

Tips & Best Practices for Exchange Server 2010 & 2013

Tip: DAG on Exch
2013 is rock solid!

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

Presented January 10, 2017 at NYExUG Meeting
Last Updated on January 13, 2017

About Ben Serebin

- Working in the IT field since 1996 (over 20 years)
- Specialty is Exchange Environments, Spam Filtering, DNS, & complex wireless deployments.
- Upcoming Fun Tech Projects: Working to design Exchange-aware Cloud Redundant (AWS & Azure) based Geo Load Balancing, Finalizing 100' view for OCR Security Camera, Monitoring Solar Energy Production w/Overall Usage Overlay
- Current Environment: BlackBerry Priv (natively running Android Lollipop) Hyper-V 2012 R2/2012 & ESXi 5.x. HA LBed DAGed Exchange 2013. Clustered Barracuda Spam Filters and Mail Gateway (IceWarp). Lots of SSD DAS, RAID 5 (4-6 840/850's SSDs) based Dell R410/610 1U Servers, iSCSI Storage, and 10Gb SFP/UTP.

Agenda for Tips & Best Practices for Exchange 2010/2013

1. DAG Servers still require manual Maintenance Mode
2. Prevent public Exchange Admin Console access
3. Distribution Group management by multiple users via Outlook
4. How to enable the faster better Outlook HTTPS protocol of MAPI
5. How to automatically purge IIS logs older than x days
6. Running low on space, can I safely delete transaction logs?
7. What is needed to run Exchange on Azure in supported configuration?
8. Monitoring Solution for Watching RBLs (public cloud based)
9. Monitoring Solution for Email Roundtrip Flow (public cloud based)

Manual Maintenance Mode for DAG and Standalone

- What is Maintenance Mode? For 2013/2016.
- What is Maintenance State? For 2010 (see ref)
- Why is it important to use?
- Which servers should use Maintenance Mode?

5 Major Steps for Mission Critical Exchange Servers (see ref)

1. Put in Maintenance Mode
2. Verify in Maintenance Mode
3. Perform Exchange Server A Work
4. Remove from Maintenance
5. Verify out of Maintenance Mode
6. Repeat for Exchange Server B – see Step 1-5.

Closer Look at Steps 1-2 for DAG Maintenance Mode

*** PUT IN MAINTENANCE MODE ***

- Set-ServerComponentState ny1ex13a -Component HubTransport -State Draining -Requester Maintenance
- Get-Queue -Server ny1ex13a | ? {\$_.Identity -notmatch "Poison" -AND \$_.Identity -notmatch "Shadow"}
- Suspend-ClusterNode ny1ex13a
- Set-MailboxServer ny1ex13a -DatabaseCopyActivationDisabledAndMoveNow \$True
- Get-MailboxServer ny1ex13a | Select DatabaseCopyAutoActivationPolicy
- Set-MailboxServer ny1ex13a -DatabaseCopyAutoActivationPolicy Blocked
- Set-ServerComponentState ny1ex13a -Component ServerWideOffline -State Inactive -Requester Maintenance
- Get-Mailboxdatabasestatus **

*** VERIFY IN MAINTENANCE MODE ***

- Get-ServerComponentState ny1ex13a | ft Component,State -AutoSize

Tips

- If you have a DAG, include commands in red.
- If you have a SINGLE Standalone Server, skip commands in red.
- See Ref line 4, for script which adds “check the transport queues every minute until empty

Closer Look at Steps 3-4 for DAG Maintenance Mode

*** REMOVE FROM MAINTENANCE MODE ***

- Set-ServerComponentState ny1ex13a -Component ServerWideOffline -State Active -Requester Maintenance
- **Resume-ClusterNode ny1ex13a**
- **Set-MailboxServer ny1ex13a -DatabaseCopyActivationDisabledAndMoveNow \$False**
- **Set-MailboxServer ny1ex13a -DatabaseCopyAutoActivationPolicy Unrestricted**
- Set-ServerComponentState ny1ex13a -Component HubTransport -State Active -Requester Maintenance
- Set-ServerComponentState ny1ex13a -Component ForwardSyncDaemon -State Active -Requester Maintenance
- Set-ServerComponentState ny1ex13a -Component ProvisioningRps -State Active -Requester Maintenance
- Restart-Service MExchangeTransport
- Restart-Service MExchangeFrontEndTransport

*** VERIFY OUT OF MAINTENANCE MODE *** Everything should say "Active"

- Get-ServerComponentState ny1ex13a | ft Component,State -AutoSize
- Get-Mailboxdatabasecopystatus **

