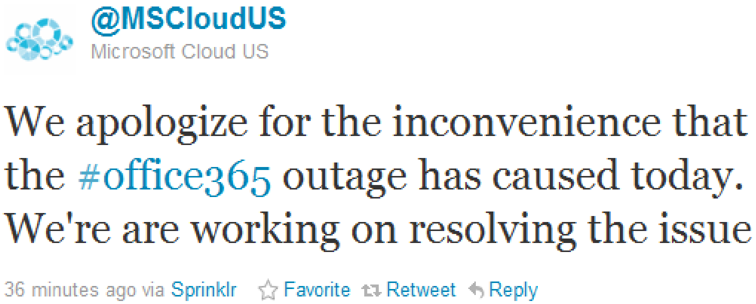
An Exchange Expert’s Guide to Troubleshooting Common Exchange Server & Cloud Issues

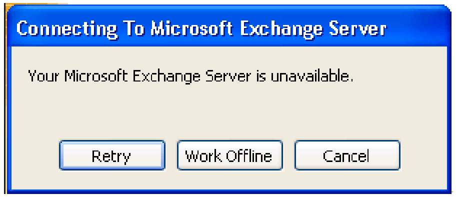
tip: mo’ monitors!



@MSCloudUS
Microsoft Cloud US

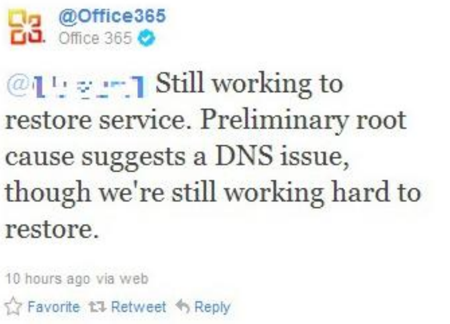
We apologize for the inconvenience that the #office365 outage has caused today. We're are working on resolving the issue

36 minutes ago via Sprinklr ☆ Favorite Retweet Reply



Connecting To Microsoft Exchange Server

Your Microsoft Exchange Server is unavailable.



@Office365
Office 365

@[redacted] Still working to restore service. Preliminary root cause suggests a DNS issue, though we're still working hard to restore.

10 hours ago via web

☆ Favorite Retweet Reply

Ben Serebin
Ehlo & Network Consultant
REEF Solutions (www.reefsolutions.com)

Presented October 13, 2015 at NYExUG Meeting
Last Updated on October 14, 2015

About Ben Serebin

- Working in the IT field since 1996 (almost 20 years)

- Specialty is Exchange Server, Spam Filtering, DNS, & complex wireless deployments.

- Upcoming Fun Tech Projects: Working to design Exchange-aware Cloud Redundant (AWS & Azure) based Geo Load Balancing, Upgrading Security Cameras to Trimode Devices, Deploying 100' view for LPR Security Camera, Monitoring Solar Energy Production w/Overall Usage Overlay

- Current Environment: ESXi 5.x, Hyper-V 2012, & 2012 R2. Exchange 2007 & 2013 w/BES 5 and BES 10. Clustered Barracuda Spam Filters and Mail Gateway (IceWarp). Lots of DAS, RAID 5 (4-6 840/850's SSDs) based Dell R410/610 1U Servers, iSCSI Storage, and 10Gb SFP/UTP.

Agenda for “Email isn’t working…”

- Review of Email Process
- Email not arriving
- Email not sending
- Outlook disconnected
- Missing Email Message
- Email Slow
- Spammers/RBLs

tip: mo’ monitors!

So, “Email isn’t working…”

