Microsoft

Using Exchange User Monitor (ExMon) For Exchange 2013 and 2016

Published: February 2016

Introduction 1

When to use ExMon 2

Installing ExMon 3

Data collection 6

Collecting Data Directly with ExMon 6

Collecting Data using Logman 6

Displaying Data in ExMon 8

ExMon ExRPC View 8

Exporting ExMon Data 14

Using ExMon UI 14

Interpreting ExMon Data 15

CPU Time 15

Server Latency 15

Feedback 18

Introduction

The Microsoft® Exchange Server User Monitor (ExMon) tool enables administrators to view and evaluate individual users' usage and experience with Microsoft Exchange Server. With this tool, administrators can gather real-time data that helps them better understand current client usage patterns and plan for future use.

Using ExMon, administrators can view the following:

- Show the RPC data based on the user
- Show the RPC data based on the RPC Operation
- Show the RPC data based on the specific application
- Show the RPC data based on the Admin Client Type
- Show the RPC data in the Raw form
- Show the RPC data in the Admin Raw form
- Show the RPC data in the Task by client Type
- Show the RPC data in the Task raw

Within each view, the user can drill down to get additional information on:

- Microsoft Office Outlook® versions and mode
- Client monitoring data
- Resource use, such as:
- CPU usage
- Server-side processor latency
- Network bytes
- RPC Operations, components and Action

When to use ExMon

ExMon enables administrators to view and analyze how individual users affect the health and performance of an Exchange server, including CPU usage and network traffic. It also enables administrators to view and analyze how the server affects those individual users' experience.

Note that ExMon does not report all information about server health or user experience. For example, ExMon does not report on the following factors that can affect Exchange Server performance:

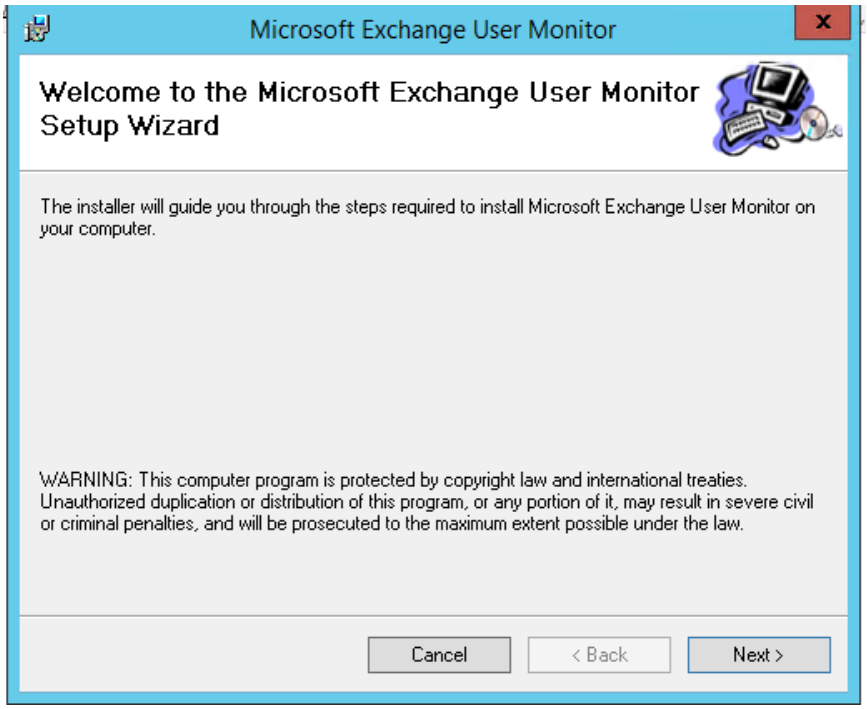
- Incoming unsolicited commercial e-mail (also known as spam) from the Internet
- Incoming SMTP mail flow from the Internet or from other sites in your organization
- Use of non-MAPI protocols for account access, such as POP3 and IMAP4
- Use of mobile devices, although some Exchange ActiveSync® client traffic is included

ExMon provides an overview of individual users' behavior only. Use it with other procedures and tools that are recommended by Microsoft to fully understand the performance.