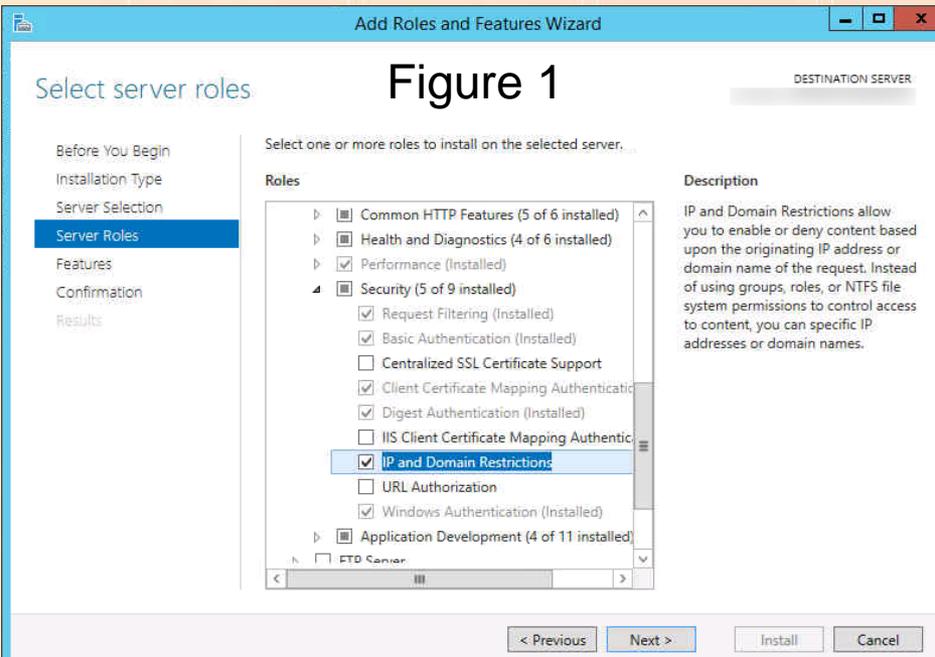
Tips

If you have a DAG, include commands in red.

If you have a SINGLE Standalone Server, skip commands in red.

Prevent public Exchange Admin Console access

1) Add Server Role, under Web Server (IIS), Web Server, Security, check JUST "IP and Domain Restrictions". Next/Next, do NOT enable Server Restarts.



2) Open Administrator cmd and run "iisreset /noforce"
3) Launch IIS Manager

4) Default Web Site – ecp, launch IP Address and Domain Restrictions

5) Click "Edit Feature Settings", change Access for unspecified clients to "Deny" and OK. See Figure 5.

6) Click "Allow Entry", for IP address range add in LAN subnet (e.g. 10.0.43.0 and Mask 255.255.255.0)

7) Click "Allow Entry" and list the IP of the Exchange Server. See Figure 7

Figure 5

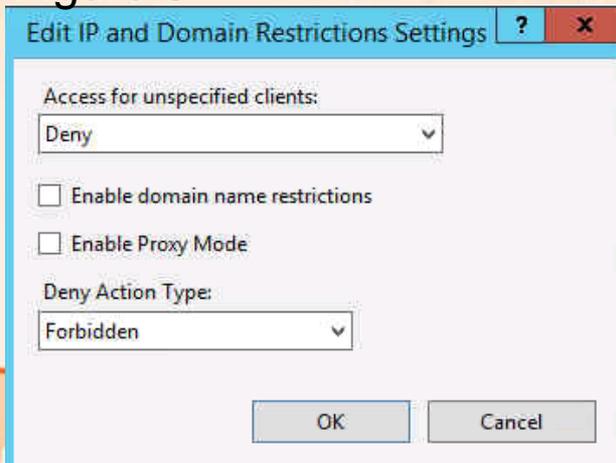
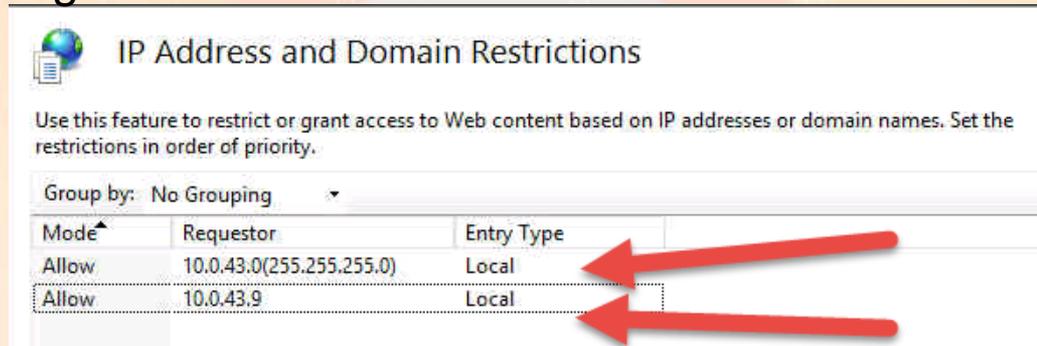


