3-1-11：邮箱管理-通过搜索传输日志查看邮件收发状况

作者简介

曾垂鑫，毕业于中国人民大学商务管理专业。微软（2013-2017五届）MVP，具有丰富的项目实施和解决方案经验，51CTO传媒推荐博客、博客之星，微软MCP/MCTS/MCITP/MCSA/MCSE认证系统专家和解决方案顾问。
属于实战派的讲师，具备丰富的万人规模以上企业的运维经验。课程内容侧重于实战实用。

曾垂鑫的博客地址：http://543925535.blog.51cto.com/
曾垂鑫的课程地址：http://edu.51cto.com/lecturer/index/user_id-639838.html

课程后续会形成完善的Windows运维工程师路线图，涵盖企业常用的Windows平台运维技术，后期课程包括但不限于AD、Exchange、Windows、System Center、Powershell、Hyper-v、Office 365等。

应用场景

查询用户邮件是否成功投递
查询用户邮件投递失败的原因
协助分析产生邮件退信的原因（邮件可能根本没有到我们的服务器）

---

powershell查看传输日志

常见EVENTID的含义
DELIVER 邮件已传递到邮箱。
DEFER 邮件传递延迟。
FAIL 邮件传递失败。
RECEIVE 邮件已接收并提交到数据库。
SEND 简单邮件传输协议 (SMTP) 将邮件发送到不同的服务器。
邮件跟踪 https://technet.microsoft.com/zh-cn/library/bb124375(v=exchg.160).aspx

查看特定收件人之间的邮件投递信息
Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com

```
PS C:\share> Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com

Timestamp            EventId         Source      Sender                    Recipients                    MessageSubject
---------            -------         ------      ------                    ----------                    --------------
2017/4/12 17:14:38   HAREDIRECTFAIL  SMTP        zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04-12-2017 - 星期
2017/4/12 17:14:38   RECEIVE         SMTP        zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04-12-2017 - 星期
2017/4/12 17:14:39   AGENTINFO       AGENT       zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04-12-2017 - 星期
2017/4/12 17:14:49   SEND            SMTP        zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04-12-2017 - 星期
2017/4/12 17:14:49   DELIVER         STOREDRIVER zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04-12-2017 - 星期
```

查看某一时间段，状态为deliver的投递信息
Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com -Start "2017/4/11 09:00:00" -End "2017/4/13 09:00:00" -EventId deliver

```
PS C:\share> Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com -Start "2017/4/11 09:0

Timestamp            EventId         Source      Sender                    Recipients                    MessageSubject
---------            -------         ------      ------                    ----------                    --------------
2017/4/12 17:14:49   DELIVER         STOREDRIVER zengchuixin@contoso.com   {administrator@contoso.com}   磁盘巡检情况报告 for 04
```

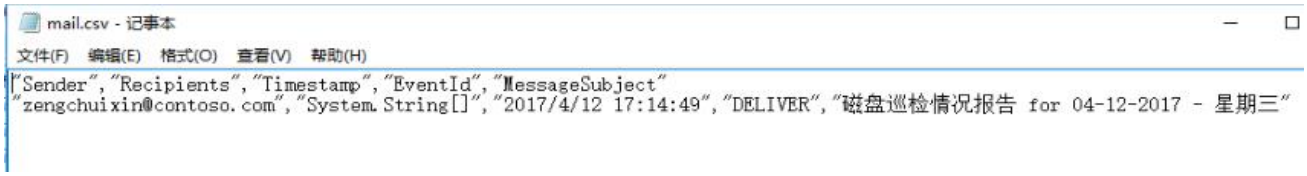
筛选结果并输出
Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com -Start "2017/4/11 09:00:00" -End "2017/4/13 09:00:00" -EventId deliver | Select Sender,Recipients,timestamp,eventid,messagesubject

```
PS C:\share> Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@con

Sender         : zengchuixin@contoso.com
Recipients     : {administrator@contoso.com}
Timestamp      : 2017/4/12 17:14:49
EventId        : DELIVER
MessageSubject : 磁盘巡检情况报告 for 04-12-2017 - 星期三
```

