Troubleshooting DNS Problems in an Exchange Environment, Part 2

Contributed by David Noel-Davies

In a previous article I explained that the health of your DNS operations is crucial to the health of your Exchange environment. I covered two types of DNS problems that affect Exchange: connectivity between Exchange servers and DNS servers, and performance of DNS servers. In this article, I explain the importance of DNS server integrity, including zone integrity, Active Directory (AD) DNS, and name resolution. Note that before you can troubleshoot DNS, you must validate connectivity to your DNS service.

Zone Integrity

Zone integrity refers to how well the DNS zone is structured so that it complies with DNS standards and can properly support DNS clients such as Exchange servers. This integrity has little to do with the zone’s AD-related components but instead focuses on the zone’s overall makeup. In other words, does the zone violate any rules that are crucial to a healthy Exchange environment? You should perform zone integrity tests against every DNS server that every Exchange server in your organization uses. You might have zones on your DNS servers that your Exchange servers don’t rely on directly. Ideally, all your DNS zones should meet similar standards to ensure that they’re properly designed for optimal performance and stability in your Exchange environment, in case you end up using those zones if you need to deliver mail to those domains. For the purposes of this article, let’s assume that the zone Exchange depends on exists and is loaded. The zone that Exchange depends on is its own AD DNS zone. At this point, we won’t worry about how this zone integrates with AD. The requirements that Exchange has for the DNS zone it uses are minimal. Validating a zone’s integrity is a fairly simple task. Simple response. The first thing your DNS server must do when queried is respond. Responsiveness is a prerequisite for checking the zone data. If your DNS server can’t respond to simple queries, then you can’t successfully examine the zone. In Windows, these tests are found on the Monitoring tab of the DNS server properties in DNS Management. Forward zones. The forward lookup zone resolves host names for the domain. The forward zone is more important than the reverse zone for Exchange. In fact, the forward zone is required, whereas the reverse zone is optional. Three simple items should be validated in the forward lookup zone:

- There should be an A record for every Exchange server.
- There should be no unusual Time to Live (TTL) values on the A records.
- Each A record for an Exchange server should be valid. These three requirements sound simple enough, but validating them can often be tricky or time consuming. First, every Exchange server must have an A record. If records are missing, mail delivery will fail and servers will be unable to locate one another. A couple of options exist for validating the presence of A records. One simple method is to log on to your DNS servers, open the DNS administration tool (dnsmgmt.msc), and locate the records for your Exchange servers in DNS. Another option is to use Nslookup. From the command line, you enter a lookup in the following format: nslookup -querytype=A <ServerFQDN> <TargetDNSServer>For example, entering nslookup -querytype=A nycexch1.mycompany.com 10.1.0.11 would perform a lookup of the A record for nycexch1.mycompany.com against the 10.1.0.11 DNS server. This method lets you quickly check all of your DNS servers for valid records of your Exchange servers. If you’re adventurous, you could write a script that extracts a list of Exchange servers and DNS servers from AD and runs a loop that looks up each Exchange server against each DNS server. Third-party products from various vendors are also available that verify A records as part of their regular Exchange health checks. Second, unusually high or low TTL values can cause excessive activity on a DNS server that can affect performance, or can prevent proper maintenance of records for accuracy. Before you change the TTL value, you must understand the effect of doing so. TTL is the amount of time a record remains in the DNS cache before it’s looked up again from the authoritative DNS server. Caching DNS records is often useful for performance so that a DNS server can return “common” queries to users without having to retrieve the record several times in a row. For example, if several users go to http://www.msexchangelibrary.com, the DNS server looks up this record once, then caches the value for however long it’s allowed. Many IT professionals believe that setting a low TTL value will speed up propagation of DNS record changes—especially Internet DNS changes. However, most people don’t realize that some DNS providers override this setting and cache records for an amount of time they deem appropriate for their user base. Setting an unusually low TTL can cause performance problems because DNS servers are forced to refresh records more often than necessary. In addition, this practice might be ineffective for Internet-facing DNS. The default TTL on a Windows DNS server is 15 minutes, which means that the DNS server will cache the record for 15 minutes before requesting a refreshed record from the authoritative DNS server that provided the record. You can use the DNS administration tool (dnsmgmt.msc) to look up a record’s TTL, just as for an A record. You can also perform a lookup through the command line, although scripting the command and parsing the output is more of a challenge. To use the command line to look up a record’s TTL, add the debug option to the command: nslookup -debug -querytype=A <ServerFQDN> <DNSServer>The resulting output will tell you the TTL for a particular server’s record (which can be useful if you want to know how long your favorite DNS server will cache your records). In addition, the TTL output provided by Nslookup in debug mode will tell you when WINS resolution (which I discuss later in the article) is the source of the lookup for a particular record. Third-party products exist that examine TTL as part of their environment health checks, although many Exchange-oriented products might overlook TTL. Third, each Exchange server’s A record must be valid. Ensuring the validity of each record can be time consuming and difficult, but doing so is crucial. This becomes especially difficult when the server is multi-homed or has multiple IP addresses assigned to the same NIC. If your server has multiple IP addresses, knowing on which IP address your Exchange server is listening will help you know which IP address should be registered in DNS. For example, you might have set your SMTP virtual server to listen on a specific IP address instead of All Addresses. If your server is

