Splunk® Supported Add-ons
Splunk Add-on for Microsoft Exchange released

Generated: 11/24/2022 10:20 am

Copyright (c) 2022 Splunk Inc. All Rights Reserved

Table of Contents

Introduction

About the Splunk Add-on for Microsoft Exchange

The Splunk Add-ons for Microsoft Exchange let you collect Exchange data from the hosts in your Exchange Server environment. The add-ons have been designed to work with the Splunk App for Microsoft Exchange, but are now available as a separate download from Splunkbase. You can use them with the app or to provide knowledge objects for Splunk Enterprise dashboards that you design by yourself.

Get the add-ons

The Splunk Add-ons for Microsoft Exchange are available on Splunkbase.

Install the add-ons

The add-ons require configuration before they can be used. Each add-on must be configured for the version of Exchange Server or Windows Server (for TA-Windows-Exchange-IIS) that you run in your Exchange Server environment. See the "Configure" topics in the chapter for each add-on for installation instructions.

See Where to install Splunk add-ons and Install an add-on in a distributed Splunk Enterprise deployment in the Add-ons *Overview* manual for more information about deploying the Splunk Add-on for Microsoft Exchange.

Prerequisites

- Ensure that the SplunkForwarder service is running as a local system account.
- Download the Splunk Add-on for Microsoft Exchange Indexes from Splunkbase for required index definitions to store the data.

Here's how to run the SplunkForwarder service as a local system account:

1. Navigate to **Services**.
2. Right click **SplunkForwarder Service**.
3. Click **Properties**.
4. Navigate to the **Log On** tab.
5. Select **Local System Account**.
6. Click **Apply**.
7. Restart the SplunkForwarder service.

Add-on package contents

The Splunk Add-ons for Microsoft Exchange come in a bundle and include the following:

TA-Exchange-ClientAccess

This add-on collects Exchange data from Exchange Server hosts that hold the Client Access Server role. It has support for Exchange Server 2010, 2013, 2016, 2019. See Overview of TA-Exchange-ClientAccess.

TA-Exchange-Mailbox

This add-on collects Exchange data from Exchange Server hosts that hold the Mailbox Store/Mailbox Server roles. It has support for Exchange Server 2010, 2013, 2016, and 2019. See Overview of TA-Exchange-Mailbox.

TA-Exchange-HubTransport

This add-on collects Exchange data from Exchange Server hosts that hold the Hub Transport role. It has support for Exchange Server 2010. Exchange Server versions 2013, 2016 and 2019 do not have this role. See Overview of TA-HubTransport.

TA-Windows-Exchange-IIS

This add-on collects Internet Information Server (IIS) data from Exchange Server hosts that hold the Client Access Server role. It has support for Windows Server2008 R2, 2012 R2, 2016 and 2019 and must be configured for the version of Windows Server that the Exchange Client Access Server hosts run. See Overview of TA-Windows-Exchange-IIS.

Splunk Add-on for Microsoft Exchange Component Installation Locations

The table below lists what components to install and where to install them:

Add-on	Indexer	Universal Forwarder	Heavy Forwarder
TA-Exchange-ClientAccess		X	
TA-Exchange-HubTransport		X	
TA-Exchange-Mailbox		X	
TA-Windows-Exchange-IIS		X	
TA-SMTP-Reputation			X
Splunk Add-on for Microsoft Exchange Indexes	X		

If you run into performance issues, see Troubleshoot Splunk App for Microsoft Exchange performance issues.

Release Notes for Splunk Add-ons for Microsoft Exchange

This topic contains information on new features, known issues, and updates of this version of the Splunk Add-ons for Microsoft Exchange. Version 4.0.4 of the Splunk Add-ons for Microsoft Exchange was released on July 12, 2022.

What's new

Update	Description
Added triggers stanza for custom configuration files	To avoid unnecessary restarts of the Splunk platform, the app.conf file has been updated with a `triggers` stanza and a reload setting for custom file configuration.

Known Issues

This version of the Splunk Add-ons for Microsoft Exchange has the following reported known issues and workarounds. If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2016-12-29	EXC-2052, EXC-2101	read-audit-logs_2010_2013.ps1 failure/crash Workaround: Currently no workaround known.

Fixed Issues

This version of the Splunk Add-ons for Microsoft Exchange has the following fixed issues. If no fixed issues appear below, none have yet been reported.

Upgrade the Splunk Add-on for Microsoft Exchange

Step 1. Upgrade the Forwarders

Upgrade the forwarders with the deployment server

Prepare the new Add-ons

1. Download the Splunk Add-on for Microsoft Exchange from Splunkbase.
2. Extract the Splunk Add-on for Microsoft Exchange to the deployment apps directory %SPLUNK_HOME%\etc\deployment-apps on the deployment server.
3. Within each Exchange Add-on directory in the deployment apps directory, create a `local` directory. For example, in %SPLUNK_HOME%\etc\deployment-apps\TA-Exchange-ClientAccess, create %SPLUNK_HOME%\etc\deployment-apps\TA-Exchange-ClientAccess\local.
4. For each Exchange add-on, copy the inputs.conf from the default directory of the add-on to the local directory you just created.
5. For each Exchange add-on, use a text editor to edit the inputs.conf files in the local directory and enable stanzas for the version of Exchange server that you run.
6. If you have made any customizations to the old set of Exchange add-ons, copy and paste those configurations from the local directory of those add-ons into the local directory of the new Exchange add-ons.

Create server classes, push the new add-ons, and delete old add-ons

1. On the deployment server, create a server class for each of the new Exchange add-ons.
2. Assign the add-ons to the appropriate server class. For example, the **TA-Exchange-HubTransport** add-on should be assigned to the `Exchange HubTransport` server class.
3. Assign the Windows Server, Exchange Server, and Active Directory hosts in your Exchange deployment to the appropriate server classes, depending on the roles that they perform. For example, Exchange Server hosts that hold the Hub Transport role should be assigned to the server class that has the **TA-Exchange-HubTransport** add-on assigned to it.
4. Delete all of the old add-ons on the deployment server (for example: **TA-DomainController-NT5**, **TA-Exchange-2013-Mailbox**).

5. Use the deployment server to push the new add-ons to all of the hosts in the deployment.
6. Restart the deployment server.
7. Restart all forwarders.

Upgrade the forwarders without the deployment server

Perform these steps on all the Exchange servers:

1. Download the Splunk Add-on for Microsoft Exchange from Splunkbase.
2. Stop the Splunk forwarder.
3. Extract the Splunk Add-on for Microsoft Exchange to the apps directory %SPLUNK_HOME%\etc\apps.
4. Start the Splunk forwarder.

Step 2. Upgrade the indexers

1. Download the Splunk Add-on for Microsoft Exchange Indexes from Splunkbase and extract its components to the /apps folder for your deployment.
    1. For a non-indexer cluster deployment, extract to $SPLUNK_HOME/etc/apps.
    2. For the indexer-clustering deployments, extract to $SPLUNK_HOME/etc/master-apps.
2. For indexer-clustering deployments, push the configuration bundle from the cluster master node.
3. For non-clustered indexers, restart Splunk on each indexer.
4. Disable maintenance mode on the cluster master node.

TA-Exchange-ClientAccess

Overview of TA-Exchange-ClientAccess

The TA-Exchange-ClientAccess add-on comes with the Splunk Add-on for Microsoft Exchange package. It collects Performance Monitoring and Windows Host Monitoring data from Exchange Server hosts that hold the Client Access Exchange Server role. It supports collection of data from Exchange Server 2010, Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019.

The add-on should be installed on a universal forwarder that has been installed on the Exchange Server host. Because the add-on collects data for all supported versions of Exchange Server by default, when you install the add-on you must configure it to collect only the data for the version of Exchange Server that you run.

Use a deployment server to manage distribution of this add-on to your Exchange Server hosts.

TA-Exchange-ClientAccess inputs

The TA-Exchange-ClientAccess add-on collects performance and Windows host monitoring data from Windows hosts that run Exchange Server and hold the Client Access Server role. See Configure TA-Exchange-ClientAccess to learn how to configure the add-on for your version of Exchange Server prior to deploying it to Exchange Server hosts.

The add-on includes the following data inputs:

Common data inputs

```
[WinHostMon://Processes]
[WinHostMon://Services]
[perfmon://Total_Processor_Time]
[perfmon://Processor]
[perfmon://System]
[perfmon://Available_Memory]
[perfmon://Memory]
[perfmon://DotNET_CLR_Memory]
[perfmon://Network_Utilization]
[perfmon://TCPv4]
[perfmon://TCPv6]
[perfmon://MSExchange_Control_Panel]
[perfmon://MSExchangePop3]
[perfmon://MSExchangeImap4]
[perfmon://MSExchange_Availability_Service]
[perfmon://MSExchange_FDS_OAB]
[perfmon://MSExchangeAutodiscover]
[perfmon://MSExchangeWS]
[perfmon://Web_Service]
```

Exchange Server 2010 data inputs

```
[perfmon://OWA_2010]
[perfmon://ActiveSync_2010]
[perfmon://MSExchange_Throttling_2010]
```

```
[monitor://C:\Program Files\Microsoft\Exchange Server\V14\Logging\RPC Client Access]
[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2007_2010.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-throttling-policies_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010_2013.ps1]
```

Exchange Server 2013, 2016, and 2019 data inputs

```
[perfmon://MSExchange_Throttling_2013]
[perfmon://MSExchange_Authentication]
[perfmon://MSExchange_SmtpReceive]
[perfmon://MSExchange_SmtpSend]
[monitor://C:\Program Files\Microsoft\Exchange Server\V15\Logging\RPC Client Access]
[script://.\bin\exchangepowershell.cmd v15 get-hoststats_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 read-audit-logs_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-throttling-policies_2010_2013.ps1]
```

For the admin audit log data collection, the PowerShell script saves the checkpoint (date) when this data was previously collected. Saving this checkpoint creates and uses splunk-msexchange-auditfile.clixml, which uses %TEMP% as a location and C:\Windows\Temp as a path for the NT Authority\SYSTEM account.