Figure 7



Distribution Group management by multiple users via Outlook

1. Create Role Based Access Control entry (a) & confirm roles (b):

(a)> ***New-ManagementRole -Name DL-MemEdit1 -Parent MyDistributionGroups***

(b)> ***Get-ManagementRoleEntry DL-MemEdit1****

2. Remove extra roles

Remove-ManagementRoleEntry DL-MemEdit1\Remove-Distributiongroup

Remove-ManagementRoleEntry DL-MemEdit1\Set-DynamicDistributiongroup

Remove-ManagementRoleEntry DL-MemEdit1\New-Distributiongroup

3. Edit Default Role Assignment Policy (EAC\permissions\user roles\edit Default Role Assignment Policy\check DL-MemEdit1 box under “Distribution Groups”)

4. Create new Security Group & add user(s) for those needing access to editing distribution group membership

5. Edit Group Owners of each group via Exchange admin center

*FYI: tested with
Exchange 2013*

How to enable the *Faster & Better* Outlook HTTPS protocol of MAPI

“MAPI” on slide is referencing MAPI over HTTPS

Why you want to switch from RPC over HTTPS to MAPI over HTTPS

- 1) *Faster Connection Established (MAPI 30 sec vs RPC 40 sec+)*
- 2) *Faster Reconnects (MAPI 5 sec vs RPC 30 sec+)*

MAPI Road Blocks

- *Exchange co-existence mode (no 2007, native 2010 or higher)*
 - *No Outlook 2007 support*
- *Running Legacy Public Folders (migrate to Modern Public Folders = Exch 2013 Native PFs)*

RPC over HTTPS Connection

MAPI over HTTPS Connection

Outlook Connection Status

General Local Mailbox

Activity

| CID | SMTP Address | Di... | Proxy Server | Server name | Status | Protocol | Authn |
|-----|----------------------|-------|--------------|----------------------------|-------------|----------|---------|
| 5 | Administrator@Bla... | mail | blu... | b0331733-d0d1-48bc-b85... | Established | RPC/HTTP | NTLM [N |
| 10 | Administrator@Bla... | mail | blu... | b0331733-d0d1-48bc-b85... | Established | RPC/HTTP | NTLM [N |
| 14 | Administrator@Bla... | mail | blu... | b0331733-d0d1-48bc-b85... | Established | RPC/HTTP | NTLM [N |
| 17 | Administrator@Bla... | mail | blu... | b0331733-d0d1-48bc-b85... | Established | RPC/HTTP | NTLM [N |
| 23 | Administrator@Bla... | mail | blu... | 97b98425-ea2c-4001-bcbb... | Established | RPC/HTTP | NTLM [N |

Reconnect

Close

Outlook Connection Status

General Local Mailbox

Activity

| CID | SMTP Address | Display Name | Proxy Server | Server name | Status | Protocol | Authn | Encrypt | RPCPort |
|-----|----------------------|-----------------|--------------|-----------------|-------------|----------|-------|---------|---------|
| 5 | Administrator@Bla... | | | https://mail... | Established | HTTP | Nego* | SSL | |
| 10 | Administrator@Bla... | | | https://mail... | Established | HTTP | Nego* | SSL | |
| 14 | Administrator@Bla... | OpenCap A... | | https://mail... | Established | HTTP | Nego* | SSL | |
| 18 | Administrator@Bla... | Public Folds... | | https://mail... | Established | HTTP | Nego* | SSL | |
| 22 | Administrator@Bla... | | | https://mail... | Established | HTTP | Nego* | SSL | |
| 26 | Administrator@Bla... | OpenCap A... | | https://mail... | Established | HTTP | Nego* | SSL | |
| 29 | Administrator@Bla... | MSF Backu... | | https://mail... | Established | HTTP | Nego* | SSL | |
| 33 | Administrator@Bla... | | | https://mail... | Established | HTTP | Nego* | SSL | |
| 38 | Administrator@Bla... | MSF Backu... | | https://mail... | Established | HTTP | Nego* | SSL | |