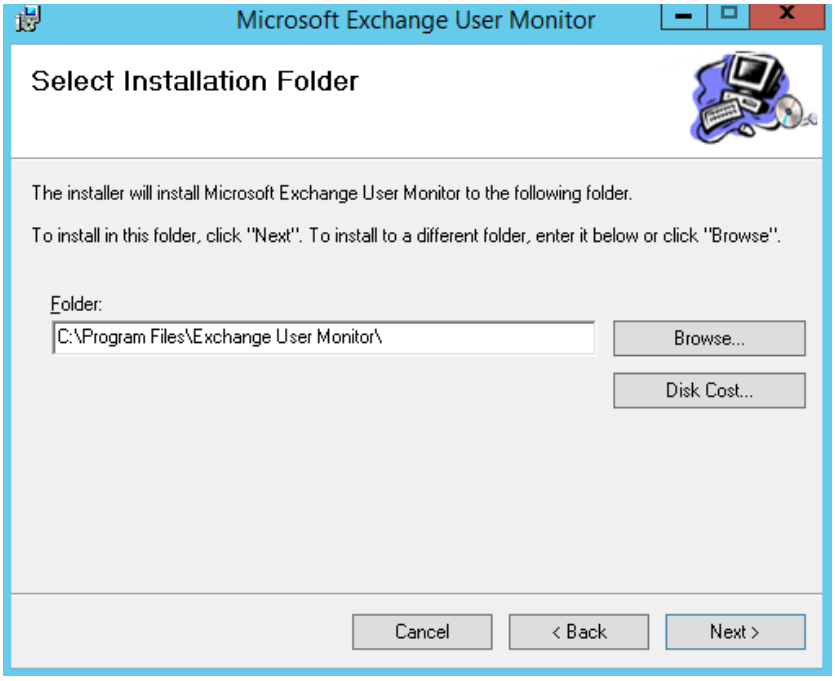
Installing ExMon

ExMon can be installed on Exchange 2013 (or later) Mailbox Server. You can collect data that is relevant to the Exchange server on which ExMon is installed.
To view data, you do not need to install ExMon on an Exchange server. It can be installed on any Windows client, Windows 7 or higher

Please see the screen captures below for details:







The following files will be installed by default under C:\Program Files\Exchange User Monitor\

- ExMonAdvancedUI.exe
- Microsoft.Exchange.ExMonParser.dll

Data collection

You must configure ExMon to collect data by one or more of the following methods:

- Collecting data directly with ExMon
- Collecting data by using command-line tools

Collecting Data Directly with ExMon

Collecting data directly with ExMon is the simplest method for short-term data collection. ExMon saves data in one minute intervals. Collecting data directly with ExMon is most useful for quick spot checks of server performance; it is not for large-scale or long-interval data collection. For large-scale or long-interval data collection, use the data collection methods that are described in the next sections.

To collect data in ExMon

- Verify that all the Exchange Services for the Mailbox Role are running.
- Run **ExmonAdvancedUI.exe**. ExMon starts collecting data immediately and displays collected data when you hit refresh in the Exmon UI.

  Note:

  By default, ExMon saves collected data in a ETL file such as those shown below. To make sure that data is being collected, periodically click **Refresh** on the toolbar



- To stop data collection, click **Stop** on the toolbar.
- To resume data collection, click **Start** on the toolbar.

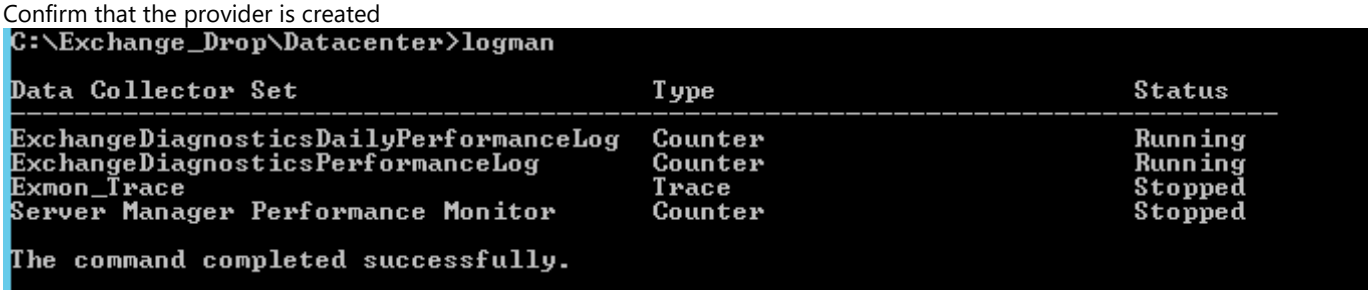
Collecting Data using Logman

The Logman tool manages and schedules performance counter and event trace log collections on local and remote systems.
Note: For more details, see https://technet.microsoft.com/en-us/library/bb490956.aspx
Exmon tracing uses the ETW (Event Tracing for Windows) facility of Windows. To enable and collect the ETW via logman follow the steps below. Please make sure that you run these steps from a command prompt and not from Exchange Management Shell.

1) Create the Exmon provider

```
logman create trace Exmon_Trace -p {2EACCEDF-8648-453e-9250-
27F0069F71D2} -o c:\Tracing\exmon
```

Confirm that the provider is created



2) Start the Trace

```
logman start Exmon_Trace
```

3) Collect the traces by stopping the trace

```
logman stop Exmon_Trace
```

Displaying Data in ExMon

The ExMon user interface can be used to show the data in real time as well as display the data from the ETL collected from a different machine.

ExMon ExRPC View

By using ExMon ExRPC view, you can display the data in the following ways.