listening on a specific IP address, you must ensure that other machines use the correct IP address to contact your server and that this address is registered in DNS. In addition, it’s also important to make sure that other host records (i.e., A records) that are pointed to an Exchange server IP address are valid and expected. You might also need to know on which IP address your server is sending mail. To easily check the address, look at the headers of messages that have already passed through your Exchange server. Typically, a multi-homed server has only one gateway, which can also help you determine which IP address is used when mail is sent. This doesn’t mean that an interface without a gateway would never be used to route IP traffic (including mail). An interface without a gateway would be used if the destination were on the same subnet as that interface and the other interfaces were on different subnets or the other interfaces were lower in the binding order than the interface in question when multiple interfaces are on the same subnet. You can check your binding order by viewing Network Connections and examining the Advanced menu’s Advanced Settings option. Another method for determining IP traffic flow is to run the route print command from the command line. This is especially important when you have multiple gateways and/or static routes configured. Validating Exchange server A records quickly and efficiently is a challenge. Although you can certainly use IPconfig to obtain a server’s IP addresses, you must log on to each server or use a tool such as the Microsoft Windows Server Resource Kit’s Remote Command service. As an alternative, you can gather this information from Windows Management Instrumentation (WMI), which you can run against remote and local servers. To query only the IP addresses for all interfaces on a server, go to the command line and enter wmic nicconfig get ipaddressInserting the option /node:server lets you point to a remote machine. For example, entering the command wmic /node:NYCEXCH1 nicconfig get ipaddress returns the IP addresses on the NYCEXCH1 server’s interfaces. Troubleshooting forward zones involves examining the Name Server (NS) record. You need to know which servers are “supposed” to be authoritative for the zone. Begin by verifying that the proper servers are assigned as NS servers, then evaluate individual records as necessary. Reverse zones. Reverse zones are handled in much in the same way as forward zones. As I mentioned previously, reverse zones are optional from an Exchange perspective—however, they should be configured properly if used. If you have a reverse zone, ensure that every Exchange server has a PTR record, no unusual TTL values exist on PTR records, and each PTR record is valid. In addition, avoid using Canonical Names (CNAMEs) with PTR records. The reasons for these recommendations are similar to those for the forward zone as well. However, because the reverse zone is optional, these recommendations are more for accuracy of data and performance of the DNS server than to prevent specific Exchange problems. Like forward zones, troubleshooting reverse zones involves examining the NS record. Knowing which servers are “supposed” to be authoritative for the zone is important. Begin by verifying that the proper servers are assigned as NS servers, then evaluate individual records as necessary. You can use the same techniques as for forward zones to validate these records. Start with the DNS administration tool (dnsmgmt.msc). If you prefer to use Nslookup from the command line instead, remember to set querytype as PTR rather than A, and use the IP address rather than the server name to target the reverse record. For example, entering nslookup -querytype=PTR 10.1.0.100 dns1.mycompany.com at the command line performs a reverse lookup of the IP address 10.1.0.100 against the DNS server dns1.mycompany.com. MX record. Many administrators don’t realize that MX records aren’t required for Exchange to function internally. MX records are required on Internet-facing DNS servers for your Exchange organization to ensure that mail is delivered to it, but Exchange doesn’t rely on MX records internally for delivery of mail or anything else. If MX records are present for domains that Exchange isn’t responsible for, they’ll be used by Exchange for delivery of mail to those external domains. However, Exchange won’t rely on MX records for delivery of mail within the Exchange organization. To determine which domains Exchange is “responsible” for, examine your recipient policies within the Exchange System Manager. If MX records are used, the following guidelines should be observed:

- The same server shouldn’t be used more than once with a different MX priority.
- The target of the MX record should be resolvable.
- The target of the MX record shouldn’t be a CNAME. Again, because Exchange doesn’t rely on MX records for proper operation, validate your MX records to ensure a properly designed zone. Listing a server multiple times with different priorities does nothing to enhance mail delivery or reliability—it only bogs down the mail delivery process by forcing mail servers to try a down server multiple times instead of going to the next potentially working alternate. Mail delivery will be retried regardless of the MX record configuration and depends on the sending server’s settings. The MX record needs to be resolvable, to ensure mail delivery to a given domain. An administrator can easily enter an invalid host name for the MX record. Finally, using a CNAME as the MX target isn’t advisable, because of compatibility issues with various mail systems and standards as defined in the Request for Comments. RFC 1035 describes DNS records in detail. Other problems to avoid. Several additional components of a DNS zone are relevant to ensuring a good design. Although the following aren’t necessarily related to Exchange, any DNS zone issue that causes performance or stability problems will also ultimately affect Exchange, as well as any other application that relies on DNS.
- CNAME chains—Pointing a CNAME to another CNAME isn’t advisable.
- CNAME loops—A CNAME chain that eventually loops back to the original CNAME will cause performance problems.
- Irresolvable CNAMEs—CNAMEs are often not validated and can be used in various places even if not resolvable.
- Duplicates—Duplicates of certain records (e.g., CNAMES) aren’t appropriate because there’s no additional functionality (e.g., round robin for A records)
- Out-of-sync zones—Out-of-sync zones can cause name resolution problems.
- Nonfunctional NS/Start of Authority (SOA): A zone must have a functional and existingNS and SOA record.

