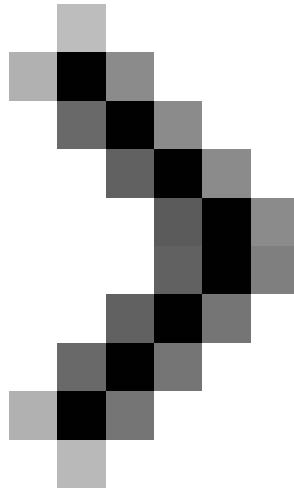


Working with the Domain Controller Diagnostic Utility - Part 3

In this article, I will continue the discussion by showing you how to work with the Domain Controller Diagnostic Utility by examining some tests.



Working with the Domain Controller Diagnostic Utility - Part 1



Working with the Domain Controller Diagnostic Utility - Part 2

Brien M. Posey

In this article, I will continue the discussion by showing you how to work with the Domain Controller Diagnostic Utility by examining some tests.

Now that you know that the Domain Controller Diagnostic Utility has many problems you can use to configure the utility to run in the most appropriate way for each of your own situations. We have already introduced you to the switches, and now go back to the individual tests that the utility is capable of performing.

Advertising - service promotion

The first test you can perform is advertising. This test performs a test to find out if the Directory System Agent is advertising itself. If the Directory System Agent is advertising itself, the test will ensure that the advertisement lists the domain controller with the capabilities of the Directory System Agent.

In case you are not familiar with the concept of the Directory System Agent, you need to understand that the Directory System Agent (commonly abbreviated as DSA) is a collection of services and processes that run on domain controllers. Its job is to provide access to the Active Directory database. DSA is a child component in the Local System Authority (LSA). The reason why it relates to such processes and services is because of its ability to provide multiple mechanisms for client access.

The best known of these mechanisms is the Light Weight Directory Access Protocol, or LDAP for short. LDAP is a protocol through which most recent Windows operating systems are used to query Active Directory. Older clients still require DSA access, but are typically done through Security Account Manager (SAM). This is

because there is no mechanism to access DSA. For example, Microsoft exchange communicates with DSA by MAPI calls. DSAs also communicate with another DSA using remote procedure calls.

CheckSDRefDom

This test will verify that all partitions contain the application directory with the security directive for the appropriate reference domains. This test will be meaningless for those who are not familiar with Active Directory. Therefore, we will take a moment to introduce what this test is.

You probably already know this, each object in the Active Directory includes a security directive. The job of the security indicator is to maintain a list of access control information. Usually, the security security indicator usually works well for maintaining a record of who has access and what components they access are components. However, the problem may appear here if an organization uses application directory partitions (formerly known as Active Directory Application Mode or ADAM). The reason for that is that the application directory partitions are independent domains. In fact, it is possible to create an application directory partition and then create replicas for other domain controllers in multiple domains. Because of this, Windows assigns a security indicator set with domain references to each application directory partition when created.

This reference domain notifies you of the application directory partition which domain name to use when a domain value needs to be entered inside a security directive. Windows has a lot of rules to distinguish which domain is used. Simplify, if you create a new application domain partition that is not the child of any partition and the reference domain of the security directive uses the forest root domain as the domain name to use within the security directive set. different secrets. If the application directory partition is a child of an object, it will assume the reference domain of its parent object security indicator.

CheckSecurityError

The next test that I want to show you is Check Security Error. Unlike the previous test that we introduced for you. Check Security Error does not work by default. If you want to run this test, you must specify it within the DCDIAG command.

When running this test, DCDIAG will find errors related to security issues, as well as possible related errors, then try to diagnose the problem. There is an optional parameter that you can use with this switch. The / ReplSource switch allows you to specify a specific domain controller to run the test. You can use any desired domain controller, regardless of its error state or whether it is an existing partner. Simply enter the name of the test (CheckSecurityError), and add the / ReplSource, colon and the name of the domain controller you want to test.

Connectivity

Connectivity is one of the most useful tests you can do with it. In fact, this test is so important that even DCDIAG does not allow you to ignore it. If you run a default instance of DCDIAG, the Connectivity will run completely automatically.

Connectivity will check if domain controllers are registered in DNS. It also checks to see if it can ping each domain controller and whether it can establish an LDAP and RDP connection.

CrossRefValidation

This is a test that you won't be able to see many documents about. What we can recommend to you is like informal references. If you encounter a reference validation error, the problem can be solved by using ADSI edit to remove the error-causing object.

We also want to point out that if you use ADSI edit incorrectly, you can destroy your Active Directory. Therefore, perform a full backup of the system state for domain controllers from before making any changes.

CutOffServers

Our final test is about Cut off Servers. The basic idea in this test is that in most cases, domain controllers have one or more replication partners. If the domain controller's replication partner is in trouble, the domain controller may not be able to update Active Directory updates and DCDIAG will report a Cut off Servers error.

One trick that can solve this problem is that you have to show what copy partners are domain controllers. The actual method varies greatly depending on the Windows version, but in Windows Server 2003, you can look up replication partners through the Active Directory Site and Services console.

When opening the tree view, open the Site section to display a list of sites in your Active Directory. Next, double-click the site that contains the domain controller you want to check. Next, open the Servers folder, then the folder corresponding to the name of the domain controller you are interested in. Finally, double click on NTDSSettings, and Windows will display the list of connected objects. This list displays replica partners in the From Server column.

Conclude

In this section, I have discussed some tests that run with the DCDIAG utility. In the next part of this series, I will continue the discussion by showing you some more tests.

You finished reading the article "**Working with the Domain Controller Diagnostic Utility - Part 3**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.