Tạo báo cáo đồ họa cho Exchange 2007

Trong loạt bài này chúng tôi sẽ giới thiệu cho các bạn về cách tạo những báo cáo bằng đồ họa bắt mắt từ các phần mềm dành cho Exchange Server.

Giới thiệu

Một trong những yêu cầu phổ biến nhất từ tất cả các nhà quản trị thư tín trên toàn thế giới là khả năng tạo các báo cáo toàn diện cho môi trường mà họ quản lý. Nếu một bức tranh đáng giá hàng nghìn từ thì mọi người có thể hiểu một cách dễ dàng sự cần thiết phải chuyển đổi hàng nghìn file bản ghi mà một máy chủ Exchange có thể tạo vào một thứ gì đó thân thiện với con người.

Từ khi Exchange Server 2007 (và tất cả các phiên bản trước đó) không có khả năng tạo các báo cáo đồ họa phong phú, tuy nhiên có một vài công ty đã khỏa lấp khoảng trống này bằng cách xây dựng các phần mềm báo cáo cho Microsoft Exchange.

Với Microsoft, phát hành khổng lồ của phần mềm năm 2005, SQL Server 2000 Report Pack for Microsoft Exchange, là một phiên bản riêng của Exchange Reporter, một phần mềm thương mại được phát triển bởi công ty và mang tên gọi SSW. Thực sự có rất ít người đã sử dụng SQL Server 2000 Report Pack for Microsoft Exchange vì các yêu cầu của SQL Server và SQL Server Reporting Services đòi hỏi khá cao.

Microsoft đã thực hiện động thái khá thú vị với một phương pháp khác. Microsoft Operations Manager (MOM) 2005 với Exchange Server Management Pack có nhiều tính năng tạo báo cáo rất mạnh. Tuy nhiên Exchange Server Management Pack cho phiên bản tiếp theo của phần mềm quản lý Microsoft, System Center Operations Manager (SCOM) 2007 đã mất đi một số báo cáo trước đó vẫn có. Mặc dù vậy Microsoft Exchange Server 2007 Management Pack for System Center Operations Manager 2007 R2 mới

nhất có cung cấp đến hơn 30 báo cáo cụ thể cho Exchange Server 2007 để kiểm tra khả năng sẵn có và hiệu suất.

Khi chúng tôi quyết định giới thiệu hướng dẫn này, chúng tôi chưa bao giờ có ý tưởng sử dụng phần mềm thương mại, hoặc sử dụng các tính năng báo cáo của phần mềm quản lý hệ thống mà thay vì đó chúng tôi muốn cung cấp cho các bạn nhiều khả năng báo cáo bằng đồ họa cho Exchange Server, bằng cách sử dụng một công cụ đơn giản và miễn phí, một số từ Microsoft, còn số khác được phát triển bởi Microsoft MVP và một số cá nhân trên khắp thế giới.

Tất cả nằm ở các file bản ghi

Ở trên chúng tôi đã giới thiệu rằng Exchange Server không có các tính năng báo cáo bằng đồ họa nguyên bản, tuy nhiên điều này không có nghĩa rằng nó không thể tạo ra các thông tin mà bạn cần (thậm chí còn nhiều hơn). Tất cả đều nằm ở các file bản ghi!

Bạn biết được những kiểu file bản ghi thông tin gì có trong tổ chức Exchange Server thông thường? Bảng 1 dưới đây sẽ liệt kê các bảng ghi chung nhất. Lưu ý rằng các bản ghi này có thể trải rộng trong toàn bộ các máy chủ Exchange, lý do là tất cả các role Exchange sẽ không thể đặt trên cùng một máy.

Bản ghi	**Đường dẫn mặc định**
Protocol Logs (SMTP Send)	\Exchange Server\TransportRoles\Logs\ProtocolLog\SmtpSend
Protocol Logs (SMTP Receive)	\Exchange Server\TransportRoles\Logs\ProtocolLog\SmtpReceive
Agent Logs	\Exchange Server\TransportRoles\Logs\AgentLog
IIS Logs	[Windows 2003] \Windows\System32\LogFiles\W3SVC1

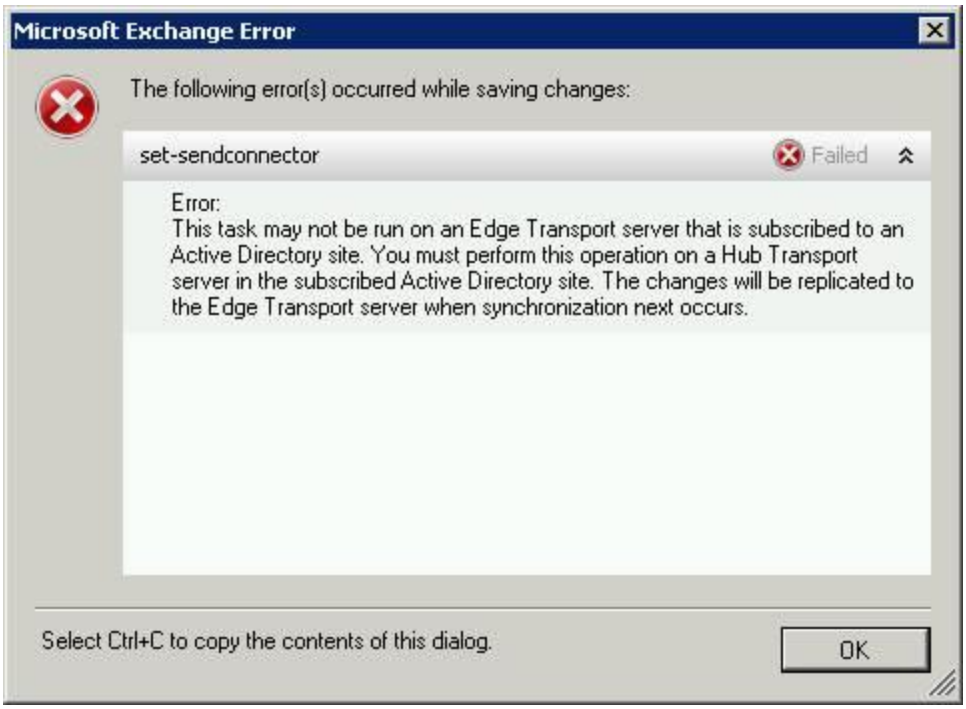
	[Windows 2008] \Inetpub\Logs\LogFiles\W3SVC1
Message Tracking Logs	\Exchange Server\TransportRoles\Logs\MessageTracking
POP3/IMAP Logs	\Exchange Server\ClientAccess\PopImap
Connectivity Logs	\Exchange Server\TransportRoles\Logs\Connectivity
Pipeline Tracing Logs	\Exchange Server\Transport Roles\Logs\PipelineTracing
Routing Table Logs	\Exchange Server\TransportRoles\Logs\Routing
MRM Logs	\Exchange Server\Logging\Managed Folder Assistant

Bảng 1: Các file bản ghi chung trong Exchange

Bước tiếp theo là cấu hình đúng mức ghi, do không phải tất cả các bản ghi đều được kích hoạt mặc định và một trong số chúng cần một vài điều chỉnh đối với dữ liệu lịch mà chúng ta muốn giữ.