- Improper CNAME use—CNAMEs shouldn’t be used improperly (e.g., on MX, NS, or SOA records).
Detecting general DNS problems can be challenging, especially in larger environments. Although you can use the DNS administration tool (dnsmgmt.msc) to visually inspect your zones, using scripts or third-party tools is ideal. Using Nslookup in debug mode (i.e., nslookup -debug DNSrecord) is also helpful for troubleshooting DNS problems. If your zone conforms to best practices in design, you’ll avoid many DNS problems. To ensure that your zone complies with best practices, you must examine the zone as a whole (not just the parts relevant to Exchange). DNS configurations that aren’t directly related to Exchange are beyond the scope of this article. To find Microsoft resources (e.g., white papers, tools) for general DNS troubleshooting and configuration problems, go to the Microsoft Windows 2000 Domain Name System (DNS) Center Web site and Microsoft’s DNS Technical Library, at the Windows Server 2003 Domain Name System (DNS) Web site Active Directory DNS
How well DNS supports your Exchange environment depends most directly on the presence and validity of the AD components in the zone. Exchange requires AD, and both AD and Exchange require DNS that’s capable of supporting their needs. For this reason, only specific versions of DNS are considered compatible with AD deployments. Without the crucial AD-integrated components found in a properly configured DNS, Exchange can’t operate properly. The AD-related records help Exchange locate essential resources for operation. Requirements. A few basic requirements absolutely must be met in order for a DNS zone to support AD. SRV records in DNS help servers (e.g., Exchange servers) locate other servers that provide specific services. An SRV record is specific to a provided service. Several types of SRV records exist. Common SRV records include AD-related ones (type PDC, GC, etc.); however, there are services such as IM that use their own SRV records in DNS (e.g., _sip._tls.domain.com) to advertise the server to use for secure IM, for example.The most basic requirements are
- Only one PDC SRV record can exist per domain.
- At least one Global Catalog (GC) SRV record must exist per forest.
- At least one GCIPAddress record must exist per forest.
- At least one Key Distribution Center (KDC) SRV record must exist per domain. The requirement for a single PDC SRV record in a domain comes from the PDC emulator role. This requirement lets servers locate the server that holds the PDC emulator role, which is crucial for domain functions such as time synchronization. This function is critical to all domain members and can exist on only one server per domain. The requirement for at least oneGC SRV record per domain is directly related to Exchange. Exchange relies on GC servers for directory information. The GC is a subset of attributes in the domain that are most relevant to Exchange; as such, it contains information for all domains in the forest and provides Exchange a full “view” of the organization. The GCIPAddress record helps Exchange locate the GC. A GCIPAddress record and a GC SRV record should exist for every GC server. The KDC SRV record is essential so that servers can locate a server advertising Kerberos for security. The availability of Kerberos is also important for Exchange to function properly. Several other records are also essential for Exchange. Because Exchange depends on domain controllers (DCs), being able to locate DCs is imperative. Exchange uses DNS to locate these servers, some of which are GC servers or are advertising Kerberos. In addition, Exchange uses DNS to determine whether records exist for the LDAP services these servers offer. An LDAP SRV record must exist for the server, site, and GUID. Various services use these LDAP SRV records to locate the servers that advertise Kerberos or are GC servers. DNS is crucial not only to Exchange but also to your entire environment. For example, because desktops also use Kerberos, a “slow logon” might be caused by a client machine not having DNS configured properly with the records that are necessary for the client to use Kerberos to log on—which results in a timeout looking for the services. SRV records. SRV records are critical to Exchange. There are several requirements for SRV records. Specific requirements depend on the type of SRV record. All SRV records must
- have a valid A record for the SRV pointer
- A PDC SRV record must
- have an associated DC account
- refer to the PDC Flexible Single-Master Operation (FSMO) role holder
- A GC SRV record must
- have an associated DC account
- have a valid GCIPAddress record
- be defined in AD as a GC
- advertise as a GC
- A Kerberos SRV record must
- be in the correct domain
- have an associated DC account
- be advertising Kerberos Authority and replication. An obvious but important requirement of a DNS server that’s responsible for a zone is that it knows it’s authoritative. Detecting problems such as lame delegation is crucial to ensuring a domain’s health. Lame delegation is when a server is mistakenly listed as an authority for a zone. Queries passed to that server will fail. If authority is misconfigured, not only might resolution be affected, but so will replication and eventually the entire zone’s integrity. Microsoft provides tools such as DNSLint that can assist with detecting problems like lame delegation. DNSLint has several commands that are specific to mail environments and provides switches to test connectivity to SMTP, POP, and IMAP as well. For more information about DNSLint or to download the utility, see the Microsoft article “Description of the DNSLint utility” (http://support.microsoft.com/kb/321045). Replication of DNS zones depends directly on the type of zone and the configured scope. AD-integrated zones offer a unique advantage in that they can be multi-master. That is, each server maintains a writeable copy of the zone. The more “traditional” standard primary/secondary approach

