How DNS Support for Active Directory Works

In this section

Active Directory uses DNS as its domain controller location mechanism and leverages the namespace design of DNS in the design of Active Directory domain names. As a result, DNS is positioned within the discoverability and logical structure components of Active Directory technology components.

Typically, a Windows Server 2003 DNS namespace is deployed to mirror an Active Directory forest and domain infrastructure. In such a deployment, a partition of the DNS namespace is set aside for Active Directory, where a DNS domain name such as corp.contoso.com is used support the Active Directory forest root domain, and then subdomains of this name are created to suit additional Active Directory domains as needed.

Back to Top

DNS Support for Active Directory Architecture

Active Directory is dependent on DNS as a domain controller location mechanism and uses DNS domain naming conventions in the architecture of Active Directory domains. There are three components in the dependency of Active Directory on DNS:

- Domain controller locator (Locator)
- Active Directory domain names in DNS
- Active Directory DNS objects

DNS Support for Active Directory Components

Component	Description
Domain controller locator (Locator)	The Windows Server 2003 domain controller locator, implemented in the Net Logon service, enables a client to locate a domain controller. The component contains the DNS–compatible and the Windows NT 4.0–compatible locators that provide interoperability in a mixed Windows Server 2003– and Windows NT 4.0–based environment.
Active Directory domain names in DNS	Every Windows Server 2003 Active Directory domain has a DNS domain name (for example, contoso.com), and every Windows Server 2003–based computer has a DNS name (for example, win2kserver.contoso.com). Architecturally, domains and computers are represented both as objects in Active Directory and as nodes in DNS. Because DNS domains and Active Directory domains share identical domain names, it is easy to confuse their roles. The two namespaces, although typically sharing an identical domain structure, store different data and, therefore, manage different objects: • DNS stores zones and resource records, and Active Directory stores domains and domain objects. Both systems use a database to resolve names. • DNS resolves domain names and computer names to resource records through requests received by DNS servers as DNS queries to the DNS database. • Active Directory resolves domain object names to object records through requests that are received by domain controllers either as LDAP search requests or as modify requests to the Active Directory database. Thus, the Active Directory domain computer account object is in a different namespace from the DNS host record that represents the same computer in the DNS zone.
Active Directory DNS objects	When DNS data is stored in Active Directory, each DNS zone is an Active Directory container object (class **dnsZone**). The dnsZone object contains a DNS node object (class **dnsNode**) for every unique name within that zone. These unique names include the variations assigned to a specific host computer when it functions, for example, as a primary domain controller or as a global catalog server. The dnsNode object has a dnsRecord multivalue attribute that contains a value for every resource record that is associated with an object's name. For more information about Active Directory DNS objects, see How DNS Works.

Active Directory and DNS Domain Names

Active Directory domains have two types of names: DNS names and NetBIOS names. In general, both names are visible to end users. The DNS names of Active Directory domains include two parts, a prefix and a suffix. The DNS prefix is the first label in the DNS name of the domain. The suffix is the name of the Active Directory forest root domain.

When a Windows NT 4.0 master user domain (MUD) is upgraded, the decision is made whether or not to use the current NetBIOS name of the domain as a DNS prefix. If the name is appropriate to represent the organizational structure of the enterprise and satisfies the prefix naming rules in the table below, the name is typically kept. In this case, the NetBIOS name of the domain is the same as the DNS prefix of the domain.

Registered DNS Name Prefix Rules

Rule	Explanation
Select a prefix that is not likely to become outdated.	Avoid names such as a business line or operating system that might change in the future. Geographical names are recommended.
Select a prefix that includes Internet standard characters only.	A-Z, a-z, 0-9, and (-), but not entirely numeric.
Include 15 characters or less in the prefix.	If you choose a prefix length of 15 characters or less, then the NetBIOS name is the same as the prefix.

If the current NetBIOS name of the domain is inappropriate to represent the organizational structure of the enterprise or if the current name fails to satisfy the prefix naming rules, a new prefix is used. In this case, the NetBIOS name of the domain will be different from the DNS prefix of the domain.

For each new Active Directory domain, a prefix that is appropriate for the organizational structure of the enterprise and that satisfies prefix naming rules is used. Typically, the NetBIOS name of the domain will be the same as the name of the DNS prefix.

The Active Directory forest root domain is also the name of the Active Directory forest. The forest root name is a DNS name that consists of a prefix and a suffix in the form of prefix.suffix. For example, an organization might have the forest root name corp.contoso.com. In this example, corp is the prefix and contoso.com is the suffix.

The suffix is selected from a list of existing DNS names on the network. For the prefix, a new name that has not been used on the network previously is selected. By attaching a new prefix to an existing suffix, a unique namespace is created. Creating a new namespace for Active Directory ensures that any existing DNS infrastructure does not need to be modified to accommodate Active Directory.

