**Microsoft® Exchange® Server 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 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.

* + **Installation**

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 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 content pack and 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>

1. **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 the **liagent.ini** file to enable forwarding these logs to LI instance.

**Tip**: To enable protocol logging for all send and receive connectors using shell use the following commands:

***Get-ReceiveConnector | Set-ReceiveConnector -ProtocolLoggingLevel verbose***

***Get-SendConnector | Set-SendConnector -ProtocolLoggingLevel verbose***

**Exchange 2013 and 2016:**

**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

1. **Scripts :**

Copy the scripts directory from the root of the archive downloaded from Solution Exchange to a permanent location.

For example: C:\ProgramData\VMware\Log Insight Agent\exchange\

Create the following two tasks in Windows Task Scheduler with the following configurations

* 1. ***exchange\_wrapper***
     + Create exhange\_wrapper.cmd wrapper for **exchange\_wrapper.ps1** with the following content and place it into “C:\ProgramData\VMware\Log Insight Agent\exchange\scripts”
       - c:\windows\system32\Windowspowershell\v1.0\PowerShell.exe -NonInteractive -ExecutionPolicy Unrestricted -command ". 'D:\<Exchange instllation path>\bin\RemoteExchange.ps1'; Connect-ExchangeServer -auto; .'C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_wrapper.ps1'"
     + Set D:\<Exchange installation path> to your MS Exchange installation path
     + Run as user with sufficient permissions to run Exchange Management Shell
     + Set to: Run whether user is logged on or not
     + Set to: Run with highest privileges
     + Action is set to: Start a program
     + Program: C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_wrapper.cmd
     + Start in: C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\
     + Trigger is set to Daily
     + 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)

* + - Set to: Enabled

Note: The paths mentioned in above steps need to be modified as per the environment.

Place **exchange\_wrapper.ps1** file on the all servers form Exchanges cluster. It collects performance and message counters eg. capacity, number of received/sent messages. It is required to be run in short intervals.

* 1. ***exchange\_mailbox\_wrapper***
     + Create exhange\_wrapper.cmd wrapper for Exchange\_wrapper.ps1 with the following content and place it into “C:\ProgramData\VMware\Log Insight Agent\exchange\scripts”
       - c:\windows\system32\Windowspowershell\v1.0\PowerShell.exe -NonInteractive -ExecutionPolicy Unrestricted -command ". 'D:\<Exchange instllation path>\bin\RemoteExchange.ps1'; Connect-ExchangeServer -auto; .'C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_mailbox\_wrapper.ps1'"
     + Set D:\<Exchange installation path> to your MS Exchange installation path
     + Run as user with sufficient permissions to run Exchange Management Shell
     + Set to: Run whether user is logged on or not
     + Set to: Run with highest privileges
     + Action is set to: Start a program
     + Program: C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\exchange\_mailbox\_wrapper.cmd
     + Start in: C:\ProgramData\VMware\Log Insight Agent\exchange\scripts\
     + Trigger is set to Daily
     + 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)

* + - Set to: Enabled

Note: The paths mentioned in above steps need to be modified as per the environment.

Place **exchange\_mailbox\_wrapper.ps1** file only on one server from Exchange cluster. 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: they will show it if they are run by hand from the console but in Task Scheduler its window is hidden so it will not be shows.

1. **liagent.ini configuration:**

The **"Microsoft - Exchange"** content pack requires the use of the Log Insight agent with the cfapi protocol (default) and the included agent group configuration. To apply the agent group configuration:  
  
\* Go to the **Administration -> Management -> Agents** page (requires Super Admin privileges)  
\* 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"** agent group

\* Add the desired filters to restrict which agent receive the configuration (optional)  
\* Select the "Refresh" button at the top of the page  
\* Select the "Save Configuration" button at the bottom of the page