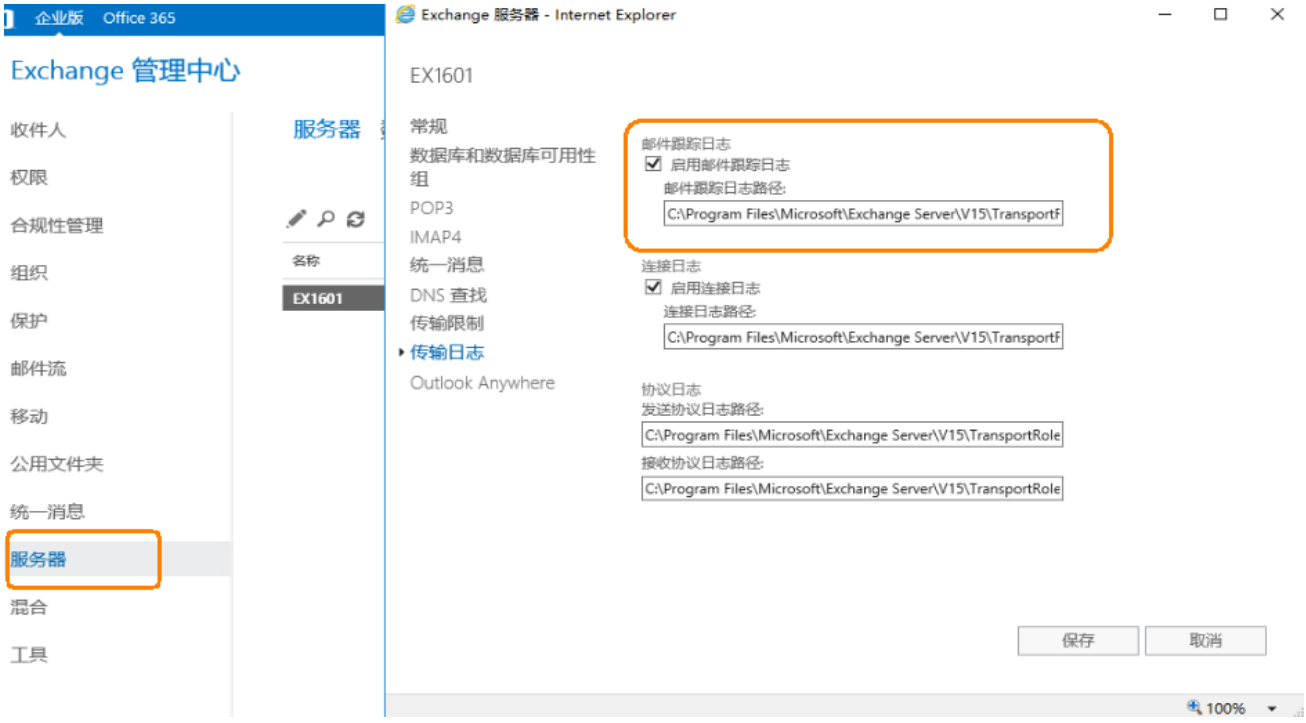
将筛选的结果输出到CSV

Get-TransportService | Get-MessageTrackingLog -Sender:zengchuixin@contoso.com -Recipients:administrator@contoso.com -Start "2017/4/11 09:00:00" -End "2017/4/13 09:00:00" -EventId deliver | Select Sender,Recipients,timestamp,eventid,messagesubject | Export-Csv c:\ps\mail.csv -Encoding Default -NoTypeInformation