Typically, the DNS names that are used in the Active Directory namespace are registered with an Internet authority. Only registered names are guaranteed to be globally unique. If two organizations register the same DNS domain name, or if an organization merges with, acquires, or is acquired by another company that uses the same DNS name, then the two infrastructures cannot interact with one another.

Note

- Using unregistered suffixes is not recommended. Using single label names, such as .local, is not supported.

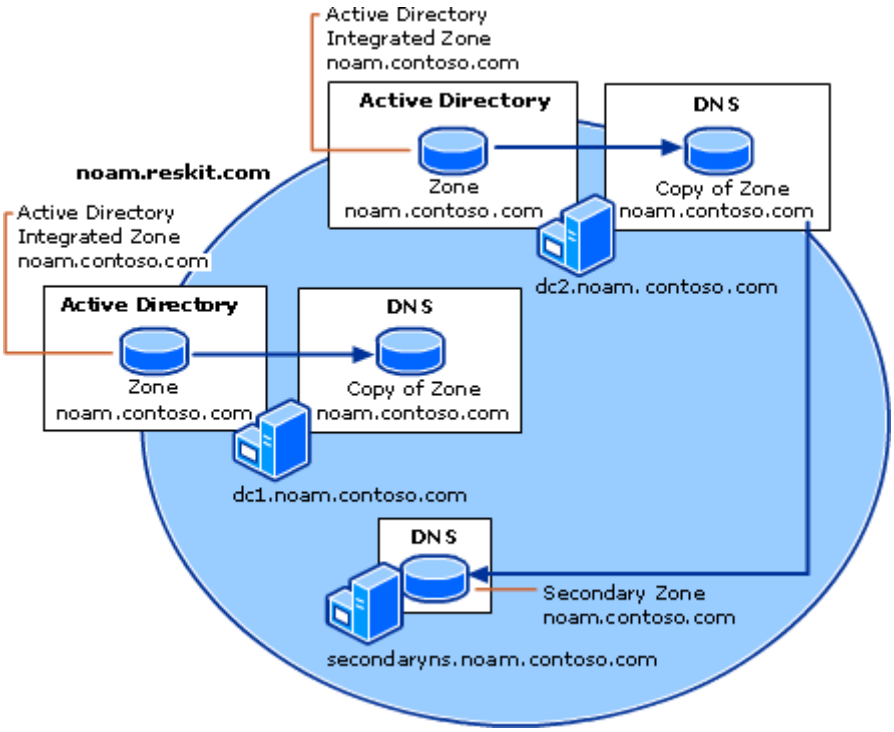
Back to Top

DNS Physical Structure in Support of Active Directory

The physical structure of Active Directory information in DNS is represented in DNS zones and resource records, which, in turn, are typically stored in Active Directory as Active Directory–integrated DNS zones. The DNS zones that support Active Directory domains can also be stored in standard, file-based, DNS zones. In addition, the DNS dynamic update protocol is utilized by Active Directory in order to make the registration of domain controller DNS resource records automatic.

The following diagram illustrates the physical storage of Active Directory domain information in DNS zones hosted on domain controllers, and in standard DNS zones hosted on member servers.

DNS Physical Structure in Support of Active Directory



The following table describes the physical components in the Active Directory/DNS physical structure.

DNS Physical Structure in Support of Active Directory Components

Active Directory/DNS Physical Structure Component	Description
Active Directory/DNS physical structure requirements	The DNS server used to support Active Directory must support the SRV resource record and, ideally, the DNS dynamic update protocol. If the DNS server does not support the DNS dynamic update protocol, the SRV resource records required to locate Active Directory domain controllers can be added to DNS manually.
_msdcs DNS subdomain	The Microsoft-specific subdomain enables location of domain controllers that have specific roles in the Active Directory domain or forest. Resource records for the DNS root domain of a new Active Directory forest are stored in a _msdcs zone instead of a subdomain, and that zone is stored in the forest-wide application directory partition.
Domain controller SRV resource records registered in DNS	There are multiple DNS SRV resource records registered on behalf of domain controllers. A description of each resource record is below.
DNS application directory partitions	In Windows Server 2003, the Active Directory–integrated DNS zones that support Active Directory domains can be stored in Active Directory application directory partitions, which is a new feature of Windows Server 2003. By default, the DNS root domain of a new Active Directory forest is stored in the domain-wide application directory partition for the forest root domain.

DNS Support for Active Directory Physical Structure Requirements

In order for a DNS server to be able to support Active Directory, the server is required to support the service (SRV) resource record type and the dynamic update protocol, as described in the RFC 2136. Active Directory uses DNS as the location mechanism for domain controllers, enabling computers on the network to obtain IP addresses of domain controllers. During the installation of Active Directory, the service (SRV) and address (A) resource records are dynamically registered in DNS. Both types of records are necessary for the functionality of the domain controller locator (Locator) mechanism.