Trong phần này, chúng tôi sẽ chỉ sử dụng 5 file bản ghi từ bảng trên. Trong 5 bản ghi này, có hai bản ghi không được kích hoạt mặc định là các bản ghi giao thức: SMTP Send và SMTP Receive. Mức ghi truyền tải SMTP được điều khiển tại mức connector của Exchange.

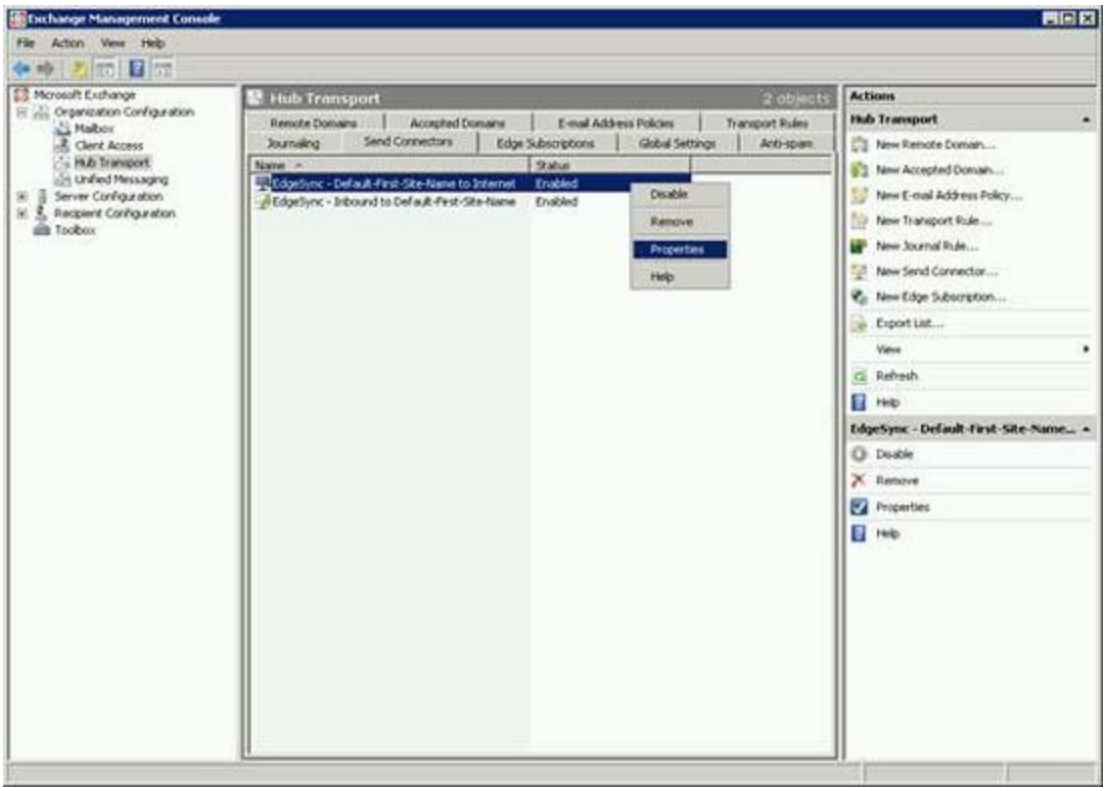
Để tạo các báo cáo đồ họa Exchange hữu dụng, chúng tôi giả sử rằng các bản ghi giao thức từ các máy chủ trên đường biên của mạng là rất quan trọng, vì chúng đăng ký các phiên giao dịch SMTP từ mail vào hoặc ra khỏi tổ chức của bạn. Trong trường hợp bạn đã triển khai máy chủ truyền tải Edge, các bản ghi này có thể được cấu hình từ máy chủ Hub Transport bên trong (nếu chỉnh sửa các thuộc tính của connector từ máy chủ Edge, bạn sẽ nhận được lỗi như thể hiện trong hình 1).



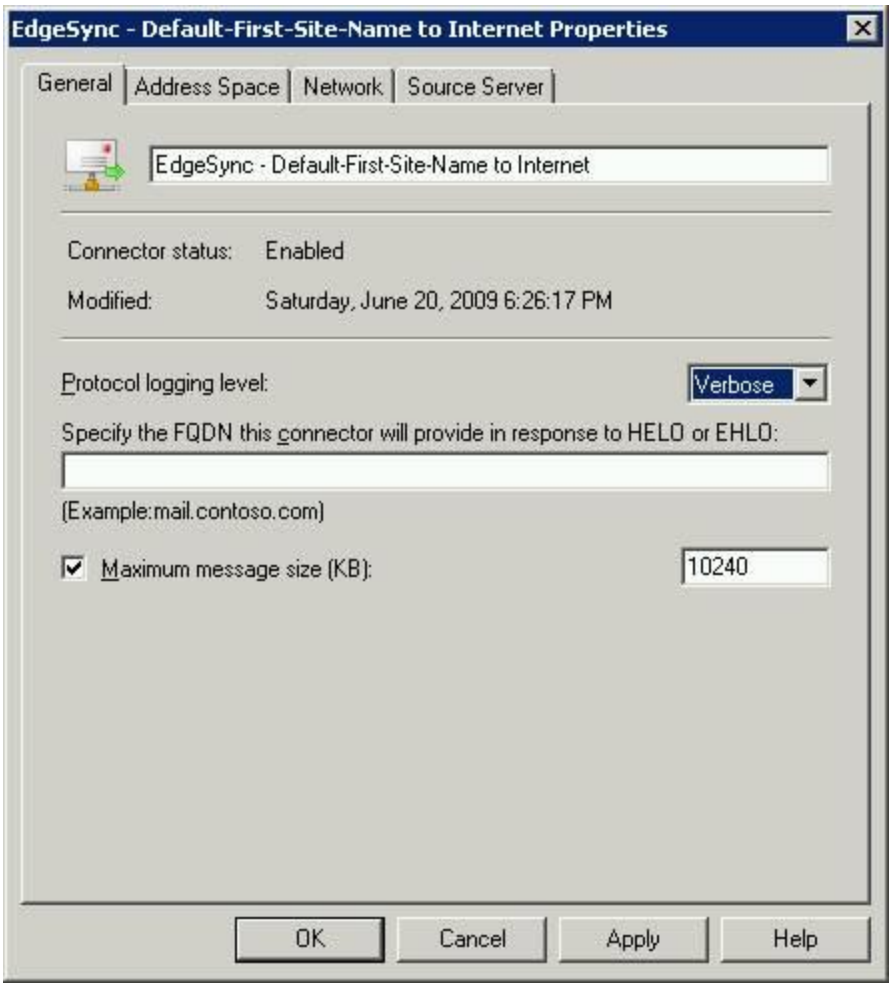
Hình 1: Lỗi trong khi thay đổi mức khi trên Edge server