Configure TA-Exchange-ClientAccess

The Splunk Add-ons for Microsoft Exchange must be configured before you can deploy them to Exchange Server hosts. This is because you must specifically enable support for the version of Exchange Server that you run.

Each add-on within the Splunk Add-ons for Microsoft Exchange package includes an `inputs.conf` file that has all of the data inputs that are necessary to get Exchange Server data. These inputs are disabled by default.

Download and unpack the TA-Exchange-ClientAccess add-on

1. Download the Splunk Add-ons for Microsoft Exchange package from Splunkbase.
2. Unpack the add-on bundle to an accessible location.

Create and edit inputs.conf

1. Open a PowerShell window, command prompt, or Explorer window.
2. Create a `local` directory within the `TA-Exchange-ClientAccess` add-on.
3. Copy `inputs.conf` from the `TA-Exchange-ClientAccess\default` directory to the `TA-Exchange-ClientAccess\local` directory.
4. Use a text editor such as Notepad to open the `TA-Exchange-ClientAccess\local\inputs.conf` file for editing.
5. Modify the `inputs.conf` file so that the common data inputs and the inputs that are for the version of Exchange Server that you run are enabled. Do this by changing `disabled = true` to `disabled = false` for all input stanzas that are associated with your version of Exchange Server. See the example inputs.conf later in this topic.
6. After you update the `inputs.conf` file, save it and close it.

Distribute the add-ons

If you do not have a deployment server to distribute apps and add-ons, set one up. A deployment server greatly reduces the overhead in distributing apps and add-ons to hosts. You can make one change on the deployment server and push that change to all universal forwarders in your Splunk App for Microsoft Exchange deployment. The Splunk App for

Microsoft Exchange manual uses deployment server extensively in its setup instructions.

If you run more than one version of Exchange Server in your environment, set up a deployment server for each version of Exchange. This is because the Splunk Add-ons for Microsoft Exchange include data inputs for all versions of Exchange Server.

1. Copy the TA-Exchange-ClientAccess add-on to the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server.
2. Create a server class for all hosts that run Exchange Server and hold the Client Access Server role.
3. Add all Exchange Server hosts that hold the Client Access Server role to this server class.
4. Push the add-on to all hosts in this server class.

Example inputs.conf

The following `inputs.conf` listing is an example of how you should configure the TA-Exchange-ClientAccess add-on for installation on an Exchange Server 2010 host that holds the Client Access Server role. In this example, Exchange Server 2010 block has had its input stanzas changed from `disabled = true` to `disabled = false`. All other data input blocks have not been changed.

Remember to save the inputs.conf file after editing it, as changes do not take effect until the file has been saved and the add-on has been pushed to Exchange Server hosts.

```
##################################################################################################
#User should enable the stanza specific to the exchange server version by setting disabled=false #
##################################################################################################

####Common Stanzas - Start####

[WinHostMon://Processes]
index = windows
interval = 10
disabled = false
type = process

[WinHostMon://Services]
index = windows
interval = 10
disabled = false
type = service

[perfmon://Total_Processor_Time]
index=perfmon
object=Processor
counters=% Processor Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Processor]
index=perfmon
object=Processor
counters=% User Time; % Privileged Time
instances=_Total
interval=10
disabled=false
```

```
useEnglishOnly=true

[perfmon://System]
index=perfmon
object=System
counters=Processor Queue Length
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Available_Memory]
index=perfmon
object=Memory
counters=Available MBytes; Page Reads/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Memory]
index=perfmon
object=Memory
counters=Pool Nonpaged bytes; Pool Paged bytes; Cache Bytes; Committed Bytes; %Committed Bytes in Use;
Transition Pages Repurposed/sec; Pages/sec; Pages Input/sec; Pages Output/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://DotNET_CLR_Memory]
index=perfmon
object=.NET CLR Memory
counters=% Time in GC; # Bytes in all Heaps
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Network_Utilization]
index=perfmon
object=Network Interface
counters=Bytes Total/sec; Packets Outbound Errors
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv4]
index=perfmon
object=TCPv4
counters=Connections Established; Connections Reset
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv6]
index=perfmon
object=TCPv6
counters=Connection Failures
interval=10
disabled=false
useEnglishOnly=true
```

```
[perfmon://MSExchange_Control_Panel]
index=perfmon
object=MSExchange Control Panel
counters=Outbound Proxy Requests - Average Response Time; Requests - Average Response Time; ASP.Net Request
Failures/sec; Explicit Sign-On Inbound Proxy Requests/sec; Explicit Sign-On Inbound Proxy Sessions/sec;
Explicit Sign-On Outbound Proxy Requests/sec; Explicit Sign-On Outbound Session Requests/sec; Explicit
Sign-On Standard RBAC Requests/sec; Explicit Sign-On Standard RBAC Sessions/sec; Inbound Proxy Requests/sec;
Inbound Proxy Sessions/sec; Outbound Proxy Requests - Average Response Time; Outbound Proxy Requests/sec;
Outbound Proxy Sessions/sec; PowerShell Runspaces - Activations/sec; PowerShell Runspaces - Average Active
Time; PowerShell Runspaces/sec; RBAC Sessions/sec; Requests - Activations/sec; Requests - Average Response
Time
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangePop3]
index=perfmon
object=MSExchangePop3
instances=_total
counters=Connections Current; Connections Failed; Connections Rejected; Connections Total; Current
Unauthenticated Connections; Unauthenticated Connections/sec; Proxy Current Connections; Proxy Connections
Failed; Proxy Total Connections; Active SSL Connections; SSL Connections; Invalid Commands; Invalid Commands
Rate; AUTH Failures; AUTH Rate; AUTH Total; CAPA Failures; CAPA Rate; CAPA Total; DELE Failures; DELE Rate;
DELE Total; LIST Failures; LIST Rate; LIST Total; NOOP Failures; NOOP Rate; NOOP Total; PASS Failures; PASS
Rate; PASS Total; QUIT Failures; QUIT Rate; QUIT Total; Request Failures; Request Rate; Request Total; RETR
Failures; RETR Rate; RETR Total; RSET Failures; RSET Rate; RSET Total; STAT Failures; STAT Rate; STAT Total;
STLS Failures; STLS Rate; STLS Total; TOP Failures; TOP Rate; TOP Total; UIDL Failures; UIDL Rate; UIDL
Total; USER Failures; USER Rate; USER Total; XPRX Failures; XPRX Rate; XPRX Total; Average Command
Processing Time (milliseconds); Connections Rate; Transient Mailbox Connection Failures/minute; Mailbox
Offline Errors/minute; Transient Storage Errors/minute; Permanent Storage Errors/minute; Transient Active
Directory Errors/minute; Permanent Active Directory Errors/minute; Transient Errors/minute; Average RPC
Latency; Average LDAP Latency
interval=30
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeImap4]
index=perfmon
object=MSExchangeImap4
instances=_total
counters=Current Connections; Connections Failed; Connections Rejected; Connections Total; Current
Unauthenticated Connections; Unauthenticated Connections/sec; Proxy Current Connections; Proxy Connections
Failed; Proxy Total Connections; Active SSL Connections; SSL Connections; Invalid Commands; Invalid Commands
Rate; Append Failures; Append Rate; Append Total; Authenticate Failures; Authenticate Rate; Authenticate
Total; Capability Failures; Capability Rate; Capability Total; Check Failures; Check Rate; Check Total;
Close Failures; Close Rate; Close Total; Copy Failures; Copy Rate; Copy Total; Create Failures; Create Rate;
Create Total; Delete Failures; Delete Rate; Delete Total; Examine Failures; Examine Rate; Examine Total;
Expunge Failures; Expunge Rate; Expunge Total; Fetch Failures; Fetch Rate; Fetch Total; Idle Failures; Idle
Rate; Idle Total; List Failures; List Rate; List Total; Login Failures; Login Rate; Login Total; Logout
Failures; Logout Rate; Logout Total; LSUB Failures; LSUB Rate; LSUB Total; Namespace Failures; Namespace
Rate; Namespace Total; NOOP Failures; NOOP Rate; NOOP Total; Rename Failures; Rename Rate; Rename Total;
Request Failures; Request Rate; Request Total; Search Failures; Search Rate; Search Total; Select Failures;
Select Rate; Select Total; STARTTLS Failures; STARTTLS Rate; STARTTLS Total; Status Failures; Status Rate;
Status Total; Store Failures; Store Rate; Store Total; Subscribe Failures; Subscribe Rate; Subscribe Total;
Unsubscribe Failures; Unsubscribe Rate; Unsubscribe Total; XPROXY Failures; XPROXY Rate; XPROXY Total;
Average Command Processing Time (milliseconds); Connections Rate; SearchFolder Creation Rate; SearchFolder
Creation Total; Folder View Reload Rate; Folder View Reload Total; Transient Mailbox Connection
Failures/minute; Mailbox Offline Errors/minute; Transient Storage Errors/minute; Permanent Storage
Errors/minute; Transient Active Directory Errors/minute; Permanent Active Directory Errors/minute; Transient
Errors/minute; Average RPC Latency; Average LDAP Latency; Total IMAP UID Fixes; Current IMAP UID Fixes;
Total IMAP UID Items Fixed
interval=30
```

```
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Availability_Service]
index=perfmon
object=MSExchange Availability Service
counters=Average Time to Process a Free Busy Request; Availability Requests (sec)
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_FDS_OAB]
index=perfmon
object=MSExchangeFDS:OAB
counters=Download Task Queued; Download Tasks Completed
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeAutodiscover]
index=perfmon
object=MSExchangeAutodiscover
counters=Requests/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeWS]
index=perfmon
object=MSExchangeWS
counters=Requests/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Web_Service]
index=perfmon
object=Web Service
counters=Current Connections; Connection Attempts/sec; ISAPI Extension Requests/sec; Other Request
Methods/sec
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

####Common Stanzas - End####

###From Exchange app/add-on version 3.5.2,support for exchange server 2007 has ended.###
####Exchange Server 2007 - Start####

[perfmon://OWA_2007]
index=perfmon
object=MSExchange OWA
counters=Average Response Time; Average Search Time; Requests/sec; Current Unique Users
interval=10
disabled=true
useEnglishOnly=true

[perfmon://ActiveSync_2007]
index=perfmon
object=MSExchange ActiveSync
```

```
counters=Average Request Time; Requests/sec; Ping Commands Pending; Sync Commands/sec; Sync Commands
Pending; Current Requests
interval=10
disabled=true
useEnglishOnly=true

[monitor://C:\Program Files\Microsoft\Exchange Server\Logging\RPC Client Access]
whitelist=\.log$|\.LOG$
sourcetype=MSExchange:2007:RPCClientAccess
queue=parsingQueue
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-hoststats_2007_2010.ps1]
source=Powershell
sourcetype=MSExchange:2007:Topology
interval=300
index=msexchange
disabled=true

####Exchange Server 2007 - End####


####Exchange Server 2010 - Start####

[perfmon://OWA_2010]
index=perfmon
object=MSExchange OWA
counters=Average Response Time; Average Search Time; Requests/sec; Current Unique Users
interval=10
disabled=false
useEnglishOnly=true

[perfmon://ActiveSync_2010]
index=perfmon
object=MSExchange ActiveSync
counters=Average Request Time; Requests/sec; Ping Commands Pending; Sync Commands/sec; Sync Commands
Pending; Current Requests
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Throttling_2010]
index=perfmon
object=MSExchange Throttling
instances=*
counters=Average Thread Sleep Time; Active PowerShell Runspaces; Active PowerShell Runspaces/Sec; Exchange
Executing Cmdlets; Exchange Executing Cmdlets/Sec; Organization Throttling Policy Cache Hit Count;
Organization Throttling Policy Cache Miss Count; Organization Throttling Policy Cache Length; Organization
Throttling Policy Cache Length Percentage; Throttling Policy Cache Hit Count; Throttling Policy Cache Miss
Count; Throttling Policy Cache Length; Throttling Policy Cache Length Percentage
interval=30
disabled=false
useEnglishOnly=true

[monitor://C:\Program Files\Microsoft\Exchange Server\V14\Logging\RPC Client Access]
whitelist=\.log$|\.LOG$
sourcetype=MSExchange:2010:RPCClientAccess
queue=parsingQueue
index=msexchange
disabled=false
```

```
[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2007_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:Topology
interval=300
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-throttling-policies_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:ThrottlingPolicy
interval=86400
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:AdminAudit
interval=300
index=msexchange
disabled=false

####Exchange Server 2010 - End####


####Exchange Server 2013/2016/2019 - Start####

[perfmon://MSExchange_Throttling_2013]
index=perfmon
object=MSExchange User Throttling
instances=*
counters=Unique Budgets OverBudget; Total Unique Budgets; Delayed Threads; Users At MaxConcurrency; Users Locked Out; Percentage Users Micro Delayed; Percentage Users At Maximum Delay; Number Of Users At Maximum Delay; Number Of Users Micro Delayed; Budget Usage Five Minute Window 99.9%; Budget Usage Five Minute Window 99%; Budget Usage Five Minute Window 75%; Average Budget Usage Five Minute Window; Budget Usage One Hour Window 99.9%; Budget Usage One Hour Window 99%; Budget Usage One Hour Window 75%; Average Budget Usage One Hour Window
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Authentication]
index=perfmon
object=MSExchange Authentication
instances=_Total
counters=Outstanding Authentication Requests; Total Authentication Requests; Rejected Authentication Requests; Authentication Latency
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_SmtpReceive]
index=perfmon
object=MSExchangeFrontEndTransport SmtpReceive
counters=Average bytes/inbound message; Inbound Messages Received/sec
instances=_total
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_SmtpSend]
index=perfmon
object=MSExchangeFrontEndTransport SmtpSend
```

```
counters=Average message bytes/message; Messages Sent/sec
instances=_total
interval=10
disabled=true
useEnglishOnly=true

[monitor://C:\Program Files\Microsoft\Exchange Server\V15\Logging\RPC Client Access]
whitelist=\.log$|\.LOG$
sourcetype=MSExchange:2013:RPCClientAccess
queue=parsingQueue
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-hoststats_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:Topology
interval=300
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 read-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:AdminAudit
interval=300
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-throttling-policies_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:ThrottlingPolicy
interval=86400
index=msexchange
disabled=true

####Exchange Server 2013/2016/2019 - End####
```

