Monitoring Exchange Server using EventTracker
Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker’s built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

With EventTracker you can monitor all of your servers running Microsoft Exchange from a single view. EventTracker checks the status and availability of Exchange Servers critical server processes and it centrally consolidates all the event logs, SMTP logs and connectivity logs. Through consolidated logging you can monitor the performance, availability, and security of your servers running Exchange, alerting you to events that have a direct impact on server availability while filtering out events that require no action. Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a catastrophic failure occurs. EventTracker also includes reports that allow you to summarize server availability.

Scope


Audience

EventTracker users, who wish to monitor Microsoft Exchange Server.
# Table of Contents

Abstract .......................................................................................................................................................... 1

Monitor Exchange Server ................................................................................................................................. 3

Event Log Consolidation .................................................................................................................................. 3
  Enable Diagnostics Logging for Exchange Server ......................................................................................... 4

Enable Message Tracking on Exchange Server .............................................................................................. 7
  Enable Message Tracking on Exchange Server 2013 and Exchange server 2016 ...................................... 9

IIS Logging ..................................................................................................................................................... 11
  Enable IIS Logging in 2003 .......................................................................................................................... 11
  Enable IIS Logging in 2008 and above ......................................................................................................... 13
  Enable Log File Monitoring in EventTracker Agent .................................................................................. 15

Monitor Uptime Status of Exchange Server .................................................................................................. 21

Monitor Disk and Memory Problem on Exchange Server .............................................................................. 22

Monitor Microsoft Exchange Server Services ............................................................................................... 22

Monitor Mailbox Operation in Exchange Server ........................................................................................... 24
  Monitor Mailbox Operation in Exchange Server 2010/2013/2016 .............................................................. 25

Generate Non Owner Mailbox Audit Log Reports ............................................................................................ 30

Monitor Configuration Changes done by User/ Administrator in your Exchange Organization (Exchange 2010/2013 sp1/2016) ......................................................................................................................... 36

Generate Administrator Audit Log Reports ...................................................................................................... 37

Monitor Antivirus Engine Status ...................................................................................................................... 42

Monitor Exchange Database Backup Recovery Operation .............................................................................. 42

Monitor Exchange Clustered Resource Status ............................................................................................... 42

Monitor Exchange Database Activity and Disc, Storage Limit Threshold ..................................................... 44

Real-time Critical Alerts .................................................................................................................................. 45
Monitor Exchange Server

- Monitoring uptime status of Exchange Server.
- Monitoring disk and memory problem on Exchange Server.
- Monitoring all the services related to Exchange Servers is running as expected.
- Monitoring Antivirus Engine status.
- Monitoring Exchange database Backup recovery operation.
- Monitoring Exchange clustered resource status.
- Monitoring Exchange database Disk, storage limit and threshold.
- Monitoring Exchange database mount, Dismount.
- Monitoring mailbox operation.
- Monitor any configuration changes done by user or administrator in your Exchange organization. (Exchange 2010 sp1/2013)
- Keep track of administrator, delegate and owner access to a mailbox. (Exchange 2010 sp1/2013)
- Monitoring Active Sync usage, Policy compliance.

Event Log Consolidation

Based on audit settings, Microsoft logs the necessary audit, availability, and performance events. EventTracker collects all events to a centralized server. You can either collect all the events or you can filter any events you don’t care about. You can use http://kb.eventtracker.com to decide which events you may want to keep and which events you may want to filter. All these events are received in real-time and you can configure any event to generate an alert. You can write intensive pattern matching rules using industry standard regular expressions that parse the information within the complex event description or you can create an alert when a sequence of events occurs within a predefined time frame. Once EventTracker consolidates the event logs, you can generate hundreds of reports on various conditions.

To monitor Exchange server, following things need to be checked.

- Install the EventTracker Agent on Exchange server.
- Turn on Appropriate Auditing for Monitoring the Exchange Server.
Make sure your local security policy is set properly. Below Figure shows the typical audit policy events that you would need to configure.

**Figure 1: Local Security Settings**

**Enable Diagnostics Logging for Exchange Server**

To enable any type of diagnostics logging for an Exchange Server, you must configure the services and categories under the Diagnostics Logging tab for each particular server(s) individually.

Figure 2 shows the Services and Categories under the Diagnostics Logging tab for an Exchange Server 2003.

**Figure 2**
2. Navigate to Server Configuration and then select Mailbox.
3. Select your mailbox server.
4. Right click and select Manage Diagnostic Logging Properties.
5. Select MSExchangeIS and then select 9000 Private.

Figure 3 shows Services and Categories under the Diagnostics Logging tab for an Exchange Server 2007.
6. Expand the tree to check all the options and you will find the four options mentioned above.