Để kích hoạt SMTP Protocol Logs của EdgeSync Send Connectors, bạn hãy mở Exchange Management Console, mở **Organization Configuration**, chọn **Hub Transport,**sau đó trên panel bên phải, kích tab **Send Connectors**. Kích chuột phải vào hai connector và chọn **Properties** (hình 2).

Trên cửa sổ EdgeSync Connector Properties, thay đổi **Protocol logging level** thành **Verbose** (hình 3).



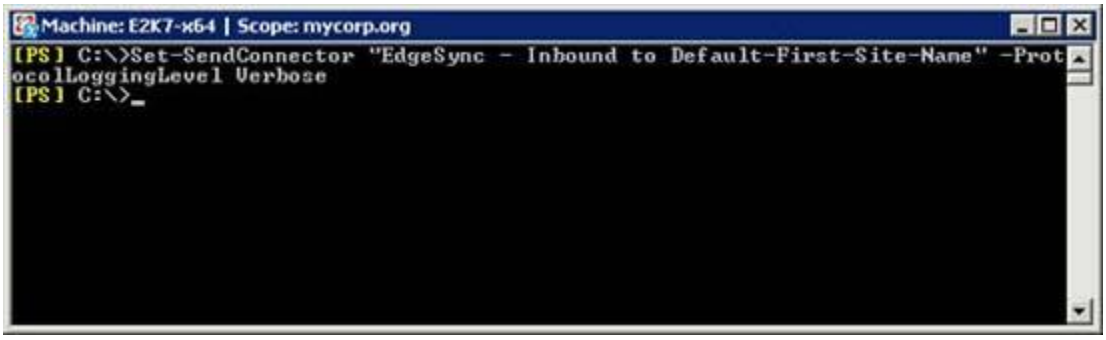
Hình 2: Cấu hình EdgeSync Send Connector



Hình 3: Các thuộc tính EdgeSync Send Connector

Nếu bạn thích sử dụng PowerShell, chạy lệnh dưới đây (cho cả hai connector) để thiết lập mức ghi là Verbose (hình 4):

Set-SendConnector "EdgeSync - Inbound to Default-First-Site-Name" -ProtocolLoggingLevel Verbose



Hình 4: Thay đổi mức ghi bằng PowerShell

Sau khi kích hoạt SMTP Transport Logs, chúng ta phải định nghĩa số lượng dữ liệu lịch sử cần giữ. Exchange Server cho phép chúng ta điều khiển kích thước file bản ghi tối đa, kích thước thư mục tối đa và tuổi thọ của file bản ghi tối đa bằng lệnh *Set-TransportServer*trong PowerShell.

Các tham số *SendProtocolLogMaxDirectorySize* và *ReceiveProtocolLogMaxDirectorySize*chỉ định kích thước tối đa của các thư mục Send và Receive Connector Protocol Log. Khi đạt đến kích thước thư mục tối đa, máy chủ sẽ xóa các file bản ghi cũ nhất. Giá trị tối thiểu là 1MB, giá trị mặc định được thiết lập là 250MB.

Do kích thước mặc định 250MB là không đủ, nên chúng ta hãy thay đổi kích thước tối đa của thư mục Send Connector thành 2GB và Receive connector thành 4GB bằng cách sử dụng lệnh Exchange Management Shell:

Set-TransportServer -Identity E2K7EDGE -
SendProtocolLogMaxDirectorySize 2048MB -
ReceiveProtocolLogMaxDirectorySize 4096MB

Lúc này chúng ta đã sẵn sàng với các bản ghi của mình, đây là lúc bắt đầu phân tích chúng.

Cần phải biết rằng, phụ thuộc vào chất lượng dữ liệu bạn đang phân tích, việc phân tích cú pháp và xử lý các bản ghi có thể diễn ra nhanh hay chậm.

Phân tích cú pháp bản ghi

Bộ phân tích cú pháp bản ghi Log Parser là một công cụ khá mạnh, cho phép bạn truy vấn dữ liệu văn bản chẳng hạn như các file bản ghi, các file XML, các file CSV cũng như nguồn dữ liệu chính trên hệ điều hành Windows, Event Log, Registry, hệ thống file hoặc thậm chí cả Active Directory. Ngoài khả năng cung cấp các thông tin phân tích cú pháp, Log Parser còn cho kết