Troubleshoot TA-Exchange-ClientAccess

The TA-Exchange-ClientAccess add-on should install on your Exchange Server hosts without problems as long as you configure it for the version of Exchange Server you run before you deploy it.

If you do not configure the add-on for your version of Exchange Server before you deploy it, then the add-on only collects data inputs that are common to all supported versions of Exchange Server. This results in missing data that is specific to your version of Exchange Server. See Configure TA-Exchange-ClientAccess for the procedure to configure the add-on and distribute it to your Exchange Server hosts.

If you upgrade from an earlier version of the Splunk App for Microsoft Exchange, complete the upgrade instructions in the Splunk App for Microsoft Exchange manual to ensure that the add-on collects all Exchange Server data for the version of Exchange Server that you run.

See the release notes for fixed and known issues.

TA-Exchange-Mailbox

Overview of TA-Exchange-Mailbox

The TA-Exchange-Mailbox add-on comes with the Splunk Add-on for Microsoft Exchange package. It collects Performance Monitoring and Windows Host Monitoring data from Exchange Server hosts that hold the Mailbox Store Exchange Server role. It supports collection of data from Exchange Server 2010, Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019.

The add-on should be installed on a universal forwarder that has been installed on the Exchange Server host. Because the add-on collects data for all supported versions of Exchange Server by default, when you install the add-on you must configure it to collect only the data for the version of Exchange Server that you run.

Use a deployment server to manage distribution of this add-on to your Exchange Server hosts.

TA-Exchange-Mailbox inputs

The TA-Exchange-Mailbox add-on collects performance and Windows host monitoring data from Windows hosts that run Exchange Server and hold the Mailbox Store role. See Configure TA-Exchange-Mailbox to learn how to configure the add-on for your version of Exchange Server prior to deploying it to Exchange Server hosts.

The add-on includes the following data inputs:

Common data inputs

```
[WinHostMon://Processes]
[WinHostMon://Services]
[perfmon://Total_Processor_Time]
[perfmon://Processor]
[perfmon://System]
[perfmon://Available_Memory]
[perfmon://Memory]
[perfmon://DotNET_CLR_Memory]
[perfmon://Network_Utilization]
[perfmon://TCPv4]
[perfmon://TCPv6]
[perfmon://MSExchange_Search_Indices]
[perfmon://MSExchange_Control_Panel]
[perfmon://Process_Microsoft.Exchange.Search.ExSearch]
[perfmon://Process_MSExchangeMailboxAssistants]
[perfmon://Process_msftesq]
[perfmon://MSExchange_Assistants_Per_Assistant]
[perfmon://MSExchange_Assistants_Per_DB]
[perfmon://MSExchange_Store_Interface_Total]
[perfmon://MSExchange_Store_Interface]
[perfmon://MSExchange_Mail_Submission]
[perfmon://MSExchange_ADAccess_Processes]
[perfmon://LogicalDisk]
[perfmon://MSExchangeIS]
[perfmon://MSExchange_Database_Edge_Transport]
[perfmon://MSExchange_Database_NoInstances]
[perfmon://MSExchange_Resourcebooking]
```

```
[perfmon://MSExchange_IS_Public]
[perfmon://MSExchange_Replication]
[perfmon://MSExchange_Calendarattendant]
[perfmon://MSExchange_IS_Mailbox]
```

Exchange Server 2010 data inputs

```
[perfmon://MSExchangeIS_Mailbox_2010]
[perfmon://MSExchange_Database_2010]
[perfmon://MSExchange_Database_Instances_2010]
[perfmon://MSExchangeIS_Client_2010]
[perfmon://MRM_Assistants_2010]
[perfmon://MSExchange_ADAccess_Caching_2010]
[perfmon://MRM_Counters_2010]
[perfmon://MSExchange_ADAccess_DC_2010]
[script://.\bin\exchangepowershell.cmd v14 get-publicfolderstats_2010.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-databasestats_2010.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-folderstats_2010.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-distlists_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 read-mailbox-audit-logs_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-mailboxstats_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-inboxrules_2010_2013.ps1]
```