Figure 4
Enable Message Tracking on Exchange Server

A message tracking log is a detailed log of all message activity as messages are transferred to and from a computer that is running Microsoft Exchange Server 2003/2007/2010 and that has the Hub Transport server role, the Mailbox server role, or the Edge Transport server role installed. Exchange servers that have the Client Access server role or Unified Messaging server role installed don’t have message tracking logs. They can be utilized for message forensics, mail flow analysis, reporting, and troubleshooting.

The following instructions will explain how you can enable Exchange Message tracking logging in Exchange Management Console. This log file can be used to analyze email delivery failures such as when an email is transferred to an external address which is invalid. Since the sender of this email is a public folder and not a mailbox, Exchange will not provide any sort of failed delivery email notification.


Tracking logs are located in `\INSTALLDIR\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking\` folder. Each daily log is named according to the date that it was created (in the MSGTRKyyyyymmdd.log format). Like all times in the tracking log, the file name date is in coordinated universal time (UTC, or Greenwich Mean Time [GMT]).

To enable message tracking in Exchange 2003/2007/2010:

1. To launch Exchange Management Console, select the **Start** button, and then select **All Programs**.
3. Expand **Server Configuration** and select **Hub Transport**.
4. Right-click the Exchange Server and then select **Properties**.

![Hub Transport](image6.png)

**Figure 6**

5. Select **Log Settings** tab.

6. Select the **Enable message tracking log** option and then specify the path.

![PFSALESEXH Properties](image7.png)

**Figure 7**
Enable Message Tracking on Exchange Server 2013 and Exchange server 2016

Tracking logs are located in C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking folder. Each daily log is named according to the date that it was created (in the MSGTRKyyyymmdd.log format). Like all times in the tracking log, the file name date is in coordinated universal time (UTC, or Greenwich Mean Time [GMT]).

Configure Message Tracking on Mailbox servers

1. In the EAC, navigate to Servers > Servers.
2. Select the Mailbox server you want to configure, and then click Edit.
3. On the server properties page, click Transport Logs.
4. In the Message tracking log section, change any of the following:
   a. Enable message tracking log - To disable message tracking on the server, clear the check box. To enable message tracking on the server, select the check box.
   b. Message tracking log path - The value you specify must be on the local Exchange server. If the folder doesn’t exist, it will be created for you when you click Save.
5. Click Save.
Procedure to execute message tracking via CMDLET

This example enables message tracking on the Mailbox server named Exchsrv1:

```
Set-TransportService Exchsrv1 -MessageTrackingLogEnabled $True
```

This example Disables message tracking on the Mailbox server named Exchsrv1:

```
Set-TransportService Exchsrv1 -MessageTrackingLogEnabled $false
```

Verify the configured message tracking

To verify that you have successfully configured message tracking, please run the following commands in the Shell.

```
Get-TransportService <ServerIdentity> | Format-List MessageTrackingLog*
Get-TransportService Exchsrv1 | Format-List MessageTrackingLog*
```

Verify that the values displayed are the values you had configured earlier.

![Figure 9](image)

Once Message tracking is enabled and logs are transferred to EventTracker, you can schedule the reports available in EventTracker for exchange message tracking logs. EventTracker Report provides the overview of Top sender, Top recipients, and Message flow by direction, Source client IP Address.
IIS Logging

Enable IIS Logging in 2003

To enable IIS Logging, Start the Internet Information Services Manager.

1. To enable IIS logging, click the Start button, click Administrative Tools, and then click Internet Information Services.
2. Double-click your server_name, where server_name is the name of the server.
3. Expand the Web Site folder.
4. Right-click the Default Web site node for which you want to turn on logging, and then click Properties.

Figure 10

Default Web Site Properties window displays.
5. On the **Website tab**, select **Enable Logging**.

**NOTE:** Both **Enable Logging** on the **Website** tab and **Log visits** on the **Home Directory** Tab must be checked for logging to be enabled.

![Default Web Site Properties](image)

6. Select a format in the **Active log format** list i.e. **W3C Extended Log File Format**.

7. Click **Apply** and **OK**.
Enable IIS Logging in 2008 and above

To enable or disable IIS logging, please follow the steps mentioned below.

1. Open IIS Manager and navigate to the level you want to manage.
2. In Management pane, double click Feature Delegation.
3. In **Features View**, double-click **Logging**.

![Image of IIS Manager with Feature Delegation settings]

**Figure 13**

4. On the **Logging** page, in the **Actions** pane, click **Read, Read/Write, or Not Delegated**.
5. Click the **OK** button.
6. In **IIS pane**, double-click **Logging** and verify all the fields.
Enable Log File Monitoring in EventTracker Agent

To enable the EventTracker Agent to start retrieving events for IIS logs, you will need to enable the Logfile Monitoring.

