**Microsoft® Exchange® Server 2013+ Log Insight Content Pack**

* **Overview:**

The vRealize Log Insight Content Pack for Microsoft® Exchange® servers offers a simple, intuitive approach for collecting, structuring, analyzing and graphically displaying Exchange log messages, with an industry leading scale out architecture. Sources of log messages including those that are database, transport, administrative, mailbox, client access, and/or LDAP related are collected and consolidated. In near real time log messages are analyzed for identifying and alerting on critical events that are impacting end user performance.

* **Highlights:**
  + Integrated with Microsoft Exchange Server 2013 and 2016
  + Access into, and viewing of logs messages, posted within Windows Event Log
  + Intelligent grouping of Exchange messages by function (transport, Client Access, database etc.)
* **Description:**

The Microsoft® Exchange® Server 2013 content pack includes 10 predefined Exchange dashboards, and around 39 widgets, several Mailbox and Transport queries and around 12 Alerts for offering a more customized user experience to Exchange administrators.  These dashboards provide visibility into a multitude of Exchange operation functions including Mailbox, Transport, Client Access & Unified Messaging, and Administrator Audit logs, SMTP, User and Database Information, mailbox size statistics.

* Specific events offered within this Exchange content pack include the following:
  + Database health checks
  + Insufficient data redundancy checks
  + Critical storage errors
  + Transport shutting down events
  + Critical service events
  + Administrative audit changes
  + Emails received
  + Mailbox size
* The top Exchange counter information closely monitored for detecting and alerting on Exchange problems include the following:
  + SMTP bytes received per message
  + SMTP messages received per second
  + Store driver inbound local delivery calls per second
  + Store driver inbound message delivery attempts per second
* **Technical Specifications:**
  + **Compatibility:**

Microsoft Exchange Server 2013 and 2016.

* **Requirement:**

This content pack requires the use of Log Insight's Windows agent and the use of the agent's CFAPI protocol

* **Installation/Configuration**

Navigate to the "Content Pack" menu in Log Insight. Select the "Import Content Pack" button. In the "Import Content Pack" menu, do the following:

* + Select the "Browse..." button and select the content pack \*.vlcp you are trying to import
  + Select the "Install as content pack" radio button
  + Select the "Import" button

Alternately, you can also install the content pack from the marketplace available on Log Insight UI

* + On Log Insight UI, browse to Content Pack -> Marketplace
  + Click on the “Microsoft Exchange2013+” content pack, accept terms of License Agreement then click ‘Install’
  + **Configuration:**

**1.**       **Enable Administrator Audit Logging :** Enable Administrator Audit Logging by following the instructions here:  
[https://technet.microsoft.com/EN-US/library/dd335109(v=exchg.150).aspx](https://technet.microsoft.com/EN-US/library/dd335109%28v=exchg.150%29.aspx)  
  
  
**2.**       **Enable SMTP Protocol Logging :**SMTP Protocol logging is not enabled by default. To enable SMTP protocol logging using EAC or shell follow the steps mentioned at:  
<https://technet.microsoft.com/en-us/library/bb124531%28v=exchg.150%29.aspx>  
  
You can set the logging interval and specify log path where SMTP logs would be generated. This path needs to be mentioned in **liagent.ini** file (Log Insight's Windows agent config file Section 4.) to enable forwarding these logs to LI Instance.  
  
**Tip**: To enable protocol logging for all send and receive connectors using Exchange Management shell to execute the following commands:  
  
***Get-ReceiveConnector | Set-ReceiveConnector -ProtocolLoggingLevel verbose***  
***Get-SendConnector | Set-SendConnector -ProtocolLoggingLevel verbose***  
  
**Exchange 2013 and 2016:**  
The default logging directories are the following (It the Exchange server installed in the different directory rather the default, directory path need to be updated in agent group configuration to have correct log collection). **Send Connector:**

* **Transport service on Mailbox servers**: %ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpSend
* **Mailbox Transport service on Mailbox servers**: %ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpSend
* **Front End Transport service on Client Access servers**: %ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpSend

**Receive Connector:**

* **Transport service on Mailbox servers**: %ExchangeInstallPath%TransportRoles\Logs\Hub\ProtocolLog\SmtpReceive
* **Mailbox Transport service on Mailbox servers**: %ExchangeInstallPath%TransportRoles\Logs\Mailbox\ProtocolLog\SmtpReceive
* **Front End Transport service on Client Access servers**: %ExchangeInstallPath%TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpReceive

**3.      Enable scripts by Windows Task Scheduler:**  
Download and extract all necessary scripts archive from Solution Exchange to a permanent location (All scripts are available on the VSX Solution Exchange Marketplace).   
As the example, scripts can be extracted under the following path:   
C:\ProgramData\VMware\Log Insight Agent\exchange\    
  
To make possible time by time extract logs from the Microsoft Exchange server scripts need to continually be executed by Windows Task Scheduler.The following two tasks in Windows Task Scheduler need to be configured.  
  
**a. How to activate "exchange\_wrapper"**  
Create **exhange\_wrapper.cmd** wrapper for **exchange\_wrapper.ps1** script with the following content and place it into the location where you have extracted all scripts. In this example it is the “C:\ProgramData\VMware\Log Insight Agent\exchange\scripts” directory.  
  
C:\windows\system32\Windowspowershell\v1.0\PowerShell.exe -NonInteractive -ExecutionPolicy Bypass -command ". 'C:\Program Files\Microsoft\Exchange Server\V15\Bin\RemoteExchange.ps1'; Connect-ExchangeServer -auto; . 'C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_wrapper.ps1'"  
  
**Note:** Do not forget to correct directory path. The **exhange\_wrapper.cmd** script if the Exchange Management shell and scripts are located under the different directory rather then in this example. The mentioned wrapper script is functional on Windows Command Prompt shell.  
  
**How to configure Windows Task Scheduler.**  
1. Open Task Scheduler  
2. The following need to be configured under the "General" section

* Give the “exchange\_wrapper” name for the task
* Specify user that have sufficient permissions to run Exchange Management Shell for the “When running the task, user the following user account:”. Usually it Exchange administrator.
* Enable checkbox for "Run whether user is logged on or not"
* Enable checkbox for "Run with highest privileges"

3. Move to the "Triggers" section and create new trigger with following parameters

* Begin the task: On a schedule
* Setting: set to "Daily" and set some start date and time which is in future
* Enable checkbox for "Synchronize across time zone"
* Recur every: 1 days
* Repeat task every: 5 minutes for the duration of 1 day. (**Note:** This duration can be set as per requirement, depending on the size and complexity of the environment.)
* Enable checkbox for "Enabled"

4. Move to the "Actions" section and create new action with following parameters

* Action is set to: "Start a program"
* Value for the Program/Script field: cmd
* Add arguments (optional): /c exchange\_wrapper.cmd > exchange\_wrapper.log 2>&1
* Start in (optional) : C:\ProgramData\VMware\Log Insight Agent\exchange\scripts (**Note:** The paths mentioned in above steps need to be modified as per the environment to point scripts directory.)

5. Move to the "Settings" section and the following parameters

* Enable checkbox for "Allow task to be run on demand"
* Enable checkbox for "Stop the task if it runs longer then 1 day"
* Enable checkbox for "If the running task does not end with requested, force it to stop"
* Set "Do not start a new instance"

Add the **exchange\_wrapper.ps1** script over all Exchange servers if any. It collects performance and message counters eg. capacity, number of received/sent messages. It is required to be run in short intervals.  
  