- By User View
- By Operation View
- By Application View
- By Version View
- By Raw View

There are also options to show you the Admin and Task view with or without the RAW data

- By AdminByClientType View
- By TasksByClient View
- By AdminRaw View
- By TaskRaw View

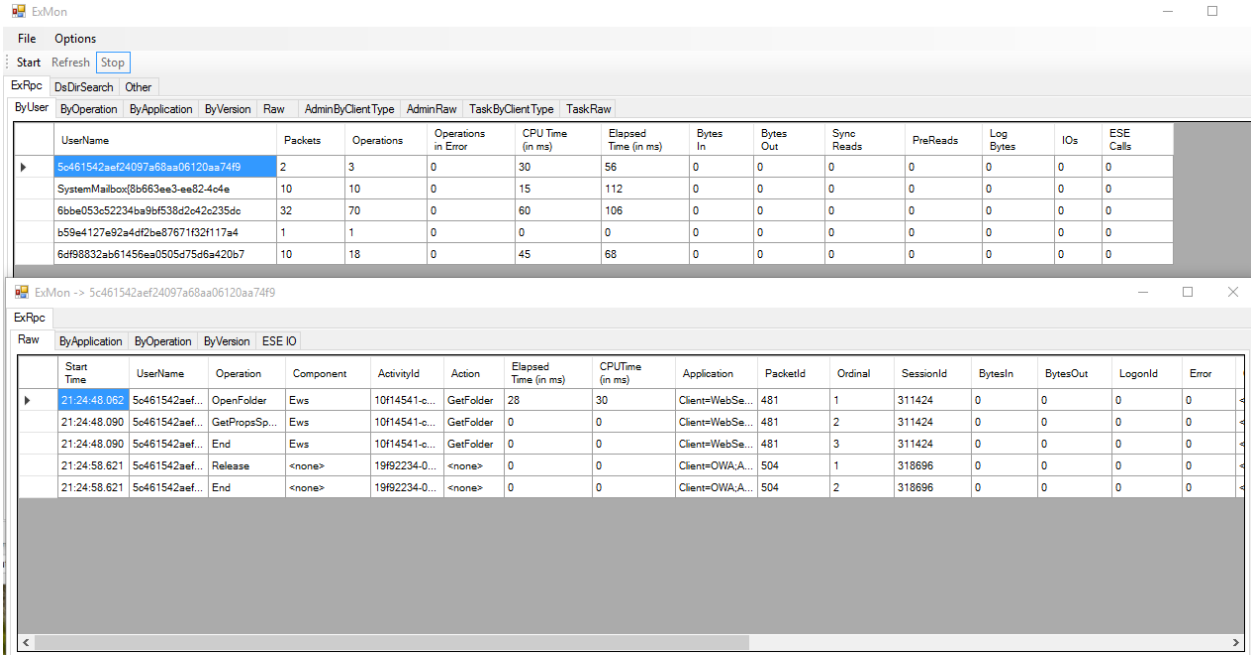
Displaying Data in By User View

The By User View aggregates data about individual users' consumption of server resources. Each row in the view contains data about one user, whether that user has only one computer or is accessing Exchange Server from multiple computers. The following table shows the types of data that are displayed in the By User View.

The table below describes the data associated with the By User View:

UserName	The GUID associated with the user.
Packets	The count of remote procedure call (RPC) packets that have been processed by the server.
Operations	The count of operations in RPC packets. Frequently, Exchange Server assembles operations together to reduce network overhead.
Operations in Error	RPC operations that are resulted in error.
CPU Time (in ms)	The sum of processing time consumed and reported in milliseconds. 1000 milliseconds corresponds to one second of 100 percent processor utilization or to two seconds of 50 percent processor utilization (and so on).
Bytes In	Sum of Exchange-related data that the server receives after compression. This sum does not include TCP/IP overhead or packet retransmission.
Bytes Out	Sum of Exchange-related data that the server sends to the client after compression. This sum does not include TCP/IP overhead or packet retransmission.

Note: Double-clicking on each user will open the raw data for each user, as shown in the screen capture below.



