Using SMTPDIAG to Diagnose Exchange 2003 Related SMTP and DNS Problems

Contributed by David Noel-Davies

This article will give you some information about how to use SMTPDiag. SMTPDiag is a diagnostic tool that is used to determine if Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) are configured to reliably deliver mail to an external e-mail address.
InstallationFirst we need to download the SMTPDIAG tool here. The download size is only 378 KB. After downloading, simply extract the download file. Now vou can use SMTPDIAG.System RequirementsSupported Operating Systems: Windows 2000, Windows Server 2003
Supported Exchange Systems: Exchange Server 2000 or Exchange Server 2003.SmtpDiag is a troubleshooting tool designed to work directly on a Windows server with IIS/SMTP service enabled or with Exchange Server installed. It utilizes the same APIs as Windows and Exchange in order to diagnose configuration and connection issues involving SMTP and DNS.SMTPDiag has two required and two optional arguments, and a built-in Help.Let's goSMTPDIAG has a simple syntax as shown in the following example.SMTPDIAG "sender address" "recipient address" [-d target DNS] [/v]SMTPDIAG syntax
Figure 1: SMTPDIAG syntaxArgumentFunctionsender addressA required argument. This is the address of the local mailbox on Exchange. This argument is used to verify SMTP transmission and to check inbound DNSrecipient addressA required argument. This is the address of the destination mailbox on a foreign mail system. This argument is used to verify DNS and the availability of the destination mailbox-d target DNSThis parameter is optional. You can specify the IP address of the target DNS server to use to look up remote MX records. This is often configured as an external DNS server in Exchange. You can configure an external DNS at the Exchange virtual server level but not for the Internet Information Services SMTP service/vThis parameter is optional and it displays additional information about each test/? This parameter displays the help for using SMTPDIAG-d target DNS ArgumentYou can specify an external DNS Server in the Exchange System Manager.
Figure 2: Specify external DNS ServerTestsSMTPDiag issues DNS queries using UDP and TCP to validate that the queries will succeed. Note:
Windows versions before Windows Server 2003 and Windows XP didn’t support UDP queries. If TCP queries fail, mail delivery will not successfull.SMTPDIAG sequence
- Verifying Syntax
- Check the SOA record for the remote address domain
- Validate that the local domain MX and A records are resolvable (This test could fail if the domain is not reachable because of a firewall. In this case, the remote domain MX/A records will be checked too. If this check fails, the problem could consist of a DNS infrastructure problem)
- DNS records will be queried. When successfull, SMTPDIAG tries to connect to all the MX records that were published for the remote and try to send an …
- EHLO
- Mail from
- RCPT TO and
- Quit commandYou can use SMTPDIAG with the /V argument. This provides more information for every argument.Examples
Figure 3: SMTPDIAG exampleWhat do we see here?
- White text indicates action being taken.
- Gray indicates informational results.
- Green indicates a successful test result.
- Red indicates a failed test result. Want to see more?Start SMTPDIAG with the same arguments as shown in Figure 1 but end the command with the /V argument:Searching for Exchange external DNS settings.
Computer name is LONDON.
VSI 1 has the following external DNS servers:
There are no external DNS servers configured.Checking SOA for it-training-grote.de.
Checking external DNS servers.
Checking internal DNS servers.Checking TCP/UDP SOA serial number using DNS server [192.9.200.113].
TCP test succeeded.
UDP test succeeded.
Serial number: 2004122525
SOA serial number match: Passed.Checking local domain records.
Starting TCP and UDP DNS queries for the local domain. This test will try to validate that DNS is set up correctly for inbound mail. This test can fail for 3 reasons.
1) Local domain is not set up in DNS. Inbound mail cannot be routed to local mailboxes.
2) Firewall blocks TCP/UDP DNS queries. This will not affect inbound mail, but will affect outbound mail.
3) Internal DNS is unaware of external DNS settings. This is a valid configuration for certain topologies.
Checking MX records using TCP: nwtraders.msft.
A: nwtraders.msft [192.9.200.113]
Checking MX records using UDP: nwtraders.msft.
A: nwtraders.msft [192.9.200.113]
Both TCP and UDP queries succeeded. Local DNS test passed.Checking remote domain records.