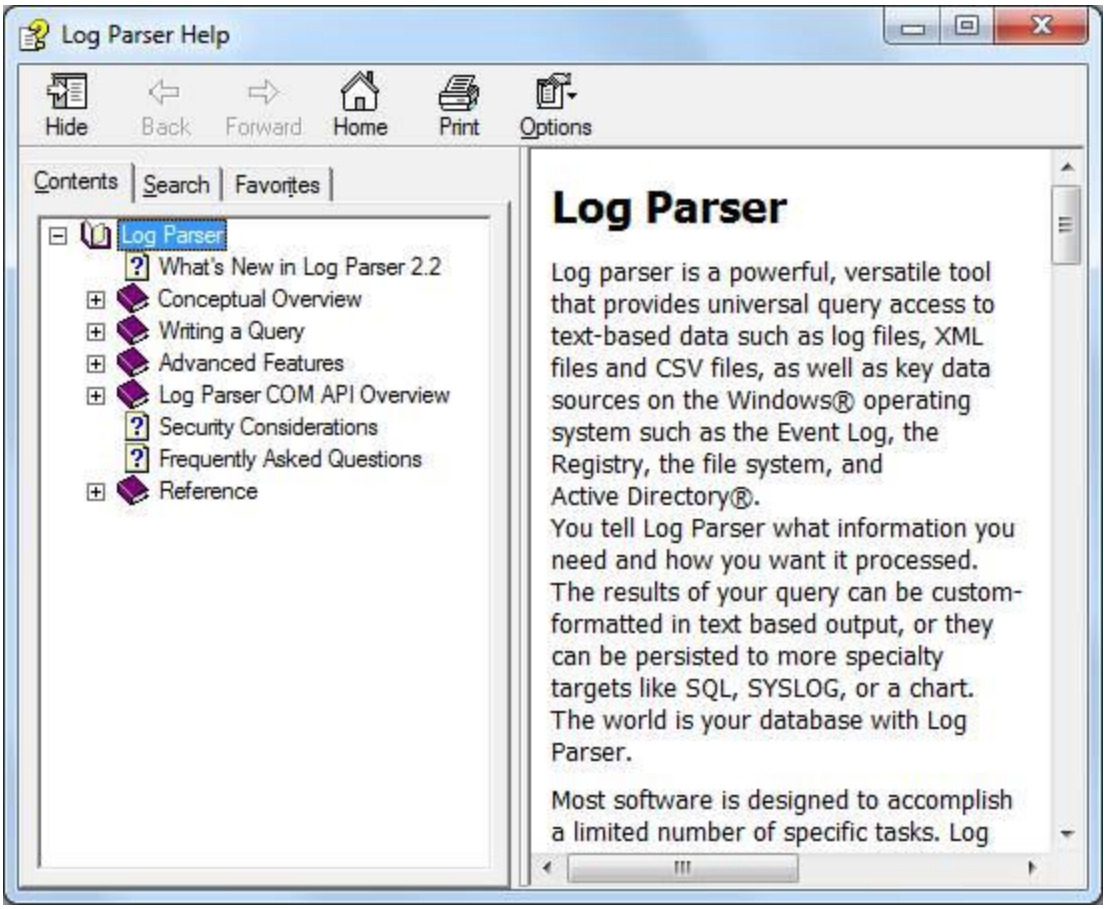
quả các truy vấn dưới định dạng tùy chỉnh ở đầu ra, chẳng hạn như lưới dữ liệu datagrid, hoặc có thể chuyển đổi thành các biểu đồ trực quan.

Log Parser không cần được cài đặt trên Exchange Server, tất cả những gì bạn cần thực hiện là bảo đảm sự truy cập cho các thư mục bản ghi của Exchange.

Thực hiện theo hướng dẫn dưới đây để cài đặt Microsoft Log Parser:

1. Download và cài đặt Microsoft Logparser 2.2.
2. Download và cài đặt Office 2003 Add-in: Office Web Components. Đây là thao tác cần thiết để cung cấp tính năng đồ họa cho Log Parser.
3. Download và cài đặt Microsoft Office 2003 Web Components Service Pack 1 (SP1) for the 2007 Microsoft Office System.

Log Parser có một file trợ giúp khá đầy đủ (hình 5), mặc định nằm tại C:\Program Files (x86)\Log Parser 2.2, các bạn nên đọc cẩn thận trợ giúp này. Cũng có một vài ví dụ được cung cấp tại C:\Program Files (x86)\Log Parser 2.2\Samples để các bạn có thể tham khảo.



Hình 5: File Log Parser

Trong các phần tiếp theo, chúng tôi sẽ giới thiệu cho các bạn một số ví dụ về các truy vấn của Log Parser dùng để tạo các báo cáo trực quan mong muốn. Các truy vấn này có thể được chạy trực tiếp từ dòng lệnh hoặc bạn có thể tạo các file batch khác với mỗi một truy vấn (nên thực hiện).

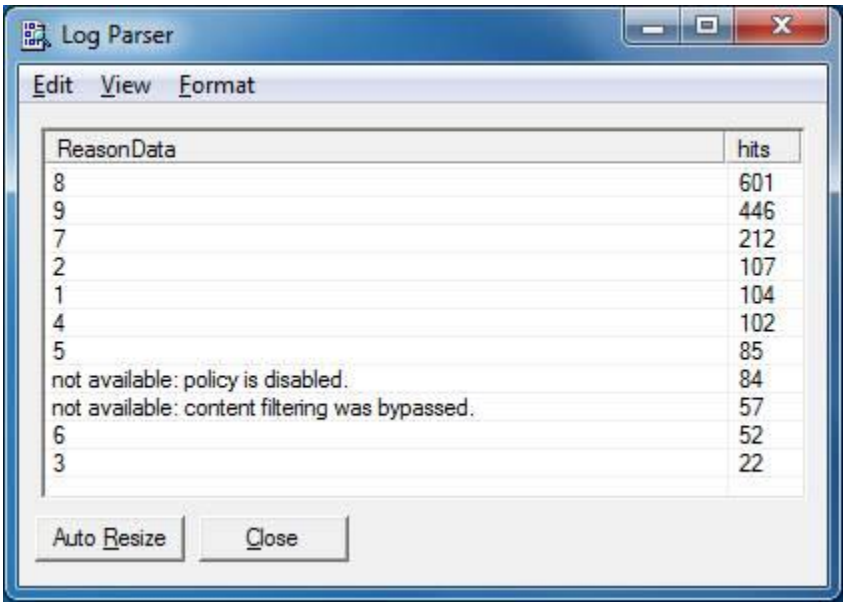
Các báo cáo sử dụng Log Parser với các bản ghi Agent

Nếu bạn đang sử dụng các tác nhân (agent) anti-spam của Exchange Server, có một vài báo cáo chúng ta có thể nhận bằng cách phân tích các bản ghi Agent. Các bản ghi này nằm trên máy chủ Exchange Edge, nếu bạn đang sử dụng nó, hoặc trong máy chủ Exchange Hub, trong trường hợp nó đã kích hoạt các tác nhân anti-spam và đang chạy.

Để có được ý tưởng về mail đang đi vào tổ chức của bạn, chúng ta có thể bắt đầu bằng cách tổ chức số các thư theo Spam Confidence Level (SCL) của chúng và hiển thị chúng trong dạng datagrid.