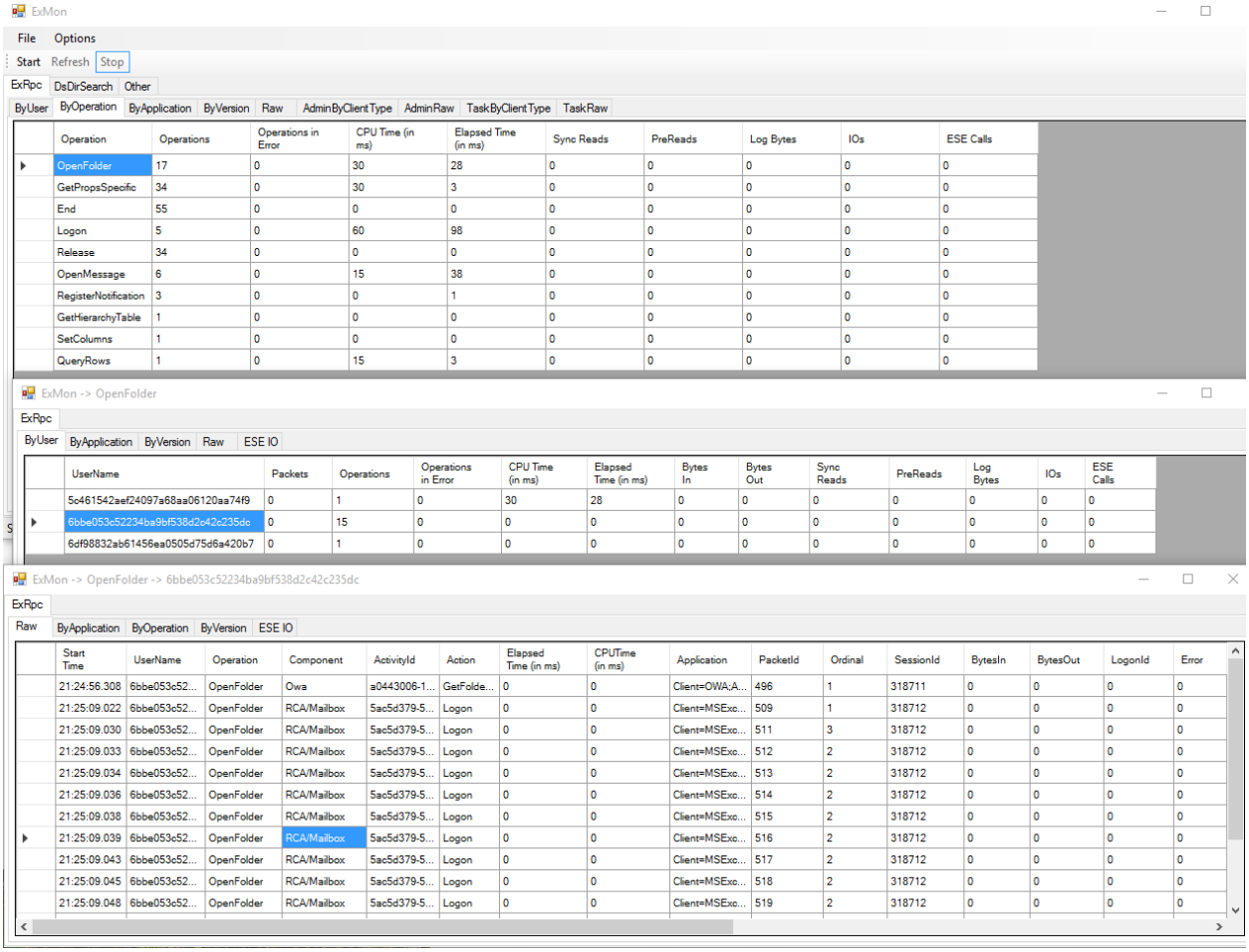
Displaying Data in By Operation View

The By Operation View aggregates data about RPC operations, how many time the operations are called and their overall impact on the CPU.

The table below describes the data associated with the By Operation View

Operation	Operation type, for example OpenFolder etc.
Operations	Number of times that operation is called
Operations in Error	RPC operations that are resulted in error
CPU Time (in ms)	The sum of processing time consumed and reported in milliseconds. 1000 milliseconds corresponds to one second of 100 percent processor utilization or to two seconds of 50 percent processor utilization (and so on).

Note: Double-clicking on each operation will open the User View showing each user that has called that operation, as shown in the screen capture below.



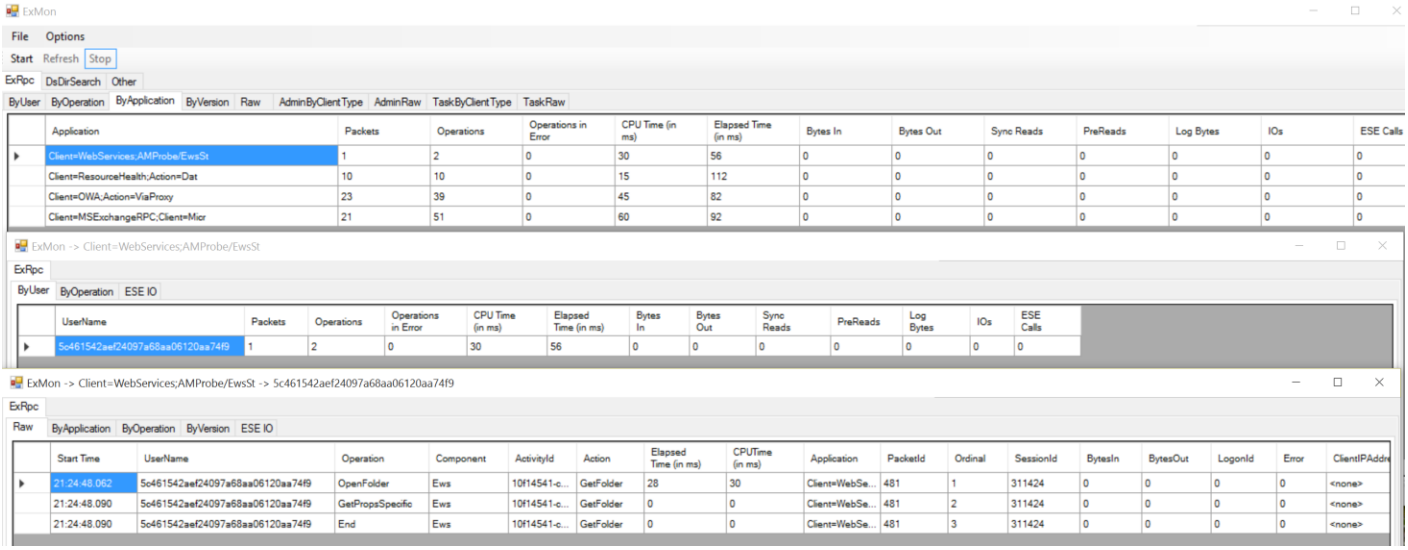
Displaying Data in By Application View

The By Application View aggregates data about the type of client that is making the request, what type of operation, number of times the operation is called, and its overall impact on the CPU.