1. Select the **Start** button, select **Prism Microsystems**, and then select **EventTracker Control Panel**.
2. Select **EventTracker Agent Configuration**.
3. Select the appropriate exchange server from the dropdown list in “Select Systems” option, which will load the system’s agent configuration.
4. Once loaded, select **Logfile Monitor** tab and check the **Logfile Monitor** option.
   
   You can now add the IIS log that you would like to monitor.
5. Click the **Add File Name** button. Enter File Name window displays.

6. Select **Get All Existing Log Files** option.

7. In **Select Log File Type** drop down, select the **IISW3C** option.

8. Enter the path of the IIS W3C logs.
9. Click the **OK** button.
10. Click the **Save** button.

To enable the EventTracker Agent to start retrieving events from the SMTP or Message Tracking log you will need to enable the Logfile Monitoring.

1. Select the **Start** button, select **Prism Microsystems**, and then select **EventTracker Control Panel**.
2. Select **EventTracker Agent Configuration**, and then select **Logfile Monitor** tab.
3. In **Logfile Monitor** tab, select **Logfile Monitor** option, and then select the **Add File Name** button. Enter File name window displays.
4. Select **Get All Existing Log Files** option.
5. Select the **Select Log File Type** drop down as **CSV**.

6. Click the **Browse** button.

7. Select **Select Folder Name**: in following path i.e. ‘C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking\’

![Select Folder/File Name](image)

**Figure 18**

8. Click the **OK** button.

Select file extension window displays.

9. Enter `\*.log` in the text box and then click the **OK** button.

![Select file extension](image)

**Figure 19**

The entire path
‘C:\ProgramFiles\Microsoft\ExchangeServer\V15\TransportRoles\Logs\MessageTracking\*.log’ is displayed.

10. Select **Enter Header Line Number of the above file**: which starts from ‘#Field’.

**NOTE:**

Please ensure that the header line number is set to 5.
11. Click the **OK** button.

12. Click the **Save** button.
Monitor Uptime Status of Exchange Server

Exchange server Uptime status can be monitored using StatusTracker component available in EventTracker. Following are the components which should be configured in status tracker to monitor.

1. **System availability** – Status Tracker alerts when Exchange server is not reachable or down.
2. **Ports monitoring** - Status Tracker alerts when Exchange ports are not available or down. Following are the ports which should be always up and running.

<table>
<thead>
<tr>
<th>List of ports used by Microsoft Exchange Server.</th>
<th>TCP Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>389</td>
</tr>
<tr>
<td>LDAP/SSL</td>
<td>636</td>
</tr>
<tr>
<td>LDAP-SRS</td>
<td>379</td>
</tr>
<tr>
<td>LDAP-Global Catalog</td>
<td>3268</td>
</tr>
<tr>
<td>LDAP-Global Catalog/SSL</td>
<td>3269</td>
</tr>
<tr>
<td>IMAP4</td>
<td>143</td>
</tr>
<tr>
<td>IMAP4/SSL</td>
<td>993</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
</tr>
<tr>
<td>POP3/SSL</td>
<td>995</td>
</tr>
<tr>
<td>NNTP</td>
<td>119</td>
</tr>
<tr>
<td>NNTP-SSL</td>
<td>563</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>HTTP-SSL</td>
<td>443</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of ports used by Microsoft Exchange Server.</th>
<th>TCP Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>SMTP-SSL</td>
<td>465</td>
</tr>
<tr>
<td>SMTP-LSA</td>
<td>691</td>
</tr>
<tr>
<td>IRC/IRCX</td>
<td>6667</td>
</tr>
<tr>
<td>IRC-SSL</td>
<td>994</td>
</tr>
<tr>
<td>X.400</td>
<td>102</td>
</tr>
<tr>
<td>MS-RPC</td>
<td>135</td>
</tr>
<tr>
<td>T.120</td>
<td>1503</td>
</tr>
<tr>
<td>ULS</td>
<td>522</td>
</tr>
<tr>
<td>H.323 (video)</td>
<td>1720</td>
</tr>
<tr>
<td>H.323-Audio</td>
<td>1731</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
</tbody>
</table>

Following are the Knowledge packs available, which can be used for monitoring Exchange server and generating reports on that.

**EventTracker: StatusTracker resource down:** – This predefined alert, and category enables you to get alerted and generating reports for resource downtime status when Exchange server system or exchange services ports are down.
Monitor Disk and Memory Problem on Exchange Server

EventTracker Agent can be configured to monitor disk space, CPU usage, and memory usage threshold. Once Disk space, Memory usage or CPU usage on exchange server it generates warning events.

Following are the Knowledge packs available in EventTracker which can be used for alerting and reporting.

