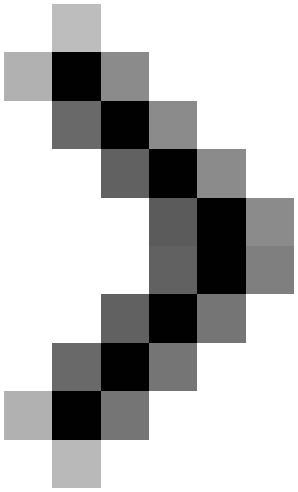
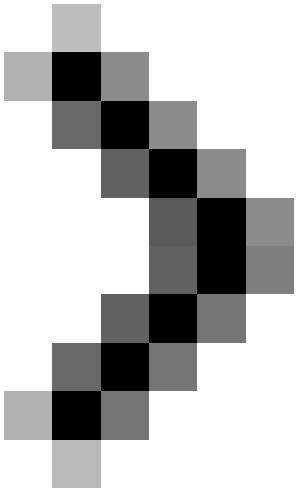
Working with the Domain Controller Diagnostic Utility - Part 5

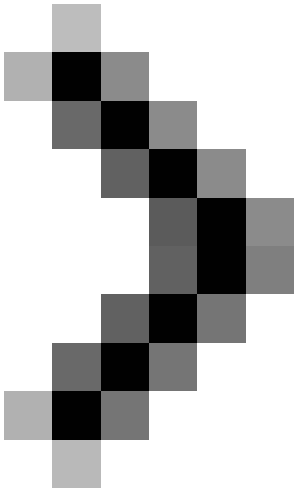
In this article, I will show you some of the tests that you can perform with the Domain Controller Diagnostic Utility.



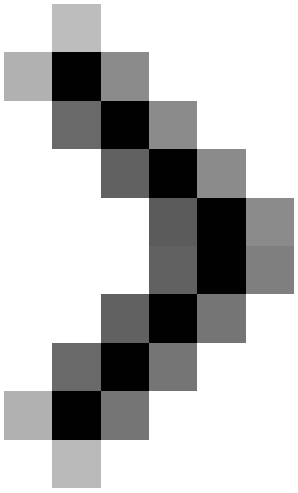
Working with the Domain Controller Diagnostic Utility - Part 1



Working with the Domain Controller Diagnostic Utility - Part 2



Working with the Domain Controller Diagnostic Utility - Part 3



Working with the Domain Controller Diagnostic Utility - Part 4

Brien M. Posey

In this next article, I will show you some tests that you can perform with the Domain Controller Diagnostic Utility.

Introduce

In the previous article of this series, I have discussed some of the tests that you can perform using the Domain Controller Diagnostic Utility. Although until now, we have introduced quite a few tests, but there are many types that you can do. And in this section, we will select one of these types of examples and introduce them so that you can perform the Domain Controller Diagnostic Utility.

Locator Check

Locator Check is one of the important tests that you can perform with DCDIAG. You probably know, the Active Directory assigns different Flexible Single Master Operations roles (FSMOs) to certain domain controllers within the forest. The global FSMO roles are initially assigned to the first domain controller in the forest. However, there are also several domain-level FSMO roles that are assigned by default to the first domain controller in each domain.

The Locator Check will perform a test to ensure that the servers that are hosting the global FSMO roles are known and can be located. More importantly, it checks to ensure that servers that hold global FSMO roles are responding to requests.

The implementation of this test is relatively simple. All you need to do is enter the following command:

```
DCDIAG / TEST: LocatorCheck
```

Obviously, this is the simplest example of how you will run the test locator check. In addition, you still have other options such as specifying certain domain controllers and setting authentication standards as you would with other tests.

Intersite Test

Depending on the Active Directory topology, Intersite is also an important test. When you run this test, the Domain Controller Diagnostic Utility will perform a series of test actions to see if there are any problems with the bridges that may cause the Active Directory information to be replicated across the boundaries of site or not.

The syntax used to run this test is similar to the syntax used for locator check. If you want to do this, just enter the following command:

DCDIAG / Test: Intersite

KCCEvent

Another copy-related test is KCCEvent. This test is used to ensure that the Knowledge Consistency Checker (KCC) is working, and whether it is performing the task without causing any errors. You can run KCCEvent by entering the following command:

DCDIAG / Test: KCCEvent

KnowsofRoleHolders

Knows of Role Holders are tests to check if the Directory Service Agent knows which servers are hosting the Flexible Single Operations Master roles. If you just want to run it simply, you can do so by entering the following command:

DCDIAG / Test: KnowsOfRoleHolders

Although this test will usually do a pretty good job, sometimes you may want to check which domain controller the Directory Service Agent thinks holds the roles. If you want to identify separate servers, you need to run this test in detailed mode. To do so, enter the following command:

DCDIAG / Test: KnowsofRoleHolders / v

Machine Account

In an Active Directory environment, servers and workstations are joined to a domain. The process of joining a machine to one domain needs to create one account for each machine. Like a user account, the machine account also has a corresponding password and a number of other attributes designed to distinguish the machines from each other. If the machine account fails or fails to synchronize with Active Directory, the machine corresponding to that account will not be able to connect to the domain. However, there is a test that allows you to check the integrity of the machine account. You can do this test by entering the command below:

DCDIAG / Test: MachineAccount

During the process of working with Active Directory, there may be some situations where the account password is not synchronized with the password of the machine account stored in the Active Directory database.

If the machine account has such a problem, there are several switches that can help you fix that problem. One such switch is / FixMachineAccount, which will reset the flag for the accounts. If you do not fix the problem, you may need to recreate the machine account using the / RecreateMachineAccount switch.

Naming Context Security Descriptors

One of the confusing tests to mention here is to check if the security identifiers on the naming contexts work properly. If the security identifiers are invalid, the replication may fail. You can run this test by entering the

command below:

DCDIAG / Test: NCSecDesc

NetLogons

A similar test related to that copy is NetLogons. This test checks to see if the copy failed because of a lack of login privileges. You can run this test by entering the command below:

DCDIAG / Test: NetLogons

Objects Replicated

The Object Replicated test is another important test. This test is used primarily to confirm that the computer accounts have been copied on all of your domain controllers, but it is also used to check if other types of objects are also copied. .

To use this test, you will have to know the unique name (DN) of the object you want to test. If the object you want to test is not a machine account, you need to know the object's naming context. The syntax for this test is as follows:

DCDiag / Test: ObjectsReplicated / ObjectDN: / N:

Outbound Secure Channels

When machines store user passwords and other security settings, the Domain Controller is one of the most sensitive servers on the network. Therefore, Microsoft configured the domain controllers to communicate with each other on a secure channel whenever possible. This helps to prevent other people from using sniff attacks to steal Active Directory information when it creates a copy from one Domain Controller to another.

By definition, a secure channel is an authenticated RPC (remote procedure call) connection between two machines in a domain with a security context set to use for signing and encrypting RPC packets.

Therefore, it is not surprising that the Domain Controller Diagnostic Utility provides a test for checking outbound secure channels. This is one of the tests that is not run by default, so you need to run it yourself if you want to use it. The syntax of the command is as follows:

DCDIAG / Test: OutboundSecureChannels / TestDomain:

Typically, this test only checks Domain Controllers within the current site. However, you can also test external sites by adding the / NoRestriction switch.

Conclude

In this article, I have shown you some more tests that can be performed with your domain controller using the Domain Controller Diagnostic Utility. Believe it or not, do it to know its results. Because there are still some more tests, in the next part of this article series, I will continue the discussion on the remaining tests.