Finding a Domain Controller in the Closest Site

Article • 07/18/2012 • 12 minutes to read

During a search for a domain controller, the Locator attempts to find a domain controller in the site closest to the client. When the domain that is being sought is a Windows 2000 domain, the domain controller uses the information stored in Active Directory to determine the closest site. When the domain being sought is a Windows NT 4.0 domain, domain controller discovery occurs when the client starts and uses the first domain controller that it finds.

As described in "SRV Records Registered by Net Logon" earlier in this chapter, each Windows 2000–based domain controller registers DNS records that indicate the site where the domain controller is located. The site name (the relative distinguished name of the site object in Active Directory) is registered in several records so that the various roles the domain controller might perform (for example, Global Catalog server or Kerberos server) can be associated with the domain controller's site. When DNS is used, the Locator searches first for a site-specific DNS record before it begins to search for a DNS record that is not site-specific (thereby preferentially locating a domain controller in that site).

A client computer stores its own site information in the registry, but the computer is not necessarily located physically in the site associated with its IP address. For example, a portable computer that was moved to a new location contacts a domain controller in its home site, which is not the site to which the computer is currently connected. In this situation, the domain controller looks up the client site on the basis of the client IP address by comparing the address to the sites that are identified in Active Directory, and returns the name of the site that is closest to the client. The client then updates the information in the registry.

The domain controller stores site information for the entire forest in the Configuration container. The domain controller uses the site information to check the IP address of the client computer against the list of subnets in the forest. In this way, the domain controller ascertains the name of the site in which the client is assumed to be located, or the site that is the closest match, and returns this information to the client.

Active Directory Site and Subnet Objects

A site is a collection of subnets that have high-speed connections. In Active Directory, a site is defined by a site object in the cn=Sites,cn=Configuration,dc= *ForestRootDomain* container. A subnet is an addressed segment within a site and is represented by an object in the cn=Subnets,cn=Sites,cn=Configuration,dc= *ForestRootDomain* container.

The site in which a domain controller is located is identified in the Configuration container by the domain controller object that is located within the cn=Servers container beneath the site object for a particular site. A domain controller can identify the site of a client by using the subnet object in the Sites container. Each subnet object has a *siteObject* property ("attribute#34;) that links it to a site object; the value of the *siteObject* property is the distinguished name of the site object. This link enables a domain controller to identify clients that have an IP address in the specified subnet as being in the specified site.

Subnet names in Active Directory take the form "network/bits masked" (for example, the subnet object 172.16.72.0/22 has a subnet of 172.16.72.0 and a 22-bit subnet mask. If this subnet had a *siteObject* property value that contained the distinguished name of the Seattle site object, all IP addresses in the 172.16.72.0/22 subnet would be considered to be in the Seattle site. The *siteObject* property is a single value, which implies that a single subnet maps to a single site. However, multiple subnet objects can be linked to the same site object. The directory administrator manually creates subnet objects and, hence, the *siteObje* c *t* property value.

The Configuration container (including all of the site and subnet objects in it) is replicated to all domain controllers in the forest. Therefore, any domain controller in the forest can identify the site in which a client is located, compare it to the site in which the domain controller is located, and indicate to the client whether that domain controller's site is the closest site to the client.

For more information about site and subnet objects, see "Active Directory Replication" in this book. For more information about networks, subnets, and subnet masks, see "Introduction to TCP/IP" in the *TCP/IP Core Networking Guide* .

Mapping IP Addresses to Site Names

During Net Logon startup, the Net Logon service on each domain controller enumerates the site objects in the Configuration container. Net Logon on each domain controller is

also notified of any changes made to the site objects. Net Logon uses the site information to build an in-memory structure that is used to map IP addresses to site names.

When a client that is searching for a domain controller receives the list of domain controller IP addresses from DNS, the client begins querying the domain controllers in turn to find out which domain controller is available and appropriate. Active Directory intercepts the query, which contains the IP address of the client, and passes it to Net Logon on the domain controller. Net Logon looks up the client IP address in its subnet-to-site mapping table by finding the subnet object that most closely matches the client IP address and then returns the following information:

- The name of the site in which the client is located, or the site that most closely matches the client IP address.
- The name of the site in which the current domain controller is located.
- A bit that indicates whether the found domain controller is located (bit is set) or not located (bit is not set) in the site closest to the client.

The domain controller returns the information to the client. The response also contains various other pieces of information that describe the domain controller. The client inspects the information to determine whether to try to find a better domain controller. The decision is made as follows:

- If the returned domain controller is in the closest site (the returned bit is set), the client uses this domain controller.
- If the client has already tried to find a domain controller in the site in which the domain controller claims the client is located, the client uses this domain controller.
- If the domain controller is not in the closest site, the client updates its site information and sends a new DNS query to find a new domain controller in the site. If the second query is successful, the new domain controller is used. If the second query fails, the original domain controller is used.

If the domain that is being queried by a computer is the same as the domain to which the computer is joined, the site in which the computer resides (as reported by a domain controller) is stored in the computer registry. The client stores this site name in the **DynamicSiteName** registry entry in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Netlogon\Parameters. Therefore, the DsGetSiteName API returns the site in which the computer is located.

Never change dynamically determined values. To override the dynamic site name, add the **SiteName** entry with the REG_SZ data type in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters. When a value is present for the **SiteName** entry, the **DynamicSiteName** entry is not used. For more information about **SiteName** and **DynamicSiteName** , see the *Microsoft Windows 2000 Resource Kit* Technical Reference to the Windows 2000 Registry (Regentry.chm).