Exchange Server 2013, 2016, and 2019 data inputs

```
[perfmon://OWA]
[perfmon://ActiveSync]
[perfmon://MSExchangePop3]
[perfmon://MSExchangeImap4]
[perfmon://Disk]
[perfmon://MSExchangeIS_Store]
[perfmon://MSExchange_Queue_Lengths]
[perfmon://MSExchange_Transport_Dumpster]
[perfmon://MSExchange_Store_Driver]
[perfmon://MSExchange_SmtpReceive]
[perfmon://MSExchange_SmtpSend]
[perfmon://MSExchange_Extensibility_Agents]
[perfmon://MSExchangeIS_Client_2013]
[perfmon://MSExchange_ADAccess_Caching_2013]
[perfmon://MRM_Counters_2013]
[perfmon://MSExchange_Database_2013]
[perfmon://MSExchange_Database_Instances_2013]
[perfmon://MSExchange_ADAccess_DC_2013]
[perfmon://MRM_Assistants_2013]
[monitor://C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]
[script://.\bin\exchangepowershell.cmd v15 get-databasestats_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-folderstats_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-distlists_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-hoststats_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 read-audit-logs_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 read-mailbox-audit-logs_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-mailboxstats_2010_2013.ps1]
[script://.\bin\exchangepowershell.cmd v15 get-inboxrules_2010_2013.ps1]
```

For the admin audit log data collection, the PowerShell script saves the checkpoint (date) when this data was previously collected. Saving this checkpoint creates and uses splunk-msexchange-auditfile.clixml and splunk-msexchange-mailboxauditlogs.clixml, which uses %TEMP% as a location and C:\Windows\Temp as a path for the NT Authority\SYSTEM account.

Configure TA-Exchange-Mailbox

The Splunk Add-ons for Microsoft Exchange must be configured before you can deploy them to Exchange Server hosts. This is because you must specifically enable support for the version of Exchange Server that you run.

Each add-on within the Splunk Add-ons for Microsoft Exchange package includes an `inputs.conf` file that has all of the data inputs that are necessary to get Exchange Server data. These inputs are disabled by default.

Download and unpack the TA-Exchange-Mailbox add-on

1. Download the Splunk Add-ons for Microsoft Exchange package from Splunkbase.
2. Unpack the add-on bundle to an accessible location.

Create and edit inputs.conf

1. Open a PowerShell window, command prompt, or Explorer window.
2. Create a `local` directory within the `TA-Exchange-Mailbox` add-on.
3. Copy `inputs.conf` from the `TA-Exchange-Mailbox\default` directory to the `TA-Exchange-Mailbox\local` directory.
4. Use a text editor such as Notepad to open the `TA-Exchange-Mailbox\local\inputs.conf` file for editing.
5. Modify the `inputs.conf` file so that the common data inputs and the inputs that are for the version of Exchange Server that you run are enabled. Do this by changing `disabled = true` to `disabled = false` for all input stanzas that are associated with your version of Exchange Server. See the example inputs.conf later in this topic.
6. After you update the `inputs.conf` file, save it and close it.

Distribute the add-ons

If you do not have a deployment server to distribute apps and add-ons, set one up. A deployment server greatly reduces the overhead in distributing apps and add-ons to hosts. You can make one change on the deployment server and push that change to all universal forwarders in your Splunk App for Microsoft Exchange deployment. The Splunk App for Microsoft Exchange manual uses deployment server extensively in its setup instructions.

If you run more than one version of Exchange Server in your environment, set up a deployment server for each version of Exchange. This is because the Splunk Add-ons for Microsoft Exchange include data inputs for all versions of Exchange Server.

1. Copy the TA-Exchange-Mailbox add-on to the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server.
2. Create a server class for all hosts that run Exchange Server and hold the Mailbox Store role.
3. Add all Exchange Server hosts that hold the Mailbox Server role to this server class.
4. Push the add-on to all hosts in this server class.

Example inputs.conf

The following `inputs.conf` listing is an example of how you should configure the TA-Exchange-Mailbox add-on for installation on an Exchange Server 2010 host that holds the Mailbox Server role. In this example, Exchange Server 2010 block has had its input stanzas changed from `disabled = true` to `disabled = false`. All other data input blocks have not been changed.

