Troubleshooting Mail Flow Issues with Exchange 2010

Troubleshooting Inbound Mail Issues:

Cause 0: Reboot. If Exchange tries to start before any Domain Controllers are fully up and running, such as after power loss to a site, then the transport services will fail. Rebooting the Exchange Server takes care of this.

Cause 1: Disk Space:

The most common reasons for inbound mail failing is that of disk space. Before doing anything, check the space on the drives. If it falls below 3 GB on the system drive or on the drive that holds the transaction logs and/or databases, then Exchange will stop receiving mail.

If the issue is a system partition that is getting close to full, free up space as necessary and reboot. Then test to see if the problem is resolved.

If the issue is that of transaction logs, then it is important that you do NOT delete these files manually. Instead, take an offline backup of the Exchange Databases and Transaction Logs, then enable circular logging on the mail databases. You will need to unmount and remount your databases after enabling this for it to take effect. Once the space has been cleared up (which does not take long,) turn off circular logging and unmount/remount the database.

Cause 2: Troubleshooting Connectivity to the Receive Connector

Install the Telnet client through Server Manager's Features section. Open a command prompt and test with the following, substituting your server's EXTERNAL IP address for the one below:

telnet 170.211.108.2 25

Notice any error messages, such as connection refused. You may have to add your server's IP address to the accepted servers on the Receive connector, then disable and re-enable it. If this works, then test it from an outside connection.

If you get a HELO prompt from inside the server, but not outside, then firewalls or the connection from the server to the router are suspect.

Cause 3: Other Errors

If there are bounce messages when outside senders attempt to mail you, then it is important to get copies of these forwarded to you at an outside address. While some will spell out the exact

nature of the error, others will be at best cryptic. In the latter case, you are looking for two pieces of information: The server reporting it and the SMTP error message.

EXAMPLE OF AN SMTP ERROR MESSAGE
Diagnostic information for administrators: Generating server: mail.myschooldistrict.local Jack.Ryan@mysd.k12.ar.us #554 5.4.4 SMTPSEND.DNS.MxLoopback; DNS records for this domain are configured in a loop ##

This example indicates that the MX records for a multi-domained server is pointing to one another, which doesn't give the mail a clear idea of its destination. That indicates a problem with DNS.

This means that the sender's domain is being blocked by your mailserver:

Generating server: mail.myschooldistrict.local

#5.5.0 smtp;553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)

COMMON SMTP ERROR CODES AND THEIR RESOLUTION	
421 Service Not Available	Receive Connector is trying to perform a shutdown
451 4.7.1 This server is currently unavailable	Sender's address is graylisted by AntiSpam
552 Mail action aborted/Storage Allocation	Recipient has exceeded storage quotas
554 Transaction Failed	Vague, usually has additional information
550 5.7.1 Unauthorized Mail Prohibited	Check your site's SPF record
550 failed to meet SPF requirements	Check your site's SPF record
550 5.4.1 Relay Access Denied	Check Send Connector and Accepted Domains

Finally, if using any antispam features, try disabling the filtering components, one by one, until the problem disappears. When the problem does disappear, you may have to modify the last component that was disabled.

Troubleshooting Outbound Mail Issues:

Troubleshooting outbound mail is likewise as easy:

If the mail sends to all but one recipient or domain, try performing a telnet test to that domain from the mailserver. Error codes will be easier to see in a session like this. Instructions for doing so will be at the end of this manual.

If mail does not send outside the local domain at all, then check the following:

- Ensure that the send connector is enabled and that it is configured correctly.
- Ensure that the aggregator, if present, is forwarding all outbound SMTP traffic from the server through the state router. This is a special route that must be set.

- If using an outbound relay like a mail filtering appliance or the state spam relay, try sending a mail via a telnet test to its IP address. Also make sure that the send connector on Exchange is set to relay through the correct address.

If mail will not send out from a single user or small group of users, then again check to ensure that their mailboxes are not over quota. You get a listing of user mailbox sizes by logging into the Exchange Management Shell and issuing the following command (note, do not split the lines):

Get-MailboxDatabase "Your Database Name Here" | Get-MailboxStatistics | Sort totalitemsize –desc | ft displayName, totalItemSize, itemCount > MailboxSizeReport.txt

This will create a text report featuring the users' names and mailbox sizes, sorted by size.

PERFORMING A TELNET TEST:

A telnet test allows you to see verbatim the discussion between your Exchange Server and another mail server (or filtering device). This is incredibly useful for diagnosing flow issues.

> Unless you are doing one against your own exchange server or to an internal filtering device, you will first need to know where to make the connection to. In this case, I prefer following the same procedure that a sending server does—looking up the server by MX. This can be skipped and the IP address used for the telnet connection if you're using your own server or filtering device.
>
> F:\>**nslookup**
>
> Default Server: cm-ark-dc-01.arkgov.net
>
> Address: 170.94.248.16
>
> > **set q=mx**
>
> > **theirdomain.com**
>
> Server: cm-ark-dc-01.arkgov.net
>
> Address: 170.94.248.16
>
> Non-authoritative answer:
>
> theirdomain.com MX preference = 10, mail exchanger = ASPMX.L.GOOGLE.com
>
> theirdomain.com MX preference = 20, mail exchanger = ALT1.ASPMX.L.GOOGLE.com
>
> theirdomain.com MX preference = 30, mail exchanger = ALT2.ASPMX.L.GOOGLE.com
>
> theirdomain.com MX preference = 40, mail exchanger = ASPMX2.GOOGLEMAIL.com

This tells us which servers are accepting mail, sorted by priority (10, 20, 30, 40). Since 10 is the lowest number on the list, it's the highest priority server, which is ASPMX.L.GOOGLE.com. This means if you were to send a mail to Jason@theirdomain.com, the server would choose that address first.

Next, we emulate the mail session. The portions that one would need to type are in bold:

F:\>**telnet aspmx.l.google.com 25**

220 mx.google.com ESMTP ac9si6518163obc.94

ehlo mysd.k12.ar.us

250-mx.google.com at your service, [170.94.253.113]

250-SIZE 35882577

250-8BITMIME

250-STARTTLS

250 ENHANCEDSTATUSCODES

MAIL FROM: Jason.black@mysd.k12.ar.us

250 OK – MAIL FROM Jason.black@mysd.k12.ar.us

RCPT TO: Jason@theirdomain.com notify=success,failure

DATA

354 Send data. End with CRLF.CRLF

Subject: Test Message. //hit ENTER twice

This is a test message.

. //A period on its own line ends the message.

QUIT

221 closing connection

If at any part during this exercise the test fails, jot down the exact error message. These are very sensitive to typos and consequently not very forgiving, so type slowly. Many will not allow for backspaces.