- **EventTracker: Disk space low** - This event is logged by EventTracker when the disk space is below the defined threshold.
- **EventTracker: Runaway processes** - This Event is logged by EventTracker when system resource usage by processes crosses the configured threshold.
- **MSExchange: Database disk full** - This Events is logged by Exchange server when disk containing exchange database is full.
- **MSExchange: Database log disk full** - All Events related to Exchange server when log disk for database is full.
- **MSExchange: Disk IO error** - All Events generated by Exchange server when ESE received an error from the operating system when tried to read or write to a file.
- **System: Disk bad block** - All events related to bad sectors found on Hard Disc.

Monitor Microsoft Exchange Server Services

You can monitor the availability of Services used by Exchange Server. If any of these services are not available – Exchange Server does not behave properly. EventTracker Agent continuously checks the status of Exchange Server Services.

<table>
<thead>
<tr>
<th>Microsoft Exchange Active Directory Topology</th>
<th>Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange EdgeSync</td>
<td>Replicates configuration and recipient data from the Hub Transport servers to the Edge Transport servers.</td>
</tr>
<tr>
<td>Microsoft Exchange File Distribution</td>
<td>Microsoft Exchange File Distribution service.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Exchange Forms-Based Authentication service</td>
<td>Provides forms-based authentication to Outlook Web App and Exchange Control Panel. If this service is stopped, Outlook Web App and the Exchange Control Panel won't authenticate the user.</td>
</tr>
<tr>
<td>Microsoft Exchange IMAP4</td>
<td>Provides Internet Message Access Protocol service to clients. If this service is stopped, clients won't be able to connect to this computer using the IMAP4 protocol.</td>
</tr>
<tr>
<td>Microsoft Exchange Information Store</td>
<td>Manages the Microsoft Exchange Information Store. This includes mailbox databases and public folder databases. If this service is stopped, mailbox databases and public folder databases on this computer are unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.</td>
</tr>
<tr>
<td>Microsoft Exchange Mail Submission</td>
<td>Submits messages from the Mailbox server to the Hub Transport servers.</td>
</tr>
<tr>
<td>Microsoft Exchange Mailbox Assistants</td>
<td>Performs background processing of mailboxes in the Exchange store.</td>
</tr>
<tr>
<td>Microsoft Exchange Monitoring</td>
<td>Processes mailbox move requests.</td>
</tr>
<tr>
<td>Microsoft Exchange POP3</td>
<td>Allows applications to call the Exchange diagnostic cmdlets.</td>
</tr>
<tr>
<td>Microsoft Exchange Replication</td>
<td>Provides Post Office Protocol version 3 service to clients. If this service is stopped, clients can't connect to this computer using the POP3 protocol.</td>
</tr>
<tr>
<td>Microsoft Exchange Protected Service Host</td>
<td>Provides a host for several Microsoft Exchange services that must be protected from other services.</td>
</tr>
<tr>
<td>Microsoft Exchange Replication</td>
<td>The Microsoft Exchange Replication service provides replication functionality for mailbox databases on Mailbox servers in a database availability group.</td>
</tr>
<tr>
<td>Microsoft Exchange RPC Client Access</td>
<td>Manages client RPC connections for Exchange.</td>
</tr>
<tr>
<td>Microsoft Exchange Server Extension for Windows Server Backup</td>
<td>Drives indexing of mailbox content, which improves the performance of content search.</td>
</tr>
<tr>
<td>Microsoft Exchange Search Indexer</td>
<td>Enables Windows Server Backup users to back up and recover application data for Microsoft Exchange Server.</td>
</tr>
<tr>
<td>Microsoft Exchange Service Host</td>
<td>Provides a host for several Microsoft Exchange services</td>
</tr>
<tr>
<td>Service Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Exchange System Attendant</td>
<td>Forwards directory lookups to a global catalog server for legacy Outlook clients, generates e-mail addresses and offline address books, updates free/busy information for legacy clients, and maintains permissions and group memberships for the server. If this service is disabled, any services that explicitly depend on it will fail to start.</td>
</tr>
<tr>
<td>Microsoft Exchange Throttling</td>
<td>Limits the rate of user operations.</td>
</tr>
<tr>
<td>Microsoft Exchange Transport</td>
<td>The Microsoft Exchange Transport Service.</td>
</tr>
<tr>
<td>Microsoft Exchange Transport Log Search</td>
<td>Provides remote search capability for Microsoft Exchange Transport log files.</td>
</tr>
<tr>
<td>Microsoft Search (Exchange)</td>
<td>Quickly creates full-text indexes on content and properties of structured and semi-structured data to allow fast linguistic searches on this data</td>
</tr>
</tbody>
</table>

- **MSExchange: Exchange services not running** - This alert and category can be used for reporting and alerting on Microsoft Exchange service status.
- **MSExchange: Information store service initialization Failed** - Exchange server when unable to initialize the Exchange Information Store service.
- **MSExchange: Information Store startup failed** - Events generated by Exchange server when one or more databases on the server could not start.