Remember to save the inputs.conf file after editing it, as changes do not take effect until the file has been saved and the add-on has been pushed to Exchange Server hosts.

```
##################################################################################################
#User should enable the stanza specific to the exchange server version by setting disabled=false.#
##################################################################################################

####Common Stanzas - Start####

[WinHostMon://Processes]
index = windows
interval = 10
disabled = false
type = process

[WinHostMon://Services]
index = windows
interval = 10
disabled = false
type = service

[perfmon://Total_Processor_Time]
index=perfmon
object=Processor
counters=% Processor Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Processor]
index=perfmon
object=Processor
counters=% User Time; % Privileged Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://System]
index=perfmon
object=System
counters=Processor Queue Length
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Available_Memory]
index=perfmon
object=Memory
counters=Available MBytes; Page Reads/sec
```

```
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Memory]
index=perfmon
object=Memory
counters=Pool Nonpaged bytes; Pool Paged bytes; Cache Bytes; Committed Bytes; %Committed Bytes in Use;
Transition Pages Repurposed/sec; Pages/sec; Pages Input/sec; Pages Output/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://DotNET_CLR_Memory]
index=perfmon
object=.NET CLR Memory
counters=% Time in GC; # Bytes in all Heaps
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Network_Utilization]
index=perfmon
object=Network Interface
counters=Bytes Total/sec; Packets Outbound Errors
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv4]
index=perfmon
object=TCPv4
counters=Connections Established; Connections Reset
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv6]
index=perfmon
object=TCPv6
counters=Connection Failures
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Search_Indices]
index=perfmon
object=MSExchange Search Indices
counters=Average Latency of RPCs Used to Obtain Content; Average Document Indexing Time; Full Crawl Mode
Status
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Control_Panel]
index=perfmon
object=MSExchange Control Panel
counters=Outbound Proxy Requests - Average Response Time; Requests - Average Response Time; ASP.Net Request
Failures/sec; Explicit Sign-On Inbound Proxy Requests/sec; Explicit Sign-On Inbound Proxy Sessions/sec;
```

```
Explicit Sign-On Outbound Proxy Requests/sec; Explicit Sign-On Outbound Session Requests/sec; Explicit
Sign-On Standard RBAC Requests/sec; Explicit Sign-On Standard RBAC Sessions/sec; Inbound Proxy Requests/sec;
Inbound Proxy Sessions/sec; Outbound Proxy Requests - Average Response Time; Outbound Proxy Requests/sec;
Outbound Proxy Sessions/sec; PowerShell Runspaces - Activations/sec; PowerShell Runspaces - Average Active
Time; PowerShell Runspaces/sec; RBAC Sessions/sec; Requests - Activations/sec; Requests - Average Response
Time
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Process_Microsoft.Exchange.Search.ExSearch]
index=perfmon
object=Process
counters=% Processor Time
instances=Microsoft.Exchange.Search.ExSearch
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Process_MSExchangeMailboxAssistants]
index=perfmon
object=Process
counters=%Processor Time
instances=MSExchangeMailboxAssistants
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Process_msftesq]
index=perfmon
object=Process
counters=%Processor Time
instances=msftesq
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Assistants_Per_Assistant]
index=perfmon
object=MSExchange Assistants - Per Database
counters=Events in Queue; Average Event Processing Time in Seconds
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Assistants_Per_DB]
index=perfmon
object=MSExchange Assistants - Per Database
counters=Events in Queue; Average Event Processing Time in Seconds; Mailboxes Processed/sec; Events
Polled/sec
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Store_Interface_Total]
index=perfmon
object=MSExchange Store Interface
counters=RPC Latency average (msec); RPC Requests outstanding
instances=_Total
interval=10
```

```
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Store_Interface]
index=perfmon
object=MSExchange Store Interface
counters=ROP Requests outstanding; RPC Requests Outstanding; RPC Requests Sent/sec; RPC Slow Requests
latency average (msec); RPC Requests failed (%); RPC Slow Requests (%);
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Mail_Submission]
index=perfmon
object=MSExchange Mail Submission
counters=Successful Submissions Per Second; Hub Servers In Retry; Failed Submissions Per Second; Temporary
Submission Failures/sec
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_Processes]
index=perfmon
object=MSExchange ADAccess Processes
instances=*
counters=LDAP Read Time; LDAP Search Time
interval=10
disabled=false
useEnglishOnly=true

[perfmon://LogicalDisk]
index=perfmon
object=LogicalDisk
instances=*
counters=Avg. Disk sec/Read; Avg. Disk sec/Write
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeIS]
index=perfmon
object=MSExchangeIS
counters=RPC Requests; RPC Averaged Latency; RPC Operations/sec; RPC Client Backoff/sec; Client: RPCs
Failed/sec; Slow QP Threads; Slow Search Threads; User Count
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Database_Edge_Transport]
index=perfmon
object=MSExchange Database ==> Instances
counters=I/O Log Writes/sec; I/O Log Reads/sec; Log Generation Checkpoint Depth; Version buckets allocated;
I/O Database Reads/sec; I/O Database Writes/sec; Log Record Stalls/sec; Log Threads Waiting
instances=edgetransport/Transport Mail Database
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Database_NoInstances]
index=perfmon
```

```
object=MSExchange Database
counters=I/O Database Reads (Attached) Average Latency; I/O Database Writes (Attached) Average Latency; IO
Log Writes Average Latency; Log Record Stalls/sec; Log Threads Waiting; I/O Database Reads (Recovery)
Average Latency; I/O Database Writes (Recovery) Average Latency; IO Log Read Average Latency;
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Resourcebooking]
index=perfmon
object=MSExchange Resource Booking
counters=Average Resource Booking Processing Time; Requests Submitted; Requests Failed; Requests Processed
interval=30
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_IS_Public]
index=perfmon
object=MSExchangeIS Public
counters=Replication Receive Queue Size; Messages Queued for Submission
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Replication]
index=perfmon
object=MSExchange Replication
instances=*
counters=CopyQueueLength; ReplayQueueLength; ReplayGenerationsPerMinute
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Calendarattendant]
index=perfmon
object=MSExchange Calendar Attendant
instances=*
counters=Average Calendar Attendant Processing Time; Meeting Messages Processed; Requests Failed
interval=30
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_IS_Mailbox]
index=perfmon
object=MSExchangeIS Mailbox
counters=Slow Findrow Rate; RPC Averaged Latency; Search Task Rate
instances=*
interval=10
disabled=false
useEnglishOnly=true

####Common stanzas - End####

###From Exchange app/add-on version 3.5.2,support for exchange server 2007 has ended.###
####Exchange Server 2007 - Start####

[WinEventLog://Exchange Auditing]
sourcetype="WinEventLog:Exchange Auditing"
index=msexchange
queue=parsingQueue
disabled=true
```

```
[perfmon://MSExchangeIS_Mailbox_2007]
index=perfmon
object=MSExchangeIS Mailbox
instances=_Total
counters=Messages Delivered/sec; Messages Sent/sec; Messages Submitted/sec; Messages Queued for Submission;
RPC Averaged Latency
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MRM_Assistants_2007]
index=perfmon
object=MSExchange Assistants
instances=msexchangemailboxassistants-total
counters=Average Event Processing Time in Seconds;Average Event Queue Time in seconds;Average Mailbox
Processing Time In seconds;Events Polled/sec;Mailboxes processed/sec;Number of Failed Event
Dispatchers;Percentage of Failed Event Dispatchers
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_Caching_2007]
index=perfmon
object=MSExchange ADAccess Caches
instances=*
counters=LDAP Searches/sec
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_DC_2007]
index=perfmon
object=MSExchange ADAccess Domain Controllers
instances=*
counters=LDAP Read Time; LDAP Search Time; LDAP Searches timed out per minute; Long running LDAP
operations/Min
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchangeIS_Client_2007]
index=perfmon
object=MSExchangeIS Client
instances=*
counters=RPC Average Latency; RPC Operations/sec; JET Log Records/sec; JET Pages Read/sec; Directory Access:
LDAP Reads/sec; Directory Access: LDAP Searches/sec
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MRM_Counters_2007]
index=perfmon
object=MSExchange Managed Folder Assistant
counters=Items Moved; Items Deleted but Recoverable; Items Permanently Deleted; Items Moved to Discovery
Holds; Items deleted due to Eha expiry date; Items moved due to Eha expiry date; Items deleted by EHA hidden
folder cleanup enforcer; Items Marked as Past Retention Date; Items Subject to Retention Policy; Items
Journaled; Mailbox Dumpsters Skipped; Mailbox Dumpsters Expired Items; System Data Expired Items; Total Over
Quota Dumpsters; Total Over Quota Dumpster Items; Total Over Quota Dumpster Items Deleted; Size of Items
subject to Retention Policy (In Bytes); Size of Items Deleted but Recoverable (In Bytes); Size of Items
Permanently Deleted (In Bytes); Size of Items Moved to Discovery Holds (In Bytes); Size of Items Moved due
to an Archive policy tag (In Bytes); Items Moved to Archive due to migration; Migrated items Hard deleted
```

```
due to item age based hold; Items stamped with Personal Tag; Items stamped with Default Tag; Items stamped
with Cleanup System Tag; Items expired by a Default Policy Tag; Total items expired by a Personal Tag; Total
items moved by a default Archive tag; Items Moved due to an Archive Tag; Mailbox Dumpsters Moved Items;
Health Monitor Average Delay (In Milliseconds); Health Monitor Delays/sec; Health Monitor Count of Unhealthy
Database Hits
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Database_2007]
index=perfmon
object=MSExchange Database
counters=Log Generation Checkpoint Depth; Database Page Fault Stalls/sec; Log Record Stalls/sec; Log Threads
Waiting; Version buckets allocated; Database Cache Size (MB); Database Cache % Hit; Log Bytes Write/sec
instances=Information Store
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Database_Instances_2007]
index=perfmon
object=MSExchange Database ==> Instances
counters=I/O Database Reads Average Latency; I/O Database Writes Average Latency
instances=_Total
interval=10
disabled=true
useEnglishOnly=true

[script://.\bin\exchangepowershell.cmd v8.0 get-databasestats_2007.ps1]
source=Powershell
sourcetype=MSExchange:2007:Database-Stats
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-folderstats_2007.ps1]
source=Powershell
sourcetype=MSExchange:2007:Folder-Usage
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-publicfolderstats_2007.ps1]
source=Powershell
sourcetype=MSExchange:2007:PublicFolder-Stats
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-hoststats_2007.ps1]
source=Powershell
sourcetype=MSExchange:2007:Topology
interval=300
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-mailboxstats_2007.ps1]
source=Powershell
sourcetype=MSExchange:2007:Mailbox-Usage
interval=3600
index=msexchange
disabled=true
```

```
####Exchange Server 2007 - End####


####Exchange Server 2010 - Start####

[perfmon://MSExchangeIS_Mailbox_2010]
index=perfmon
object=MSExchangeIS Mailbox
instances=_Total
counters=Messages Delivered/sec; Messages Sent/sec; Messages Submitted/sec; Messages Queued for Submission
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Database_2010]
index=perfmon
object=MSExchange Database
instances=Information Store
counters=Defragmentation Tasks; Defragmentation Tasks Pending; Sessions In Use; Sessions % Used; Table Open
Cache % Hit; Table Open Cache Hits/sec; Table Open Cache Misses/sec; Table Opens/sec; Table Closes/sec;
Tables Open; Log Bytes Write/sec; Log Bytes Generated/sec; Log Threads Waiting; Log Writes/sec; Log Record
Stalls/sec; Version Buckets Allocated; Database Cache Misses/sec; Database Cache % Hit; Database Cache % Hit
(Uncorrelated); Database Cache Requests/sec; Database Page Faults/sec; Database Page Evictions/sec; Database
Page Fault Stalls/sec; Database Cache Size (MB); Database Cache Size; Database Cache Size Effective (MB);
Database Cache Size Effective; Database Cache Memory Committed (MB); Database Cache Memory Committed;
Database Cache Memory Reserved (MB); Database Cache Memory Reserved; Database Cache Size Resident; Database
Cache Size Resident (MB); Database Cache % Dehydrated; Database Maintenance Duration; Database Maintenance
Pages Bad Checksums; I/O Database Reads (Attached)/sec; I/O Database Reads (Attached) Average Latency; I/O
Database Reads (Recovery)/sec; I/O Database Reads (Recovery) Average Latency; I/O Database Reads/sec; I/O
Database Reads Average Latency; I/O Log Reads/sec; I/O Log Reads Average Latency; I/O Database Writes
(Attached)/sec; I/O Database Writes (Attached) Average Latency; I/O Database Writes (Recovery)/sec; I/O
Database Writes (Recovery) Average Latency; I/O Database Writes/sec; I/O Database Writes Average Latency;
I/O Log Writes/sec; I/O Log Writes Average Latency
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Database_Instances_2010]
index=perfmon
object=MSExchange Database ==> Instances
counters=I/O Database Reads Average Latency; I/O Database Writes Average Latency
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeIS_Client_2010]
index=perfmon
object=MSExchangeIS Client
instances=*
counters=RPC Average Latency; RPC Operations/sec; JET Log Records/sec; JET Pages Read/sec; Directory Access:
LDAP Reads/sec; Directory Access: LDAP Searches/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MRM_Assistants_2010]
index=perfmon
object=MSExchange Assistants - Per Database
instances=msexchangemailboxassistants-total
counters=Events in queue; Average Event Processing Time In seconds; Events Polled; Events Polled/sec;
```

```
Polling Delay; Highest Event Counter Polled; Elapsed Time Since Last Event Polled; Elapsed Time Since Last
Event Polling Attempt; Elapsed Time Since Last Database Status Update Attempt; Percentage of Interesting
Events; Events Interesting to Multiple Asssitants; Mailbox Dispatchers; Mailbox Sessions In Use By
Dispatchers; Average Mailbox Processing Time In seconds; Mailboxes Processed; Mailboxes processed/sec;
Number of Threads Used; Health Measure
interval=30
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_Caching_2010]
index=perfmon
object=MSExchange ADAccess Caches
instances=*
counters=LDAP Searches/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MRM_Counters_2010]
index=perfmon
object=MSExchange Managed Folder Assistant
counters=Items Moved; Items Deleted but Recoverable; Items Permanently Deleted; Items Moved to Discovery
Holds; Items deleted due to Eha expiry date; Items moved due to Eha expiry date; Items deleted by EHA hidden
folder cleanup enforcer; Items Marked as Past Retention Date; Items Subject to Retention Policy; Items
Journaled; Mailbox Dumpsters Skipped; Mailbox Dumpsters Expired Items; System Data Expired Items; Total Over
Quota Dumpsters; Total Over Quota Dumpster Items; Total Over Quota Dumpster Items Deleted; Size of Items
subject to Retention Policy (In Bytes); Size of Items Deleted but Recoverable (In Bytes); Size of Items
Permanently Deleted (In Bytes); Size of Items Moved to Discovery Holds (In Bytes); Size of Items Moved due
to an Archive policy tag (In Bytes); Items Moved to Archive due to migration; Migrated items Hard deleted
due to item age based hold; Items stamped with Personal Tag; Items stamped with Default Tag; Items stamped
with Cleanup System Tag; Items expired by a Default Policy Tag; Total items expired by a Personal Tag; Total
items moved by a default Archive tag; Items Moved due to an Archive Tag; Mailbox Dumpsters Moved Items;
Health Monitor Average Delay (In Milliseconds); Health Monitor Delays/sec; Health Monitor Count of Unhealthy
Database Hits
interval=30
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_DC_2010]
index=perfmon
object=MSExchange ADAccess Domain Controllers
instances=*
counters=LDAP Read Time; LDAP Search Time; LDAP Searches timed out per minute; Long running LDAP
operations/Min
interval=10
disabled=false
useEnglishOnly=true

[script://.\bin\exchangepowershell.cmd v14 get-publicfolderstats_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:PublicFolder-Stats
interval=3600
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-databasestats_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:Database-Stats
interval=3600
index=msexchange
disabled=false
```

```
[script://.\bin\exchangepowershell.cmd v14 get-folderstats_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:Folder-Usage
interval=3600
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-distlists_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:DistributionLists
interval=14400
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:Topology
interval=300
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:AdminAudit
interval=300
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 read-mailbox-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:MailboxAudit
interval=300
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-mailboxstats_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:Mailbox-Usage
interval=3600
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-inboxrules_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2010:InboxRules
interval=86400
index=msexchange
disabled=false

####Exchange Server 2010 - End####


####Exchange Server 2013/2016/2019 - Start####

[perfmon://OWA]
index=perfmon
object=MSExchange OWA
counters=Average Response Time; Average Search Time; Requests/sec; Current Unique Users
interval=10
disabled=true
useEnglishOnly=true
```

```
[perfmon://ActiveSync]
index=perfmon
object=MSExchange ActiveSync
counters=Average Request Time; Requests/sec; Ping Commands Pending; Sync Commands/sec; Sync Commands
Pending; Current Requests
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchangePop3]
index=perfmon
object=MSExchangePop3
instances=_Total
counters=AUTH Failures; Connections Current; Connections Rejected; Average Command Processing Time
(milliseconds)
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchangeImap4]
index=perfmon
object=MSExchangeImap4
instances=_Total
counters=Authenticate Failures; Login Failures; Current Connections; Connections Rejected; Average Command
Processing Time (milliseconds)
interval=30
disabled=true
useEnglishOnly=true

[perfmon://Disk]
index=perfmon
object=Logical/Physical Disk
counters=Avg. Disk sec/Read; Avg. Disk sec/Write
instances=*
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchangeIS_Store]
index=perfmon
object=MSExchangeIS Store
instances=*
counters=RPC Requests; RPC Average Latency; RPC Operations/sec; RPC Client Backoff/sec; Client: RPCs
Failed/sec
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Queue_Lengths]
index=perfmon
object=MSExchangeTransport Queues
counters=External Active Remote Delivery Queue Length; Internal Active Remote Delivery Queue Length;
External Retry Remote Delivery Queue Length; Internal Retry Remote Delivery Queue Length; Active Mailbox
Delivery Queue Length; Retry Mailbox Delivery Queue Length; Active Non-Smtp Delivery Queue Length; Retry
Non-Smtp Delivery Queue Length; Internal Aggregate Delivery Queue Length (All Internal Queues); External
Aggregate Delivery Queue Length (All External Queues); Internal Largest Delivery Queue Length; Internal
Largest Unlocked Delivery Queue Length; External Largest Delivery Queue Length; External Largest Unlocked
Delivery Queue Length; Items Queued For Delivery Total; Items Queued for Delivery Per Second; Items
Completed Delivery Total; Items Completed Delivery Per Second; Items Queued For Delivery Expired Total;
Locks Expired In Delivery Total; Items Deleted By Admin Total; Items Resubmitted Total; Messages Deferred
Due To Local Loop; Messages Queued For Delivery; Messages Queued For Delivery Total; Messages Queued for
Delivery Per Second; Messages Completed Delivery Total; Messages Completed Delivery Per Second; Unreachable
```

```
Queue Length; Poison Queue Length; Submission Queue Length; Messages Submitted Total; Messages Submitted Per
Second; Messages Submitted Recently; Submission Queue Items Expired Total; Submission Queue Locks Expired
Total; Aggregate Shadow Queue Length; Shadow Queue Auto Discards Total; Messages Completing Categorization;
Messages Deferred during Categorization; Messages Resubmitted during Categorization; Categorizer Job
Availability
instances=*
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Transport_Dumpster]
index=perfmon
object=MSExchangeTransport Dumpster
counters=Dumpster Size; Dumpster Inserts/sec; Dumpster Item Count; Dumpster Deletes/sec
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Store_Driver]
index=perfmon
object=MSExchange Store Driver
counters=Inbound: LocalDeliveryCallsPerSecond; Outbound: Submitted Mail Items Per Second; Inbound:
MessageDeliveryAttemptsPerSecond; Inbound: Recipients Delivered Per Second
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_SmtpReceive]
index=perfmon
object=MSExchangeTransport SMTPReceive
counters=Average bytes/message; Messages Received/sec
instances=_total
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_SmtpSend]
index=perfmon
object=MSExchangeTransport SmtpSend
counters=Average message bytes/message; Messages Sent/sec
instances=_total
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Extensibility_Agents]
index=perfmon
object=MSExchange Extensibility Agents
counters=Average Agent Processing Time (sec); Total Agent Invocations
instances=*
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchangeIS_Client_2013]
index=perfmon
object=MSExchangeIS Client Type
instances=*
counters=RPC Average Latency; RPC Operations/sec; JET Log Records/sec; JET Pages Read/sec; Directory Access:
LDAP Reads/sec; Directory Access: LDAP Searches/sec
interval=10
disabled=true
```

```
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_Caching_2013]
index=perfmon
object=MSExchange ADAccess Caches
instances=_Total
counters=LDAP Searches/sec
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MRM_Counters_2013]
index=perfmon
object=MSExchange Managed Folder Assistant
instances=msexchangemailboxassistants-total
counters=Items Moved; Items Deleted but Recoverable; Items Permanently Deleted; Items Moved to Discovery
Holds; Items deleted due to Eha expiry date; Items moved due to Eha expiry date; Items deleted by EHA hidden
folder cleanup enforcer; Items Marked as Past Retention Date; Items Subject to Retention Policy; Items
Journaled; Mailbox Dumpsters Skipped; Mailbox Dumpsters Expired Items; System Data Expired Items; Total Over
Quota Dumpsters; Total Over Quota Dumpster Items; Total Over Quota Dumpster Items Deleted; Size of Items
subject to Retention Policy (In Bytes); Size of Items Deleted but Recoverable (In Bytes); Size of Items
Permanently Deleted (In Bytes); Size of Items Moved to Discovery Holds (In Bytes); Size of Items Moved due
to an Archive policy tag (In Bytes); Items Moved to Archive due to migration; Migrated items Hard deleted
due to item age based hold; Items stamped with Personal Tag; Items stamped with Default Tag; Items stamped
with Cleanup System Tag; Items expired by a Default Policy Tag; Total items expired by a Personal Tag; Total
items moved by a default Archive tag; Items Moved due to an Archive Tag; Mailbox Dumpsters Moved Items;
Health Monitor Average Delay (In Milliseconds); Health Monitor Delays/sec; Health Monitor Count of Unhealthy
Database Hits
interval=30
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Database_2013]
index=perfmon
object=MSExchange Database
instances=*
counters=Defragmentation Tasks; Defragmentation Tasks Pending; Sessions In Use; Sessions % Used; Table Open
Cache % Hit; Table Open Cache Hits/sec; Table Open Cache Misses/sec; Table Opens/sec; Table Closes/sec;
Tables Open; Log Bytes Write/sec; Log Bytes Generated/sec; Log Threads Waiting; Log Writes/sec; Log Record
Stalls/sec; Version Buckets Allocated; Database Cache Misses/sec; Database Cache % Hit; Database Cache % Hit
(Uncorrelated); Database Cache Requests/sec; Database Page Faults/sec; Database Page Evictions/sec; Database
Page Fault Stalls/sec; Database Cache Size (MB); Database Cache Size; Database Cache Size Effective (MB);
Database Cache Size Effective; Database Cache Memory Committed (MB); Database Cache Memory Committed;
Database Cache Memory Reserved (MB); Database Cache Memory Reserved; Database Cache Size Resident; Database
Cache Size Resident (MB); Database Cache % Dehydrated; Database Maintenance Duration; Database Maintenance
Pages Bad Checksums; I/O Database Reads (Attached)/sec; I/O Database Reads (Attached) Average Latency; I/O
Database Reads (Recovery)/sec; I/O Database Reads (Recovery) Average Latency; I/O Database Reads/sec; I/O
Database Reads Average Latency; I/O Log Reads/sec; I/O Log Reads Average Latency; I/O Database Writes
(Attached)/sec; I/O Database Writes (Attached) Average Latency; I/O Database Writes (Recovery)/sec; I/O
Database Writes (Recovery) Average Latency; I/O Database Writes/sec; I/O Database Writes Average Latency;
I/O Log Writes/sec; I/O Log Writes Average Latency
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MSExchange_Database_Instances_2013]
index=perfmon
object=MSExchange Database ==> Instances
counters=I/O Database Reads Average Latency; I/O Database Writes Average Latency
instances=*
interval=10
disabled=true
```

```
useEnglishOnly=true

[perfmon://MSExchange_ADAccess_DC_2013]
index=perfmon
object=MSExchange ADAccess Domain Controllers
instances=_Total
counters=LDAP Read Time; LDAP Search Time; LDAP Searches timed out per minute; Long running LDAP
operations/Min
interval=10
disabled=true
useEnglishOnly=true

[perfmon://MRM_Assistants_2013]
index=perfmon
object=MSExchange Assistants - Per Database
instances=msexchangemailboxassistants-total
counters=Average Event Processing Time In Seconds;Average Mailbox Processing Time In seconds;Events
Polled/sec;Mailboxes processed/sec
interval=30
disabled=true
useEnglishOnly=true

[monitor://C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]
whitelist=\.log$|\.LOG$
time_before_close = 0
sourcetype=MSExchange:2013:MessageTracking
queue=parsingQueue
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-databasestats_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:Database-Stats
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-folderstats_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:Folder-Usage
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-distlists_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:DistributionLists
interval=14400
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-hoststats_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:Topology
interval=300
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 read-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:AdminAudit
interval=300
```

```
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 read-mailbox-audit-logs_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:MailboxAudit
interval=300
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-mailboxstats_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:Mailbox-Usage
interval=3600
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v15 get-inboxrules_2010_2013.ps1]
source=Powershell
sourcetype=MSExchange:2013:InboxRules
interval=86400
index=msexchange
disabled=true

####Exchange Server 2013/2016/2019 - End####
```