进阶

查看默认服务器上传输日志的保存位置。



进入到传输日志保存的目录下面，可以看到有很多的log，这些log就是我们的传输日志文件。

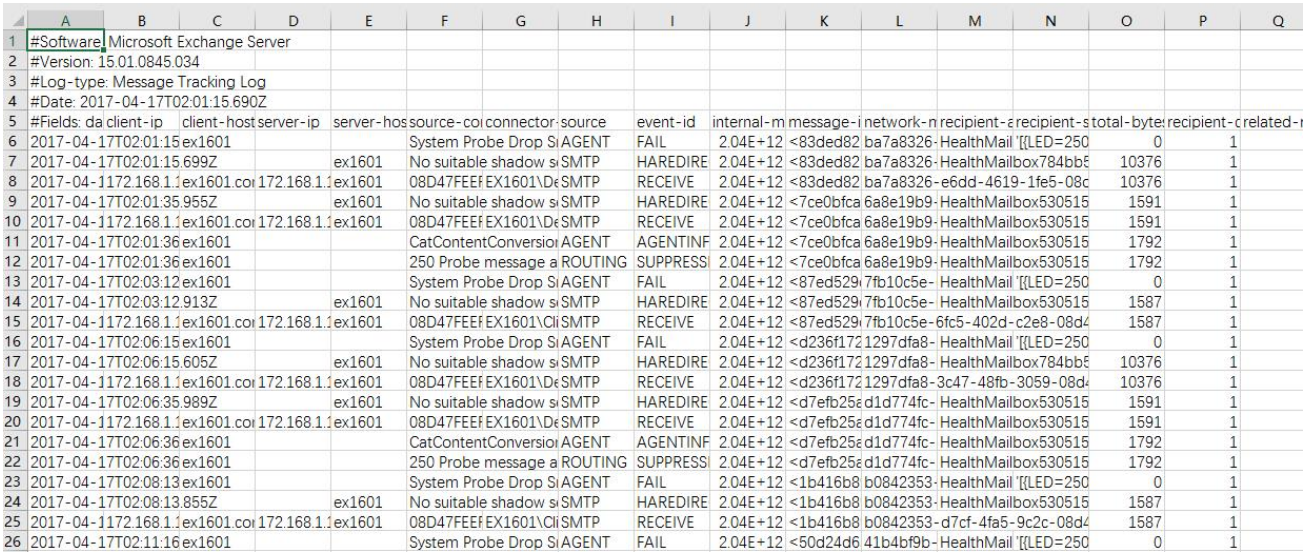
```
PS C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking> dir


    目录: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        2017/4/17     11:11                Index
-a----        2017/3/28     19:00           2742 MSGTRK2017032810-1.LOG
-a----        2017/3/28     20:00          26230 MSGTRK2017032811-1.LOG
-a----        2017/3/28     21:00          26230 MSGTRK2017032812-1.LOG
-a----        2017/3/28     22:00          26230 MSGTRK2017032813-1.LOG
-a----        2017/3/28     23:00          26230 MSGTRK2017032814-1.LOG
-a----        2017/3/29      0:00          26230 MSGTRK2017032815-1.LOG
-a----        2017/3/29      1:00          26230 MSGTRK2017032816-1.LOG
-a----        2017/3/29      2:00          26230 MSGTRK2017032817-1.LOG
-a----        2017/3/29      3:00          26230 MSGTRK2017032818-1.LOG
-a----        2017/3/29      4:00          26230 MSGTRK2017032819-1.LOG
```