The table below describes the data associated with the By Application View

Application	Name of the Client
Packets	The count of remote procedure call (RPC) packets that have been processed by the server.
Operations	The count of operations in RPC packets. Frequently, Exchange Server assembles operations together to reduce network overhead.
Operations in Error	RPC operations that are resulted in error
CPU Time (in ms)	The sum of processing time consumed and reported in milliseconds. 1000 milliseconds corresponds to one second of 100 percent processor utilization or to two seconds of 50 percent processor utilization (and so on).

Note: Double-clicking on each Application will open the User View showing each user that has called that operation and the Raw ExRPC data associated, as shown in the screen capture below.



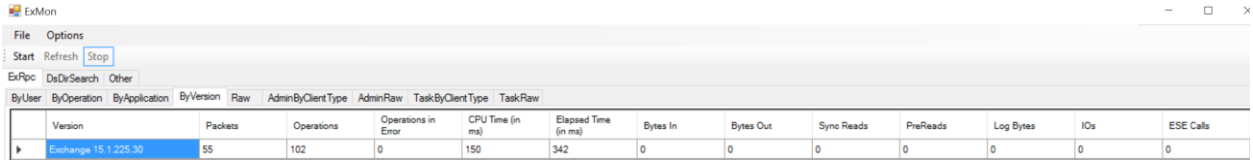
Displaying Data in By Version View

The By Version View aggregates data about the Version type of client that is making the request, and its overall impact on the CPU.

Version	Version of the client
Packets	The count of remote procedure call (RPC) packets that have been processed by the server.

Operations	The count of operations in RPC packets. Frequently, Exchange Server assembles operations together to reduce network overhead.
Operations in Error	RPC operations that are resulted in error
CPU Time (in ms)	The sum of processing time consumed and reported in milliseconds. 1000 milliseconds corresponds to one second of 100 percent processor utilization or to two seconds of 50 percent processor utilization (and so on).
Bytes In	Sum of Exchange-related data that the server receives after compression. This sum does not include TCP/IP overhead or packet retransmission.
Bytes Out	Sum of Exchange-related data that the server sends to the client after compression. This sum does not include TCP/IP overhead or packet retransmission.

Note: See the screen capture below for details on the By Version view

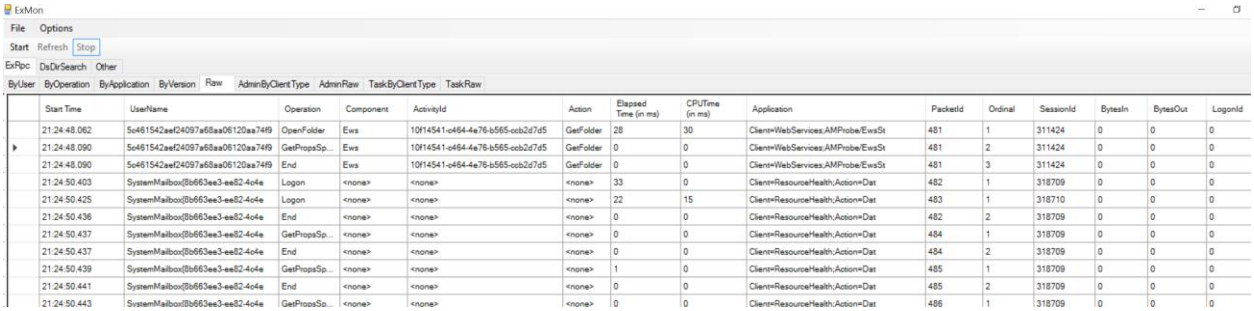


Displaying Data in By RAW View

The Raw view is unfiltered view of the data collected by ExMon.

Start Time	ExMon trace start time
UserName	GUID associated with the mailbox
Operation	RPC operation like OpenFolder etc.
Component	Exchange component associated with the operation
CPU Time (in ms)	The sum of processing time consumed and reported in milliseconds. 1000 milliseconds corresponds to one second of 100 percent processor utilization or to two seconds of 50 percent processor utilization (and so on).
Application	Client Application
BytesIn	Sum of Exchange-related data that the server receives after compression. This sum does not include TCP/IP overhead or packet retransmission.
BytesOut	Sum of Exchange-related data that the server sends to the client after compression. This sum does not include TCP/IP overhead or packet retransmission.
ClientIPAddress	IP address of the client