**b. How to activate "exchange\_mailbox\_wrapper"**  
Create **exhange\_ mailbox\_wrapper.cmd** wrapper for **exchange\_mailbox\_wrapper.ps1** script with the following content and place it into the location where you have extracted all scripts. In this example it is the “C:\ProgramData\VMware\Log Insight Agent\exchange\scripts” directory.  
  
c:\windows\system32\Windowspowershell\v1.0\PowerShell.exe -NonInteractive -ExecutionPolicy Bypass -command ". 'C:\Program Files\Microsoft\Exchange Server\V15\Bin\RemoteExchange.ps1'; Connect-ExchangeServer -auto; .'C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_mailbox\_wrapper.ps1'"  
  
**Note:** Do not forget to correct directory path. The **exchange\_mailbox\_wrapper.cmd** script if the Exchange Management shell and scripts are located under the different directory rather then in this example. The mentioned wrapper script is functional on Windows Command Prompt shell.  
  
**How to configure Windows Task Scheduler**.  
1. Open Task Scheduler  
2. The following need to be configured under the "General" section

* Give the “exchange\_ mailbox\_wrapper” name for the task
* Specify user that have sufficient permissions to run Exchange Management Shell for the “When running the task, user the following user account:”. Usually it Exchange administrator.
* Enable checkbox for "Run whether user is logged on or not"
* Enable checkbox for "Run with highest privileges"

3. Move to the "Triggers" section and create new trigger with following parameters

* Begin the task: On a schedule
* Setting: set to "Daily" and set some start date and time which is in future
* Enable checkbox for "Synchronize across time zone"
* Recur every: 1 days
* Repeat task every: 6 hours for the duration of 1 day. (**Note:** This duration can be set as per requirement, depending on the size and complexity of the environment.)
* Enable checkbox for "Enabled"

4. Move to the "Actions" section and create new action with following parameters

* Action is set to: "Start a program"
* Value for the Program/Script field: cmd
* Add arguments (optional): /c exchange\_mailbox\_wrapper.cmd > exchange\_mailbox\_wrapper.log 2>&1
* Start in (optional) : C:\ProgramData\VMware\Log Insight Agent\exchange\scripts (**Note:** The paths mentioned in above steps need to be modified as per the environment to point scripts directory.)

5. Move to the "Settings" section and the following parameters

* Enable checkbox for "Allow task to be run on demand"
* Enable checkbox for "Stop the task if it runs longer then 1 day"
* Enable checkbox for "If the running task does not end with requested, force it to stop"
* Set "Do not start a new instance"

Add the exchange\_wrapper.ps1 script over all Exchange servers if any. It will execute heavy queries to MS Exchange eg. Information about each mailbox statistics or looking into tracing logs. It will also collect information about other servers from Exchange clusters, that is needed from placing data on vRLI dashboards/widgets. Data collected by this sever are low frequently changed data (eg. Size of mailboxes, sent/received email statistics) but with each run it gathers information from last 6 hours.  
  
Both **exchange\_wrapper.ps1** and **exchange\_mailbox\_wrapper.ps1** scripts can give some additional output to stdout for troubleshooting purposes. The scripts output will show if they are run by hand from the Windows Command Prompt shell console.   
  
**4. vRLI agent configuration (setup liagent.ini):**  
The "Microsoft - Exchange" content pack requires the use of the vRealize Log Insight agent to send logs collected by the wrapper script to the vRLI server instance. So vRLI agent should be installed and configure on the Exchange Windows machine to use CFAPI protocol (default).  
To apply the agent group configuration:  
  
\* Go to the Administration -> Management -> Agents page (requires Super Admin privileges)  
\* Download the vRLI agent using "Download Log Insight Agent Version" link and install on the target Windows machine.  
\* Select the All Agents drop-down at the top of the window and select the “Copy Template” button to the right of the "Microsoft – Exchange 2013&2016" agent group   
\* Add the desired filters to restrict which agent receive the configuration (optional if there are only Exchange Windows vRLI agent in the list)  
\* Select the "Refresh" button at the top of the page  
\* Switch to the "Edit" mode of the agent configuration and updated all directory path if necessary.  
\* Select the "Save Configuration" button at the bottom of the page.  
  
Note: Please pay attention that it is very important to adjust directory path in the agent configuration file, otherwise log will be missed on the vRLI site.