Caution

Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. There are programs available in Control Panel or Microsoft Management Console (MMC) for performing most administrative tasks. These programs provide safeguards that prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Registry editors bypass the standard safeguards that are provided by these administrative tools. Modifying the registry is recommended only when no administrative tool is available. Before you make changes to the registry, it is recommended that you back up any valuable data on the computer. For instructions about how to edit registry entries, see Help for the registry editor that you are using. For more information about the registry, see the *Microsoft Windows 2000 Resource Kit* Technical Reference to the Windows 2000 Registry (Regentry.chm).

If the domain being located is the same as the domain to which the computer is joined and the computer has not physically moved to a different site since the last query, the dynamically determined site name in the registry is the actual site in which the computer is located. As such, the client finds a domain controller in the correct site without having to retry the operation. If the site name in the registry is not the current site of the computer (for example, if the computer is portable), the domain controller location process serves to update the site information in the registry.

Automatic Site Coverage

There is not necessarily a domain controller in every site. For various reasons, it is possible that no domain controller exists for a particular domain at the local site. By default, each domain controller checks all sites in the forest and then checks the replication cost matrix. A domain controller advertises itself (registers a site-related SRV record in DNS) in any site that does not have a domain controller for that domain and for which its site has the lowest-cost connections. This process ensures that every site has a domain controller that is defined by default for every domain in the forest, even if a site does not contain a

domain controller for that domain. The domain controllers that are published in DNS are those from the closest site (as defined by the replication topology.

For example, given one domain and three sites, a domain controller for that domain might be located in two of the sites, but there might be no domain controller for the domain in the third site. Replication to the domain that does not have a domain controller in the third site might be too expensive in terms of cost or replication latency. To ensure that a domain controller can be located in the site closest to a client computer, if not the same site, Windows 2000 automatically attempts to register a domain controller in every site. The algorithm that is used to accomplish automatic site coverage determines how one site can "cover" another site when no domain controller exists in the second site.

Determining Site Coverage on the Basis of Cost

Given one domain and sites A, B, and C, site A has no domain controllers for the domain. If a client in site A attempts to locate a domain controller, which domain controller should be returned? The answer depends on which site covers site A for the domain. Site coverage is determined according to site-link costs, and domain controllers register themselves in sites accordingly.

In the example, a site link exists between site A and both of the other sites — that is, the connections between domain controllers in site A, site B, and site C are configured for replication over site links in Active Directory Sites and Services. (For more information about site links and site-link costs, see "Active Directory Replication" in this book.) Costs are associated with site links based on the expense of transferring data over the connections. The administrator uses the speed of the connection between sites to assign a cost to the communication link, and replication uses the cost to establish the least expensive route for replication traffic.

Site A and site B are connected by site link AB. Site A and site C are connected by site link AC, with the following costs:

- Site link AB cost = 50.
- Site link AC cost = 100.

The link between site A and site C has a much higher cost than the link between site A and site C. The administrator configured this cost based on the expensive Integrated Services Digital Network (ISDN) line that connects site A and site C, and the administrator would prefer that resources in site B be used when possible. The site coverage algorithm ensures

that a domain controller in site B registers itself as a domain controller for site A. In this way, clients in Site A that are looking for a domain controller find one from site B, instead of possibly finding one from site C. For more information about site link cost, see "Active Directory Replication" in this book.

Site Coverage Algorithm

During registration of SRV records in DNS, the following algorithm is used to determine which domain controllers register site SRV records that designate them as preferred domain controllers in sites that do not have a specific domain represented.

For every domain controller in the forest, follow this procedure:

1. Build a list of *target sites* — sites that have no domain controllers for this domain (the domain of the current domain controller).
2. Build a list of *candidate sites* — sites that have domain controllers for this domain.
3. For every target site, follow these steps:
    a. Build a list of candidate sites of which this domain is a member. (If none, do nothing.)
    b. Of these, build a list of sites that have the lowest site link cost to the target site. (If none, do nothing.)
        - If more than one, break ties (reduce this list to one candidate site) by choosing the site with the largest number of domain controllers.
        - If more than one, break ties by choosing the site that is first alphabetically.
        - Register target-site-specific SRV records for the domain controllers for this domain in the selected site.

Cache Time-out and Closest Site

If a domain member computer requests a domain controller while all domain controllers in its site are offline, the Locator necessarily returns a domain controller in a different site. The location of this domain controller is stored in the client cache. The cache lifetime is controlled by the **CloseSiteTimeout** entry in the registry.

In addition, the domain controller performs authentication, and a secure channel is set up. On subsequent location attempts, the lifetime of the cache and the lifetime of the secure channel are secondary to the location of a domain controller in the closest site.

If the domain controller that is stored in the client cache is not in a site that is close to the client, Net Logon attempts to find a close domain controller when either of the following events occurs:

- An interactive logon process uses pass-through authentication on the secure channel.
- The value in the **CloseSiteTimeout** registry entry has elapsed since the last attempt, and any other attempt is made to use the secure channel (for example, pass-through authentication of network logons).

Thus, Net Logon attempts to find a close domain controller only on demand. The default value of the **CloseSiteTimeout** period is 15 minutes; the maximum value is 49 days, and the minimum value is 60 seconds. The implications of this setting are that if the time-out value is too large, a client never tries to find a close domain controller if there is not one available at startup. If the value of this setting is too small, secure channel traffic is unnecessarily slowed down by discovery attempts.

For more information about creating the **CloseSiteTimeout** entry, see the *Microsoft Windows 2000 Resource Kit* Technical Reference to the Windows 2000 Registry (Regentry.chm).

Clients with No Apparent Site

Sometimes the client pings a domain controller and the client IP address cannot be found in the subnet-to-site mapping table. In this case, the domain controller returns a NULL site name, and the client uses the returned domain controller.

For more information about locating sites, see "Active Directory Replication" in this book.