Reconnect

Close

How to enable the *Faster & Better* Outlook HTTPS protocol of MAPI

5 Steps for MAPI over HTTPS for your Exchange 2013 Environment (see ref)

1. **Set-MapiVirtualDirectory -Identity "NY1EX13A\mapi (Default Web Site)" -InternalURL**
2. **<https://mail.reefit.com/mapi> -ExternalUrl <https://mail.reefit.com/mapi> - IISAuthenticationMethods Negotiate**
3. **Set-MapiVirtualDirectory -Identity "NY1EX13B\mapi (Default Web Site)" -InternalURL <https://mail.reefit.com/mapi> -ExternalUrl <https://mail.reefit.com/mapi> - IISAuthenticationMethods Negotiate**
4. **Set-OrganizationConfig -MapiHttpEnabled \$true**
5. **Get-OrganizationConfig | fl *mapi***

Tips

- *The certificate used in the Exchange servers must have the internal URL & external URL specified while creating MAPI virtual directory.*
- *Make sure firewalls & load balancers are configured to allow access to MAPI/HTTP directories*
- *After running above commands run iisreset or reboot each server. The clients might prompt to restart Outlook or prompt for credentials to use MAPI/HTTP.*
- *Once MAPI over HTTPS is working - Recommend Disabling RPC over HTTPS*

How to automatically purge IIS logs older than x days

- Why? IIS log files will NEVER delete. Confirmed through 2012 R2. 2016?
- What does script do? Purges older log files in IIS recursively that are older than x days.

3 Easy Steps (see reference)

1. Import Task XML file or manually create task (recommend 30-90 days).
 2. Run task and confirm older than x days are deleted
 3. Check in a few days later and confirm older than x days are deleted
- Tip: Set Compression on x:\inetpub\logs\LogFiles folder (saved almost 250% space)
 - Tip: Run backups on this server and capture this folder, so purging IIS log files isn't an issue if you need them for historical purposes (set retention accordingly).

| Name | Status | Triggers | Next Run Time | Last Run Time | Last Run Result |
|--------------------------------|----------|-----------------------|-----------------------|------------------------|---|
| Clear IIS Logs after 90 Days | Ready | At 12:01 AM every day | 1/11/2017 12:01:00 AM | 1/10/2017 12:01:00 AM | The operation completed successfully. (0x0) |
| Optimize Start Menu Cache F... | Disabled | When computer is idle | | 10/20/2016 12:13:03 AM | The operation completed successfully. (0x0) |

General Triggers Actions Conditions Settings History

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties

| Action | Details |
|-----------------|---|
| Start a program | forfiles /p "C:\inetpub\logs\LogFiles" /s /m *.* /c "cmd /c Del @path" /d -90 |

Running low on space, can I safely delete transaction logs?

YES! BUT be careful. Follow these guidelines

- If possible: run a backup to purge log files

Delete only log files that meet ALL 5 criteria below

1. Log Folder (if default path: folder with .edb)
2. Sort based on size
3. Select ONLY log files ending in .log extension
4. Make sure length of filenames match
5. Delete only log files of 1024 KB in size

After Delete – What Happens

- Incremental Backup: Next Incremental backup will report an error.
- Full Backup: Run to avoid Incremental error.
- Crash: inability to recover via log playback

| Name | Date modified | Type | Size |
|---------------------------------|--------------------|---------------|---------------|
| Mailbox Database [redacted].edb | 1/7/2017 12:29 AM | EDB File | 519,449,15... |
| tmp.edb | 1/7/2017 12:29 AM | EDB File | 8,256 KB |
| E03.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E03res0000A.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00001.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00002.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00003.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00004.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00005.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00006.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00007.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00008.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03res00009.jrs | 3/19/2014 12:53 AM | JRS File | 1,024 KB |
| E03tmp.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190745D.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190745E.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190745F.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746A.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746B.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746C.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746D.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746E.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E030190746F.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907460.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907461.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907462.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907463.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907464.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907465.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907466.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907467.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907468.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |

| | | | |
|---|-------------------|-----------------------|----------|
| E0301907475.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907476.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907477.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907478.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E0301907479.log | 1/10/2017 1:06 PM | Text Document | 1,024 KB |
| E03.chk | 1/10/2017 1:06 PM | Recovered File Fra... | 8 KB |
| E03tmp.log | 1/10/2017 1:06 PM | Text Document | 0 KB |
| CatalogData-5b436e78-5ab8-4059-b1c8-... | 1/7/2017 12:48 AM | File folder | |

What is needed to run Exchange on Azure in supported configuration?

