Knowledge Base

How Domain Controllers Are Located in Windows

PSS ID Number: 247811

Article Last Modified on 11/20/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Professional

This article was previously published under Q247811

SUMMARY

This article describes the mechanism used by Windows to locate a domain controller in a Windows-based domain. This article details the process of locating a domain by its DNS-style name and its flat-style (NetBIOS) name. The flat-style name is used for backward compatibility. In all other cases, DNS-style names should be used as a matter of policy. This article also addresses troubleshooting the domain controller location process.

MORE INFORMATION

This sequence describes how the Locator finds a domain controller:

- On the client (the computer that is locating the domain controller), the Locator is initiated as an remote procedure call (RPC) to the local Netlogon service. The Locator DsGetDcName application programming interface (API) call is implemented by the Netlogon service.
- The client collects the information that is needed to select a domain controller and passes the information to the Netlogon service by using the DsGetDcName call.
- The Netlogon service on the client uses the collected information to look up a domain controller for the specified domain in one of two ways:
  - For a DNS name, Netlogon queries DNS by using the IP/DNS-compatible Locator--that is, DsGetDcName calls the DnsQuery call to read the Service Resource (SRV) records and "A" records from DNS after it appends the domain name to the appropriate string that specifies the SRV records.
  - A workstation that is logging on to a Windows-based domain queries DNS for SRV records in the general form:

    _service._protocol.DnsDomainName

    Active Directory servers offer the Lightweight Directory Access Protocol (LDAP) service over the TCP protocol. Therefore, clients find an LDAP server by querying DNS for a record of the form:

    _ldap._tcp.DnsDomainName
  - For a NetBIOS name, Netlogon performs domain controller discovery by using the Microsoft Windows NT version 4.0-compatible Locator (that is, by using the transport-specific mechanism (for example, WINS).

    In Windows NT 4.0 and earlier, "discovery" is a process for locating a domain controller for authentication in either the primary domain or a trusted domain.
- The Netlogon service sends a datagram to the computers that registered the name. For NetBIOS domain names, the datagram is implemented as a mailslot message. For DNS domain names, the datagram is implemented as an LDAP User Datagram Protocol (UDP) search. (UDP is the connectionless datagram transport protocol that is part of the TCP/IP protocol suite. TCP is a connection-oriented transport protocol.)
- Each available domain controller responds to the datagram to indicate that it is currently operational and returns the information to DsGetDcName.

  Note that UDP allows a program on one computer to send a datagram to a program on another computer. UDP includes a protocol port number, which allows the sender to distinguish among multiple destinations (programs) on the remote computer.
- Each available domain controller responds to the datagram to indicate that it is currently operational and returns the information to DsGetDcName.
- The Netlogon service caches the domain controller information so that subsequent requests need not repeat the discovery process. Caching this information encourages consistent use of the same domain

controller and a consistent view of Active Directory.

When a client logs on or joins the network, it must be able to locate a domain controller. The client sends a DNS Lookup query to DNS to find domain controllers, preferably in the client's own subnet. Therefore, clients find a domain controller by querying DNS for a record of the form:

_LDAP._TCP.dc._msdcs.domainname

After the client locates a domain controller, it establishes communication by using LDAP to gain access to Active Directory. As part of that negotiation, the domain controller identifies which site the client is in based on the IP subnet of that client. If the client is communicating with a domain controller that is not in the closest (most optimal) site, the domain controller returns the name of the client's site. If the client has already tried to find domain controllers in that site (for example, when the client sends a DNS Lookup query to DNS to find domain controllers in the client's subnet), the client uses the domain controller that is not optimal. Otherwise, the client performs a site-specific DNS lookup again with the new optimal site name. The domain controller uses some of the directory service information for identifying sites and subnets.

After the client locates a domain controller, the domain controller entry is cached. If the domain controller is not in the optimal site, the client flushes the cache after fifteen minutes and discards the cache entry. It then attempts to find an optimal domain controller in the same site as the client.

After the client has established a communications path to the domain controller, it can establish the logon and authentication credentials and, if necessary for Windows-based computers, set up a secure channel. The client then is ready to perform normal queries and search for information against the directory.

The client establishes an LDAP connection to a domain controller to log on. The logon process uses Security Accounts Manager. Because the communications path uses the LDAP interface and the client is authenticated by a domain controller, the client account is verified and passed through Security Accounts Manager to the directory service agent, then to the database layer, and finally to the database in the Extensible Storage engine (ESE).

Troubleshooting the Domain Locator Process

To troubleshoot the domain locator process:

1. Check Event Viewer on both the client and the server. The event logs may contain error messages indicating that there is a problem. To view Event Viewer, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Event Viewer**. Check the System log on both the client and the server. Also, check the Directory Service logs on the server and DNS logs on the DNS server.
2. Check the IP configuration by using the **ipconfig /all** command at a command prompt.
3. Use the Ping utility to verify network connectivity and name resolution. Ping both the IP address and the server name. You may also want to ping the domain name.
4. Use the Netdiag tool to determine whether networking components are working correctly. To send detailed output to a text file, use the following command:

   ```
   netdiag /v >test.txt
   ```

   Review the log file, looking for problems, and investigate any implicated components. This file also contains other network configuration details.
5. To fix minor problems, use the Netdiag tool with the following syntax: **netdiag /fix**.
6. Use the **nltest /dsgetdc:*domainname*** command to verify that a domain controller can be located for a specific domain.
7. Use the NSLookup tool to verify that DNS entries are correctly registered in DNS. Verify that the server host records and GUID SRV records can be resolved.

   For example, to verify record registration, use the following commands:

   nslookup *servername*.*childofrootdomain*.*rootdomain*.com

   nslookup guid._msdcs.*rootdomain*.com
8. If either of these commands does not succeed, use one of the following methods to reregister records with DNS:
   - To force host record registration, type `ipconfig /registerdns`.
   - To force domain controller service registration, stop and start the Netlogon service.
9. To detect domain controller problems, run the DCdiag utility from a command prompt. The utility runs a number of tests to verify that a domain controller is running correctly. Use this command to send the results to a text file:

   ```
   dcdiag /v >dcdiag.txt
   ```
10. Use the Ldp.exe tool to connect and bind to the domain controller to verify appropriate LDAP connectivity.

11. If you suspect that a particular domain controller has problems, it may be helpful to turn on Netlogon debug logging. Use the NLTest utility by typing this command: **nltest /dbflag:0x2000ffff**. The information is then logged in the Debug folder in the Netlogon.log file.
12. If you still have not isolated the problem, use Network Monitor to monitor network traffic between the client and the domain controller.

For information about how to install Network Monitor, see the following article in the Microsoft Knowledge Base:

243270 How to Install Network Monitor in Windows 2000

REFERENCES

For additional information, see the Windows Resource Kit, Chapter 10, "Active Directory Diagnostic, Troubleshooting, and Recovery."

Additional query words: win2000hotds kbfaqw2kds

Keywords: kbDNS kbenv kbinfo kbnetwork KB247811
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Pro kbwin2000ProSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

---