To find domain controllers in a domain or forest, a client queries DNS for the SRV and A DNS resource records of the domain controller. The resource records provide the client with the names and IP addresses of the domain controllers. In this context, the SRV and A resource records are referred to as Locator DNS resource records.

When a domain controller is added to a forest, a DNS zone hosted on a DNS server is updated with the Locator DNS resource records for that domain controller. For this reason, the DNS zone must allow dynamic updates (RFC 2136), and the DNS server hosting that zone must support the SRV resource records (RFC 2782) to advertise the Active Directory directory service.

At the very least, the DNS server must support the SRV resource record; but the SRV resource records can be added to DNS manually. After installing Active Directory, these records can be found on the domain controller in the following location: *systemroot*\System32\Config\Netlogon.dns.

Note

- The configuration of reverse lookup zones is not based on the Windows Server 2003 domain structure; instead, it is based on the range of IP addresses assigned to a company. If a company is assigned B class IP addresses such as 172.56.X.Y., then a reverse lookup zone of 56.172.in-addr.arpa. will be created. It might contain delegations to some other domains such as 1.56.172.in-addr.arpa., 2.56.172.in-addr.arpa., etc. It is also possible to configure classless reverse lookup zones as described in the RFC Best Current Practice paper "Classless IN_ADDR.ARPA delegation."

_msdcs Subdomain

To facilitate locating Windows Server 2003–based domain controllers, in addition to the standard ***_Service._Protocol.DnsDomainName*** format, the Net Logon service registers SRV records that identify the well-known server-type pseudonyms "dc" (domain controller), "gc" (global catalog), "pdc" (primary domain controller), and "domains" (globally unique identifier, or GUID) as prefixes in the _msdcs subdomain. This Microsoft-specific subdomain enables location of domain controllers that have Windows Server 2003–specific roles in the domain or forest, as well as the location by GUID when a domain has been renamed. To accommodate locating domain controllers by server type or by GUID (abbreviated "dctype"), Windows Server 2003-based domain controllers register SRV records in the following form:

*_Service._Protocol.DcType.***_msdcs.***DnsDomainName*

Note

- There are also site–specific DNS resource records that use a slightly different format. For more information about site discovery, see "Domain Controller Location in the Closest Site" later in this document.

The subdomain _msdcs.*DnsDomainName* is used to find an LDAP server that is running TCP and also functioning in a particular Windows Server role. The name "_msdcs" is reserved for locating domain controllers and Kerberos servers. The single keyword "_msdcs" was chosen to avoid cluttering the DNS namespace unnecessarily. Other constant, well-known names (pdc, dc, and gc) were kept short to avoid exceeding the maximum length allowed for a DNS name.

Domain Controller SRV Resource Records

When a Windows Server 2003–based domain controller starts up, the Net Logon service uses dynamic updates to register SRV and A resource records in the DNS database, as described in Internet Engineering Task Force (IETF) RFC 2782, "A DNS RR for specifying the location of services (DNS SRV)." Windows Server 2003 also uses secure dynamic update using the GSS-TSIG algorithm, as described in RFC 3645, "Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)."

The SRV record is used to map the name of a service (in this case, the LDAP service) to the DNS computer name of a server that offers that service. In a Windows Server 2003 network, an LDAP resource record locates a domain controller.

When a workstation logs on to a Windows Server 2003 domain, it queries DNS for SRV records in this general form:

_Service._Protocol.DnsDomainName

Because Active Directory servers offer the LDAP service over the TCP protocol, clients find an LDAP server by querying DNS for a record of the form:

_ldap._tcp.*DnsDomainName*

Note

- The service and protocol strings require an underscore (_) prefix to prevent potential collisions with existing names in the namespace.

Active Directory site-specific resource records are also used during logon. For more information, see "Domain Controller Location in the Closest Site" later in this document.

SRV Records Registered by Net Logon

The list in the following table provides the definitions of the names associated with registered SRV records. It also describes the lookup criteria supported by each record and the checks performed by Net Logon as each record is registered.

In the descriptions of registered SRV records, *DnsDomainName* refers to the DNS domain name that is used during creation of the domain controller when the domain tree is joined or created (that is, when the computer runs the Active Directory Installation Wizard). *DnsForestName* refers to the DNS domain name of the forest root domain.

An owner name is the name of the DNS node to which a resource record pertains. These resource records are used by domain controller Locator. The following table lists the owner names of the SRV records that are registered by Net Logon.