- Yes, Exchange Standalone or DAG Witness Server is supported (see ref)

Versions (see ref – as of 1/10/17)

- Exchange 2013 (all roles) on Windows Server 2008 R2 SP1, 2012, & 2012 R2
- Exchange 2016 (all roles) on Windows Server 2012 or 2012 R2 (no 2016)

Azure Configurations

- Windows boot volume must be 15GB + virtual memory size (e.g. ram is 64GB, you would need 79GB of storage).
- Volumes holding the Exchange Databases & Transaction Log must be on Azure Premium Storage (boot volume does not need to be)
- Outbound emails must use SMTP smart host (Azure or 3rd party)
- No snapshots permitted

Monitoring Solution for Watching Real Time Block Lists

FYI: No Compensation Received for Recommendation

MXtoolbox.com

- Inexpensive (\$80/yr/10 hosts)
- Daily RBL check (MX, A, etc)
- Almost every RBLs monitored that is relevant to your needs
- Emailed alert if added to a RBL
- Email alert includes instructions for removal

Tue 1/3/2017 9:35 PM

MxToolBox <noreply@mxtoolbox.com>
BLACKLIST - ADDED - SpamCop1 (NY1) - Added to URIBL multi

To [redacted]

 If there are problems with how this message is displayed, click here to view it in a web browser.

Not rendering correctly? View this email as a web page [here](#).

SpamCop1 (NY1)

Added to URIBL multi at 1/3/2017 9:34:33 PM (UTC-05:00) Eastern Time (US & Canada)

| | |
|---------------------------------------|---|
| Blacklist Severity: | Low |
| MxRep Current Score: | 95 |
| Delisting link: | https://admin.uribl.com/?section=users;method=register |
| Get more information: | blacklist:spamcop.reefsolutions.com |
| Tags: | |
| Learn more about this problem: | URIBL-multi |
| Current Checks failing: | 1 |
| Email Sent On: | 1/3/2017 8:34:32 PM |

| Check | Severity | Blacklist Detail | Delisting Link |
|--|----------|----------------------------|----------------|
|  On URIBL multi | Low | Learn More | |

 **TOOLBOX®**

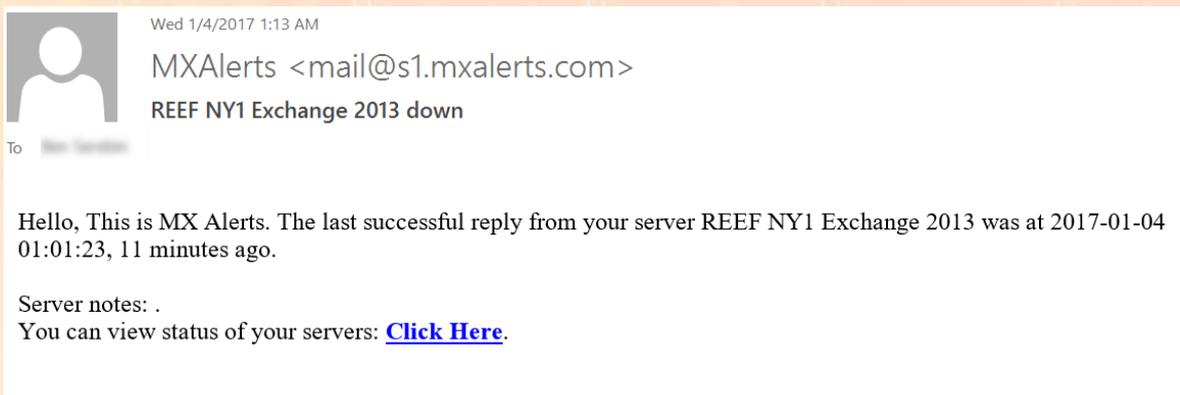
This message was sent according to your **Default** notification policy.
Click here to [edit](#) or [unsubscribe](#).