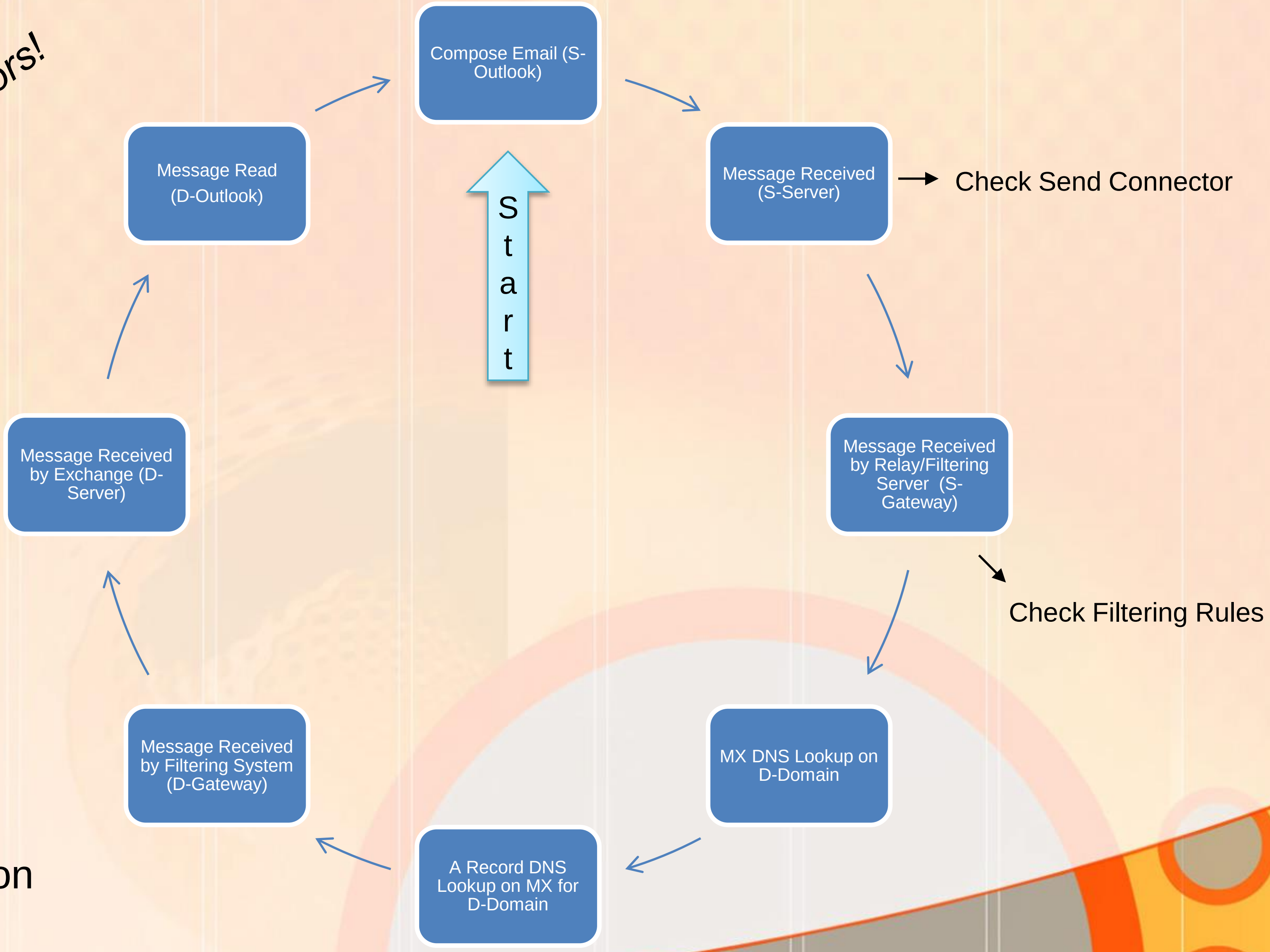
The Long Check List

- Is Outlook showing as Online/Connected?
- Does OWA work?
- Does a phone work (send or receive)?
- Can you ping the Exchange Server?
- Can you RDP into the Exchange Server?
- Can you launch EMC/ECP?
- Check all “Automatic” Exchange Services are running?
- Are all the disk volumes present & have space?
- Are Databases mounted?
- Are Queues low?
- Is Exchange Server network connection is showing “internet” connectivity?
- Check MX Records?
- Check A Record of MX?

tip: mo’ monitors!

Review of How Email Works

tip: mo' monitors!



Start

Compose Email (S-Outlook)

Message Received (S-Server)

Check Send Connector

Message Received by Relay/Filtering Server (S-Gateway)

Check Filtering Rules

MX DNS Lookup on D-Domain

A Record DNS Lookup on MX for D-Domain

Message Received by Filtering System (D-Gateway)

Message Received by Exchange (D-Server)

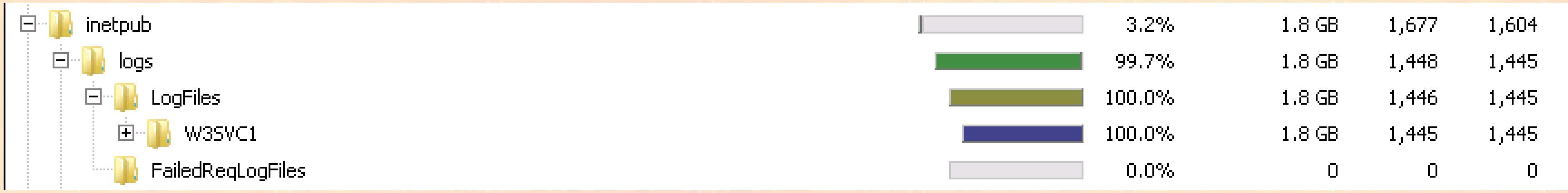
Message Read (D-Outlook)

<u>Legend</u>

S = Source

D = Destination

Running Low on Space – Due to IIS Logs



inetpub	3.2%	1.8 GB	1,677	1,604
logs	99.7%	1.8 GB	1,448	1,445
LogFiles	100.0%	1.8 GB	1,446	1,445
W3SVC1	100.0%	1.8 GB	1,445	1,445
FailedReqLogFiles	0.0%	0	0	0

Tip: install WinDirStat.info (free/open-source) or FolderSizes.com (cheap!) No reboot needed.

tip: mo' monitors!