Đây là lệnh tạo datagrid đó (hình 6):

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT ReasonData, count(*) AS hits FROM C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\AgentLog\AGENT*.log WHERE ReasonData<>NULL GROUP BY ReasonData ORDER BY hits DESC" -i:CSV -nSkipLines:4  -o:DATAGRID -dtlines:800 -rtp:-1
```

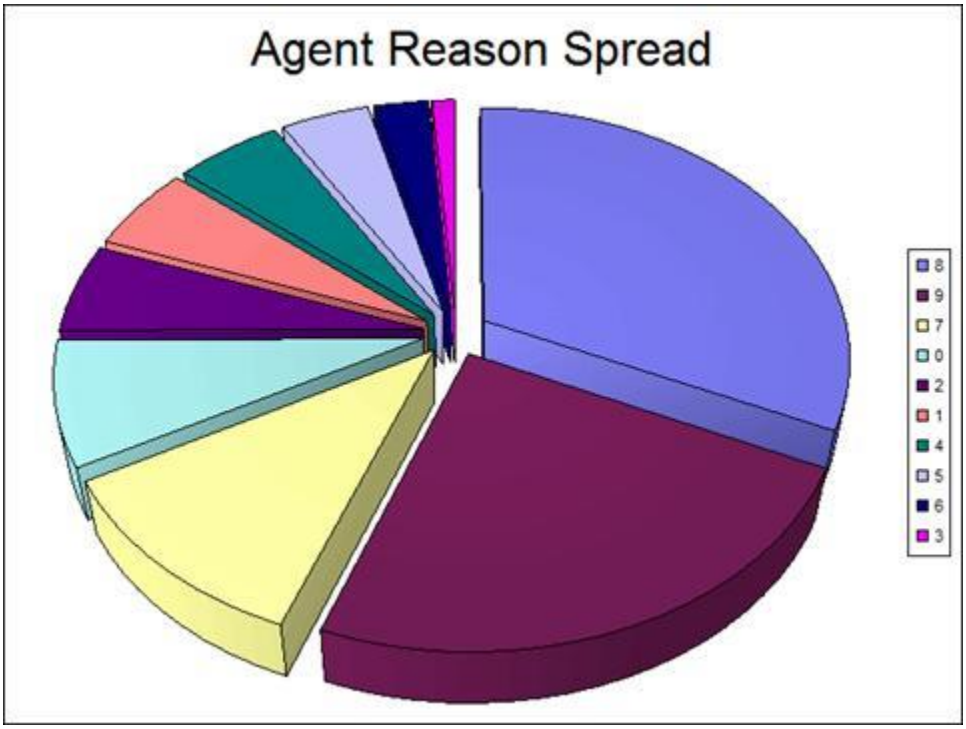


Hình 6: Agent reason spread (Datagrid)

Nếu bạn thích một biểu đồ cho các kết quả trước, cách thực hiện rất dễ dàng. Bằng cách sử dụng tham số *–chartType:PieExplode3D* trong lệnh dưới đây, chúng ta sẽ nhận được một biểu đồ trực quan như thể hiện trong hình 7.

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT CASE TO_INT(ReasonData) WHEN NULL THEN 0 ELSE TO_INT(ReasonData)
```

```
END AS ReasonData2, count(*) AS hits INTO agentreasonspread.gif from
C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\AgentLog\AGENT*.
log GROUP BY ReasonData2 ORDER BY hits DESC" -i:CSV -
nSkipLines:4  -o:CHART  -chartType:PieExploded3D -chartTitle:"Agent
Reason Spread" -e 200 -dtlines:600
```

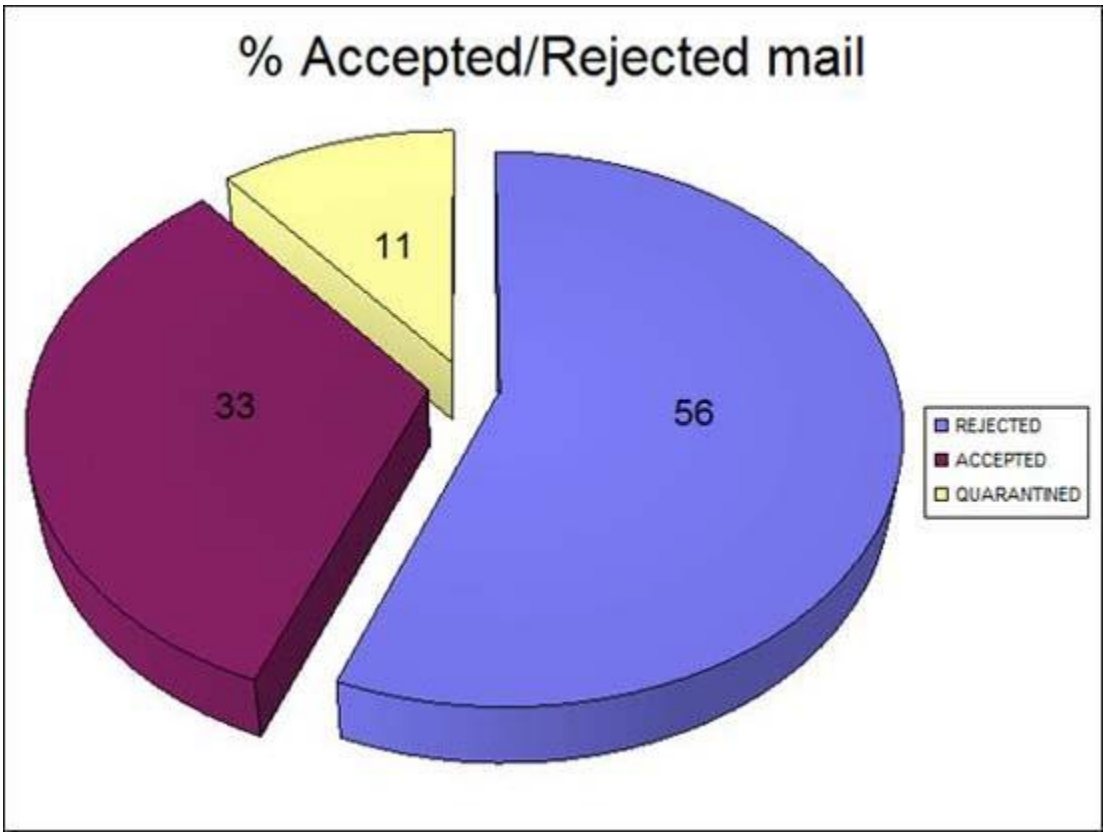


Hình 7: Agent reason spread

Mặc dù SCL thay đổi từ 1 đến 9, nhưng các bạn sẽ thấy rằng có một lát mỏng của biểu đồ trước có giá trị 0. Giá trị 0 biểu thị cho tất cả chính sách bị vô hiệu hóa và chức năng lọc nội dung bị vô hiệu hóa (xem datagrid trước), nghĩa rằng nó thể hiện mail đi vào tổ chức bạn.

Nếu bạn thích có một khung nhìn hợp nhất hơn đối với biểu đồ trước, với chỉ mail được chấp nhận và được loại bỏ, truy vấn logparser dưới đây sẽ thực hiện công việc đó. Lưu ý rằng các thư có tỉ lệ SCL bằng 8 hoặc cao hơn sẽ được coi như bị loại bỏ, SCL 7 có nghĩa bị cách ly, còn lại là được chấp nhận.