Monitoring Solutions for Mail Roundtrip Flow (public cloud hosted)

FYI: No Compensation Received for Recommendation

MXAlerts.com

- Inexpensive (\$59/yr/1 server, \$149/yr/3 servers, \$299/yr/10 servers)
- Easy to Setup: add Exch mailbox, add fwd contact, setup mxalerts profile
- 5 Minute Interval Monitoring
- Email and Cell alerts supported



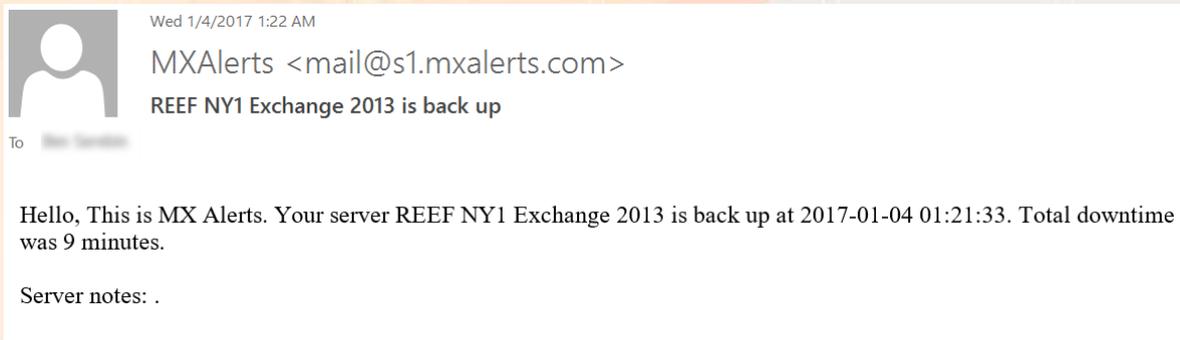
Wed 1/4/2017 1:13 AM

 MXAlerts <mail@s1.mxalerts.com>
REEF NY1 Exchange 2013 down

To: [Redacted]

Hello, This is MX Alerts. The last successful reply from your server REEF NY1 Exchange 2013 was at 2017-01-04 01:01:23, 11 minutes ago.

Server notes: .
You can view status of your servers: [Click Here](#).



Wed 1/4/2017 1:22 AM

 MXAlerts <mail@s1.mxalerts.com>
REEF NY1 Exchange 2013 is back up

To: [Redacted]

Hello, This is MX Alerts. Your server REEF NY1 Exchange 2013 is back up at 2017-01-04 01:21:33. Total downtime was 9 minutes.

Server notes: .

References Details

1. 2013 Maintenance Mode Script from Microsoft - <https://gallery.technet.microsoft.com/office/Exchange-2013-Maintenance-7b84d45e#content>
2. 2013 Maintenance Mode Commands Explanations - <https://letsexchange.blogspot.com/2013/03/exchange-2013-maintenance-mode.html>
3. Technet Explained 2013 Maintenance Mode - <https://blogs.technet.microsoft.com/nawar/2014/03/30/exchange-2013-maintenance-mode/>
4. 2013 Maintenance Mode Commands Explained DAG vs Standalone - <http://www.be-com.eu/?p=978>
5. Technet Explained 2010 Maintenance State using native pre-installed scripts - <https://blogs.technet.microsoft.com/timcmic/2013/04/23/exchange-2010-stopdagservermaintenance-ps1-resets-server-and-database-suspension-states/>
6. How to automatically purge IIS logs older than x days – <http://www.diaryofaninja.com/blog/2011/02/22/set-up-scheduled-log-file-cleaning-for-windows-servers-running-iis>
7. How to enable MAPI over HTTPS <http://msexchangeguru.com/2015/03/30/mapi-over-http/>
<http://www.itnotes.eu/?p=2603>
8. Production Exchange in Azure is Microsoft Support - <https://support.microsoft.com/en-us/kb/2721672>
9. Technet Summary of Azure VM as a DAG Witness Server - <https://blogs.technet.microsoft.com/exchange/2015/01/09/using-an-azure-vm-as-a-dag-witness-server/>
10. Technet In-Depth of Azure VMs as a DAG Witness Server (Exch 2013 & 2016) - [https://technet.microsoft.com/en-us/library/dn903504\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dn903504(v=exchg.150).aspx)
11. Technet Azure VMs for Running Exchange 2013 Natively Supported Config [https://technet.microsoft.com/en-us/library/jj619301\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj619301(v=exchg.150).aspx)
12. Technet Azure VMs for Running Exchange 2016 Natively Supported Config [https://technet.microsoft.com/en-us/library/jj619301\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj619301(v=exchg.160).aspx)