Knowledge Base

DNS Server Becomes an Island When a Domain Controller Points to Itself for the _Msdcs.ForestDnsName Domain

PSS ID Number: 275278

Article Last Modified on 12/18/2003

The information in this article applies to:

- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2

This article was previously published under Q275278

SYMPTOMS

When a domain controller, with a Domain Name System (DNS) service installed, is authoritative for the _msdcs.*ForestDnsName* domain (the forest root), it may not successfully participate in Active Directory replication.

The preceding behavior can occur under the following circumstances:

- Multiple domain controllers are in the forest root with the DNS service installed.
- The domain controller/DNS server is a primary for the _msdcs. *ForestDnsName* domain.
- The domain controller/DNS server is pointed to itself as the preferred or alternate DNS server.

CAUSE

This behavior may occur because a DNS server may not have the necessary domain controller locator CNAME record for *DsaGuid*._msdcs.*ForestDnsName* in its zone for another domain controller.

RESOLUTION

To resolve this behavior, read the following example, and then use either of the following two methods:

Example:

Two domain controllers in the forest root are not replicating, DC1.*example*.com and DC2.*example*.com. Both domain controllers have the DNS service and are authoritative for the *example*.com domain.

Both domain controller's NetLogon service attempts to register their DNS records, and finds that their preferred DNS server (themselves) are authoritative for the *example*.com zone. Both servers register the records with their local DNS service. One of these records is a domain controller locator CNAME record for *DsaGuid*._msdcs.*ForestDnsName*. When DC1 attempts replication with DC2, it queries its local DNS server for this CNAME record for DC2, but cannot find it. Therefore, the replication process is unsuccessful.

Several possible methods are available to resolve this behavior. The method that is best for an organization depends upon its server load and network considerations. Two possible methods are:

Method 1

Select one DNS server in the forest root and point all other domain controllers in the root domain to it as their primary DNS server. Each domain controller may also be configured with an alternate DNS server, provided that it does not point to itself. The domain controller that functions as the primary location for other forest root domain controllers should point to itself for DNS resolution.

NOTE: This implementation process may not be suitable if the server that functions as the primary server is subject to heavy loads or the domain controllers in the forest root are geographically dispersed.

Example:

Domain = *example*.com (first domain in the forest)
Three domain controllers with DNS service = DC1, DC2, DC3
example.com is an Active Directory integrated zone
DC1 is designated as the primary location for this configuration

DC1 is configured to point to itself for DNS server settings in TCP/IP properties.
DC2 points to DC1 as the primary location and DC3 as an alternate
DC3 points to DC1 as the primary location and DC2 as an alternate.

Method 2

When you promote a server to a domain controller in the forest root, configure its primary DNS server as a domain controller or DNS server that has the following record for all other domain controllers in the root: domain controller locator CNAME record for *DsaGuid*._msdcs.*ForestName*.

Install the DNS service and enable the integrated Active Directory DNS zone to replicate to the new domain controller. Then the domain controller may be changed to point to itself as the primary or alternate DNS server.

If there are any Internet Protocol (IP) address changes for domain controllers in the root, it may be necessary to follow the steps in Method 1 until no longer necessary. When you have verified that the changes have replicated to the domain controller's DNS zone, the domain controllers may be configured to point to themselves as the primary or alternate DNS server again.

MORE INFORMATION

You can configure a domain controller to point to itself as a preferred or alternate DNS server. The only scenario where there is a possibility of the "island" problem is when a domain controller points to itself as the preferred or alternate DNS server and the server is a primary server for the DNS (not necessarily zone) _msdcs.*ForestDnsName* domain.

When the domain controller has registered the *DsaGuid*._msdcs.*ForestDnsName* CNAME record, the domain controller may be configured to point to itself as the preferred or alternate DNS server. An administrator must be aware that the CNAME record for another domain controller could accidentally be deleted, for example, an action caused by human error. Although the NetLogon service automatically registers this record, it may be created only locally, and the replication from this domain controller can be prevented because of the island problem.

The following example is one scenario in which pointing a server to itself as a preferred DNS server may cause an Active Directory replication problem:

- DC1.*example*.com. is the first domain controller in a forest. It is configured to point to itself as a preferred DNS server. The DNS server is authoritative for the *example*.com zone.
- Server2 is a W2K server with a local DNS server. Server2 is configured to point to itself as a preferred DNS server. Server2 has a forwarder that is set to DC1.
- Promote Server2 as a replica domain controller, DC2.*example*.com. During promotion the Active Directory integrated *example*.com zone is replicated to Server2.
- Restart the new domain controller, DC2.*example*.com. When the DNS server starts, it loads the *example*.com zone from Active Directory and becomes the primary location for the *example*.com zone and therefore for the _msdcs.*example*.com zone. The domain controller locator CNAME record registered by DC2.*example*.com is added to the local copy of the *example*.com zone, but cannot be replicated to another domain controller, DC1.*example*.com. This behavior may occur because DC1.*example*.com queries its local DNS server that is authoritative for the *example*.com zone, but does not contain the CNAME record registered by DC2.*example*.com.

Additional query words: replication failure fails

Keywords: kbDNS kbnetwork kbnofix kbprb KB275278
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbWin2000AdvServSP1 kbWin2000AdvServSP2 kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbwin2000ServSP1 kbwin2000ServSP2 kbWinAdvServSearch

Send feedback to Microsoft