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT CASE TO_INT(ReasonData) WHEN 9 THEN 'REJECTED' WHEN 8 THEN 'REJECTED' WHEN 7 THEN 'QUARANTINED' ELSE 'ACCEPTED' END AS ReasonData2, TO_INT(mul(100.0,PropCount(*))) as Percent, count(*) as hits INTO agentAcceptedRejected.gif FROM C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\AgentLog\AGENT*.log GROUP BY ReasonData2 ORDER BY hits DESC" -i:CSV -nSkipLines:4  -o:CHART -chartType:PieExploded3D -chartTitle:"%% Accepted/Rejected mail" -dtlines:600 -categories:OFF -values:ON -view:ON
```



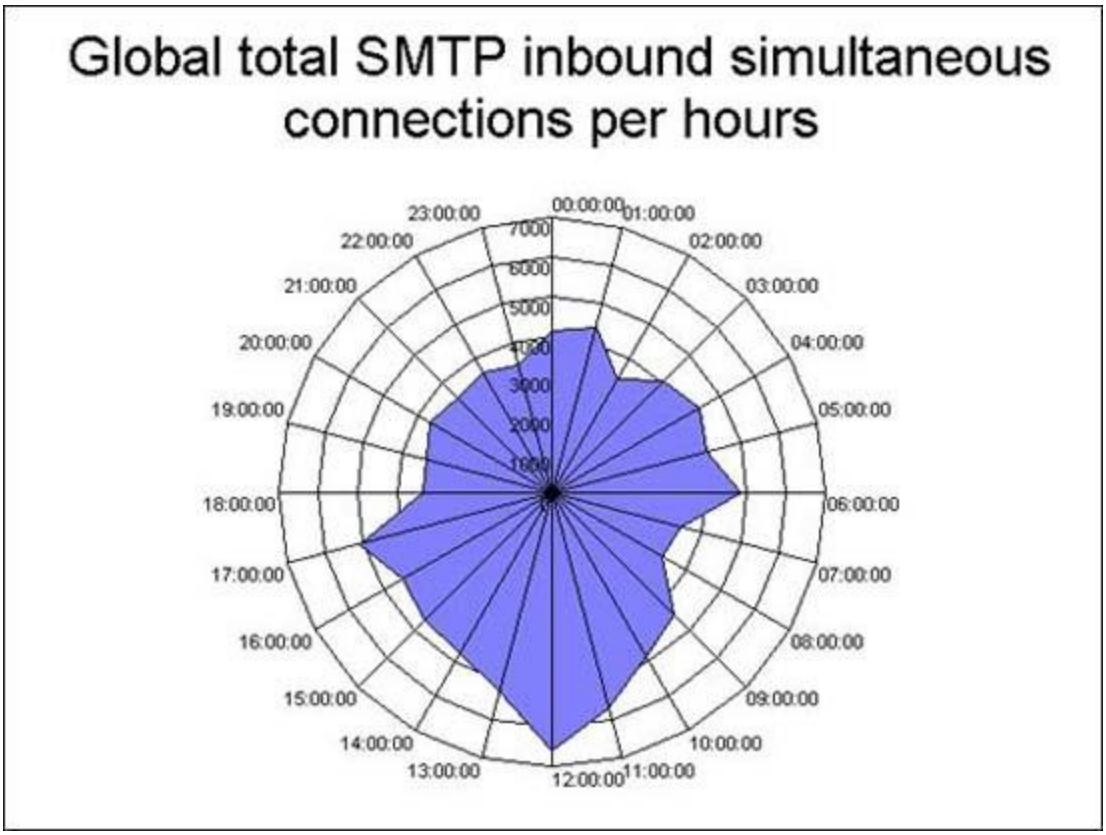
Hình 8: % mail được chấp nhận và được loại bỏ

Các báo cáo bằng Log Parser với các bản ghi giao thức

Phần tiếp theo, chúng ta sẽ sử dụng các bản ghi giao thức SMTP. Với các bản ghi giao thức này, chúng ta có thể trích các thông tin hữu dụng về phân vùng của các kết nối SMTP và về các host (không phải người dùng).

Để có một image của Total Inbound Simultaneous Connections, chúng ta sẽ sử dụng mã dưới đây:

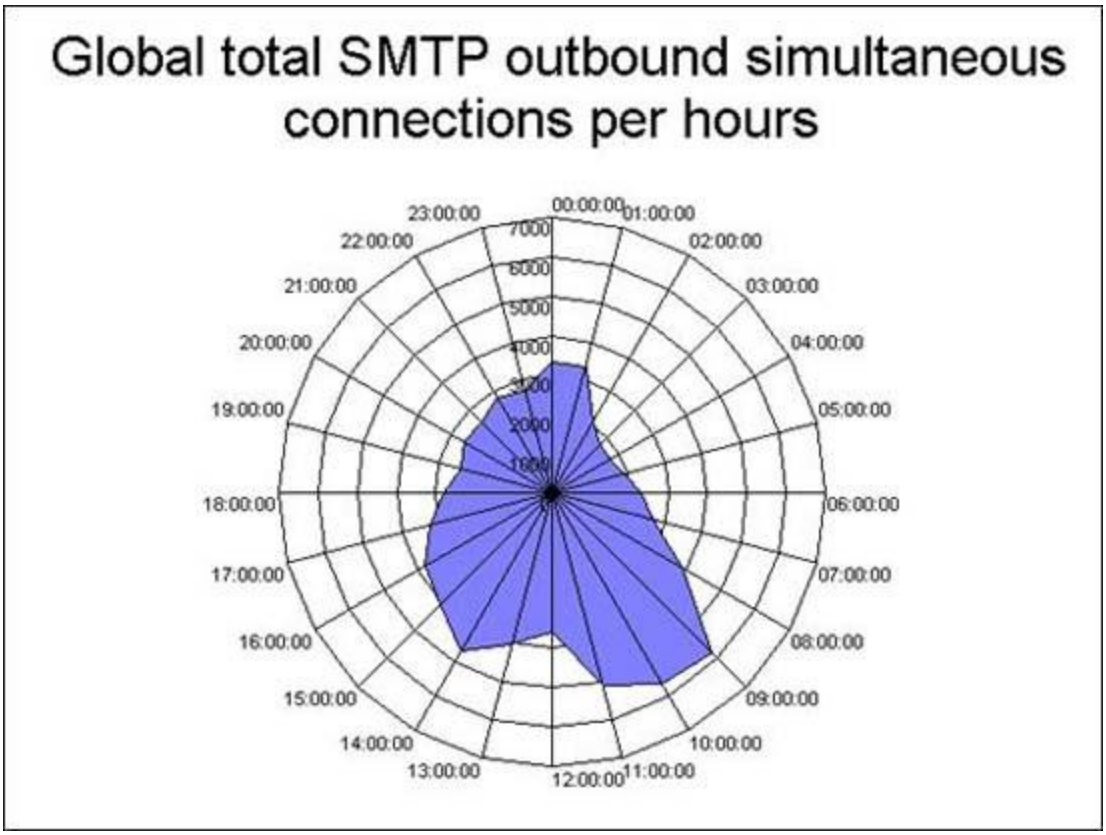
```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT
QUANTIZE(TO_TIMESTAMP
(EXTRACT_PREFIX(TO_STRING(EXTRACT_SUFFIX([#Fields: date-
time],0,'T')),0,'.'), 'hh:mm:ss'),3600) AS Hour, COUNT(*) AS Hits INTO
radar_traffic.gif FROM
C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\ProtocolLog\SmtpRe
ceive\RECV*.LOG WHERE event='+' GROUP BY Hour ORDER BY Hour
ASC" -i:CSV -nSkipLines:4 -o:CHART -charttype:RadarLineFilled -
charttitle:" Global total SMTP inbound simultaneous connections per hours"
```



Hình 9: Các kết nối SMTP đi vào

Nếu bạn thích hình 9 và bạn thích thấy một biểu đồ tương tự như vậy cho các kết nối gửi đi, đầu ra của lệnh dưới đây là một biểu đồ radar mô tả trong hình 10.

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT
QUANTIZE(TO_TIMESTAMP
(EXTRACT_PREFIX(TO_STRING(EXTRACT_SUFFIX([#Fields: date-
time],0,'T')),0,'.'), 'hh:mm:ss'),3600) AS Hour, COUNT(*) AS Hits INTO
radar_traffic_send.gif FROM
C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\ProtocolLog\SmtpSe
nd\SEND*.LOG WHERE event='+' GROUP BY Hour ORDER BY Hour
ASC" -i:CSV -nSkipLines:4 -o:CHART -charttype:RadarLineFilled -
charttitle:" Global total SMTP outbound simultaneous connections per hours"
```