SRV Records That Are Registered by Net Logon

SRV Resource Record	Description
_ldap._tcp.*DnsDomainName***.**	Enables a client to locate a server that is running the LDAP service in the domain named *DnsDomainName*. The server is not necessarily a domain controller — that is, the only assumption that can be made about the server is that it supports the LDAP application programming interface (API). All Windows Server 2003–based domain controllers register this SRV record (for example, _ldap._tcp.contoso.com.).
_ldap._tcp.*SiteName***.** **_sites.***DnsDomainName***.**	Enables a client to locate a server that is running the LDAP service in the domain named *DnsDomainName* in the site named *SiteName*. *SiteName* is the relative distinguished name of the site object that is stored in the Configuration container in Active Directory. All Windows Server 2003–based domain controllers register this SRV record (for example, _ldap._tcp.charlotte._sites.contoso.com.).
_ldap._tcp.dc._msdcs.*DnsDomainName***.**	Enables a client to locate a domain controller (dc) of the domain named *DnsDomainName*. All Windows Server 2003–based domain controllers register this SRV record.
_ldap._tcp.*SiteName***.** **_sites.dc._msdcs.***DnsDomainName***.**	Enables a client to locate a domain controller for the domain named *DnsDomainName* and in the site named *SiteName*. All Windows Server 2003–based domain controllers register this SRV record.
_ldap._tcp.pdc._msdcs.*DnsDomainName***.**	Enables a client to locate the server that is acting as the primary domain controller (PDC) in the mixed-mode domain named *DnsDomainName*. Only the PDC emulator master of the domain (the Windows Server 2003–based domain controller that advertises itself as the primary domain controller to computers that need a primary domain controller) registers this SRV record.
_ldap._tcp.gc._msdcs.*DnsForestName***.**	Enables a client to locate a global catalog (gc) server for this forest. Only domain controllers that are functioning as gc servers for the forest named in *DnsForestName* register this SRV record (for example, _ldap._tcp.gc._msdcs.contoso.com.).
_ldap._tcp.*SiteName***.** **_sites.gc._msdcs.***DnsForestName***.**	Enables a client to locate a global catalog (gc) server for this forest in the site named in SiteName. Only domain controllers that are serving as gc servers for the forest named in DnsForestName register this SRV record (for example, _ldap._tcp.charlotte._sites.gc._msdcs.contoso.com.).
_gc._tcp.*DnsForestName***.**	Enables a client to locate a global catalog (gc) server for this domain. The server is not necessarily a domain controller. Only a server that is running the LDAP service and functioning as the GC server for the forest named *DnsForestName* registers this SRV record (for example, _gc._tcp.contoso.com.). In Windows Server 2003, a GC server is a domain controller. Other implementations of directory services (that are not Windows Server 2003 implementations) can also register servers as GC servers.
_gc._tcp.*SiteName***.** **_sites.***DnsForestName***.**	Enables a client to locate a global catalog (gc) server for this forest in the site named *SiteName*. The server is not necessarily a domain controller. Only a server that is running the LDAP service and functioning as the GC server for the forest named *DnsForestName* registers this SRV record (for example, _gc._tcp.charlotte._sites.contoso.com.).
_ldap._tcp.*DomainGuid***.** **domains._msdcs.***DnsForestName***.**	Enables a client to locate a domain controller in a domain on the basis of its GUID. A GUID is a 128-bit number that is automatically generated for referencing objects in Active

	Directory — in this case, the domain object. This operation is expected to be infrequent; it occurs only when the DnsDomainName of the domain has changed, the DnsForestName is known, and DnsForestName has not also been renamed (for example, _ldap._tcp.4f904480-7c78-11cf-b057-00aa006b4f8f.domains._msdcs.contoso.com.). All domain controllers register this SRV record.
_kerberos._tcp.*DnsDomainName***.**	Enables a client to locate a server that is running the Kerberos KDC service for the domain that is named in *DnsDomainName*. The server is not necessarily a domain controller. All Windows Server 2003–based domain controllers that are running an RFC 1510–compliant Kerberos KDC service register this SRV record.
_kerberos._udp.*DnsDomainName***.**	Same as _**kerberos._tcp.***DnsDomainName*, except that UDP is implied.
_kerberos._tcp.*SiteName***.** **_sites.***DnsDomainName***.**	Enables a client to locate a server that is running the Kerberos KDC service for the domain that is named *DnsDomainName* and is also in the site named *SiteName*. The server is not necessarily a domain controller. All Windows Server 2003–based domain controllers that are running an RFC 1510–compliant Kerberos KDC service register this SRV record.
_kerberos._tcp.dc._msdcs.*DnsDomainName***.**	Enables a client to locate a domain controller that is running the Windows Server 2003 implementation of the Kerberos KDC service for the domain named in *DnsDomainName*. All Windows Server 2003–based domain controllers that are running the KDC service (that is, that implement a public key extension to the Kerberos v5 protocol Authentication Service Exchange subprotocol) register this SRV record.
_kerberos.tcp.*SiteName***.** **_sites.dc._msdcs.***DnsDomainName***.**	Enables a client to locate a domain controller that is running the Windows Server 2003 implementation of the Kerberos KDC service for the domain that is named *DnsDomainName* and that is also in the site named *SiteName*. All Windows Server 2003–based domain controllers that are running the KDC service (that is, that implement a public key extension to the Kerberos v5 protocol Authentication Service Exchange subprotocol) register this SRV record.
_kpasswd._tcp.*DnsDomainName***.**	Enables a client to locate a Kerberos Password Change server for the domain. All servers that provide the Kerberos Password Change service (which includes all Windows Server 2003–based domain controllers) register this name. This server must at least conform to the Kerberos Change Password Protocol. (For more information about this draft, see the Microsoft Platform SDK.) The server is not necessarily a domain controller. All Windows Server 2003–based domain controllers that are running an RFC 1510–compliant Kerberos KDC service register this SRV record.
_kpasswd._udp.*DnsDomainName***.**	Same as _**kpasswd._tcp.***DnsDomainName*, except that UDP is implied.