**NOTE:** EventTracker Agent should be deployed to Exchange Server system and Service-monitoring feature must be enabled.

### Monitor Mailbox Operation in Exchange Server


- **MS Exchange: Mailbox creation failed** - This category report contains all Mailbox creation failed records.
- **MS Exchange: Move mailbox started** - This category report contains all move mailbox operation started records.
- **MS Exchange: Move mailbox failed** - This category report contains all move mailbox failure operation records.
- **MS Exchange: Move mailbox completed** - This category report contains all move mailbox operation completed records.
Monitoring Exchange Server using EventTracker

- **MS Exchange: Non owner mailbox Access** - This category report contains records when users mailbox is accessed by other authorized user or Administrator.
- **MS Exchange: Unauthorized mailbox access Attempt** - This category report contains records when users fail to access mailbox because of access denied.
- **MS Exchange: User accessed own Mailbox** - This category report contains records when user accessed successfully its own mailbox.
- **MS Exchange: User sent message as other user** - This category report contains records related to user sent message on behalf of other user.
- **MS Exchange: Logon failure on mailbox Database** - This category report contains records related to mailbox access login failure.

**Monitor Mailbox Operation in Exchange Server 2010/2013/2016**

Exchange 2010/2013 introduces new mailbox audit logging functionality to allow you to track mailbox access by administrators, delegates, and mailbox owners, and actions taken on mailbox items such as moving or deleting a message, using SendAs or SendOnBehalf rights to send messages, and accessing a mailbox folder or a message.

Mailbox audit logging is not enabled by default on a per-mailbox basis. So, in order for you to review mailbox audit logs, you'll need to enable mailbox audit logging.

**To enable or disable mailbox audit logging using Shell**

```powershell
Set-Mailbox ljefferson -AuditEnabled $true
```

To enable mailbox audit logging for all user mailboxes in your organization, run the following commands.

```powershell
$UserMailboxes = Get-mailbox -Filter {((RecipientTypeDetails -eq 'UserMailbox')}
$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}
```

**Verify Mailbox Audit Logging**

To verify that you have successfully enabled mailbox audit logging for a mailbox and specified the correct logging settings for administrator, delegate, or owner access, use the GetMailbox cmdlet to retrieve the mailbox audit logging settings for that mailbox.

This example retrieves Ben Smith’s mailbox settings and pipes the specified audit settings, including the audit log age limit, to the **Format-List** cmdlet.

```powershell
Get-Mailbox "Karen" | Format-List *audit*
```

To check whether audit logging is configured for All Mailboxes:

```powershell
Get-Mailbox | FL Name,AuditEnabled
```
Logging Configuration

- Request Exchange script pack from EventTracker Support.
- Download and extract the files provided at a preferred path.

- In Task scheduler windows, click on Import Task in Actions pane.
- Browse and select the xml file named “Exchange admin and mailbox audit.xml” from earlier mentioned extraction location.
• Double-click to edit the imported task named “Exchange admin and mailbox audit”.

![Exchange admin and mailbox audit Properties (Local Computer)](image)

Figure 25
- Click General tab and change the user account settings in Security options section. Please ensure concerned user has exchange admin privileges.

![Edit Trigger](image)

Figure 26
• Click Triggers tab and select edit. Please select an appropriate time for script execution.

![Edit Action dialog box](image)

**Figure 27**

• Click Actions tab and select edit. Please edit expression provided in Add parameters as shown below.

```powershell
-file 'C:\Exchange admin and mailbox audit\Exchange audit.ps1'
```

-Script Location

• Click OK to apply changes.
• When the script is executed, reports named ExchangeAdminAuditreport** and ExchangeMailboxAuditReport will be generated in CSV format at the script location.

**Please note this report will be generated only when admin audit logs are enabled. Admin audit logs have been covered later in this guide.**
Generate Non Owner Mailbox Audit Log Reports

Using Search-MailboxAuditLog cmdlet Exchange Mailbox audit log can be exported to CSV through agent LFM to EventTracker for offline processing and report generation.

EventTracker agent LFM configuration

1. Navigate to <%EventTracker install directory%>\Prism Microsystems\EventTracker\Agent.

2. Right-click etaconfig.exe and select run as administrator.

Figure 28

Figure 29
3. Select Get All Existing Log Files checkbox.
4. Select CSV from Log File Type drop-down.

![Select Folder/File Name](image)

Figure 30

5. Select report named “ExchangeMailboxAuditreport.csv” from earlier selected file path.
6. Select “1” from Header Line Number drop-down and click OK.