Hình 10: Các kết nối đồng thời đi ra

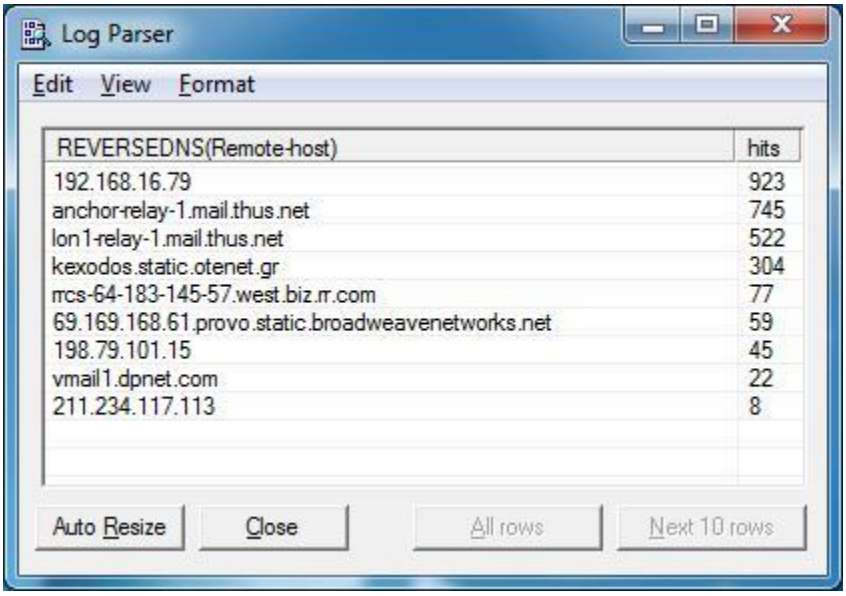
Lệnh tiếp theo phân tích đâu là người gửi nghi ngờ đến tổ chức bạn. Để thực hiện mục tiêu đó, chúng ta cần trích từ SMTP Receive Log tất cả các host có trạng thái mã 500 và lớn hơn, chẳng hạn như 504, 535, 550,…

Quá trình này được thực hiện trong hai bước: truy vấn logparser đầu tiên trích dữ liệu từ các bản ghi, lệnh thứ hai thực hiện một tra cứu DNS ngược đối với đầu ra ban đầu. Lý do chúng ta cần thực hiện theo hai bước là gì việc thực hiện một hành động tra cứu DNS ngược trong quá trình trích dữ liệu sẽ rất mất thời gian.

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT EXTRACT_PREFIX(remote-endpoint,0,':') AS Remote-host, count (*) AS hits INTO SuspiciousSenders.xml  FROM C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\ProtocolLog\SmtpRe
```

```
ceive\RECV*.log WHERE TO_INT(SUBSTR(DATA,0,3)) > 500 AND
event = '>' GROUP BY Remote-host ORDER BY hits DESC" -i:CSV -
nSkipLines:4 -o:XML
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT TOP 10
REVERSEDNS(Remote-host), hits FROM SuspiciousSenders.xml" -i:XML -
o:DATAGRID
```

Lưu ý có một host bên trong trên các kết quả mô tả trong hình 11. Host này có thể là một máy chủ ứng dụng bên trong hoặc một chuyển tiếp mail bên trong đã được thẩm định.

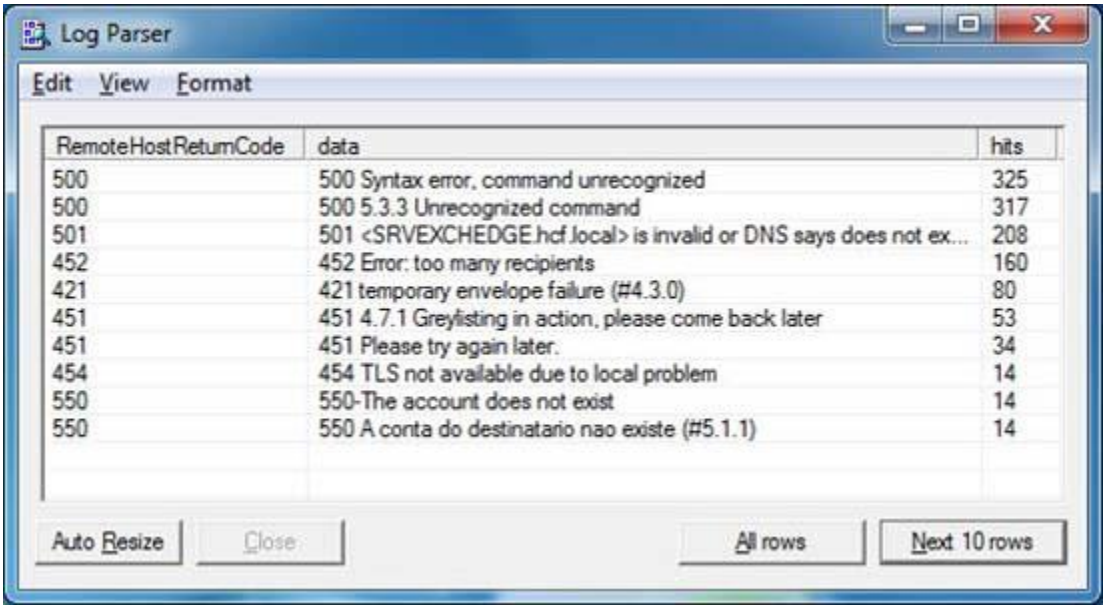


Hình 11: Các host nghi ngờ đang gửi mail đến tổ chức bạn

Chúng ta cũng có thể tạo một datagrid với Top Outbound Rejection Errors bằng cách phân tích SMTP Send Protocol Log. Điều này rất hữu dụng đối với việc nhận dạng các lỗi gửi ra hoặc trong việc tìm xem máy chủ của bạn có được liệt kê trong một số danh sách đen hay không. Đây là lệnh để tạo datagrid từ hình 12:

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT CASE
TO_INT( SUBSTR(DATA,0,3)) when NULL then 0 else TO_INT(
```

```
SUBSTR(DATA,0,3)) END AS RemoteHostReturnCode, data, count (*) AS hits FROM C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\ProtocolLog\SmtpSend\SEND*.log WHERE RemoteHostReturnCode > 400 AND context <> 'Certificate thumbprint' AND context <> 'sending message' GROUP BY RemoteHostReturnCode, data ORDER BY hits DESC" -i:CSV -nSkipLines:4 -o:DATAGRID
```