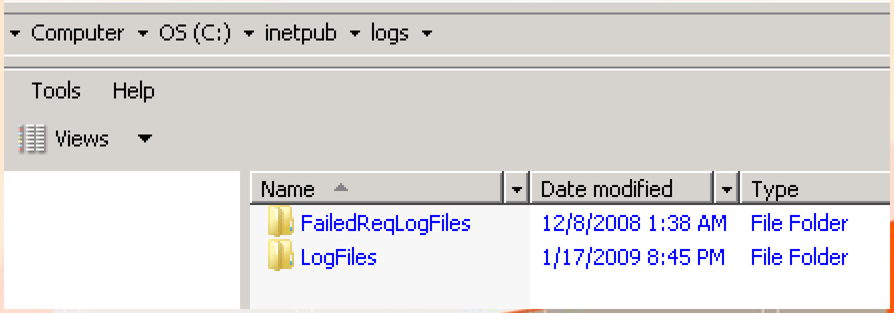
Where are they? Standard path C:\inetpub\logs\LogFiles

Just do it! Auto-purge after x days. Walk-through of how to setup a daily scheduled task to auto delete logs 60+ days old. Deletes logged.

http://www.diaryofaninja.com/blog/2011/02/22/set-up-scheduled-log-file-cleaning-for-windows-servers-running-iis

Don't do it!   >>>>>>>>>>

Enable compression of logs.

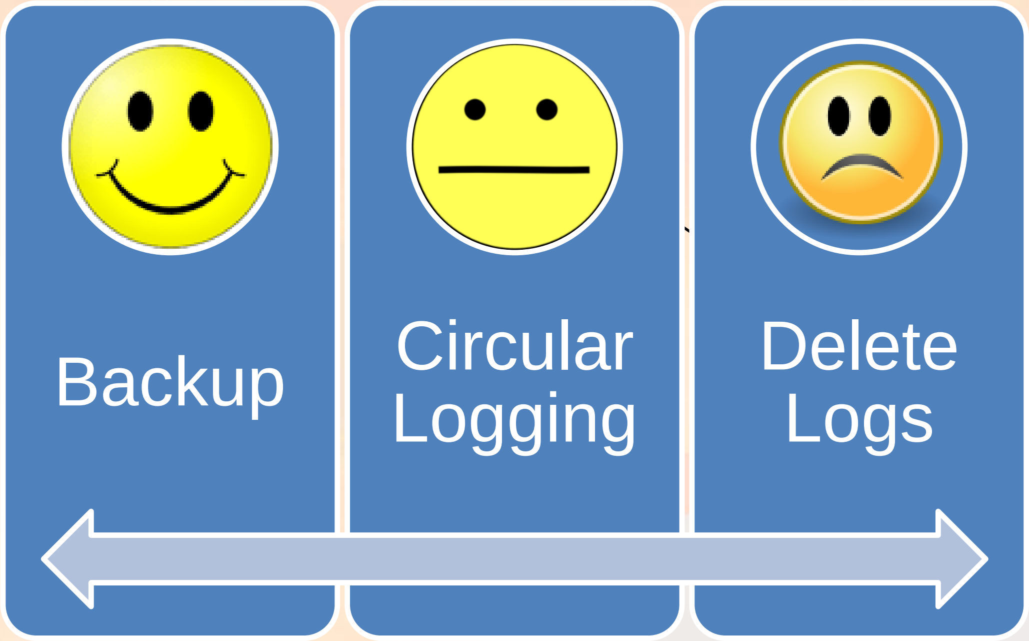


Name	Date modified	Type
FailedReqLogFiles	12/8/2008 1:38 AM	File Folder
LogFiles	1/17/2009 8:45 PM	File Folder

Running Low on Space - Transaction Logs

- Email is bouncing. You login to the Exchange Server, and see database volume at 0 bytes free. WinDirStat shows it's transaction logs for Mailbox Database 023987129.

tip: mo' monitors!



Backup

Circular Logging

Delete Logs

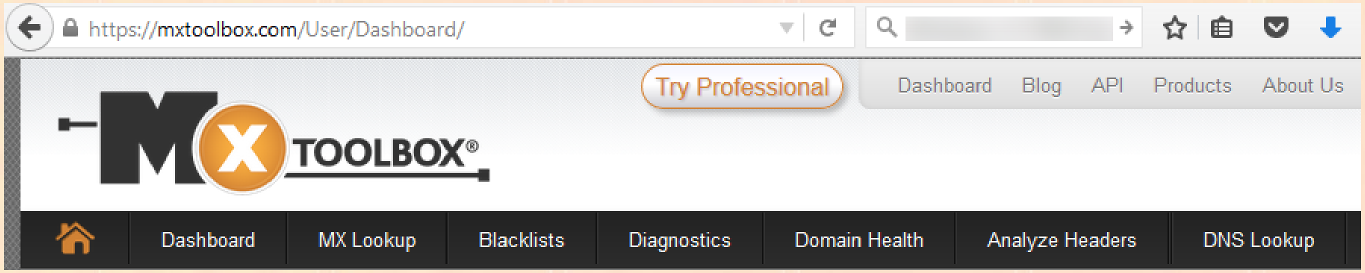
P = 100% recommended
C = heavy I/O, can take a while, one time fix