![Enter Search String](image)

Figure 31
7. Select “LastAccessed” from Field Name drop-down.
8. Use “*” (asterisk) as search string.
9. Select Current DateTime checkbox.
10. Click Ok and Save.

**Verify logs on EventTracker manager**

1. Logon to EventTracker manager with appropriate credentials.

![Figure 32](image)

2. Click **Search** from EventTracker homepage ribbon.

![Figure 33](image)

3. In log search window, initiate search with following criteria.
   - Select File Transfer checkbox and choose appropriate systems.
   - Select appropriate time duration.
   - In Custom Criteria, Event Id contains 3230.
   - In Custom Criteria, Source contains EventTracker.
Monitoring Exchange Server using EventTracker

Figure 34

4. Consumed logs will be displayed as shown below.

Figure 35
Import Exchange Reports

1. Double-click EventTracker Control Panel.

![EventTracker Control Panel](image)

Follow these steps to import Exchange reports:

3. Click on Export Import Utility.
4. Select Import tab and choose Reports in Options section.
5. Click \[\] and select file named ‘All Exchange group of reports.issch’.
6. Click Import.

Verify Exchange Reports

1. Open EventTracker enterprise on browser.
2. Navigate to Reports-> Configuration-> Defined.
4. Imported reports are displayed in the right-pane.
A sample report of non-owner mailbox access is given below.

**Exchange-Mailbox audit details**

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Changed By Role</th>
<th>Operation Performed</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>Folder Changed</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/06/2016 11:03:56 AM</td>
<td>PROC-EX2010</td>
<td>Administrator</td>
<td>Delegate</td>
<td>SoftDelete</td>
<td>Succeeded</td>
<td>John Doe</td>
<td>PortAP.local</td>
<td>Inbox</td>
<td>fe80::cc4e:7188::e832:8aef</td>
</tr>
<tr>
<td>04/06/2016 11:03:22 AM</td>
<td>PROC-EX2016</td>
<td>Administrator</td>
<td>Delegate</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Cathy Lee</td>
<td>prdAP.local</td>
<td>Inbox File</td>
<td>fe80::cc4e:7188::e676:874a</td>
</tr>
<tr>
<td>04/06/2016 11:03:12 AM</td>
<td>PROC-EX2016</td>
<td>Administrator</td>
<td>Delegate</td>
<td>Create</td>
<td>Succeeded</td>
<td>Mary Jane</td>
<td>prdAP.local</td>
<td>Inbox</td>
<td>fe80::cc4e:7188::e632:8aef</td>
</tr>
<tr>
<td>04/06/2016 11:03:10 AM</td>
<td>PROC-EX2010</td>
<td>Administrator</td>
<td>Delegate</td>
<td>SoftDelete</td>
<td>Succeeded</td>
<td>Peter Lang</td>
<td>prdAP.local</td>
<td>Inbox</td>
<td>fe80::cc4e:7188::e672:8aef</td>
</tr>
</tbody>
</table>
Monitor Configuration Changes done by User/Administrator in your Exchange Organization (Exchange 2010/2013 sp1/2016)

Microsoft has introduced a new feature called Administrator Audit Logging in Exchange 2010. You can use administrator audit logging to log when a user or an administrator runs a cmdlet. This helps you to track the changes that are done, and the person who did the changes etc. Cmdlets are logged that are run directly on Exchange Management Shell (EMS), or when an action executed in Exchange Management Console (EMC), or when an operation performed using the Exchange web management.

Configure Administrator Audit Logging

The configuration of administrator audit logging can be achieved using the Set-AdminAuditLogConfig cmdlet and viewed using the Get-AdminAuditLogConfig cmdlet. The Set-AdminAuditLogConfig cmdlet has a number of parameters associated with it but the most important parameters to discuss in this article all contain the string “log” in their names. Therefore, we can use the Get-AdminAuditLogConfig cmdlet and pipe the results to the format-list cmdlet choosing only to show cmdlet parameters that contain the string log in their names. To do this, the following cmdlet would need to be run:

Get-AdminAuditLogConfig

You can see the results of running this cmdlet in Figure 6. Note that this cmdlet has been run on a default installation of Exchange 2010, which therefore means that the parameter values shown below are default settings.

![Figure39: Results of Get-AdminAuditLogConfig](image-url)
Before administrator audit logging is enabled, it makes sense to first configure the required settings such as the name of the audit logging mailbox that will be used to store the results of the logging and the list of cmdlets and associated.

- **Run following cmdlet to configure Administrator Auditing**

  ```powershell
  Set-AdminAuditLogConfig –AdminAuditLogMailbox user@mailserver.com
  Set-AdminAuditLogConfig –AdminAuditLogCmdlets *
  ```

- Use the procedure provided earlier in **Monitor Mailbox Operation** section for generating audit report.
- Script execution and task scheduling steps have been provided earlier in **Monitor Mailbox Operation** section.