Note: See the screen capture below for details on the Raw view



Start Time	UserName	Operation	Component	ActivityId	Action	Elapsed Time (in ms)	CPUTime (in ms)	Application	PacketId	Ordinal	SessionId	BytesIn	BytesOut	LogonId
21:24:48.062	5c461542aef24097a68aa06120aa74f9	OpenFolder	Ews	10f14541-c464-4e76-b565-ccb2d7d5	GetFolder	28	30	Client=WebServices;AMProbe/EwsSt	481	1	311424	0	0	0
21:24:48.090	5c461542aef24097a68aa06120aa74f9	GetPropsSp...	Ews	10f14541-c464-4e76-b565-ccb2d7d5	GetFolder	0	0	Client=WebServices;AMProbe/EwsSt	481	2	311424	0	0	0
21:24:48.090	5c461542aef24097a68aa06120aa74f9	End	Ews	10f14541-c464-4e76-b565-ccb2d7d5	GetFolder	0	0	Client=WebServices;AMProbe/EwsSt	481	3	311424	0	0	0
21:24:50.403	SystemMailbox{8b663ee3-ee82-4c4e	Logon	<none>	<none>	<none>	33	0	Client=ResourceHealth;Action=Dat	482	1	318709	0	0	0
21:24:50.425	SystemMailbox{8b663ee3-ee82-4c4e	Logon	<none>	<none>	<none>	22	15	Client=ResourceHealth;Action=Dat	483	1	318710	0	0	0
21:24:50.436	SystemMailbox{8b663ee3-ee82-4c4e	End	<none>	<none>	<none>	0	0	Client=ResourceHealth;Action=Dat	482	2	318709	0	0	0
21:24:50.437	SystemMailbox{8b663ee3-ee82-4c4e	GetPropsSp...	<none>	<none>	<none>	0	0	Client=ResourceHealth;Action=Dat	484	1	318709	0	0	0
21:24:50.437	SystemMailbox{8b663ee3-ee82-4c4e	End	<none>	<none>	<none>	0	0	Client=ResourceHealth;Action=Dat	484	2	318709	0	0	0
21:24:50.439	SystemMailbox{8b663ee3-ee82-4c4e	GetPropsSp...	<none>	<none>	<none>	1	0	Client=ResourceHealth;Action=Dat	485	1	318709	0	0	0
21:24:50.441	SystemMailbox{8b663ee3-ee82-4c4e	End	<none>	<none>	<none>	0	0	Client=ResourceHealth;Action=Dat	485	2	318709	0	0	0
21:24:50.443	SystemMailbox{8b663ee3-ee82-4c4e	GetPropsSo...	<none>	<none>	<none>	0	0	Client=ResourceHealth;Action=Dat	486	1	318709	0	0	0

Other Views

There are also options to show you the Admin and Task view, with Raw data.

- By AdminByClientType View
- By TasksByClient View
- By AdminRaw View
- By TaskRaw View

Exporting ExMon Data

Exmon data can be exported out directly from the Exmon UI

Using ExMon UI

Within the Exmon UI, one can highlight and select the data that need to export, by simply copying and pasting the highlighted into an Excel spreadsheet

Interpreting ExMon Data

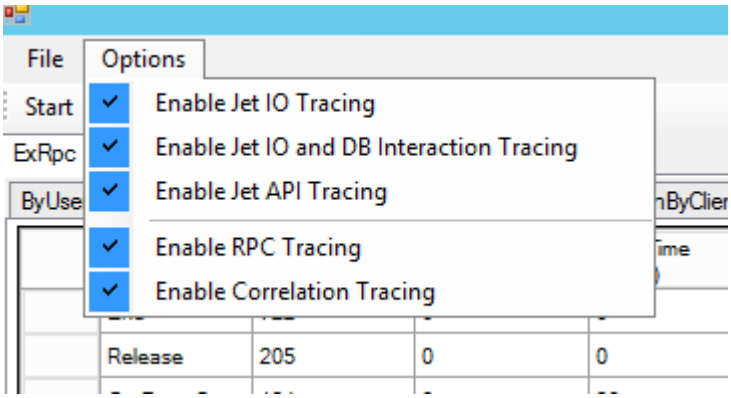
Several factors, such as time of day, usage patterns, server load, server configuration, and applications, can cause variations in the data that is collected and displayed in ExMon. An administrator can best understand any data by comparing it with baseline data that is collected during normal operations.

CPU Time

The data displayed in the CPU Time (ms) column represents the processing time that the Mailbox role services require to process all requests, specifically the managed store host and worker processes. There is a single worker process per database.
Some operations require more processing than others. For example, sophisticated searches and large data exports require more processing time than viewing of a single mail item. This data along with the daily performance data can be used to isolate the application, client, or the operation that may be causing high CPU.