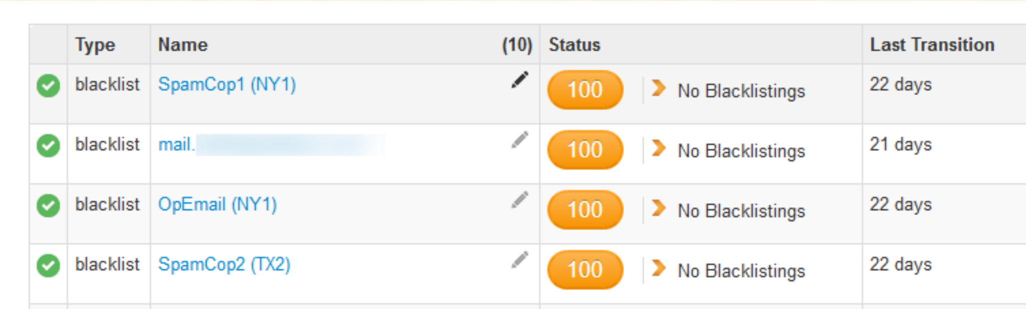
P = forever fix issue
C = bit recommended, potential loss of data, restart DB service

P = fastest
C = causes error on follow-up backup, not recommended, use caution in DAG config delete 1+ day old)

Emails Bouncing (demo)

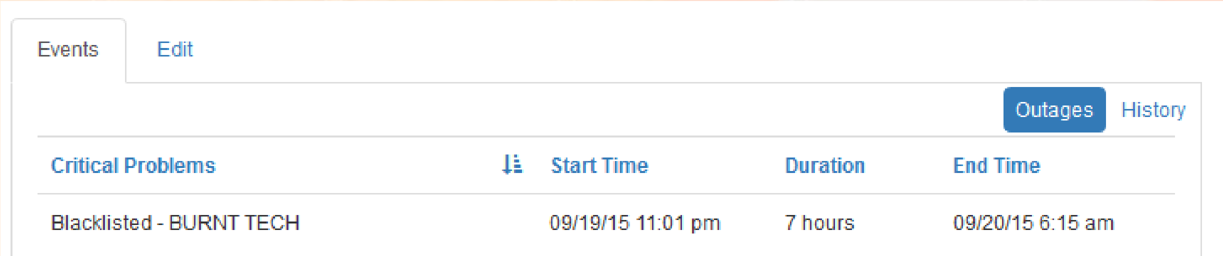
- Emails start bouncing with fatal 5xx errors. 4xx non-fatal.
- Why does "Last Transition" show activity 21-22 days ago?





	Type	Name (10)	Status		Last Transition
✓	blacklist	SpamCop1 (NY1)	100	No Blacklistings	22 days
✓	blacklist	mail.[redacted]	100	No Blacklistings	21 days
✓	blacklist	OpEmail (NY1)	100	No Blacklistings	22 days
✓	blacklist	SpamCop2 (TX2)	100	No Blacklistings	22 days

tip: use MX Toolbox to monitor your IP/hostname on RBLs



Critical Problems	Start Time	Duration	End Time
Blacklisted - BURNT TECH	09/19/15 11:01 pm	7 hours	09/20/15 6:15 am

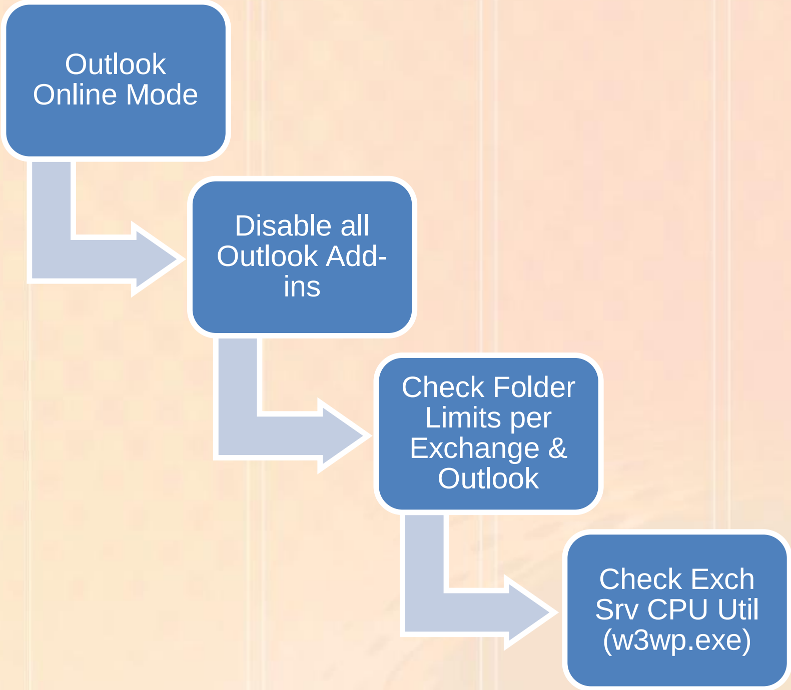
FYI: RBLs shutting down respond "POSITIVE" to encourage sites/servers from using a dying RBL.