### Generate Administrator Audit Log Reports

Using `Search-AdminAuditLog` cmdlet Exchange organization configuration change audit log can be exported to CSV through agent LFM to EventTracker for offline processing and report generation.

- Successful execution of script ‘`Exchange audit.ps1`’ will generate a report named `ExchangeAdminAuditreport.csv`.

### EventTracker agent LFM configuration

1. Navigate to `<%EventTracker install directory%>\Prism Microsystems\EventTracker\Agent\`. 

![Image of EventTracker directory](image)
2. Right-click `etaconfig.exe` and select run as administrator.

![Figure 41](image)

3. Select Get All Existing Log Files checkbox.
4. Select CSV from Log File Type drop-down.

![Figure 42](image)

5. Select report named `ExchangeAdminAuditreport.csv` from earlier selected file path.
6. Select ‘1’ from Header Line Number drop-down and click OK.
7. Select RunDate from Field Name drop-down.
8. Use '*' (asterisk) as search string.
9. Select Current DateTime checkbox.
10. Click Ok and Save.

Verify logs on EventTracker manager

1. Logon to EventTracker manager with appropriate credentials.
2. Click **Search** from EventTracker homepage ribbon.

![EventTracker homepage ribbon](image)

**Figure 45**

3. In log search window, initiate search with following criteria.
   - Select **File Transfer** checkbox and choose appropriate systems.
   - Select appropriate time duration.
   - In Custom Criteria, Event Id contains **3230**.
   - In Custom Criteria, Source contains **EventTracker**.

![Log search window](image)

**Figure 46**
4. Consumed logs will be displayed as shown below.

![Figure 47](image)

5. KP import steps are provided earlier in **Import Exchange Reports** section.
6. KP verification procedure is provided earlier in **Verify Exchange Reports** section.

A sample report of administrator audit is given below.

**Exchange-Admin audit details**

![Figure 48](image)
Monitor Antivirus Engine Status

When Antivirus Scanning Engine installed on Exchange server, the Engine status needs to be monitored.

- **MSEExchange: Antivirus engine started** - This category report contains records related to Antivirus engine startup on exchange server.
- **MSEExchange: Antivirus engine stopped** - This category report contains records related to Antivirus engine stopped on exchange server.
- **MSEExchange: Antivirus scanning engine Error** - This category report contains records related to Antivirus engine error occurred on exchange server.
- **MSEExchange: Virus cleaned from message** - This category report contains records related to virus detected and cleaned.
- **MSEExchange: Virus detected in message** - This category report contains records related to virus detected.

Monitor Exchange Database Backup Recovery Operation

- **MSEExchange: Exchange store database backup started** - This category report contains records for exchange store database backup started.
- **MSEExchange: Database backup completed** - This category report contains records for exchange store database backup completed successfully.
- **MSEExchange: Storage group backup failed** - This category report contains records for exchange backup software encountered any problem when backup operation is performed.
- **MSEExchange: Database restore started** - This category report contains records for database restore started.
- **MSEExchange: Database restore successful** - This category report contains records for successful database restore.
- **MSEExchange: Database recovery failed** - This category report contains records for database recovery failure.
- **MSEExchange: Exchange store database recovery completed** - This category report contains records for successful database recovery.
- **MSEExchange: VSS writer failed restoring a backup** - This category report contains records for database restore from backup failed by VSS service.

Monitor Exchange Clustered Resource Status

- **MSEExchange: Clustered mailbox server moved/failed over** - This category report contains records of clustered mailbox server moved or failed over to passive node.
- **MSExchange: Clustered mailbox server stopped** - This category report contains records for clustered mailbox server stopped. Need to check clustered mailbox server status and bring it online otherwise in case of active node failure it won’t be able to failover to passive node.

- **MSExchange: Clustered resource failed to stop** - This category report contains records for cluster service failed to stop exchange services.

- **MSExchange: Clustered resource failed to terminate** - This category report contains records for cluster service failed to terminate the clustered exchange resource.

- **MSExchange: Exchange clustered resource failed to be online** - This category report contains records for exchange system attendant failed to bring clustered exchange resource online.

- **MSExchange: Exchange clustered resource failed to go offline** - This category report contains records for exchange system attendant failed to bring clustered exchange resource offline.