In addition to the SRV records listed in the table above, Net Logon also registers a DNS alias (CNAME) record for use by Active Directory replication, in the format: *DsaGuid***._msdcs.***DnsForestName*. The Locator does not use this record. This record enables a client to locate any domain controller in the forest by looking up an A record. The only information that is known about the domain controller is the GUID of the directory system agent (DSA) object for the domain controller and the name of the forest in which the domain controller is located. This record is used to facilitate renaming a domain controller.

If multiple domain controllers have the same criteria, multiple records exist with the same owner name. A client that is looking for a domain controller with specific criteria would receive all the applicable records from the DNS server. The client would pick one of the returned records to select a domain controller, as described in RFC 2782.

Other SRV Record Content

The following information is also included in an SRV record.

SRV Record Field	Description
Priority	The priority of the server. Clients attempt to contact the server with the lowest priority.
Weight	A load-balancing mechanism that is used when selecting a target host from those that have the same priority. Clients randomly choose SRV records that specify target hosts to be contacted, with probability proportional to the weight.
Port number	The port where the server is listening for this service.
Target	The fully qualified domain name of the host computer.

The algorithm by which clients interpret and select among SRV resource records is defined in RFC 2782, "A DNS RR for specifying the location of services (DNS SRV)."

Host Records for Non-SRV-Aware Clients

Net Logon registers the following DNS A records for the use of LDAP clients that do not support DNS SRV records (that is, clients that are non-SRV-aware). Locator does not use these records.

Host (A) Records Registered by Net Logon

Host (A) Resource Record	Description
DnsDomainName.	Enables a non-SRV-aware client to locate any domain controller in the domain by looking up an A record. A name in this form is returned to the LDAP client through an LDAP referral. A non-SRV-aware client looks up the name; an SRV-aware client looks up the appropriate SRV resource record.
gc._msdcs.*DnsForestName*.	Enables a non-SRV-aware client to locate any global catalog server in the forest by looking up an A record. A name in this form is returned to the LDAP client through an LDAP referral. A non-SRV-aware client looks up this name; an SRV-aware client looks up the appropriate SRV resource record.

Example of Registered Resource Records

The following example illustrates the combined information that is contained in A resource records and SRV resource records.

A domain controller named Phoenix in the domain contoso.com has an IP address of 157.55.81.157. It registers the following A records and SRV records with DNS:

```
phoenix.contoso.com   A   157.55.81.157
_ldap._tcp.contoso.com    SRV  0 0 389 phoenix.contoso.com
_kerberos._tcp.contoso.com   SRV  0 0 88 phoenix.contoso.com
_ldap._tcp.dc._msdcs.contoso.com  SRV  0 0 389 phoenix.contoso.com
_kerberos._tcp.dc._msdcs.contoso.com  SRV  0 0 88 phoenix.contoso.com.
```

When the appropriate SRV records and A records are in place, a DNS query for _ldap._tcp.dc._msdcs.contoso.com returns the names and addresses of all domain controllers in the domain.

For more information about A records, SRV records, DNS, and dynamic updates, see "DNS Protocol" and "DNS Physical Structure" in How DNS Works.

DNS Application Directory Partitions

DNS zones stored in Active Directory replicate to Active Directory domain controllers according to different replication scopes. In Windows 2000 Server, a DNS zone stored in Active Directory is replicated to all domain controllers in the Active Directory domain. Windows Server 2003 has added application directory partitions, which enable the DNS zone to be stored in different replication scopes. The following table describes all of the replication scopes available to a DNS zone stored in Active Directory.

Windows Server 2003 Active Directory Storage Options

Active Directory Storage Option	Replication Scope
Domain partition	Active Directory domain partition for each domain in the forest. DNS zones stored in

	this partition are replicated to all domain controllers in the domain. This is the only Active Directory storage option for DNS zones that are replicated to domain controllers running Windows 2000 Server.
Forest-wide DNS application directory partition	DNS application directory partition for the entire forest. DNS zones stored in this application directory partition are replicated to all DNS servers running on domain controllers in the forest. This DNS application directory partition is created when you install the DNS Server service on the first Windows Server 2003 domain controller in the forest.
Domain-wide DNS application directory partition	DNS application directory partition for each domain in the forest. DNS zones stored in this application directory partition are replicated to all DNS servers running on domain controllers in the domain. For the forest root domain, this DNS application directory partition is created when you first install the DNS Server service on a Windows Server 2003 domain controller in the forest. For each new domain in the forest (child domain), this DNS application directory partition is created when you first install the DNS Server service on a Windows Server 2003 domain controller for the new domain.
Custom DNS application directory partition	DNS application directory partition for any domain controller that is enlisted in its replication scope. This type of DNS application directory partition does not exist by default and must be created. DNS zones stored in this application directory partition are replicated to all DNS servers running on domain controller that enlist in the partition.