“My Phone is Not Working!”

- What’s not working exactly?
- Confirm internet is working on device
- Was it previously working or 1st time setup?
- Previously working – reboot phone.
- Is EAS working for other end users?
- Confirm ActiveSync is working for user account? **Remote Connectivity Analyzer -** MSFT: TestExchangeConnectivity.com [demo]
- Confirm user’s OWA is working
- Delete phone EAS setup and reboot and re-add.
- Check Exch Srv Application Event Logs for EAS errors.
- Tell user to get a better phone.

Pssst user it might be time for a new phone. Sorry!

Outlook Online is Sluggggggish



Outlook Online Mode

Disable all Outlook Add-ins

Check Folder Limits per Exchange & Outlook

Check Exch Srv CPU Util (w3wp.exe)

<u>Throttling Policies</u>
Changes to Prevent End users running EAS and Exch Web Services from causing a Denial of Service. Modification of DefaultThrottlingPolicy_0b6f2f05.........

EASMaxConcurrency UNLIMITED -> 3
EASPercentTimeInAD UNLIMITED -> 25
EASPercentTimeInCAS UNLIMITED -> 25
EASPercentTimeInMailboxRPC UNLIMITED -> 25
EASMaxDevices UNLIMITED -> 10
EWSPercentTimeinCAS 90 > 30
EWSPercentTimeinMailboxRPC 60 > 30

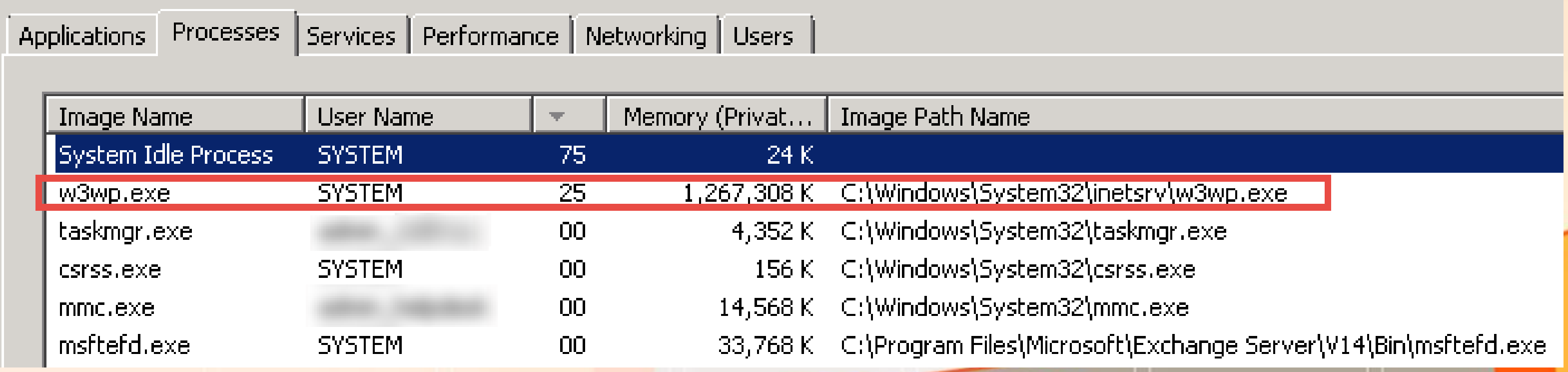
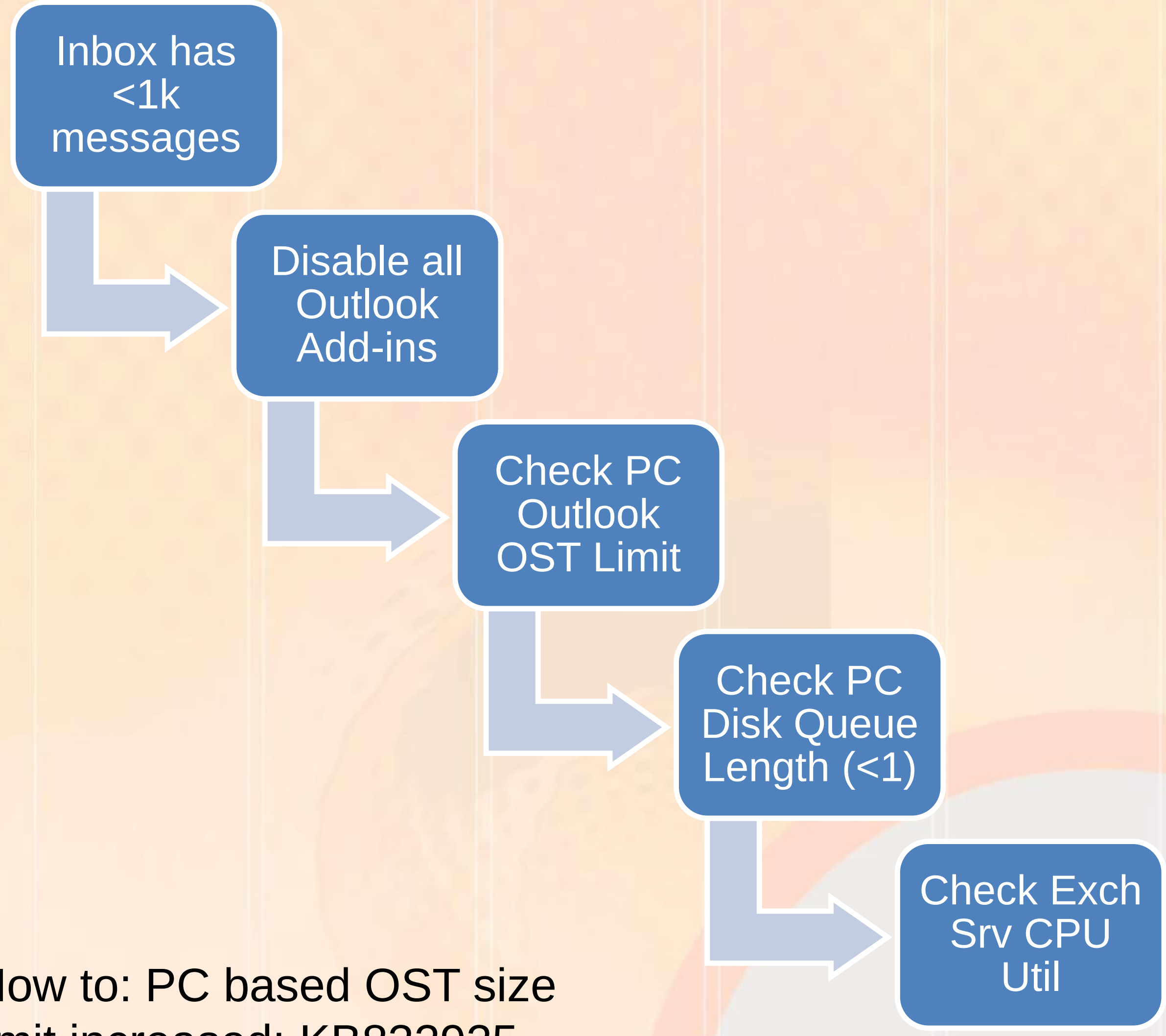