Troubleshoot TA-Exchange-Mailbox

The TA-Exchange-Mailbox add-on should install on your Exchange Server hosts without problems as long as you configure it for the version of Exchange Server you run before you deploy it.

If you do not configure the add-on for your version of Exchange Server before you deploy it, then the add-on only collects data inputs that are common to all supported versions of Exchange Server. This results in missing data that is specific to your version of Exchange Server. See Configure TA-Exchange-Mailbox for the procedure to configure the add-on and distribute it to your Exchange Server hosts.

If you upgrade from an earlier version of the Splunk App for Microsoft Exchange, complete the upgrade instructions in the Splunk App for Microsoft Exchange manual to ensure that the add-on collects all Exchange Server data for the version of Exchange Server that you run.

In DAG, `read-audit-logs_2010_2013.ps1` script will index the data of the mailbox server only where this script is running. So it is required to enable this script on all servers in DAG.

Mailbox audit log collection failure

Mailbox audit log collection failure produces the below error log.

```
Search-MailboxAuditLog : The requesting account doesn't have permission to access the audit log.
At C:\Program
Files\SplunkUniversalForwarder\etc\apps\TA-Exchange-Mailbox\bin\powershell\read-mailbox-audit-logs_2010
_2013.ps1:49char:2
+     Search-MailboxAuditLog -Identity $Identity -LogonTypes Owner,Delegate,Admin -Sh ...
+    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Search-MailboxAuditLog], AuditLogAccessDeniedException
    + FullyQualifiedErrorId :
[Server=SRRZ2EXC01,RequestId=a61a5900-6e29-4b12-b703-680246db44d4,TimeStamp=16.11.2016 0
   7:25:13] [FailureCategory=Cmdlet-AuditLogAccessDeniedException]
```

```
55A06F96,Microsoft.Exchange.Management.SystemConfigurationTasks.SearchMailboxAuditLog
```

Workarounds

There are two workarounds for this error.

Run Splunk as a local system account

This error might occur when the Splunk Forwarder Service isn't running as a local sytem account. Complete the following steps on the forwarder machine to run Splunk as a local system account:

1. Navigate to Services.
2. Right click on **SplunkForwarder Service**.
3. Click on **Properties**.
4. Navigate to the **Log On** tab.
5. Select **Local System Account**.
6. Click **Apply**.
7. Restart the Splunkforwarder service.

Ensure the mailbox audit log script is able to read the timestamp of each mailbox

This error might also occur when the mailbox audit log script is unable to read the timestamp of each mailbox. Complete the following steps to fix this issue:

1. Navigate to `C:/Windows/Temp` on your Forwarder/Exchange Server machine.
2. Delete `splunk-msexchange-auditfile.clixml` and `splunk-msexchange-mailboxauditlogs.clixml`.

TA-Exchange-HubTransport

Overview of TA-Exchange-HubTransport

The TA-Exchange-HubTransport add-on comes with the Splunk Add-on for Microsoft Exchange package. It collects Performance Monitoring and Windows Host Monitoring data from Exchange Server hosts that hold the Hub Transport Exchange Server role. It supports collection of data from Exchange Server 2010. Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019 does not have this role, as it has been integrated into the Client Access and Mailbox Server roles.

The add-on should be installed on a universal forwarder that has been installed on the Exchange Server host. Because the add-on collects data for all supported versions of Exchange Server by default, when you install the add-on you must configure it to collect only the data for the version of Exchange Server that you run.

Use a deployment server to manage distribution of this add-on to your Exchange Server hosts.

TA-Exchange-HubTransport inputs

The TA-Exchange-HubTransport add-on collects performance and Windows host monitoring data from Windows hosts that run Exchange Server and hold the Hub Transport role. See Configure TA-Exchange-HubTransport to learn how to configure the add-on for your version of Exchange Server prior to deploying it to Exchange Server hosts.

The add-on includes the following data inputs:

```
####Common Stanzas - Start####
[WinHostMon://Processes]
[WinHostMon://Services]
[perfmon://Total_Processor_Time]
[perfmon://Processor]
[perfmon://System]
[perfmon://Available_Memory]
[perfmon://Memory]
[perfmon://DotNET_CLR_Memory]
[perfmon://Network_Utilization]
[perfmon://TCPv4]
[perfmon://TCPv6]
[perfmon://Disk]
[perfmon://MSExchange_Control_Panel]
[perfmon://MSExchange_Queue_Lengths]
[perfmon://MSExchange_Transport_Dumpster]
[perfmon://MSExchange_Store_Driver]
[perfmon://MSExchange_SmtpReceive]
[perfmon://MSExchange_SmtpSend]
[perfmon://MSExchange_Extensibility_Agents]
####Common Stanzas - End####

####Exchange Server 2010 - Start####
[monitor://C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking]
[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010.ps1]
[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2007_2010.ps1]
####Exchange Server 2010 - End####
```

```
###From Exchange app/add-on version 3.5.2,support for exchange server 2007 has ended.###
####Exchange Server 2007 - Start####
[monitor://C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking]
[script://.\bin\exchangepowershell.cmd v8.0 get-hoststats_2007_2010.ps1]
####Exchange Server 2007 - End####
```

> For the admin audit log data collection, the PowerShell script saves the checkpoint (date) when this data was previously collected. Saving this checkpoint creates and uses splunk-msexchange-auditfile.clixml, which uses %TEMP% as a location and C:\Windows\Temp as a path for the NT Authority\SYSTEM account.

Configure TA-Exchange-HubTransport

The Splunk Add-ons for Microsoft Exchange must be configured before you can deploy them to Exchange Server hosts. This is because you must specifically enable support for the version of Exchange Server that you run.

Each add-on within the Splunk Add-ons for Microsoft Exchange package includes an `inputs.conf` file that has all of the data inputs that are necessary to get Exchange Server data. These inputs are disabled by default.

Download and unpack the TA-Exchange-HubTransport add-on

1. Download the Splunk Add-ons for Microsoft Exchange package from Splunkbase.
2. Unpack the add-on bundle to an accessible location.

Create and edit inputs.conf

1. Open a PowerShell window, command prompt, or Explorer window.
2. Create a `local` directory within the `TA-Exchange-HubTransport` add-on.
3. Copy `inputs.conf` from the `TA-Exchange-HubTransport\default` directory to the `TA-Exchange-HubTransport\local` directory.
4. Use a text editor such as Notepad to open the `TA-Exchange-HubTransport\local\inputs.conf` file for editing.
5. Modify the `inputs.conf` file so that the common data inputs and the inputs that are for the version of Exchange Server that you run are enabled. Do this by changing `disabled = true` to `disabled = false` for all input stanzas that are associated with your version of Exchange Server. See the example inputs.conf later in this topic.
6. After you update the `inputs.conf` file, save it and close it.

Distribute the add-ons

If you do not have a deployment server to distribute apps and add-ons, set one up. A deployment server greatly reduces the overhead in distributing apps and add-ons to hosts. You can make one change on the deployment server and push that change to all universal forwarders in your Splunk App for Microsoft Exchange deployment. The Splunk App for Microsoft Exchange manual uses deployment server extensively in its setup instructions.

If you run more than one version of Exchange Server in your environment, set up a deployment server for each version of Exchange. This is because the Splunk Add-ons for Microsoft Exchange include data inputs for all versions of Exchange Server.

1. Copy the TA-Exchange-HubTransport add-on to the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server.
2. Create a server class for all hosts that run Exchange Server and hold the Hub Transport role.

3. Add all Exchange Server hosts that hold the Hub Transport role to this server class.
4. Push the add-on to all hosts in this server class.

Example inputs.conf

The following `inputs.conf` listing is an example of how you should configure the TA-Exchange-HubTransport add-on for installation on an Exchange Server 2010 host that holds the Hub Transport role. In this example, Exchange Server 2010 block has had its input stanzas changed from `disabled = true` to `disabled = false`. All other data input blocks have not been changed.