As stated earlier, the Locator DNS resource records for an Active Directory domain are stored in the _msdcs.*DnsDomainName* subdomain for the Active Directory domain. In Windows Server 2003, when the DNS root domain of a new Active Directory forest is created on a Windows Server 2003 domain controller, a DNS zone is automatically created for the _msdcs.*DnsForestName* and stored in the forest-wide DNS application directory partition, which replicates to all Windows Server 2003 domain controllers in the forest running the Windows Server 2003 DNS Server service.

Note

- DNS zones stored in application directory partitions cannot be accessed by Windows 2000 Server domain controllers.

Back to Top

DNS Support for Active Directory Processes and Interactions

When a Windows Server 2003 member server is promoted to an Active Directory domain controller by installing Active Directory, the Net Logon service registers the DNS resource records necessary for network hosts and services to be able to locate the domain controller on the network. When network hosts and services attempt to perform an operation (such as joining a domain, for example) that requires an Active Directory domain controller, the Locator mechanism is used to locate the domain controller through DNS. The following table describes the processes and interactions involved in the registration and location of domain controllers in DNS.

Active Directory and DNS Processes and Interactions

Process or Interaction	Description
Domain controller DNS name registration	The Net Logon service registers DNS resource records on behalf of the Active Directory domain controller in the DNS zone with the same name as the Active Directory domain hosted by the domain controller.
DNS delegation, forwarders	DNS delegation resource records are created in the zone that is a parent of the zone supporting the Active Directory domain. The delegation enables the DNS name of the domain controller to be resolved downward from the root of the DNS hierarchy. DNS forwarders are another DNS feature that enable domain controller location, and are commonly used for an Active Directory client in one domain to locate a domain controller in another domain.
DNS domain controller location	Network hosts and services use the DNS Locator mechanism to locate domain controllers in the Active Directory forest.

Domain Controller Name Registration

Every Windows Server 2003–based domain controller registers two types of names at startup:

- A DNS domain name with the DNS service (for example, noam.contoso.com).
- A NetBIOS name with Windows Internet Name Service (WINS) or another transport-specific service (for example, noam).

When a user starts a computer and logs on to a domain, the computer must do one of two things:

- If the name of the logon domain is a DNS name, the computer must query DNS to find a domain controller with which to authenticate.
- If the name of the logon domain is a NetBIOS name, the computer must send a mailslot message to find a domain controller for the specified domain.

After the computer has found a domain controller, the information is cached so that a new query is not required for subsequent logon sessions.

DNS Domain Name Registration

Active Directory supports dynamic registration of domain controller addresses in DNS. After Active Directory has been installed during domain controller creation, the Net Logon service dynamically creates records in the DNS database that are used to locate the server. Dynamic update (described in RFC 2136) is a recent addition to the DNS standard; this addition to the standard defines a protocol for dynamically updating a DNS server with new or changed resource record values. Before the advent of this new protocol, administrators had to manually create the records that are stored on DNS servers. The implementation of DNS server that is included with Windows Server 2003 supports dynamic updates, as does the Berkeley Internet Name Domain (BIND) version 8.*x* implementation of DNS.

Note

- By default, the Windows Server 2003 DNS Server service running on a domain controller is configured to accept secure dynamic update only.

Every Windows Server 2003–based domain controller dynamically registers SRV records in DNS. The SRV records enable servers to be located by service type (for example, LDAP) and protocol (for example, TCP). Because domain controllers are LDAP servers that communicate over TCP, SRV records can be used to find the DNS computer names of domain controllers. In addition to registering LDAP-specific SRV records, Net Logon also registers Kerberos v5 authentication protocol–specific SRV records to enable locating servers that run the Kerberos Key Distribution Center (KDC) service.

Every Windows Server 2003–based domain controller also dynamically registers a single host resource record (an A resource record) that contains the name of the domain (*DnsDomainName*) where the domain controller is and the IP address of the domain controller. The A resource record makes it possible for clients that do not recognize SRV records to locate a domain controller by means of a generic host lookup.

NetBIOS Domain Name Registration

A domain controller registers its NetBIOS name (*DomainName*[1C]) by broadcasting or directing a NetBIOS name registration request to a NetBIOS name server, such as a WINS server. Registering the NetBIOS name makes it possible for Windows-based clients that are not DNS-enabled to find the domain controllers that are running Windows Server 2003, Windows 2000, Windows NT 4.0, or Windows NT 3.51. In this case, the client finds the domain controller by sending a Net Logon mailslot request that is based on the NetBIOS domain name.

