

3-1-4：邮箱管理-查询邮箱的登录创建信息

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。

使用场景

- 1) 周报，月报，年报里面需要一些统计数据；
- 2) 定期出exchange的用户创建，登录分析；
- 3) 梳理当前环境中哪些用户配置了**完全访问的权限（公共邮箱）**；

获取可以使用的属性

Get-Mailbox -Identity user3 | Get-Member

查询所有邮箱并筛选排序

```
PS C:\> Get-Mailbox | select Name,WhenCreated | Sort-Object name -Descending
```

Name	WhenCreated
投影仪2	2016/12/4 20:36:00
投影仪1	2016/12/4 14:11:47
zengchuixin101	2016/11/27 15:22:14
User9	2016/11/27 15:29:48
User8	2016/11/27 15:29:37
User7	2016/11/27 15:29:25
User6	2016/11/27 15:29:14
User5	2016/11/27 15:29:02
User4	2016/11/27 15:28:50

注意：下面的高级查询功能，如果查询不出正常的结果，建议重启Exchange 2016 RTM服务器。

按天查询创建信息

可以看到最近7天内，我们创建了发现搜索邮箱。

```
[PS] C:\>Get-Mailbox | Where-Object {$_.WhenCreated -ge ((Get-Date).AddDays(-7))}
```

Name	Alias	ServerName	ProhibitSendQuota
----	-----	-----	-----
DiscoverySearchMailbox...	DiscoverySearchMa...	ex1601	50 GB (53,687,091,200 bytes)

按月查询创建信息

```
Get-Mailbox | Where-Object {($_.WhenCreated).Month -gt 1}
```

```
PS C:\> Get-Mailbox | Where-Object {($_.WhenCreated).Month -gt 1}
```

Name	Alias	ServerName	ProhibitSendQuota
Administrator	Administrator	ex1601	Unlimited
exadmin	exadmin	ex1601	Unlimited
mailuser20	mailuser20	ex1601	Unlimited
mailuser2	mailuser2	ex1601	Unlimited
rmsuser1	rmsuser1	ex1601	Unlimited
usatest01	usatest01	ex1601	Unlimited
mailuser10	mailuser10	ex1601	Unlimited
mailuser11	mailuser11	ex1601	Unlimited
mailuser12	mailuser12	ex1601	Unlimited
mailuser13	mailuser13	ex1601	Unlimited
mailuser14	mailuser14	ex1601	11 GB (11,811,160,064 bytes)

按年查询创建信息

```
Get-Mailbox | Where-Object {($_.WhenCreated).Year -gt 2015}
```

```
PS C:\> Get-Mailbox | Where-Object {($_.WhenCreated).Year -gt 2015}
```

Name	Alias	ServerName	ProhibitSendQuota
exadmin	exadmin	ex1601	Unlimited
mailuser20	mailuser20	ex1601	Unlimited
rmsuser1	rmsuser1	ex1601	Unlimited
usatest01	usatest01	ex1601	Unlimited
mailuser10	mailuser10	ex1601	Unlimited
mailuser11	mailuser11	ex1601	Unlimited
mailuser12	mailuser12	ex1601	Unlimited
mailuser13	mailuser13	ex1601	Unlimited
mailuser14	mailuser14	ex1601	11 GB (11,811,160,064 bytes)
mailuser15	mailuser15	ex1601	Unlimited
mailuser16	mailuser16	ex1601	Unlimited

查询具有代理发送权限的邮箱

```
Get-Mailbox | Get-ADPermission | Where-Object {$_.extendedRights -like "*send-as*"} | ft -AutoSize
```

```
PS C:\> Get-Mailbox | Get-ADPermission | Where-Object {$_.extendedRights -like "*send-as*"} | ft -AutoSize
```

