The Importance of Proper DNS

*Questions? From your BS&A program, go to **Help>Contact Customer Support** and select **Request Support Phone Call** or **Email Support**. Or, you may call us at (855) 272-7638 and ask for the appropriate support department. Questions for our I.T. department may be submitted by phone (same number), or by emailing tech@bsasoftware.com.*

BS&A Software's new .NET software is a highly integrated suite of applications. Each application is integrated with multiple applications in the suite. But more than that, each application is integrated with and relies on base level Windows components included in Microsoft's .NET Framework.

For all of these applications and Windows components to interact properly, flawless DNS resolution is critical. This paper will outline the basics of DNS resolution in Windows networking, point out common pitfalls to avoid, and outline some overall best practices.

DNS Name Resolution

Historically, specifically back in the days of Windows 9.x operating systems, DNS was the last or nearly the last method of name resolution an operating system would use. Somewhere around the year 2000 that was all turned on its head. As outlined in Microsoft KB article 172218, DNS is now used for name resolution before Netbios methods like Wins/LMHosts/Broadcast.

DNS is integrated tightly with Active Directory. An Active Directory Domain cannot be set up without it. It is therefore critical that a network should be running a properly configured internal DNS server.

Internal DNS Server

When a host PC boots, it uses DNS to locate its logon server. Configuring a Windows host PC to use an external DNS server renders the host incapable of accomplishing that effectively. There is no way an external (i.e., the isp) DNS server can answer queries related to the internal network. SOA records, locations of domain controllers and global catalog servers are frequently requested by the host PC. At best, configuring an external DNS server on the client will slow network performance. At worst, it will cause authentication issues, network time-outs, and software failure.

Consider the following excerpt from Microsoft's "How DNS Works" Article cc772774

The DNS Client service queries the DNS servers in the following order:

1. *The DNS Client service sends the name query to the first DNS server on the preferred adapter's list of DNS servers and waits one second for a response.*
2. *If the DNS Client service does not receive a response from the first DNS server within one second, it sends the name query to the first DNS servers on all adapters that are still under consideration and waits two seconds for a response.*
3. *If the DNS Client service does not receive a response from any DNS server within two seconds, the DNS Client service sends the query to all DNS servers on all adapters that are still under consideration and waits another two seconds for a response.*
4. *If the DNS Client service still does not receive a response from any DNS server, it sends the name query to all DNS servers on all adapters that are still under consideration and waits four seconds for a response.*
5. *If it the DNS Client service does not receive a response from any DNS server, the DNS client sends the query to all DNS servers on all adapters that are still under consideration and waits eight seconds for a response.*

If the DNS Client service receives a positive response, it stops querying for the name, adds the response to the cache and returns the response to the client.

If the DNS Client service has not received a response from any server within eight seconds, the DNS Client service responds with a time-out. Also, if it has not received a response from any DNS server on a specified adapter, then for the next 30 seconds, the DNS Client service responds to all queries destined for servers on that adapter with a time-out and does not query those servers. Only computers running Windows 2000 or Windows Server 2003 return this time-out.

If at any point the DNS Client service receives a negative response from a server, it removes every server on that adapter from consideration during this search. For example, if in step 2, the first server on Alternate Adapter A gave a negative response, the DNS Client service would not send the query to any other server on the list for Alternate Adapter A.

The DNS Client service keeps track of which servers answer name queries more quickly, and it moves servers up or down on the list based on how quickly they reply to name queries.

Note especially that "if at any point the DNS Client service receives a negative response from a server it removes every server on that adapter from consideration……and [will] not send the query to any other server on the list." In other words, recursion is the responsibility of the DNS server, not the client. If a client receives a negative response from a server, it assumes that negative response is complete. The purpose then for the alternate DNS server entry is in case the client receives no response at all from the primary DNS server.

Therefore it is important that the DNS client is configured to point to an internal DNS server or a set of internal DNS servers. **No pc that is a member of a domain should ever point its dns client directly to an external DNS server, even as an alternate.**

Recursion

How, then, does a host/client PC resolve an external domain name (i.e., a website or email address) to its IP address? The answer is, the properly configured internal DNS server does the lookup work for the client. This process is called recursion. When a DNS server receives a request for name resolution, it checks things in the following order:

1. Does the server itself host this domain's zone file? If it does, it resolves the name to a number and returns an "authoritative response" to the client.
2. If the server does not host this domain's zone file, it checks the cache to see if this request was recently resolved. If it finds the result in cache, it resolves the name to a number and returns a "non-authoritative response" to the client.
3. If the server does not contain the result in its cache, it passes the request to upstream DNS servers that will know the answer (recursion). This is done utilizing either predefined "Root Hint" servers, or custom defined "forwarders". Once it receives a response from either the Root Hint servers or the Forwarder it returns a non-authoritative response to the client and places the result in its cache for future reference.
    a. Note that in Windows 2003 (and earlier) servers, the use of DNS forwarders excludes the use of the Root Hint servers. Thus in these situations, great caution should be used in selecting a forwarder or set of forwarder servers. Selection of un-reliable forwarder servers will adversely affect Internet name resolution.
    b. Windows 2008 Server can be configured to use Root Hints, should the forwarder(s) fail to respond. Given the often faster response time of the more local forwarder server, and the local server's ability to fail over to root hint servers; DNS server Forwards are recommended in Windows 2008 server.

Domain Subfolders

In a properly configured active directory DNS zone, four domain subfolders will appear. Each of these subfolders will begin with an underscore. They are as follows:

_msdcs

_sites

_tcp

_udp

The underlying domain structure is revealed within these subfolders. They contain records that identify mission critical domain information like: Domain Controllers, LDAP Servers, Global Catalog Servers, and Kerberos Servers. Without this information, network replication, authentication, and resource lookup will be hindered and possibly fail.

Refer to Microsoft KB article Q310568 should any or all of these domain folders be missing.

Dynamic Updates

The General tab of the properties on the domain zone contains the option to configure dynamic updates. The choices here include "none", "non-secure and secure", and "secure only". This option works in conjunction with a setting on the host/client to register the client PC's name and IP address within the domain zone.

Certain procedures within BS&A Software applications require MSDTC communication from the server back to the PC. It is therefore recommended that dynamic updates (either secured or not) be allowed to facilitate the server's ability to communicate with the client PC.

The reason there is an option to secure dynamic updates is due to the possibility of rogue injection of inaccurate data. Generally, if incoming dns traffic is blocked at the firewall, securing dynamic update traffic is unnecessary.

Reverse DNS

Finally, a properly configured DNS server will have associated reverse DNS zones. These zones allow for the resolution of IP addresses back to fully qualified domain names. While this is not directly required for the proper functioning of BS&A Software's .NET suite of applications, it does help in the overall troubleshooting and functionality of the network.

With Reverse DNS configured, monitoring tools and various other applications can more easily return machine names in their logs as opposed to IP addresses.

Conclusion

The single biggest thing that can be done to prepare a network for the BS&A suite of applications is to ensure proper name resolution both from the PC to the server and from the server to the PC. Host files will not suffice. These applications use components like MSDTC that make DNS specific calls. Having a proper DNS configuration is critical to this; its importance cannot be overstated.

Dan Eggleston is the director of I.T. Right, a mid-Michigan based I.T. consulting firm that specializes in installing, configuring, and managing I.T. infrastructure for local government. In addition to consulting with over 200 local government customers, I.T. Right has been the I.T. consulting arm for BS&A Software for well over ten years.