Starting TCP and UDP DNS queries for the remote domain. This test will try to validate that DNS is set up correctly for outbound mail. This test can fail for 3 reasons.
1) Firewall blocks TCP/UDP queries which will block outbound mail. Windows 2000/NT Server requires TCP DNS queries. Windows Server 2003 will use UDP queries first, then fall back to TCP queries.
2) Internal DNS does not know how to query external domains. You must either use an external DNS server or configure DNS server to query external domains.
3) Remote domain does not exist. Failure is expected.
Checking MX records using TCP: it-training-grote.de.
MX: mailin.webmailer.de (10)
A: mailin.webmailer.de [192.67.198.37]
A: mailin.webmailer.de [192.67.198.48]
A: mailin.webmailer.de [192.67.198.32]
Checking MX records using UDP: it-training-grote.de.
MX: mailin.webmailer.de (10)
Both TCP and UDP queries succeeded. Remote DNS test passed.Checking MX servers listed for grotem@it-training-grote.de.
Connecting to mailin.webmailer.de [192.67.198.32] on port 25.
Received:
220 mailin.webmailer.de ESMTP Sendmail 8.13.1/8.13.1; Sat, 25 Dec 2004 09:37:58 +0100 (MET)Sent:
ehlo nwtraders.msftReceived:
250-mailin.webmailer.de Hello I89ae.i.pppool.de [85.73.137.174], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250 HELPSent:
mail from: <administrator@nwtraders.msft>Received:
250 2.1.0 <administrator@nwtraders.msft>... Sender okSent:
rcpt to: <grotem@it-training-grote.de>Received:
250 2.1.5 <grotem@it-training-grote.de>... Recipient okSent:
quitReceived:
221 2.0.0 mailin.webmailer.de closing connectionSuccessfully connected to mailin.webmailer.de.
Connecting to mailin.webmailer.de [192.67.198.48] on port 25.
Received:
220 mailin.webmailer.de ESMTP Sendmail 8.13.1/8.13.1; Sat, 25 Dec 2004 09:38:00 +0100 (MET)Sent:
ehlo nwtraders.msftReceived:
250-mailin.webmailer.de Hello I89ae.i.pppool.de [85.73.137.174], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250 HELPSent:
mail from: <administrator@nwtraders.msft>Received:
250 2.1.0 <administrator@nwtraders.msft>... Sender okSent:
rcpt to: <grotem@it-training-grote.de>Received:
250 2.1.5 <grotem@it-training-grote.de>... Recipient okSent:
quitReceived:
221 2.0.0 mailin.webmailer.de closing connectionSuccessfully connected to mailin.webmailer.de.
Connecting to mailin.webmailer.de [192.67.198.37] on port 25.
Received:
220 mailin.webmailer.de ESMTP Sendmail 8.13.1/8.13.1; Sat, 25 Dec 2004 09:38:01 +0100 (MET)Sent:
ehlo nwtraders.msftReceived:
250-mailin.webmailer.de Hello I89ae.i.pppool.de [85.73.137.174], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250 HELPSent:
mail from: <administrator@nwtraders.msft>Received:
250 2.1.0 <administrator@nwtraders.msft>... Sender okSent:
rcpt to: <grotem@it-training-grote.de>Received:
250 2.1.5 <grotem@it-training-grote.de>... Recipient okSent:

quitReceived:
221 2.0.0 mailin.webmailer.de closing connectionSuccessfully connected to mailin.webmailer.de.ConclusionSMTPDIAG is a great tool to determine SMTP and DNS problems in your Exchange organization. I like this tool because it sees the SMTP Message Flow like the two core components IIS and Exchange.Related LinksDownload Link for SMTPAdmin http://www.microsoft.com/downloads/details.aspx?familyid=bc1881c7-925d-4a29-bd42-71e8563c80a9&displaylang=enHow To Configure the SMTP Connector to Link to Internet Domains in Exchange http://support.microsoft.com/?kbid=319426Telnet to Port 25 to Test SMTP Communication http://support.microsoft.com/?kbid=153119How to obtain Internet Mail Exchanger records with the Nslookup.exe Utility http://support.microsoft.com/?kbid=203204