Image Name	User Name		Memory (Privat...	Image Path Name
System Idle Process	SYSTEM	75	24 K	
w3wp.exe	SYSTEM	25	1,267,308 K	C:\Windows\System32\inetsrv\w3wp.exe
taskmgr.exe	[redacted]	00	4,352 K	C:\Windows\System32\taskmgr.exe
csrss.exe	SYSTEM	00	156 K	C:\Windows\System32\csrss.exe
mmc.exe	[redacted]	00	14,568 K	C:\Windows\System32\mmc.exe
msftefd.exe	SYSTEM	00	33,768 K	C:\Program Files\Microsoft\Exchange Server\V14\Bin\msftefd.exe

Outlook Cached Mode is Sluggggish & Not Updating



Inbox has <1k messages

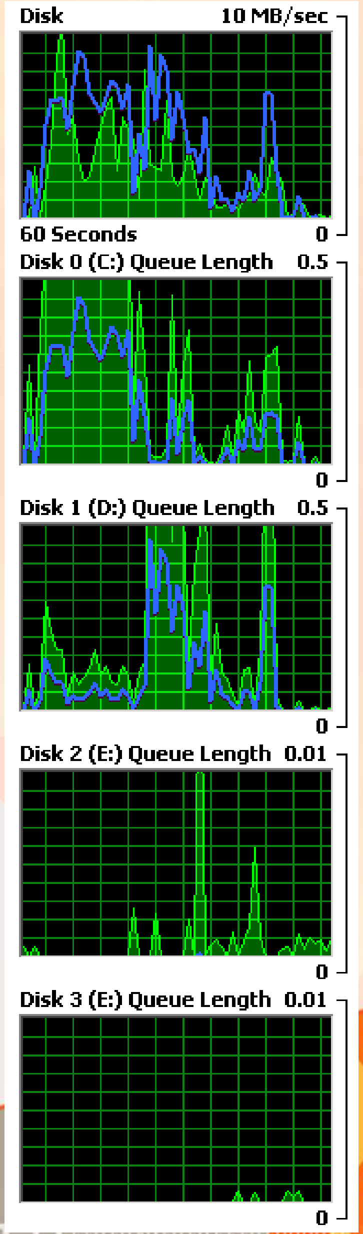
Disable all Outlook Add-ins

Check PC Outlook OST Limit

Check PC Disk Queue Length (<1)

