

Presented March 13, 2012 at NYExUG Meeting
Last Updated on March 15, 2012

Troubleshooting Techniques & Tips for Exchange 2010/2007/2003 (HANDS ON)

** throughout presentation indicates additional information on reference page in back of presentation*

Ben Serebin
Ehlo & Network Consultant
REEF Solutions (www.reefsolutions.com)
If you can't get enough Exchange & technology
read my blog <http://blog.reefsolutions.com>

About Ben Serebin

- Working in the IT sector since 1996 (16 years)
- Specialty is Exchange Server, Spam Filtering, DNS, & complex wireless deployments.
 - Recently Completed Projects Q1 2012: Designed & implemented a 3 node cluster of Windows RDS and implementation of VMware resource clustering for load balancing of CPU/Memory/storage.
- Upcoming Fun Projects: Exchange 2007 (single server) to 2010 (HA/LB DAG) Migration, Deploying KVM over IP for cluster of ESXi hosts, iSCSI SAN Storage Expansion Project, & SAN Failover Testing
 - Current Environment: Running Exchange 2010 & 2007 Environment on Windows 2008 & 2008 R2 on 3 node ESXi 4 Cluster with 4 iSCSI based systems, server computing environment is entirely virtual, Blackberry Enterprise Server Express 5. Current “smart” phone is a BlackBerry Bold 9650.

Discussion/Agenda for Presentation

- Common Issues
- Built-in Tools
- Free Add-on Tools
- Helpful Free Websites
- Diving into Troubleshooting

Common Issues

- Email not arriving
- Email not sending
- Outlook disconnected
- Missing Email Message
- Email Slow
- Email Database Offline
- Spammers/RBLs

- Native Tool – **Best Practices Analyzer**
Health Check – good general Exchange & OS overview
Connectivity Test – all Exchange & AD Servers operational
- Native Tool – **Remote Connectivity Analyzer** (aka ExRCA).
Really just a website TestExchangeConnectivity.com
- Native Tool – **Mail Flow Troubleshooter** (lookup error [DSN] codes, Queues, mail flow testing, & poor performance)
- Native Tool – **Message Tracking**
- Native Tool – **Queue Viewer** – reporting queue levels
- Native Tool – **Performance Monitor** – OS PerfMon
- Native Tool – **Task Manager** – memory/cpu
- Native Tool – **Performance Troubleshooter**

Add-On Tools for your Toolbox (Exchange 2010/2007/2003)



- **Exchange Profile Analyzer (ExPA)** - collect statistical information about the Exchange organization that is helpful for understanding the size and makeup of the Exchange data (from mailbox to all servers). No reboot needed. Free from Microsoft.



- **Exchange Server User Monitor (ExMon)** – view and evaluate individual users MAPI connections (connecting IP's, versions, latency for network and processing, etc). Latest Release 12/5/11. Start Menu shortcut not created see Program Files for it. No reboot needed. Free from Microsoft.

Exchange User Monitor for Microsoft Exchange Server: EX-4f5fbe34.etl

File Help

Update Interval (min): 1

By User	By Version	By Clientmon								
User Name	Packets	Operati...	CPU Ti...	CPU (%)	Avg. S...	Max. S...	Bytes In	Bytes Out	Client Versions	Client IP Addresses
	17	50	45	50.00%	3	29	3665	4233	6.0.8244.0 8.3.213.0	10.1.1.26 EX
	27	90	45	50.00%	1	29	8161	17486	6.0.8244.0 14.0.6109.5000 8.3.213.0	10.1.1.26 10.1.1.5 98.113.82.70 EX
	12	0	0	0.00%	0	0	24	1063	6.0.8244.0 14.0.6109.5000	
	1	2	0	0.00%	0	0	22	24	6.0.8244.0	10.1.1.26
	10	23	0	0.00%	0	1	820	1764	8.3.213.0	EX 10.1.1.24
	1	2	0	0.00%	0	0	22	24	6.0.8244.0	10.1.1.26



Add-On Tools for your Toolbox (Exchange 2010/2007/2003)

- **WinDirStat** – quickly find large files/folders (too many transaction logs, large databases, IIS log files, etc). Free open-source application. No reboot needed.



- Remotely Testing Outlook (RPC), ActiveSync, Web Services, Email (smtp) and even Office 365
<https://www.testexchangeconnectivity.com>
- Review DNS Records for Auto Discovery -
<http://centralops.net>
- Review DNS Records for basic MX/A Records –
<http://tools.appriver.com>
- Stress Testing for generating email -
<http://www.icewarp.com/downloads/tools/>
- Checking for RBLs – <http://www.mxtoolbox.com>

Hunting down a spammer attack

Here is what an OWA sent email SMTP header looks like:

Received: from MailStore.client.local ([10.20.20.57]) by MailStore ([10.20.20.57]) with mapi; Thu, 22 Dec 2011 10:54:36 -0500

USELESS = The logs at: C:\WINDOWS\system32\LogFiles\HTTPERR, Only show ActiveSync Users.

USEFUL = **C:\inetpub\logs\LogFiles\W3SVC1\u_ex111217.log** (Control-F for "{gwashington}")

**2011-12-17 14:15:53 10.20.20.57 POST /owa/ev.owa
oeh=1&ns=Notify&ev=Poll&prfltncy=27&prfrpcnt=6&prfrpctncy=31&prfldp
cnt=0&prfldpltncy=0&prfavlcnt=0&prfavlltncy=0 443 gwashington
41.71.148.159
Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Trident/5.0;+SLCC2;
+.NET+CLR+2.0.50727;+.NET+CLR+3.5.30729;+.NET+CLR+3.0.30729;+CPNT
DF;+InfoPath.2;+.NET4.0C;+AskTbHIP/5.11.3.15590;+Crazy+Browser+3.0.5)
200 0 0 1372**

Source IP = 41.71.148.159

Location NIGERIA, ABUJA CAPITAL TERRITORY, ABUJA

Connection through VISAFONE COMMUNICATIONS LIMITED

Net Speed DSL

References Details

Exchange User Monitor (ExMon)

<http://www.msexchange.org/tutorials/microsoft-exchange-server-user-monitor.html>

<http://www.microsoft.com/download/en/details.aspx?id=11461>

WinDirStat – folder/volume sizing statistics

<http://windirstat.info/>

See Ben Serebin's blog post on March 15, 2011 on

<http://ehlotech.blogspot.com/> for additional information as discussed during the meeting.

Thank you for attending tonight's NY Exchange User Group Meeting.

TechHit.com (Outlook add-ons) – raffling off any one of their products (SimplyFile [intelligent filing], EZ-Detach [easily detach multi-emails of attachments], MessageSave [backup, archive, save msgs], AutoRead [mark as read/remove new mail icon], & QuickJump [quickly open/move between Windows folders]).

Now for Question of the Month.....