Identity	User	Deny	Inherited
demo.com/IT/rmsuser1	NT AUTHORITY\SELF	False	False
demo.com/USA/usatest01	NT AUTHORITY\SELF	False	False
demo.com/Users/mailuser10	NT AUTHORITY\SELF	False	False
demo.com/IT/IT1/mailuser11	NT AUTHORITY\SELF	False	False
demo.com/IT/IT1/mailuser12	NT AUTHORITY\SELF	False	False
demo.com/IT/IT1/mailuser13	NT AUTHORITY\SELF	False	False
demo.com/IT/IT1/mailuser14	NT AUTHORITY\SELF	False	False
demo.com/IT/IT1/mailuser15	NT AUTHORITY\SELF	False	False

查询具有完全访问权限的邮箱

```
Get-Mailbox | Get-MailboxPermission | Where-Object {$_.AccessRights -like "*fullaccess*"} | ft -AutoSize
```

```
PS C:\> Get-Mailbox | Get-MailboxPermission | Where-Object {$_.AccessRights -like "*fullaccess*"} | ft -AutoSize
```

Identity	User	AccessRights
demo.com/Users/Administrator	NT AUTHORITY\SELF	{FullAccess, ReadPermission}
demo.com/Users/Administrator	DEMO\administrator	{FullAccess}
demo.com/Users/Administrator	DEMO\Domain Admins	{FullAccess}
demo.com/Users/Administrator	DEMO\Enterprise Admins	{FullAccess}
demo.com/Users/Administrator	DEMO\Organization Management	{FullAccess}
demo.com/Users/Administrator	NT AUTHORITY\SYSTEM	{FullAccess}
demo.com/Users/Administrator	DEMO\administrator	{FullAccess, DeleteItem, ReadPerm.
demo.com/Users/Administrator	DEMO\Domain Admins	{FullAccess, DeleteItem, ReadPerm.
demo.com/Users/Administrator	DEMO\Enterprise Admins	{FullAccess, DeleteItem, ReadPerm.

按天查询登录信息

100天内的登陆信息

```
Get-Mailbox | Get-MailboxStatistics | Where-Object {$_.LastLogonTime -lt (get-date).AddDays(-100)}
```

```
PS C:\> Get-Mailbox | Get-MailboxStatistics | Where-Object {$_ .LastLogonTime -lt (get-date).AddDays(-100)}
```

DisplayName	ItemCount	StorageLimitStatus	LastLogonTime
exadmin	13		2016/11/27 21:25:50
mailuser20 mailuser20	19		2016/9/10 17:45:47
mailuser2	75		2016/12/3 11:59:59
rmsuser1	21		2016/11/27 15:40:25
usatest01	2		
mailuser10	12		2016/12/3 11:03:18
mailuser11	2		

查询从未登陆过的邮箱

下图代表虽然收到过邮件，但是用户从未登陆查看过。

Get-Mailbox | Get-MailboxStatistics | Where-Object {\$_ .lastlogontime -eq \$null}

```
PS C:\> Get-Mailbox | Get-MailboxStatistics | Where-Object {$_ .lastlogontime -eq $null}
```

DisplayName	ItemCount	StorageLimitStatus	LastLogonTime
usatest01	2		
mailuser11	2		
mailuser12	1		
mailuser13	2		
mailuser14	2		
mailuser15	2		
mailuser16	2		
mailuser17	2		

Get-Mailbox [https://technet.microsoft.com/ZH-CN/library/bb123685\(v=exchg.160\).aspx](https://technet.microsoft.com/ZH-CN/library/bb123685(v=exchg.160).aspx)

Get-ADPermission [https://technet.microsoft.com/zh-cn/library/bb125183\(v=exchg.160\).aspx](https://technet.microsoft.com/zh-cn/library/bb125183(v=exchg.160).aspx)

-Filter 参数的可筛选属性: Exchange 2013 Help [https://technet.microsoft.com/zh-cn/library/bb738155\(v=exchg.160\).aspx](https://technet.microsoft.com/zh-cn/library/bb738155(v=exchg.160).aspx)