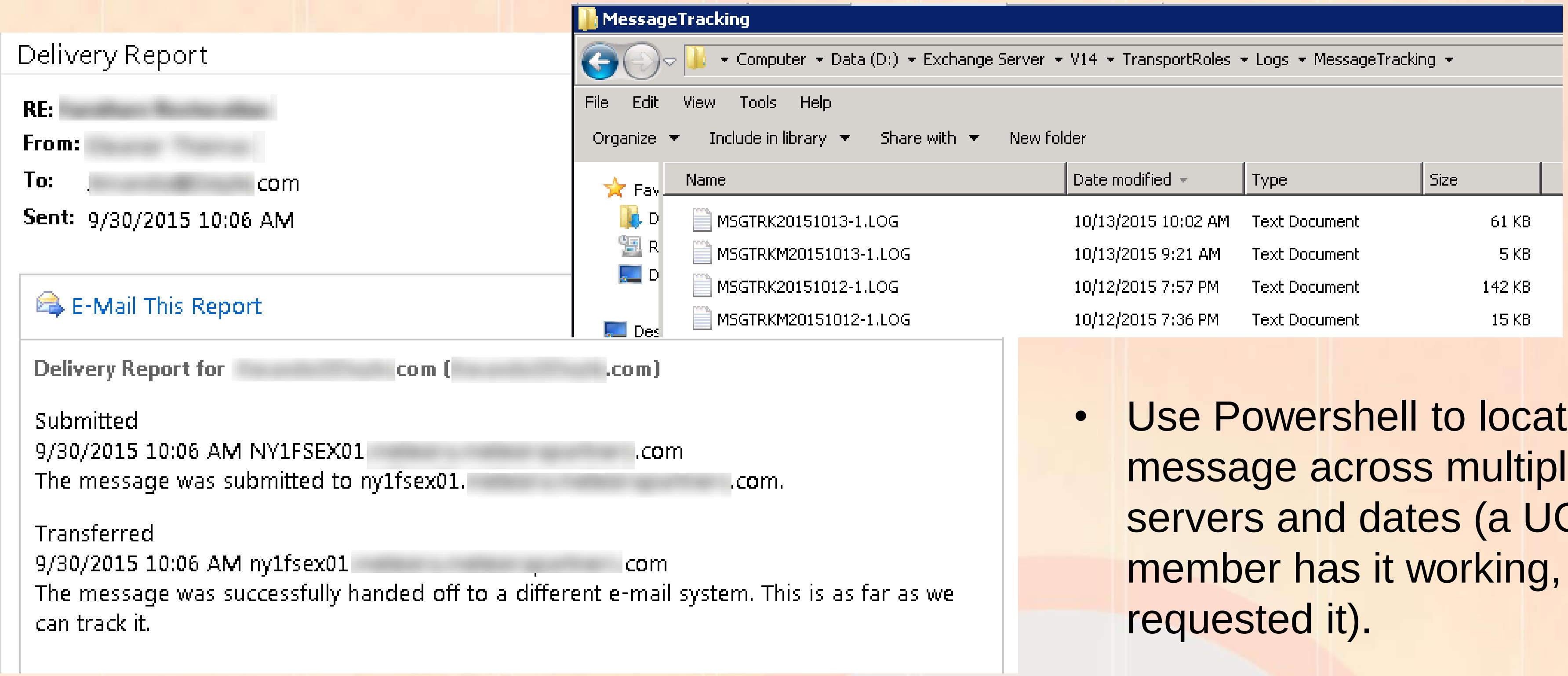
Check Exch Srv CPU Util

How to: PC based OST size limit increased: KB832925



Alleged missing email

- Exchange Message Tracking = not very helpful



MessageTracking
Computer ▸ Data (D:) ▸ Exchange Server ▸ V14 ▸ TransportRoles ▸ Logs ▸ MessageTracking
File Edit View Tools Help
Organize ▾ Include in library ▾ Share with ▾ New folder
Fav
D
R
D
Des

Name	Date modified	Type	Size
MSGTRK20151013-1.LOG	10/13/2015 10:02 AM	Text Document	61 KB
MSGTRKM20151013-1.LOG	10/13/2015 9:21 AM	Text Document	5 KB
MSGTRK20151012-1.LOG	10/12/2015 7:57 PM	Text Document	142 KB
MSGTRKM20151012-1.LOG	10/12/2015 7:36 PM	Text Document	15 KB