means that only one server is writeable—all other servers are secondary. AD-integrated zones can replicate to all DCs in the forest or domain as necessary. When running AD-integrated zones, the most important thing to ensure is that the zones are set to boot from AD in the registry. Although this setting is the default, it’s a good place to start when troubleshooting replication problems. To verify this setting, use the DNS administration tool (dnsmgmt.msc) and look at your DNS server’s properties. On the Advanced tab, set the Load zone data on startup option to From Active Directory and registry. Troubleshooting. To troubleshoot AD-integration DNS problems, you must first determine the type of problem that exists. A good place to start is to verify that the environment meets the minimum requirements for AD—that is, only one PDC SRV record per domain, at least one GC SRV record per forest, etc. Next, verify that the other basic requirements are met for each SRV record type. You can then focus your efforts depending on the type of problem. With respect to SRV records, understanding the importance of each record type and knowing its function will help you determine which records are relevant to an issue. For example, if you’re troubleshooting Kerberos issues, you should investigate the specific Kerberos SRV records, their associated DCs, and validation of advertised Kerberos services. If the problem is an overall domain delegation or authority issue, using a tool such as DNSLint will quickly identify it. Simple checks such as verifying that the zone is present on the server and that it’s set to boot from AD in the registry (for AD-integrated zones) can save a lot of time when you’re working on a problem related to replication or zone authority. Name Resolution

Name resolution problems are perhaps the most common that you’ll encounter. However, troubleshooting name resolution is fairly straightforward. Understanding name resolution depends directly on knowing when specific types of name resolution are required. That is, at times only internal name resolution is required; at other times name resolution outside of the DNS server’s authority is required. In addition, you need to understand how and when a DNS server responds to requests instead of passing them on to another server. Order of resolution. Understanding the order in which name resolution occurs is helpful in knowing why you aren’t getting the expected responses for queries. A server makes a request for name resolution in the following order (depending on the perspective of the request). Typically, the HOSTS file on the local machine takes precedence. This file is located at C:\Windows\system32\drivers\etc. If you defined some host-to-IP mapping in the HOSTS file in this location, it will take precedence over all else. This doesn’t mean that if you query a DNS server with a HOSTS file configured that you’ll get responses from its HOSTS file. Machines use only their own HOSTS files for name resolution. If a HOSTS file doesn’t define name resolution for the requested record, then DNS is used. However, if we consider WINS, things can get a bit complicated. Let’s examine two specific cases. If a Fully Qualified Domain Name (FQDN) is used, then WINS plays no additional role in name resolution. The name resolution happens as I already described. However, things change if a host name only is used. Depending on the mode that NetBIOS is running in (B, P, M, H)the order might change slightly—but DNS is always last. Although WINS and broadcasts are outside the scope of this article, you need to understand that WINS, LMHOSTS, and HOSTS files can play a role in name resolution. If you’re getting unexpected name resolution that you can’t query directly from DNS, one of these three is likely the source. As I mentioned previously, using Nslookup in debug mode can help determine whether your name resolution results are coming from WINS. However, there’s a difference between the name resolution you get from using ping (which uses all available methods, including querying local files such as HOSTS and LMHOSTS) and the name resolution you get from using Nslookup directly. If Nslookup yields the results you expect but a ping gives you different results, then the incorrect name resolution is likely caused by a local configuration. The Microsoft article “Verify WINS as the source for answering a DNS query” outlines the steps necessary to tell whether WINS is answering a DNS request. Hosts and zones. By far the most important requirement is that all Exchange servers are resolvable by all other Exchange servers. This means that every DNS server used by any of your Exchange servers should be able to resolve every Exchange server in the organization. This requirement is absolute. If a problem occurs in resolving an Exchange server name, you need to know the type of zones that are hosted on the server and where the zone of authority for that particular Exchange server exists. Depending on its configuration, the zone might be a stub zone or a delegation zone, have forwarders to another DNS server, or rely on WINS forwarding for name resolution. When evaluating the requirement for internal host resolution, you’d expect to be able to locate the authoritative servers for the zones within the environment. But when you’re dealing with external name resolution, you don’t expect to find authoritative servers. Another benefit is if all the servers resolve not only by FQDN but also by NetBIOS name. As long as you configure the proper DNS suffixes and search orders, DNS can provide resolution for NetBIOS names. Connectors. Connectors are required when users want to send mail outside of their Exchange organization. Exchange connectors have a different DNS requirement. Depending on the type of connector, it might require external as well as internal name resolution. SMTP connectors that deliver mail to the Internet must be able to resolve domains, MX records, and hosts outside of the local DNS server’s authority. Thus, the DNS server that’s used by the servers hosting these connectors has extra requirements. Not all Exchange servers require Internet resolution. This requirement is important only for DNS servers used by an Exchange server that’s assigned to an SMTP connector for the default (*) address space (when an SMTP connector is present in the organization). If no SMTP connector is present for the default address space, then all DNS servers used by all Exchange servers potentially require the ability to resolve Internet hosts if a user on a particular Exchange server wants to send mail to someone outside of the organization. Troubleshooting. When troubleshooting name resolution, always begin by querying DNS directly. This action helps to identify exactly what DNS is resolving. If the result is different from another method’s results (e.g., ping), then another type of name resolution is likely overriding DNS resolution (e.g., a hosts file, WINS). However, WINS can still be involved even if you query DNS directly. You can set DNS to use WINS forwarding for resolution. Depending on your setup, you might want to ensure that no invalid WINS records exist for your Exchange servers. Exchange doesn’t require WINS to function, but if you use WINS, you need to ensure that