Note

- NetBIOS recognizes domain controllers by the [1C] registration.

DNS Delegation, Forwarders

To fully support an Active Directory domain, the DNS infrastructure must have the DNS delegations that are necessary to enable name resolution during domain controller location. When an Active Directory domain is created, a DNS delegation entry must exist in the DNS zone that is the parent of the zone supporting the Active Directory domain. The delegation enables the name of the domain controller hosting the domain to be resolved by any host or service in the DNS namespace. The delegation resource records must be added by the network administrator who administers the DNS server hosting the parent zone. Alternately, the parent zone could host the DNS resource records for the domain name and, in this case, the delegation is unnecessary.

For example, if there is a DNS zone supporting the domain corp.contoso.com, then a delegation for this name must exist in the parent zone contoso.com. When a DNS query for the name is sent to the root of the DNS namespace, delegations can be followed until the DNS server hosting the zone for corp.contoso.com is identified. Without this delegation, only those network hosts and services configured with the IP address of the DNS server hosting the zone for corp.contoso.com will be able to resolve its DNS name. All other network hosts and services will be unable to resolve the name, and the domain controller will not be available to them for such Active Directory operations as joining a domain, logging on to a domain, or searching Active Directory.

When the Active Directory domain name is specified in the Active Directory Installation Wizard, the wizard

reads the delegation entry in DNS, prompts the user to install the DNS Server service locally and configures the corresponding DNS zone automatically. Also, if the computer is already configured with a preferred DNS server, the wizard will configure a forwarder on the DNS Server service with the IP address of the prior preferred DNS server.

Forwarders are also commonly configured on the DNS server hosting a zone in support of an Active Directory domain. Forwarders are used by a DNS server to forward queries for a domain name about which it has no local data. If an Active Directory client in one domain needs to access a resource in another Active Directory domain, it will need to locate a domain controller in that domain. If the DNS server used by that client is unable to locate a domain controller for the other domain using its local data, it can forward the client request to another DNS server, such as the DNS server that hosts the zone for the Active Directory forest root domain.

In summary, delegation enables name resolution in a descending direction from the root of the hierarchy, and forwarders enable name resolution in a ascending direction toward the root of the hierarchy.

Windows Server 2003 introduces an enhancement to forwarding called conditional forwarders. When you use conditional forwarding, you can configure your DNS servers to forward queries to different servers based on the domain name specified in the query. This eliminates steps in the standard forwarding chain and reduces network traffic. When conditional forwarding is applied, the DNS server hosting a zone in support of the one Active Directory domain can forward queries to DNS servers hosting zones in support of the Active Directory domain name specified in the client query.

Although root hints (resource records that list the DNS servers hosting the DNS root zone) can also be used to facilitate domain controller location in place of forwarders, DNS deployments commonly use forwarders for remote domain controller location to reduce the complexity of administering root hints for both internal and Internet resolution.

For more information about delegation, forwarders, and root hints, see "How DNS Works."

Domain Controller Locator

The domain controller locator (Locator) algorithm consists of two main parts:

- Locator finds which domain controllers are registered with a DNS server.
- Locator submits a DNS query to the DNS server to locate a domain controller in the specified domain.

After this query is resolved, an LDAP User Datagram Protocol (UDP) lookup is sent to one or more of the domain controllers listed in the response to the DNS query to ensure their availability. Finally, the Net Logon service caches the discovered domain controller to aid in resolving future requests.

Domain Controller Locator Process

Each Windows Server 2003–based domain controller registers its DNS domain name on the DNS server and registers its NetBIOS name by using a transport-specific mechanism (for example, WINS). Thus, a DNS client locates a domain controller by querying DNS, and a NetBIOS client locates a domain controller by querying the appropriate transport-specific name service. Because the code for the DNS-compatible Locator and the Windows NT 4.0–compatible Locator is shared, both DNS clients and NetBIOS clients are supported.

The process that the Locator follows can be summarized as follows:

1. On the client (the computer that is locating the domain controller), the Locator is initiated as a remote procedure call (RPC) to the local Net Logon service. The Locator API (DsGetDcName) is implemented by the Net Logon service.
2. The client collects the information that is needed to select a domain controller and passes the information to the Net Logon service by using the DsGetDcName API.
3. The Net Logon 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, Net Logon queries DNS by using the DNS-compatible Locator — that is, DsGetDcName calls DnsQuery to read the SRV records and A records from DNS after it appends an appropriate string to the front of the domain name that specifies the SRV record.
   - For a single label name, Net Logon performs domain controller discovery by using the Windows NT 4.0–compatible Locator — that is, by using the transport-specific mechanism (for example, WINS).

