Knowledge Base

Integrating Windows 2000 DNS into an Existing BIND or Windows NT 4.0-Based DNS Namespace

PSS ID Number: 255913

Article Last Modified on 11/4/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server

This article was previously published under Q255913

SUMMARY

One feature of Windows 2000 Domain Name System (DNS) is its support for dynamic host updates (documented in RFC 2136). To take advantage of this feature, Windows 2000 DNS can be deployed in environments that have no other DNS servers, as well as in environments that already have non-dynamic DNS servers implemented (Microsoft Windows NT 4.0 DNS server and BIND 4.9.7 and earlier, etc.). When you are deploying Windows 2000 DNS in an environment that already has BIND or Windows NT 4.0 DNS servers implemented, you have several integration options:

- Upgrade Windows NT 4.0 DNS servers to Windows 2000.
- Migrate zones from non-dynamic authoritative DNS servers to servers running Windows 2000 DNS.
- Delegate child DNS domains under a parent DNS domain. For Active Directory domain names that do not have the same name as the root of a zone, delegate the subdomain to Windows 2000 DNS. For example, if the name of the Active Directory domain is dev.reskit.com and the zone that contains this name is reskit.com, delegate dev.reskit.com to a Windows 2000-based server running DNS.
- Delegate each of the subdomains used by the domain controller (DC) locator records (SRV records) to a Windows 2000-based server. These subdomains are _msdcs.reskit.com, _sites.reskit.com, _tcp.reskit.com, and _udp.reskit.com. This option would be used where Active Directory domain names (for example, reskit.com) that are the same as the name of the root of a zone (for example, reskit.com), cannot be delegated directly to a Windows 2000-based server running DNS. Optionally, clients may be members of the Active Directory domain called reskit.com, but can register in the DNS zone called dynamic.reskit.com.

This article documents the fourth option listed above, how to integrate Windows 2000 DNS into an organization that already has a DNS namespace implemented in which the DNS server that is authoritative for the zone with the name of the Active Directory domain does not support RFC 2136 (dynamic updates). This article also discusses a scenario in which domain members use a primary DNS suffix different from the name of the Active Directory domain to allow dynamic registration of DNS records by Windows 2000-based computers when the DNS server authoritative for the zone with the name of the Active Directory domain does not support dynamic DNS updates.

MORE INFORMATION

To integrate Windows 2000 DNS into an existing namespace based on non-dynamic DNS servers, you can delegate the subdomains used by the locator records (SRV records) so that dynamic updates (as per RFC 2136) may be used. Follow these steps:

1. On the non-dynamic DNS server that is authoritative for the zone with the name of the Active Directory domain, delegate the following zones to a Windows 2000-based server running DNS:

   _udp.*DNSDomainName*
   _tcp.*DNSDomainName*
   _sites.*DNSDomainName*
   _msdcs.*DNSDomainName*

   For example, if the root zone is called reskit.com, delegate _udp.reskit.com, _tcp.reskit.com, _sites.reskit.com, and _msdcs.reskit.com to the Windows 2000-based server.

2. On the Windows 2000-based server, create the forward zones delegated in step 1, and enable the zones for dynamic update.

   To create the new zones:

   a. Start DNS Manager on the Windows 2000 server.
   b. Expand the appropriate DNS server within DNS Manager.
   c. Right-click the **Forward Lookup Zones** folder, and then click **New Zone**.
   d. When the New Zone Wizard starts, click **Next**, click either the **Active Directory-Integrated** check box (recommended) or the **Standard Primary** check box (depending on the infrastructure of the network), and then click **Next**.
   e. Type the name of the zone in the **name** box. For example, type `_msdcs.reskit.com`.
   f. Click **Next**. After reviewing the wizard's summary, click **Finish**.

   To enable the zone to accept dynamic updates:

   a. Using DNS Manager on the Windows 2000 server running DNS, right-click the new zone, click **Properties**, and then click the **General** tab.
   b. In the **Allow Dynamic Updates** box, click **Only Secure Updates** (recommended) or **Yes**. Note that the **Only Secure Updates** option is only available after the server has been promoted to a domain controller.

   Repeat this process until all four of the zones described in step 1 have been created and allowed dynamic updates. This allows domain controller locator records to be dynamically registered and de-registered in DNS.

3. Additionally, a single zone or several zones may be created and configured to allow clients and servers to dynamically register themselves with the Windows 2000 server. For example, a zone called dynamic.reskit.com could be used to register all clients and servers on a network via dynamic updates. To configure such a zone:

   a. On the non-dynamic DNS server that is authoritative for the parent zone (for example, reskit.com), delegate a new zone to the Windows 2000-based server running DNS. For example, delegate the dynamic.reskit.com. zone to the Windows 2000 server.
   b. On the Windows 2000 server, create a forward lookup zone for the zone delegated above (dynamic.reskit.com).
   c. On the Windows 2000 server, enable the zone(s) for dynamic updates.