your records are in sync. An excellent tool to use for DNS troubleshooting is Nslookup, which can tell you where name resolution is originating. You can troubleshoot everything from A records to MX records or SRV records. You simply need to specify the type of record you want to query. To query SRV records, run the command set type=srvTo determine why mail is queuing to a remote host, with a “host not found” error message, run the command set type=mxThis command will look up the MX record for a particular domain, then verify that the defined MX host exists as an A record. You’ll encounter different types of zones as you evaluate the source of DNS resolution. Stub zones, delegation zones, and standard zones all have authoritative servers. Master records must be present, and servers must be reachable and responding. This requirement is especially important for stub and delegation zones because they don’t exist on the server. If the zone for a DNS server used by a connector that requires Internet resolution isn’t present on the server (which it shouldn’t be), then the server will try to resolve the record in one of several ways. If the server has the root (.) zone, then it will attempt to resolve every Internet query because it believes it’s authoritative for the Internet. A server that’s actually expected to resolve Internet queries shouldn’t have this zone. If forwarders are configured, the server will forward all requests for domains it isn’t authoritative for to an external server defined as a forwarder. This server must be able to resolve the Internet host on behalf of the server. The target forwarder must in turn not have the root zone. The server that ultimately performs name resolution within an organization will have a forwarder to a server outside of the domain that can provide name resolution or have root hints present, as well as the ability to access the Internet on port 53 UDP to reach the root servers. If all of these conditions aren’t met, name resolution won’t occur. So, if the DNS server has a forwarder configured, the target forwarder (or its target, or its target’s target, etc.) must not have the root zone, must have root hints present, and must be able to get to the root Internet servers on port 53 UDP. If no forwarders are configured on the server, then the server itself must lack the root zone, must have root hints, and must have the ability to get to the Internet on port 53 UDP. DNS Checkup

DNS is arguably the most mission-critical service in an AD and Exchange environment. A healthy DNS is the first step toward ensuring a healthy infrastructure. Often the first place you should look when experience problems with both Exchange and AD is DNS. If you understand how DNS works and you’re aware of your Exchange server requirements, troubleshooting DNS problems can be fairly simple. Taking a methodical and calculated approach to DNS troubleshooting lets you easily diagnose and resolve just about any DNS problem.