An Efficient E-Mail Tracking Technique for Exchange Server

P Elayaraja[1], Mr. B GopiNath[2]
Consultant[1] & Programmer analyst[2]

Abstracts:

This paper proposes a new approach of an email tracking methods and approaches for Exchange Servers in an organization which has used to generate the various combinations of reports. People's use the scripts for various purposes and generally script has been used various think without any significant applications. But this approach can be used to develop a new field of an Email-Tracking called, An E-Mail Tracking Approaches and Methods for Exchange Servers

This paper deals with Local and remote power shell scripts using the Microsoft Technology and this concept can be used for the secure transfer of tracking emails from exchange server to local machines. This paper also verifies the bulk size of tracking emails from local/ remote location servers

Keywords: email tracking, Power Shell, Exchange Server, WMI

Introduction

An Email Tracking Mechanism is widely used for all organizations and they are monitoring their email servers mail traffics and transaction reports. Email tracking mechanism will be providing the security and confidentiality about the entire organization mail transaction. Because mail transaction is the only possible way to share the confidentiality information across the organization.

It is an advanced and cost-effective reporting approach that enables Exchange Server administrators and IT managers to obtain valuable information about all aspects of their email system. It is an Exchange Server mail tracking and Log Reporting solution that addresses collecting, archiving and reporting all types of mail transaction details from your Exchange Server. Our approaches allows you to track and import the Exchange Message Tracking Log data to a database and generate reports on all mail transactions in your Exchange Server.

With its powerful and easy-to-understand features, Email Tracking Mechanism produces comprehensive reports that you can rely on to ensure better security, business continuity, and to improve Exchange organization performance.

Email Tracking Mechanism about several types of Mail Transaction reports, Mail Status reports and Traffic reports. You can specify report filter criteria to view reports on Sender Mails, Recipients mails, Distribution groups/lists etc. across Exchange mail users in the Exchange Organization. The reports can be generated for the Exchange Organization and Administrative Group based on the message tracking logs that are stored in your Exchange Server message tracking transport logs.

The following information fields are available across the Exchange Servers in the Exchange Organization: Mail transaction Date & Time, Client IP, Client Host Name, Server IP, Server Host Name, Source Context, Connector ID, Source, Event ID, Internal Message ID, Message ID, Recipient Address, Recipient Status, Total Bytes, Recipient Count, Related Recipient Address, Reference, Message Subject, Sender Address, Return Path, Message Info, Directionality, Tenant ID, Original Client IP and Original Server IP.

Our proposed approach supports to Microsoft Exchange Server 2013 / 2010 / 2007 and 2003.

The proposed approach provides the following major reporting features to address different users' reporting requirements – Email Collector, Email Tracking Reports and Tracking History for Exchange server 2003 to 2013 versions

Algorithm and Script Design:

Exchange Server 2013/2013:

Server URL: http://ServerFQDNname/powershell?serializationLevel=Full

```
Shell URI: http://schemas.microsoft.com/powershell/Microsoft.Exchange

Snappins: Microsoft.Exchange.Management.PowerShell.Admin

Sample Script: Get-MessageTrackingLog -Server Mailbox01 -Start "03/13/2013 09:00:00"
-End "03/15/2013 17:00:00" -Sender john@contoso.com
```

- The dashes are removed from the field names. For example **internal-message-id** is displayed as `InternalMessageId`.
- The **date-time** field is displayed as `Timestamp`.
- The **recipient-address** field is displayed as `Recipients`.
- The **sender-address** field is displayed as `Sender`.

Exchange Server 2007: The following scripts supports only local machine or Exchange server trusted domain machines

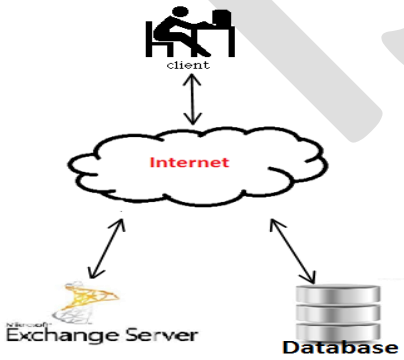
```
Sample Script: Get-Exchangeserver|where {$_.isHubTransportServer -eq $true -or
$_.isMailboxServer -eq $true}|Get-MessageTrackingLog -ResultSize Unlimited
```

Exchange Server 2003:

Connection Path: `\\EchangeServerName\root\MicrosoftExchangeV2`

```
WQL Query: Select * from Exchange_MessageTrackingEntry
```

Client & Exchange Server:



Report Categories

Email Tracking Reports: Provides all mail transaction reports and status reports based on Exchange mail transaction for viewing, printing, exporting and e-mailing the reports.