Delivery Report

RE: [redacted]
From: [redacted]
To: [redacted]com
Sent: 9/30/2015 10:06 AM

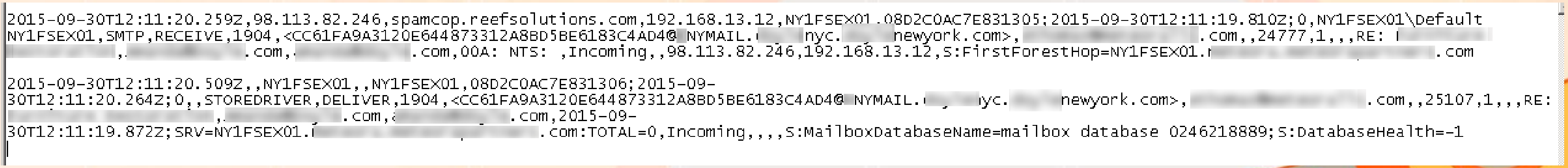
E-Mail This Report

Delivery Report for [redacted]com ([redacted].com)

Submitted
9/30/2015 10:06 AM NY1FSEX01 [redacted].com
The message was submitted to ny1fsex01.[redacted].com.

Transferred
9/30/2015 10:06 AM ny1fsex01 [redacted] com
The message was successfully handed off to a different e-mail system. This is as far as we can track it.

- Use Powershell to locate message across multiple servers and dates (a UG member has it working, requested it).



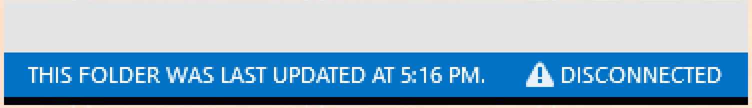
```
2015-09-30T12:11:20.259Z,98.113.82.246,spamcop.reefsolutions.com,192.168.13.12,NY1FSEX01,08D2C0AC7E831305;2015-09-30T12:11:19.810Z;0,NY1FSEX01\Default
NY1FSEX01,SMTP,RECEIVE,1904,<CC61FA9A3120E644873312A8BD5BE6183C4AD4@[redacted]NYMAIL.[redacted]nyc.[redacted]newyork.com>,[redacted].com,,24777,1,,,RE: [redacted]
[redacted],[redacted].com,[redacted].com,00A: NTS: ,Incoming,,98.113.82.246,192.168.13.12,S:FirstForestHop=NY1FSEX01.[redacted].com

2015-09-30T12:11:20.509Z,,NY1FSEX01,,NY1FSEX01,08D2C0AC7E831306;2015-09-
30T12:11:20.264Z;0,,STOREDRIVER,DELIVER,1904,<CC61FA9A3120E644873312A8BD5BE6183C4AD4@[redacted]NYMAIL.[redacted]yc.[redacted]newyork.com>,[redacted].com,,25107,1,,,RE:
[redacted],[redacted].com,[redacted].com,2015-09-
30T12:11:19.872Z;SRV=NY1FSEX01.[redacted].com:TOTAL=0,Incoming,,,,S:MailboxDatabaseName=mailbox database 0246218889;S:DatabaseHealth=-1
```

Received Delivery Status Notification

- Internal or External?
- Verify the email address (check domain carefully – phishing is common)
- Have user forward email
- Review DNS Records (e.g. tools.appriver.com, centralops.net, mxtoolbox.com, nslookup)
- Check spam filtering on message body URLs and message headers

```
---------- Forwarded message ----------
From: Mail Delivery Subsystem <mailer-daemon@googlemail.com>
Date: Thu, Dec 4, 2014 at 2:15 PM
Subject: Delivery Status Notification (Failure)
To: brian@SENDER.com

Delivery to the following recipient failed permanently:

    Luciana@RECEIVER.com

Technical details of permanent failure:
Google tried to deliver your message, but it was rejected by the server for the recipient domain receiver.com by
spamcopcluster2.reefsolutions.com. [216.230.231.138].

The error that the other server returned was: 554 rejected due to spam content

----- Original message -----

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
       d=1e100.net; s=20130820;
       h=x-gm-message-state:mime-version:in-reply-to:references:date
        :message-id:subject:from:to:content-type;
       bh=Ei4Py52rENvb8+V0A1Kaa1Jh6bYkQmOwobj5pm056v
```

Outlook is Disconnected



THIS FOLDER WAS LAST UPDATED AT 5:16 PM. ⚠ DISCONNECTED

- Does this affect everyone?
- Is OWA working?
- Check Server is online (RDP)?
- Check Databases are Mounted
- Confirm Exchange Services are running
- Confirm IIS Services are running

Name the Potential Issue (Cause/Effect)

Symptoms

- 1 User’s Outlook not working (shows disconnected)
- 1 User’s OWA not working (login fails)
- Internet is working on laptop (workgroup)

Possible Causes (See Email isn’t working)

- Audience? [Answer: Password expired]

Symptoms

- Outlook works internally
- Outlook sending to external does not work
- OWA & EAS works internally but not to external users
- Inbound Emails work

Possible Causes (See Email isn’t working)

- Audience? [Answer: Check Send Connector]

References Details

- Microsoft hosted - Remotely Testing Outlook Anywhere, ActiveSync including Autodiscover, 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
- Checking for RBLs, Message Header Analysis – http://www.mxtoolbox.com

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……