using its old password. It is the most typical issue;
2. A computer with the same name has been created in AD, or somebody has reset the computer account in the domain using the ADUC console (`dsa.msc`);

3. The computer account in the domain has been disabled by the administrator (for example, during a regular procedure of disabling inactive AD objects);
4. Quite a rare case when the system time on a computer is wrong.

Here is the classical way to repair trust relationship between the computer and domain:

1. Reset the computer account in AD;
2. Move the computer from the domain to a workgroup under the local administrator;
3. Reboot;
4. Rejoin the computer to the domain;
5. Restart the computer again

The method seems simple, but it is too clumsy, requires at least two restarts of the computer and takes 10-30 minutes. Also you may face problems with using old local user profiles.

There is a smarter way to repair trust relationship using PowerShell without rejoining the domain or restarting the computer.

Check and Restore the Trust Relationship Between Computer and Domain Using PowerShell

If you cannot authenticate on a computer under a domain account and the following error appears: *The trust relationship between this workstation and the primary domain failed*, you need to logon to the computer using your local administrator account. You can also unplug the network cable and authenticate on the computer with the domain account logged on to the computer recently using Cached Credentials.

Open the elevated PowerShell console and using **Test-ComputerSecureChannel** cmdlet make sure if the local computer password matches the password stored in AD.

```
Test-ComputerSecureChannel –verbose
```

Image not found or type unknown
Test-ComputerSecureChannel -The Secure channel between the local computer and the domain is b

If the passwords do not match and the computer cannot establish trust relationship with the domain, the command will return **False** – `The Secure channel between the local computer and the domain woshub.com is broken`.

To force reset the computer account password in AD, run this command:

```
Test-ComputerSecureChannel –Repair –Credential (Get-Credential)
```

Image not found or type unknown
Repair the domain trust relationship with Test-ComputerSecureChannel PowerShell cmdlet

To reset a password, enter the credentials of a user account having the privilege to reset a computer account password. The user must be delegated the permissions to manage computers in Active Directory (you may also use a Domain Admins group member).

Then run Test-ComputerSecureChannel again to make sure it returns **True** (`The Secure channel between the local computer and the domain woshub.com is in good condition`).

So the computer password has been reset without a restart or manual domain rejoin. Now you can logon to the computer using your domain account.

Also to force reset a password, you may use the **Reset-ComputerMachinePassword** cmdlet.

```
Reset-ComputerMachinePassword -Server mun-dc01.woshub.com -Credential woshub\adm_user1
```

`mun-dc01.woshub.com` is the name of the closest DC to change the computer password on.

It is worth to reset a computer password each time before creating a virtual machine snapshot or a computer restore point. It will be easier for you to roll back to the previous computer state.

If you have a development or test environment, where you often have to recover a previous VM state from a snapshot, you may want to disable password change in the domain for these computers using GPO. To do it, set the **Domain member: Disable machine account password changes** policy located in Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options. You can target the policy to the OU with test computers or use GPO WMI filters.

Using the Get-ADComputer cmdlet (from the Active Directory module for Windows PowerShell), you can check the date of the last computer password change in AD:

```
Get-ADComputer –Identity mun-wks5431 -Properties PasswordLastSet
```

The Test-ComputerSecureChannel and Reset-ComputerMachinePassword cmdlets are available starting from version PowerShell 3.0. You will have to update PowerShell version in Windows 7/Windows Server 2008 R2.
You can also check if there is a secure channel between a computer and a DC using this command:

```
nltest /sc_verify:woshub.com
```

The following lines confirm that trust has been successfully repaired:

nltest /sc_check Trusted DC Connection Status

Image not found or type unknown

```
Trusted DC Connection Status = 0 0x0 NERR_Success
Trust Verification Status = 0 0x0 NERR_Success
```

Repair the Domain Trust Using Netdom

In Windows 7/2008R2 and in previous Windows versions without PowerShell 3.0, you cannot use Test-ComputerSecureChannel and Reset-ComputerMachinePassword cmdlets to reset a computer password and repair trust relationship with the domain. In this case, use the `netdom.exe` tools to restore a secure channel with the domain controller.

Netdom is included in Windows Server 2008 or newer, and can be installed on users' computers from RSAT (Remote Server Administration Tools). To repair trust relationship, log on under local administrator credentials (by typing *.\Administrator* on the logon screen) and run the following command:

```
Netdom resetpwd /Server:DomainController /UserD:Administrator /PasswordD:Password
```

The machine account password for the local machine has successfully reset.


```
The machine account password for the local machine has successfully reset.
```

- **Server** is the name of any available domain controller
- **UserD** is the name of the user with the domain administrator permissions or having delegated privileges on the OU containing the computer account
- **PasswordD** user password

```
Netdom resetpwd /Server:mun-dc01 /UserD:jsmith /PasswordD:Pra$$w0rd
```

After running the command, you do not need to reboot the computer: just log off and log on again using your domain account.

As you can see, it is quite easy to repair trust between a computer and a domain.

Revision #1
Created 5 January 2024 05:03:29 by ColtM
Updated 7 August 2024 23:24:39 by ColtM