4. Clients and servers will have to be configured to register themselves in the correct zone. By default, clients register themselves in a DNS zone with the same name as the Windows 2000 domain they are members of. To configure a Windows 2000 client to register itself in a zone with a name that is different from the name of the Windows NT or Windows 2000 domain that the client is a member of, follow the procedure below.

   Note that this change requires that the client be rebooted after the change has been completed.

   a. Right-click **My Computer**, click **Properties**, and then click the **Network Identification** tab.
   b. Click **Properties**, and then click **More**.
   c. Click to clear the **Change primary DNS suffix when domain membership changes** check box.
   d. Type the appropriate zone name in the **Primary DNS suffix of this computer** box. For example, type `dynamic.reskit.com`.
   e. Click **OK**.

   After the computer is rebooted, it dynamically registers itself in the new zone. Configuring the client to register itself in the new zone can also be accomplished by using group policies. For additional information, click the article number below to view the article in the Microsoft Knowledge Base:

   240942 Active Directory DNSHostName Property Does Not Include Subdomain

   Earlier-version clients can be configured to register in the zone as well.

5. When Windows 2000 domain controllers start up, the Netlogon service attempts to register several SRV records in the authoritative zone. Because the zones in which the SRV records are to be registered have been delegated (in steps 1 and 2) to a Windows 2000 server where they can be dynamically updated, these registrations will succeed. Additionally, a DC will attempt to register the A record(s) listed in its Netlogon.dns file in the root zone (for example reskit.com). In this case, because the root zone is located on a non-dynamic DNS server, these updates will not succeed. The following event will be generated in the system log on the DC:
   Event Type: Warning
   Event Source: NETLOGON
   Event Category: None
   Event ID: 5773
   Date: 3/29/2000
   Time: 3:16:14 PM
   User: N/A
   Computer: DC
   Description:
   The DNS server for this DC does not support dynamic DNS. Add the DNS records from the file '%SystemRoot%\System32\Config\netlogon.dns' to the DNS server serving the domain referenced in that file.
   To correct this behavior:

   a. Every Windows 2000 DC has a Netlogon.dns file located in its %SystemRoot%\System32\Config folder. This file contains a list of DNS records that the DC will attempt to register when the Netlogon service starts. It is a good idea to make a copy of this file before making the following changes so that you will have a list of the original records that the DC tries to register with the DNS server. Note that each DC will have different records because these records are specific to each network adapter on each DC. Examine the Netlogon.dns file to identify all A records in the file. You can identify A records by the record type following the "IN" class descriptor. For example, the following two entries are A records:

      reskit.com. 600 IN A 10.10.10.10
      gc._msdcs.reskit.com. 600 IN A 10.10.10.10

      The number of A records in the Netlogon.dns file depends on the number of adapters the DC has, the number of IP addresses that each adapter has been configured with, and the role of the DC. DCs register:

      - One A record per each of its IP addresses for the name of the domain.
      - If the DC is also a global catalog (GC) server, it registers gc._msdcs.*DnsForestName* for each of its IP addresses.

   b. The number of A records in the Netlogon.dns file depends on the number of adapters the DC has, the number of IP addresses that each adapter has been configured with, and the role of the DC. DCs register: Because the non-dynamic DNS server will not accept the domain controller's attempts to dynamically register the A records, the A records have to be manually configured on the authoritative DNS server (in the example in this article, the DNS server authoritative for the zone reskit.com). Addition of the A record corresponding to the name of the domain (for example, reskit.com) is not required for the Windows 2000 deployment and may be needed only if third-party LDAP clients that do not support SRV DNS records are searching for the Windows 2000 DCs.

      On the Windows 2000 server, create the GC server-specific A records that were identified in step A, in the appropriate zone. For example, create an A record for the GC server in the _msdcs.reskit.com zone.

      On the non-dynamic DNS server that is authoritative for the root of the zone, create A records in the root zone (for example, reskit.com) for the non-GC server-specific A records that were identified in step A. For example, create an A record for reskit.com in the reskit.com zone.

   c. The number of A records in the Netlogon.dns file depends on the number of adapters the DC has, the number of IP addresses that each adapter has been configured with, and the role of the DC. DCs register: The following registry key should be used to disable the DC from attempting to register the A records seen in the Netlogon.dns file. Set the REG_DWORD RegisterDnsARecords value to 0 (zero) under:

      HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

6. To correct this behavior:Once you have an Active Directory forest and domain in place, you should integrate Active Directory with the DNS domains that the Windows 2000 server running DNS is responsible for. Also, you should reconfigure zones that have been configured to accept dynamic updates to accept only secure dynamic updates.

Keywords: kbDNS kbenv kbhowto KB255913
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch

---