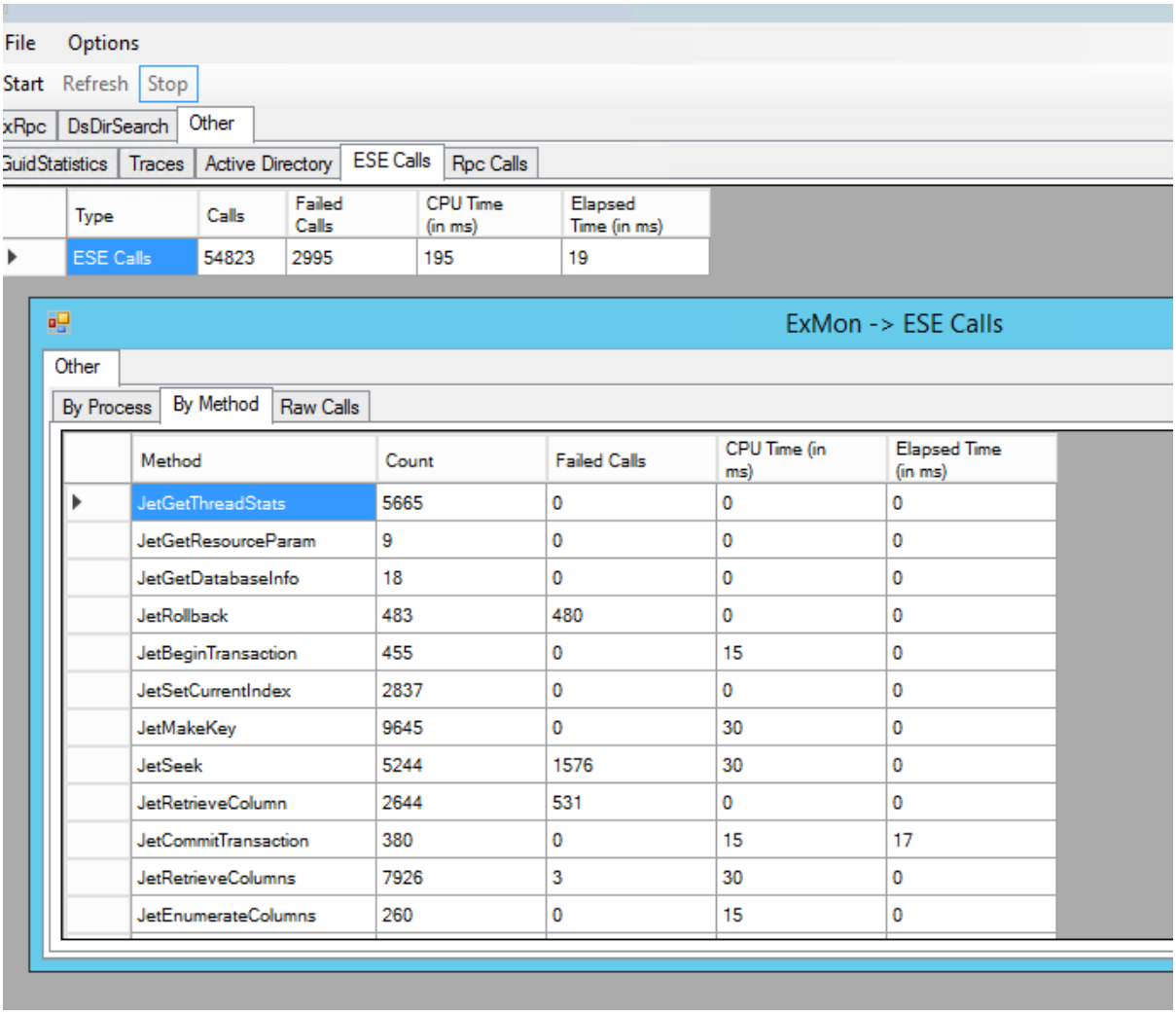
Server Latency

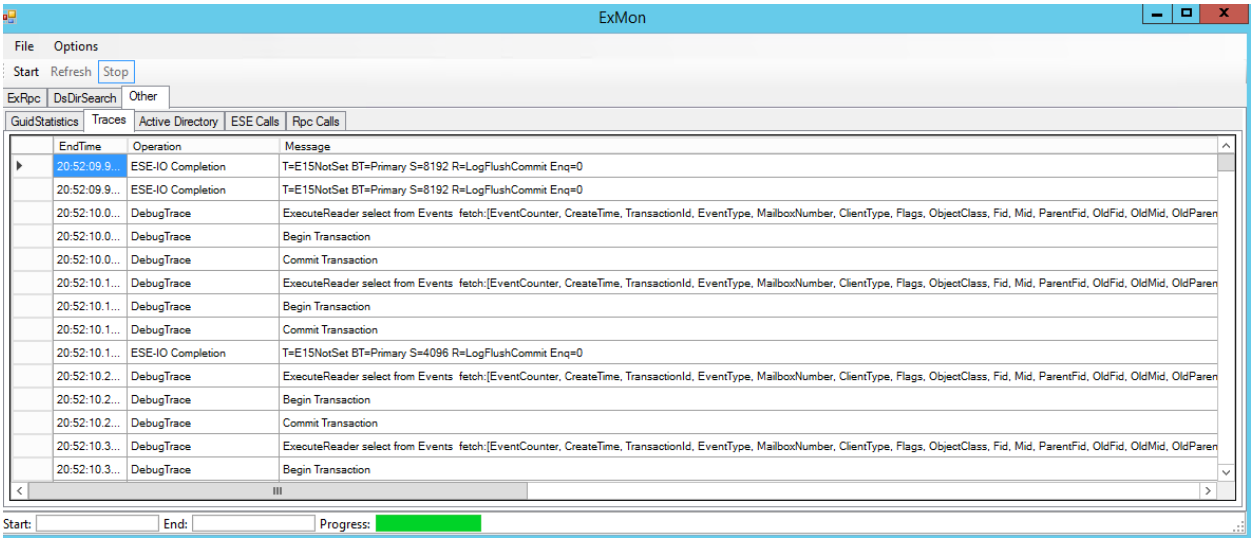
When JET related option are enable during ExMon Tracing, this data along with the daily performance logs can be used to analyze the server latency in regards to the backend storage.



