Working with the Domain Controller Diagnostic Utility - Part 1

In this article we will introduce you to the Domain Controller error diagnosis utility, how to use them to fix problems with Active Directory.

Brien M. Posey

In this article we will introduce you to the Domain Controller error diagnosis utility, how to use them to fix problems with Active Directory.

Domain controllers - Domain Controllers - are the backbone for any Windows-based network. Therefore, if your domain controllers do not work, the Active Directory will not work either. If Active Directory does not work, users cannot log on, group policies are not enforced and all other features are not available. Fortunately, Windows comes with a tool that you can use to keep your domain controllers running smoothly. This tool is called the Domain Controller Diagnostic Tool. In this article, we will show you how to use this tool to perform some basic maintenance and diagnostic actions on domain controllers.

Before start

The Domain Controller Diagnostic Tool is now part of Windows. For the purposes of this article, we will only work with this version of the utility that is included with Windows Server 2008. Most, but not all, of the features we will talk about are available in Windows. Server 2003 SP1. DCDIAG already exists before Windows Server 2003 SP1, but many of the commands used today have been introduced in this Windows Server 2003 SP1 version.

You can access the Domain Controller diagnostic tool by running the DCDIAG command from the Windows command prompt.

Run the Domain Controller Diagnostic Tool

If you want to keep things simple, run this tool by entering the DCDIAG command in the Windows command prompt. By doing so, the utility will perform a series of checks against the Domain Controller that you are connected to. You can see an example of what is tested in Figure A below.

Figure A: The Domain Controller Diagnostic Tool runs a number of tests against the Domain Controller.

By entering the DCDIAG command, it is indeed very simple, but there is really no article that specifically introduces these commands. There are also many things you can do with this tool. Before you can appreciate all the features of this tool, you need to be friendly with the optional parameters to use in conjunction with the DCDIAG command. If you look at Figure B, you can see that the syntax of the DCDIAG command is too long. Like most commands are complicated, the syntax of this command is not as bad as it originally appeared. When you understand how this command works, its use becomes much simpler.

Figure B: The DCDIAG command syntax is very long

Interrupt between command syntax

As you can see in the picture above, the basic syntax of the DCDIAG command will be as follows:

dcdiag.exe / s: [:] [/ u:
*/ p: * || ""]*
[/ hqv] [/ n:] [/ f:] [/x:XMLLog.xml]
[/ skip:] [/ test:]

Although the screen capture shown in Figure B lists what a switch does, but still needs a better explanation of them. Here are some details about these switches.

/HOUR

If you run the DCDIAG command with the / H parameter, it will display the syntax of this command as shown in Figure B. If you look at the image above, you will see that you can also use the /? to display the syntax of the command.

/S

The / S parameter allows you to specify a server (this server is home server). In essence, this means that you can use this parameter to specify the name of the Domain Controller that you want to run the DCDIAG command with. However, when we ran the DCDIAG command in Figure A, we did not specify the home server. If you do not specify a home server, then the DCDIAG command will automatically select a server.

There are some examples of problems that the specified home server will be ignored. DCPROMO and the Register In DNS tests are run internally instead of running on a domain controller. Therefore, if you want to specify a home server for these tests, it will be ignored. We will talk more about this in the next sections.

/ N

The / N parameter allows you to specify a domain context. In case you are not familiar with the term, it is important to know that every domain is represented by a domain context. Domain context stores objects for domains, objects such as users, computers, groups, etc. You do not need to specify a domain context, but if you choose to use a context, you can enter it as NetBIOS, DNS, or distinguished domain name form.

/ U

Unless you are logged in as an administrator of the test domain, you will have to use the DCDIAG command with some administrative standards. The administrative standards here are typically the username and password. The / U switch is used to specify the username. Since you are entering the account name with domain administrator permissions, you will have to enter the username in domainusername format.

/ P

Another switch used when entering a set of standards is the / P switch. Following this switch will be a password of the account you specified through the / U switch.

/ A

Active Directory is often grouped into sites. A typical site will represent a collection of domain controllers that can reliably and quickly connect between them. For example, if an organization has two different sites connected together by a WAN link, each of these sites will be configured to act as a separate site because the computers within them are all located on a LAN, however there is no LAN connection between these sites.

If your organization is divided into sites, you will feel useful with this switch. Use this command to instruct DCDIAG to check all domain controllers in the current site.

/ E

The / E switch is the same as the / E, external switch instead of instructing DCDIAG to check all domain controllers in the current site, instructing DCDIAG to check the domain controller in its entirety. enterprise.

/ Q

As you can see, the output of the DCDIAG command is quite long. Therefore, it is very easy to lose error messages in such a long output screen. If that happens to you, you can use the / Q switch to run DCDIAG in 'Quiet' mode, the mode will only list error messages.

/ V

The / V switch is a type of switch against the / Q switch. While the / Q switch reduces the size of the output, this switch increases the output size again. That way you can get more detailed information about the problem you are trying to fix.

/ I

Sometimes DCDIAG will generate meaningless error messages that are confusing for less experienced administrators. If that happens to you, you can use the / I switch to instruct DCDIAG to ignore unimportant error messages.

Conclude

In this article, I have discussed some of the basic commands used by the Domain Controller Diagnostic Tool. In Part 2 of this series, I will continue the discussion by showing you how to use other switches and how to specify specific tests that you might want to perform.