Search

How Domain Controllers Are Located in Windows XP

This article was previously published under Q314861

For a Microsoft Windows 2000 version of this article, see 247811 (http://support.microsoft.com/kb/247811/EN-US/).

Article ID : 314861
Last Review : August 6, 2002
Revision : 1.0

On This Page

SUMMARY
MORE INFORMATION
Troubleshooting the Domain Locator Process

SUMMARY

This article describes the mechanism that Windows XP Professional uses to locate a domain controller in a Windows-based domain.

The article details the process of locating a domain by its DNS-style name and by its flat-style (NetBIOS) name, which is used for backward compatibility. In all other cases, it is recommended that you use DNS-style names as a matter of policy.

The article also addresses issues that are involved in troubleshooting the domain controller location process.

MORE INFORMATION

The following sequence describes how the Locator finds a domain controller:

- On the client (the computer that is trying to locate the domain controller), the Locator is initiated as a remote procedure call (RPC) to the local Netlogon service. The Netlogon service implements the Locator **DsGetDcName** API call.
- The client collects the information that is needed to select a domain controller, and then 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 the domain name is appended 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 this 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 4.0-compatible Locator--that is, by using the transport-specific mechanism, for example, Windows Internet Name Service (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 in 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. 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 working and returns the information to **DsGetDcName**.
- The Netlogon service caches the domain controller information so that subsequent requests do not need to 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, the client 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, the client establishes communication by using Lightweight Directory Access Protocol (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 own subnet), the client uses the domain controller that is not optimal. Otherwise, the client performs a site-specific DNS lookup again by using the name of the optimal site. 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 15 minutes and discards the cache entry. The client then attempts to find an optimal domain controller in its own site.

After the client has established a communications path to the domain controller, the client can establish its 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 (SAM). 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 SAM 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 to see whether the event logs contain any error information. On both the client and the server, check the System log for failures during the logon process. Also, check the Directory Service logs on the server and the DNS logs on the DNS server.

   To view Event Viewer in Windows XP, click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Event Viewer**.
2. Check the IP configuration by running the **ipconfig /all** command at a command prompt. Verify that the configuration is correct for your network.
3. Use the Ping utility to verify network connectivity and name resolution. Ping both the IP address and the server name.
4. Check the Network Diagnostics tool in Help and Support under "Use Tools to view your computer information and diagnose problems" to determine whether the network components are correctly installed and working properly. Network Diagnostics also runs some tests and provides information about the network configuration, information that can be helpful.
5. Use the **nltest /dsgetdc:*domainname*** command to verify that a domain controller can be located for a specific domain. The NLTest tool is installed with the Windows XP support tools.

   For information about how to install these tools, refer to the following article in the Microsoft Knowledge Base:

   306794 (http://support.microsoft.com/kb/306794/EN-US/) How to Install the Support Tools from the Windows XP CD-ROM
6. 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 *server_name.child_of_root_domain.root_domain*.com

   nslookup guid._msdcs.*root_domain*.com
7. 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 then restart the Netlogon service.
8. To verify appropriate LDAP connectivity, use the Ldp.exe tool to connect and bind to the domain controller. Ldp.exe is a support tool that you can install from the Windows XP CD-ROM.

   For information about how to install these tools, refer to the following article in the Microsoft Knowledge Base:

   306794 (http://support.microsoft.com/kb/306794/EN-US/) How to Install the Support Tools from the Windows XP CD-ROM
9. If you suspect that a particular domain controller has problems, turn on the Netlogon debug logging. Use the NLTest utility by typing **nltest /dbflag:0x2000ffff** at a command prompt. The information is logged in the Debug folder in the Netlogon.log file.

10. If you still have not isolated the problem, use Network Monitor to monitor network traffic between the client and the domain controller.

For additional information, refer to the Windows 2000 Server Resource Kit, Chapter 10, "Active Directory Diagnostic, Troubleshooting, and Recovery."

APPLIES TO

- Microsoft Windows XP Professional Edition

Keywords: kbinfo kbdns kbenv kbnetwork KB314861