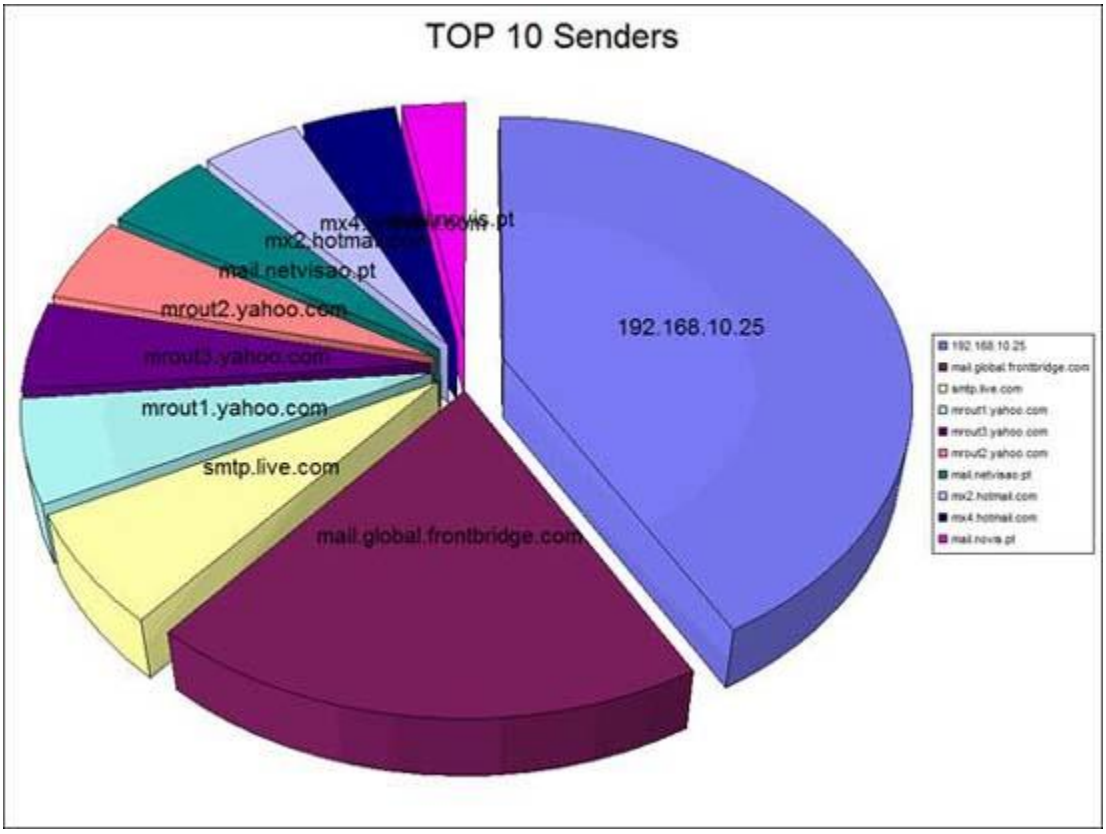
Hình 12: Top các lỗi rejection gửi đi

Một trong những báo cáo mong muốn nhất là sự phân biệt top người gửi đến tổ chức bạn. Câu trả lời được bó gọn trong các bản ghi SMTP Receive Transport Logs này.

Lưu ý trong quá trình hai bước ở trên, tra cứu DNS ngược chỉ được thực hiện với đầu ra từ truy vấn đầu tiên, mục đích để tối ưu thời gian nó diễn ra.

```
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT TOP 10 EXTRACT_PREFIX(remote-endpoint,0,':') AS RemoteSendingHost,
```

```
count(*) AS Hits INTO topsenders.xml FROM
C:\Progra~1\Microsoft\Exchan~1\TransportRoles\Logs\ProtocolLog\SmtpRe
ceive\RECV*.LOG WHERE event='+' GROUP BY RemoteSendingHost
ORDER BY Hits DESC" -i:CSV -nSkipLines:4  -o:XML
"C:\Program Files (x86)\Log Parser 2.2\logparser.exe" "SELECT TOP 10
REVERSEDNS(RemoteSendinghost), Hits INTO topsenders.gif
FROM  TopSenders.xml" -i:XML -o:CHART  -chartType:PieExploded3D -
chartTitle:"TOP 10 Senders" -groupSize:1024x768
```



Hình 13: Top các host người gửi vào tổ chức

Kết luận

Có thể bạn sẽ phân vân tại sao lại cần đến nhiều bản ghi Exchange đến vậy, hoặc bạn cho rằng xem xét các file bản ghi không mong muốn, tuy nhiên công việc trên lại rất hữu dụng và là chìa khóa để mở tất cả các kiểu thông tin

về cơ sở hạ tầng thư tín của bạn. Phần tiếp theo của loạt bài này, chúng tôi sẽ giới thiệu cho các bạn một số vấn đề có liên quan đến Log Parser và chuẩn bị cho một số truy vấn khác!