ESE Calls

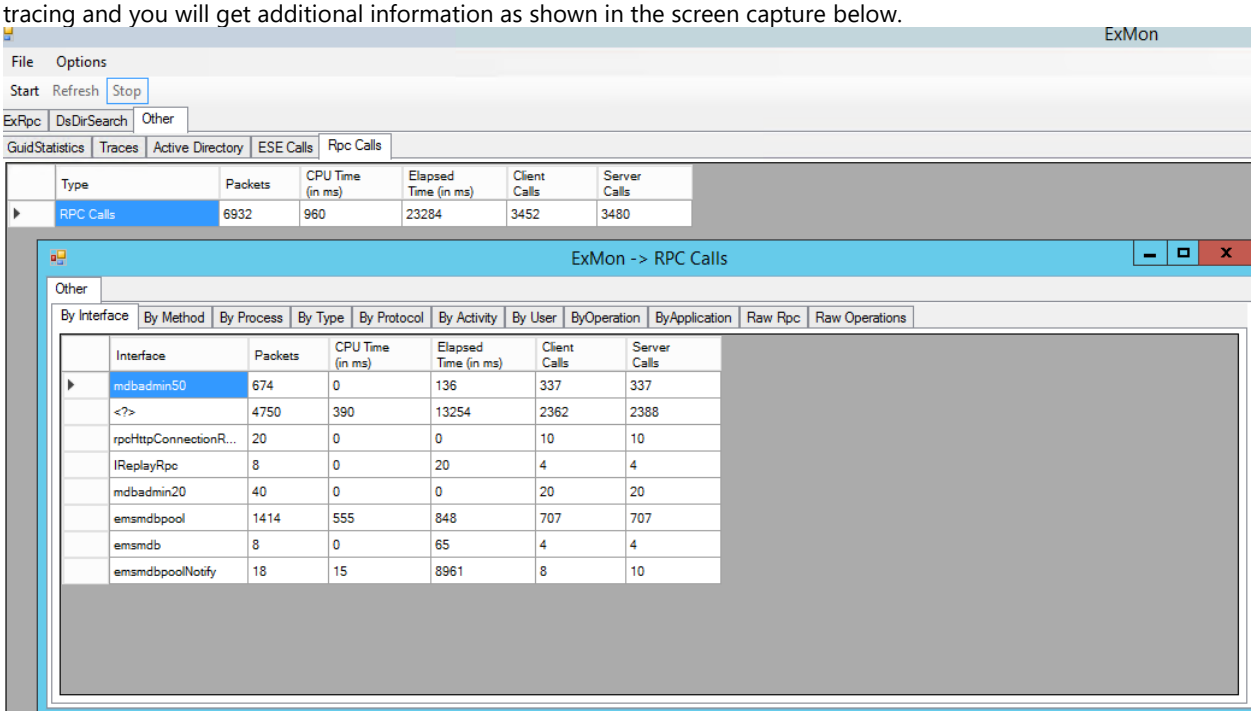
With JET tracing enabled you will get additional information on ESE calls.


File
Options
Start
Refresh
Stop
xRpc
DsDirSearch
Other
GuidStatistics
Traces
Active Directory
ESE Calls
Rpc Calls
Type
Calls
Failed Calls
CPU Time (in ms)
Elapsed Time (in ms)
ESE Calls
54823
2995
195
19
ExMon -> ESE Calls
Other
By Process
By Method
Raw Calls
Method
Count
Failed Calls
CPU Time (in ms)
Elapsed Time (in ms)
JetGetThreadStats
5665
0
0
0
JetGetResourceParam
9
0
0
0
JetGetDatabaseInfo
18
0
0
0
JetRollback
483
480
0
0
JetBeginTransaction
455
0
15
0
JetSetCurrentIndex
2837
0
0
0
JetMakeKey
9645
0
30
0
JetSeek
5244
1576
30
0
JetRetrieveColumn
2644
531
0
0
JetCommitTransaction
380
0
15
17
JetRetrieveColumns
7926
3
30
0
JetEnumerateColumns
260
0
15
0



RPC Calls

With the "Enable RPC Tracing" option enabled, RPC traces are also added as part of the tracing and you will get additional information as shown in the screen capture below.



Feedback

Feedback (issues, feature requests, general comments) can be sent to exmonfeed@microsoft.com. The ExMon tool is provided as-is, and is not directly supported by Microsoft Support. Microsoft cannot guarantee a response to all feedback sent to this address, but it will be read and triaged by the engineering team responsible for the tool.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2016 Microsoft Corporation. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Microsoft, list Microsoft trademarks used in your white paper alphabetically are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.