除了通过命令查询之外，也可以直接打开当天的log进行查看。

可以把log文件直接拖到excel里面查看。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	#Software: Microsoft Exchange Server																
2	#Version: 15.01.0845.034																
3	#Log-type: Message Tracking Log																
4	#Date: 2017-04-17T02:01:15.690Z																
5	#Fields: da	client-ip	client-host	server-ip	server-hos	source-co	connector	source	event-id	internal-m	message-i	network-n	recipient-	recipient-s	total-byte	recipient-c	related-r
6	2017-04-17T02:01:15	ex1601				System Probe Drop Si		AGENT	FAIL	2.04E+12	<83ded82	ba7a8326-	HealthMail	'[{LED=250	0	1	
7	2017-04-17T02:01:15	699Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<83ded82	ba7a8326-	HealthMailbox784bb8		10376	1	
8	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\De	SMTP	RECEIVE	2.04E+12	<83ded82	ba7a8326-	e6dd-4619-1fe5-08c		10376	1	
9	2017-04-17T02:01:35	955Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<7ce0bfca	6a8e19b9-	HealthMailbox530515		1591	1	
10	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\De	SMTP	RECEIVE	2.04E+12	<7ce0bfca	6a8e19b9-	HealthMailbox530515		1591	1	
11	2017-04-17T02:01:36	ex1601				CatContentConversio		AGENT	AGENTINF	2.04E+12	<7ce0bfca	6a8e19b9-	HealthMailbox530515		1792	1	
12	2017-04-17T02:01:36	ex1601				250 Probe message a		ROUTING	SUPPRESS	2.04E+12	<7ce0bfca	6a8e19b9-	HealthMailbox530515		1792	1	
13	2017-04-17T02:03:12	ex1601				System Probe Drop Si		AGENT	FAIL	2.04E+12	<87ed529	7fb10c5e-	HealthMail	'[{LED=250	0	1	
14	2017-04-17T02:03:12	913Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<87ed529	7fb10c5e-	HealthMailbox530515		1587	1	
15	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\Cli	SMTP	RECEIVE	2.04E+12	<87ed529	7fb10c5e-	6fc5-402d-c2e8-08d4		1587	1	
16	2017-04-17T02:06:15	ex1601				System Probe Drop Si		AGENT	FAIL	2.04E+12	<d236f172	1297dfa8-	HealthMail	'[{LED=250	0	1	
17	2017-04-17T02:06:15	605Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<d236f172	1297dfa8-	HealthMailbox784bb8		10376	1	
18	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\De	SMTP	RECEIVE	2.04E+12	<d236f172	1297dfa8-	3c47-48fb-3059-08d4		10376	1	
19	2017-04-17T02:06:35	989Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<d7efb25a	d1d774fc-	HealthMailbox530515		1591	1	
20	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\De	SMTP	RECEIVE	2.04E+12	<d7efb25a	d1d774fc-	HealthMailbox530515		1591	1	
21	2017-04-17T02:06:36	ex1601				CatContentConversio		AGENT	AGENTINF	2.04E+12	<d7efb25a	d1d774fc-	HealthMailbox530515		1792	1	
22	2017-04-17T02:06:36	ex1601				250 Probe message a		ROUTING	SUPPRESS	2.04E+12	<d7efb25a	d1d774fc-	HealthMailbox530515		1792	1	
23	2017-04-17T02:08:13	ex1601				System Probe Drop Si		AGENT	FAIL	2.04E+12	<1b416b8	b0842353-	HealthMail	'[{LED=250	0	1	
24	2017-04-17T02:08:13	855Z			ex1601	No suitable shadow s		SMTP	HAREDIRE	2.04E+12	<1b416b8	b0842353-	HealthMailbox530515		1587	1	
25	2017-04-17	172.168.1.1	ex1601.co	172.168.1.1	ex1601	08D47FEEF	EX1601\Cli	SMTP	RECEIVE	2.04E+12	<1b416b8	b0842353-	d7cf-4fa5-9c2c-08d4		1587	1	
26	2017-04-17T02:11:16	ex1601				System Probe Drop Si		AGENT	FAIL	2.04E+12	<50d24d6	41b4bf9b-	HealthMail	'[{LED=250	0	1	

实际案例

如何通过邮件头和传输跟踪日志查看原始客户端IP - 曾垂鑫的技术专栏 - 51CTO技术博客

http://543925535.blog.51cto.com/639838/1735548