- **MSExchange: IsAlive check failed for clustered resource** - This category report contains records for ISALIVE check failure for the clustered named resource. This failure could be because the other node might not be reachable from this node or because that node is really down for some reason.
Monitor Exchange Database Activity and Disc, Storage Limit Threshold

- **MSEExchange: Database disk full** - This category report contains records for disk containing exchange database which is full.
- **MSEExchange: Database error occurred** - This category report contains records for any database error occurrence.
- **MSEExchange: Database log disk full** - This category report contains records for disk containing exchange database Log which is full.
- **MSEExchange: Database log file Write error** - This category report contains records for any error occurred while writing to database log file.
- **MSEExchange: Database maximum size reached** - This category report contains records for maximum database size reached for exchange database. Exchange database size should be extended or freed up immediately.
- **MSEExchange: Database missing or corrupt** - This category report contains records for any database file missing or corruption. Database file need to be restored.
- **MSEExchange: Database mounts and dismounts** - This category report contains records for Exchange server database mounts and dismounts.
- **MSEExchange: Database offline** - This category report contains records for Exchange database offline. Reason for the database offline should be verified and it should be brought up online.
- **MSEExchange: Database replication error** - This category report contains records for any database replication error occurred.
- **MSEExchange: Database session limit reached** - This category report contains records for Exchange database session limits exceeded. This will not allow other users to access mailbox. Problem should be rectified immediately.
- **MSEExchange: Disk IO error** - This category report contains records for any Disk IO error occurred while writing database log file. This will interrupt Exchange database log file update process, problem should be rectified immediately.
- **MSEExchange: Exchange database free space** - This category report contains records related to database free space available after online defragmentation.
- **MSEExchange: Exchange storage group offline** - This category report contains records related to Exchange storage group offline. Reason for Storage group offline should be checked and corrected.
- **MSEExchange: Maximum number of database limit exceeded** - This category report contains records related to maximum number of mailbox or public folder databases limit on storage group exceeded.
- **MSEExchange: Maximum number of storage group limit exceeded** - This category report contains records related to number of storage groups on this server exceeded maximum limit.
- **MSEExchange: Public folder storage limit exceeded** - This category report contains records related to public folders on database exceeded the Issue Warning storage limit.
- **MSEExchange: User consuming maximum server resource** - This category report contains records related to user consuming their maximum allowed share of server resources.
- **MSExchange: User exceeded mailbox storage limit** - This category report contains records related to user exceeded mailbox storage limit exceeded.

## Real-time Critical Alerts

<table>
<thead>
<tr>
<th>Alerts name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustered resource failed</td>
<td>Exchange system attendant failed to bring clustered exchange resource online.</td>
</tr>
<tr>
<td>Database maximum size reached</td>
<td>Exchange database maximum size reached.</td>
</tr>
<tr>
<td>Database offline</td>
<td>Exchange database is offline.</td>
</tr>
<tr>
<td>Disk IO error</td>
<td>ESE receives an error from the operating system while trying to read or write to a file.</td>
</tr>
<tr>
<td>Exchange database log file Write error</td>
<td>Error occurred when writing to database log file.</td>
</tr>
<tr>
<td>Exchange database recovery failed</td>
<td>Exchange database cannot be recovered because an error occurred after a restore operation.</td>
</tr>
<tr>
<td>Exchange Server database disk full</td>
<td>Disk containing exchange database is full.</td>
</tr>
<tr>
<td>Exchange Server database error</td>
<td>An error occurred on database.</td>
</tr>
<tr>
<td>Exchange server database missing or corrupt</td>
<td>Exchange database file missing or corrupt.</td>
</tr>
<tr>
<td>Information Store service problem</td>
<td>Error occurred while initializing/starting Information store.</td>
</tr>
<tr>
<td>Exchange services not running</td>
<td>Exchange services detected not running.</td>
</tr>
<tr>
<td>IsAlive check failed for clustered resource</td>
<td>Cluster service failed the ISALIVE check for the named resource. This failure could be because the other node might not be reachable from this node or because that node is really down for some reason.</td>
</tr>
<tr>
<td>Log disk is full</td>
<td>Log disk for database is full.</td>
</tr>
<tr>
<td>Logon failure on mailbox database</td>
<td>Logon failure occurred on mailbox database.</td>
</tr>
<tr>
<td>Public folder storage limit exceeded</td>
<td>Public folders on database exceeded the Issue Warning storage limit.</td>
</tr>
<tr>
<td>User consuming maximum allowed server resource</td>
<td>User consuming their maximum allowed share of server resource.</td>
</tr>
<tr>
<td>User mailbox exceeded storage limit</td>
<td>User mailbox exceeded storage limit.</td>
</tr>
<tr>
<td>VSS writer failed to restore backup</td>
<td>Exchange VSS Writer failed to restore a backup.</td>
</tr>
<tr>
<td>Exchange Service Runaway process</td>
<td>Service running on exchange server consuming more CPU resource.</td>
</tr>
<tr>
<td>Exchange service network port is down</td>
<td>Network ports used by Exchange server is down.</td>
</tr>
</tbody>
</table>