     Note
     - 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.
4. The Net Logon service sends a datagram to the discovered domain controllers that register 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 UDP search.
5. Each available domain controller responds to the datagram to indicate that it is currently operational and then returns the information to DsGetDcName.

6. The Net Logon service returns the information to the client from the domain controller that responds first.
7. The Net Logon service caches the domain controller information so that it is not necessary to repeat the discovery process for subsequent requests. Caching this information encourages the consistent use of the same domain controller and, thus, a consistent view of Active Directory.

Domain Controller Location in the Closest Site

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 Server 2003 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.

Each Windows Server 2003–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 could contact 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 then 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") 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 *siteObject* 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 networks, subnets, and subnet masks, see "How TCP/IP Works."

IP Addresses Mapped 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 that 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 that 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 client uses the new domain controller. If the second query fails, the client uses the original domain controller.
- 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.

You can override the dynamically determined value using the registry, but you should 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.

Note

- Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows Server 2003. 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.

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. Thus, the client finds a domain controller in the correct site without having to retry the operation. On the other hand, 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 Server 2003 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 Site-link Cost

Site coverage is determined according to site-link costs, and domain controllers register themselves in sites

accordingly. For example, 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.

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. 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 (described in the next sub-section) 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.

Site Coverage Algorithm

During registration of SRV records in DNS, the following algorithm determines if the domain controllers should register site SRV records to designate themselves as preferred domain controllers in Active Directory sites where no domain controller exists for a particular domain.

For every domain controller in the forest, this procedure is followed:

- Build a list of target sites — sites that have no domain controllers for this domain (the domain of the current domain controller).
- Build a list of candidate sites — sites that have domain controllers for this domain.
- For every target site, follow these steps:
  1. Build a list of candidate sites of which this domain is a member. (If none, do nothing.)
  2. Of these, build a list of sites that have the lowest site link cost to the target site. (If none, do nothing.)
  3. If more than one, break ties (reduce this list to one candidate site) by choosing the site with the largest number of domain controllers.
  4. If more than one, break ties by choosing the site that is first alphabetically.
  5. 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; the minimum value is 60 seconds. The implications of these settings are:

- 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 time-out value is too small, secure channel traffic is unnecessarily slowed down by discovery attempts.

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.

Types of Locators

On the basis of parameters passed to Net Logon in the DsGetDcName API, the process of locating a domain controller proceeds in one of two ways:

- The DNS-compatible Locator is used if the domain name passed to DsGetDcName is a DNS-compatible name. The Net Logon service on the client looks up the name in DNS (by calling DnsQuery) after it appends an appropriate string to the front of the domain name. The DNS service supports a query for determining the set of domain controllers. If the client site name is known, the client DNS query specifies the site. DNS returns the IP addresses of domain controllers that match the DNS query. The client Net Logon service sends an LDAP UDP message to one or more of the domain controllers that have been returned by DNS in order to determine whether any of the specified domain controllers are running and support the specified domain.
- The Windows NT 4.0–compatible Locator is used if the domain name passed to DsGetDcName is a NetBIOS name. The Net Logon service on the client sends a transport-specific logon request query to locate a domain controller in a particular domain and then sends a mailslot message to one or more of the domain controllers to determine whether any of the domain controllers it found are running and support the specified domain.

DNS Client Service Configuration Elements

The DNS configuration on Active Directory client computers follows a specific computer naming scheme and specifies how these clients will locate DNS servers. The following table lists the configurations for DNS configuration elements.

DNS Configuration for Client Computers

DNS Configuration Element	Configuration
Computer naming	Use default naming. When a Windows 2000, Windows XP, or Windows Server 2003 computer joins a domain, the computer assigns itself a primary DNS name comprised of the host name of the computer and the name of the domain.
Client resolver configuration	Configure client computers to point to any DNS server on the network.

Note

- Active Directory clients and domain controllers can dynamically register their DNS names using a DNS server that is not authoritative for the DNS name of the Active Directory domain. The DNS server used by these clients will refer the registration to an the DNS server authoritative for the name of the Active Directory domain.

A computer might have an existing DNS name if the organization previously statically registered the computer in DNS or the organization previously deployed an integrated DHCP solution. If client computers already have a registered DNS name, when the domain to which they are joined is upgraded to Windows Server 2003 Active Directory, the client computers will have two names: the existing DNS name, and the new primary name.

Clients can be located by either name. Any existing DNS, DHCP, or integrated DNS/DHCP solution is left intact. The new primary names are created automatically and updated by means of dynamic update. The old names are cleaned up automatically by means of DNS scavenging.

To take advantage of Kerberos authentication when connecting to a server running Windows 2000, Windows XP, or Windows Server 2003, the client must connect to the server by using the primary name.

Back to Top

Network Ports Used by DNS in Support of Active Directory

The network ports used by DNS are documented in the DNS Technical Reference. For more information, see "Network Ports used by DNS" in How DNS Works.

Back to Top

Related Information

The following resource contains additional information that is relevant to this section.

- How DNS Works