Track Now: Provides the facility to import data from Exchange Server Message Tracking Transport Log to the application database based on Exchange mail transaction.

Track at Scheduled intervals: Provides the facility to import data from Exchange Server Message Tracking Transport Log to the Application database, at scheduled intervals, which is recommended for regular automatic mail tracking and importing to the application database.

Traffic Reports: Provides various text and graphical (chart) reports based on the e-mail transaction information. This info include number of e-mails sent, e-mail size, number of senders, number of recipients, subject, etc.

Scheduled Traffic Reports: All Traffic Reports operations can be easily automated, scheduled and published to various destinations in different format with the help of task scheduler.

Sample Reports:

Message ID	Message Subject	Total Bytes	Sender
<18AFA4F827C54645B76A65FABD7AB3006BCD@Rd49.Adventure.local>	Help me..	11655	MikeFeng@adventure.local
<18AFA4F827C54645B76A65FABD7AB30002C10A@Rd49.Adventure.local>	Process Flow	5532	MikeFeng@adventure.local
<912961E2EBF6B840820CC824D8782CA702B94A@Rd49.Adventure.local>	RE: Status Report	7946	MaeffyJoSwa@adventure.local
<912961E2EBF6B840820CC824D8782CA702C11F@Rd49.Adventure.local>	RE: Software Support Submission Form	13219	MaeffyJoSwa@adventure.local
<912961E2EBF6B840820CC824D8782CA702C125@Rd49.Adventure.local>	RE: Regarding product testing	9118	MaeffyJoSwa@adventure.local
<912961E2EBF6B840820CC824D8782CA702C12B@Rd49.Adventure.local>	RE: Regarding product testing	7641	MaeffyJoSwa@adventure.local
<94D5A57D89CB40499362A15FFE13E08662EE35@Rd49.Adventure.local>	RE: Regarding product testing	8742	Andresson@adventure.local
		8920	Andresson@adventure.local
<3a936314-e2e6-4f2a-b400-05af3e5e95e4@Rd49.Adventure.local>	Undeliverable: FW: Software Support Submission Form	12378	MicrosoftExchange329e71ec88ae

Permissions required for an Email Tracking Mechanism

The currently logged-on user, or the user-credentials entered for the Exchange Server login should have:

The user at least any one member of the following groups for collect the data in Email Tracking Mechanism

- For Exchange Server 2013/2010
  - Organization Management(Microsoft Exchange Security Groups)
  - Hygiene Management (Microsoft Exchange Security Groups)
  - Recipient Management (Microsoft Exchange Security Groups)
  - Records Management (Microsoft Exchange Security Groups)
  - View-Only Organization Management (Microsoft Exchange Security Groups)
- For Exchange Server 2007

- o Exchange Organization Administrators
- o Exchange Public Folder Administrators
- o Exchange Recipient Administrators
- o Exchange View-Only Administrators
- • For Exchange Server 2003
- o Domain Administrators (Designated administrators of the domain)

Important: The client machine should have installed the Exchange Server 2007 Management Tool, and it should be the member of the same domain as the Exchange Server 2007, or a trusted domain, for to collect the data from the Exchange Server 2007. Without installing the Exchange 2007 Management tool, and Exchange 2007 credentials, it cannot collect data from the Exchange Server 2007 by using the other computers.

Tracking Reports features reports the following types of mail transactions:

1. All mail transactions
2. DELIVER Mail Report
3. DEFER Mail Report
4. DSN Mail Report
5. DUPLICATEDELIVER Mail Report
6. EXPAND Mail Report
7. FAIL Mail Report
8. POISONMESSAGE Mail Report
9. RECEIVE Mail Report
10. REDIRECT Mail Report
11. RESOLVE Mail Report
12. SEND Mail Report
13. SUBMIT Mail Report
14. TRANSFER Mail Report

Traffic Reports feature reports the following email traffic, and Exchange Server Traffic reports:

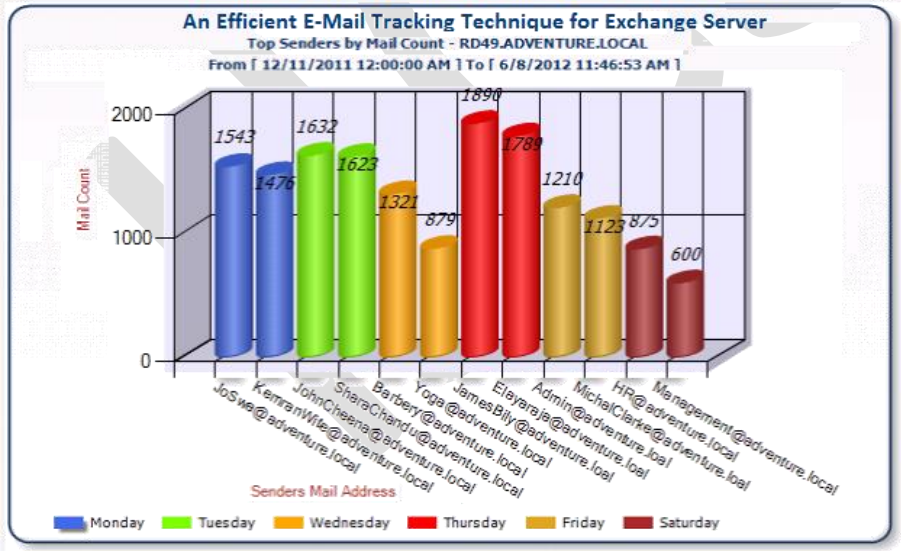
1. Top Senders by Mail Count
2. Top Senders by Mail Size
3. Top Senders by Recipient Count
4. Top Senders to Groups by Mail Count
5. Top Senders to Groups by Mail Size
6. Top Recipients by Mail Count
7. Top Recipients by Mail Size
8. Top Groups by Received Mail Count
9. Top Groups by Received Mail Size
10. Mail Count by Client IP
11. Mail Count by Server Host Name
12. Mail Count by Subject
13. Mail Count by Size Range
14. Mail Count by Custom Size Range
15. Mail Size by Client IP
16. Mail Size by Subject

Sample Traffic Reports:

Data Range : From [12/11/2011 12:00:00 AM] To [6/8/2012 11:46:53 AM]

Summarize by Day of week	Sender Address	Total Count
Monday	JoSwa@Adventure.local	1543
	KemranWite@adventure.local	1476
	JamesBilly@discoverus.local	1367
	JoregeTRichard@adventure.local	1208
	Adminuser@adventure.local	1207
Tuesday	JohnCheena@adventure.local	1632
	SharaChandu@adventure.local	1623
	JoSwaP?@adventure.local	1547
	JamesBilly@discoverus.local	1459
Wednesday	Barbery@adventure.local	1321
	YowanKem@adventure.local	879
	SharaChandu@adventure.local	832
Thursday	JamesBilly@discoverus.local	1890
	JoJames@adventure.local	1789
	KemranWite@adventure.local	1231

Traffic Graphical Reports



The Traffic Reports feature provides several types of reports about mail transaction traffics and Traffic in the Exchange Organization. These reports can be generated for the Exchange Organization based on the message tracking logs that are stored in your Exchange Server and subsequently stored in the application database.

CONCLUSION & FUTURE WORK:

In this paper a new concept of email tracking mechanism for Exchange Server 2013/2010/2007 and 2003 and it has been introduced for information security and network security. Detailed steps with illustrations, of the concept have been described. Also the strength of the algorithm is discussed by explaining the features of Email Tracking mechanism across the organizations. This concept can be further enhanced by adding digital signatures to the data transfer process. Also to avoid the tracking complexity in the bulk size of (1 TB or above), and tracking the attached file detail,. This concept can be used for basic applications such as Intranet mail transactions and internet mail transactions

REFERENCES:

[1]Rand Morimoto, Michael Noel, Chris Amaris, Andrew Abbate, and Mark Weinhardt"Exchange Server 2010 Unleashed"
[2]Siegfried Jagott and Joel Stidley "Microsoft® Exchange Server 2010 Best Practices (Best Practices (Microsoft))"
[3]Mike Pfeiffer "Microsoft Exchange 2010 PowerShell Cookbook"
[4]Rand Morimoto, Michael Noel, Guy Yardeni and Chris Amaris "Microsoft Exchange Server 2013 Unleashed"
[5]Richard Luckett, William Lefkovics and Bharat Suneja "Microsoft Exchange Server 2007 Complete Reference"
[6] http://exchangeserverpro.com/exchange-2010-message-tracking/
[7] http://technet.microsoft.com/en-us/library/bb124375(v=exchg.150).aspx
[8]William R. Stanek "Microsoft Exchange Server 2003 Administrator's Pocket Consultant"
[9]Richard Siddaway "PowerShell and WMI"
[10]Matthew Lavy and Ashley Meggitt "Windows Management Instrumentation (WMI)"