Remember to save the inputs.conf file after editing it, as changes do not take effect until the file has been saved and the add-on has been pushed to Exchange Server hosts.

```
##################################################################################################
#User should enable the stanza specific to the exchange server version by setting disabled=false #
##################################################################################################

####Common Stanzas - Start####

[WinHostMon://Processes]
index = windows
interval = 10
disabled = false
type = process

[WinHostMon://Services]
index = windows
interval = 10
disabled = false
type = service

[perfmon://Total_Processor_Time]
index=perfmon
object=Processor
counters=% Processor Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Processor]
index=perfmon
object=Processor
counters=% User Time; % Privileged Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://System]
index=perfmon
object=System
counters=Processor Queue Length
instances=*
interval=10
disabled=false
useEnglishOnly=true
```

```
[perfmon://Available_Memory]
index=perfmon
object=Memory
counters=Available MBytes; Page Reads/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Memory]
index=perfmon
object=Memory
counters=Pool Nonpaged bytes; Pool Paged bytes; Cache Bytes; Committed Bytes; %Committed Bytes in Use;
Transition Pages Repurposed/sec; Pages/sec; Pages Input/sec; Pages Output/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://DotNET_CLR_Memory]
index=perfmon
object=.NET CLR Memory
counters=% Time in GC; # Bytes in all Heaps
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Network_Utilization]
index=perfmon
object=Network Interface
counters=Bytes Total/sec; Packets Outbound Errors
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv4]
index=perfmon
object=TCPv4
counters=Connections Established; Connections Reset
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv6]
index=perfmon
object=TCPv6
counters=Connection Failures
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Disk]
index=perfmon
object=Logical/Physical Disk
counters=Avg. Disk sec/Read; Avg. Disk sec/Write
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Control_Panel]
index=perfmon
```

```
object=MSExchange Control Panel
counters=Outbound Proxy Requests - Average Response Time; Requests - Average Response Time; ASP.Net Request
Failures/sec; Explicit Sign-On Inbound Proxy Requests/sec; Explicit Sign-On Inbound Proxy Sessions/sec;
Explicit Sign-On Outbound Proxy Requests/sec; Explicit Sign-On Outbound Session Requests/sec; Explicit
Sign-On Standard RBAC Requests/sec; Explicit Sign-On Standard RBAC Sessions/sec; Inbound Proxy Requests/sec;
Inbound Proxy Sessions/sec; Outbound Proxy Requests - Average Response Time; Outbound Proxy Requests/sec;
Outbound Proxy Sessions/sec; PowerShell Runspaces - Activations/sec; PowerShell Runspaces - Average Active
Time; PowerShell Runspaces/sec; RBAC Sessions/sec; Requests - Activations/sec; Requests - Average Response
Time
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Queue_Lengths]
index=perfmon
object=MSExchangeTransport Queues
counters=*
instances=_total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Transport_Dumpster]
index=perfmon
object=MSExchangeTransport Dumpster
counters=Dumpster Size; Dumpster Inserts/sec; Dumpster Item Count; Dumpster Deletes/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Store_Driver]
index=perfmon
object=MSExchange Store Driver
counters=Inbound: LocalDeliveryCallsPerSecond; Outbound: Submitted Mail Items Per Second; Inbound:
MessageDeliveryAttemptsPerSecond; Inbound: Recipients Delivered Per Second
instances=_total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_SmtpReceive]
index=perfmon
object=MSExchangeTransport SmtpReceive
counters=Average bytes/message; Messages Received/sec
instances=_total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_SmtpSend]
index=perfmon
object=MSExchangeTransport SmtpSend
counters=Messages Sent/sec
instances=_total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Extensibility_Agents]
index=perfmon
object=MSExchange Extensibility Agents
counters=Average Agent Processing Time (sec); Total Agent Invocations
```

```
instances=*
interval=10
disabled=false
useEnglishOnly=true

####Common Stanzas - End####

###From Exchange app/add-on version 3.5.2,support for exchange server 2007 has ended.###
####Exchange Server 2007 - Start####

[monitor://C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking]
whitelist=\.log$|\.LOG$
time_before_close = 0
sourcetype=MSExchange:2007:MessageTracking
queue=parsingQueue
index=msexchange
disabled=true

[script://.\bin\exchangepowershell.cmd v8.0 get-hoststats_2007_2010.ps1]
source=Powershell
sourcetype=MSExchange:2007:Topology
interval=300
index=msexchange
disabled=true


####Exchange Server 2007 - End####

####Exchange Server 2010 - Start####

[monitor://C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking]
whitelist=\.log$|\.LOG$
time_before_close = 0
sourcetype=MSExchange:2010:MessageTracking
queue=parsingQueue
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 read-audit-logs_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:AdminAudit
interval=300
index=msexchange
disabled=false

[script://.\bin\exchangepowershell.cmd v14 get-hoststats_2007_2010.ps1]
source=Powershell
sourcetype=MSExchange:2010:Topology
interval=300
index=msexchange
disabled=false

####Exchange Server 2010 - End####
```

Troubleshoot TA-Exchange-HubTransport

The TA-Exchange-HubTransport add-on should install on your Exchange Server hosts without problems as long as you configure it for the version of Exchange Server you run before you deploy it.

If you do not configure the add-on for your version of Exchange Server before you deploy it, then the add-on only collects data inputs that are common to all supported versions of Exchange Server. This results in missing data that is specific to your version of Exchange Server. See Configure TA-Exchange-HubTransport for the procedure to configure the add-on and distribute it to your Exchange Server hosts.

If you upgrade from an earlier version of the Splunk App for Microsoft Exchange, complete the upgrade instructions in the Splunk App for Microsoft Exchange manual to ensure that the add-on collects all Exchange Server data for the version of Exchange Server that you run.

TA-Windows-Exchange-IIS

Overview of TA-Windows-Exchange-IIS

The TA-Windows-Exchange-IIS add-on comes with the Splunk Add-on for Microsoft Exchange package. It collects Performance Monitoring and Windows Host Monitoring data from Exchange Server hosts that hold the Client Access Exchange Server role. It supports the collection of data from Exchange Server 2010, Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019

The add-on should be installed on a universal forwarder that has been installed on the Exchange Server host. Because the add-on collects data for all supported versions of Exchange Server by default, when you install the add-on you must configure it to collect only the data for the version of Exchange Server that you run.

Use a deployment server to manage distribution of this add-on to your Exchange Server hosts.

TA-Windows-Exchange-IIS inputs

The TA-Windows-Exchange-IIS add-on collects performance and Windows host monitoring data from Windows hosts that run Exchange Server and hold the Client Access role. See Configure TA-Windows-Exchange-IIS to learn how to configure the add-on for the version of Windows Server that your Exchange Server Client Access Server host runs prior to deploying it to Exchange Server hosts.

The add-on includes the following data inputs:

Common data inputs

```
[WinHostMon://Processes]
[WinHostMon://Services]
[perfmon://Total_Processor_Time]
[perfmon://Processor]
[perfmon://System]
[perfmon://Available_Memory]
[perfmon://Memory]
[perfmon://DotNET_CLR_Memory]
[perfmon://Network_Utilization]
[perfmon://TCPv4]
[perfmon://TCPv6]
[perfmon://MSExchange_Control_Panel]
[perfmon://ASP_NET]
[perfmon://ASP_NET_Applications]
[perfmon://RPC_HTTP_Proxy]
[perfmon://MSExchange_RpcClientAccess]
[perfmon://MSExchangeAB]
```

Windows Server 2008 R2 data inputs

```
[monitor://C:\inetpub\logs\...\W3SVC1\*.log]
```

Windows Server 2012 R2 data inputs

```
[monitor://C:\inetpub\logs\LogFiles\W3SVC1\*.log]
```

Exchange Server Version 2010 data inputs

```
[monitor://C:\Program Files\Microsoft\Exchange Server\V14\Logging\Ews]
```

Exchange Server Version 2013, 2016, and 2019 data inputs

```
[monitor://C:\Program Files\Microsoft\Exchange Server\V15\Logging\Ews]
```

Configure TA-Windows-Exchange-IIS

The Splunk Add-ons for Microsoft Exchange must be configured before you can deploy them to Exchange Server hosts. This is because you must specifically enable support for the version of Exchange Server and Windows Server that you run.

Each add-on within the Splunk Add-ons for Microsoft Exchange package includes an `inputs.conf` file that has all of the data inputs that are necessary to get Exchange Server data. These inputs are disabled by default.

Download and unpack the TA-Windows-Exchange-IIS add-on

1. Download the Splunk Add-ons for Microsoft Exchange package from Splunkbase.
2. Unpack the add-on bundle to an accessible location.

Create and edit inputs.conf

1. Open a PowerShell window, command prompt, or Explorer window.
2. Create a `local` directory within the `TA-Windows-Exchange-IIS` add-on.
3. Copy `inputs.conf` from the `TA-Windows-Exchange-IIS\default` directory to the `TA-Windows-Exchange-IIS\local` directory.
4. Use a text editor such as Notepad to open the `TA-Windows-Exchange-IIS\local\inputs.conf` file for editing.
5. Modify the `inputs.conf` file so that the common data inputs and the inputs that are for the version of Windows Server and Exchange Server that you run are enabled. Do this by changing `disabled = true` to `disabled = false` for all input stanzas that are associated with your version of Windows Server and Exchange Server. See the example inputs.conf later in this topic.
6. After you update the `inputs.conf` file, save it and close it.

Distribute the add-ons

If you do not have a deployment server to distribute apps and add-ons, set one up. A deployment server greatly reduces the overhead in distributing apps and add-ons to hosts. You can make one change on the deployment server and push that change to all universal forwarders in your Splunk App for Microsoft Exchange deployment. The Splunk App for Microsoft Exchange manual uses deployment server extensively in its setup instructions.

1. Copy the TA-Windows-Exchange-IIS add-on to the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server.
2. Create a server class for all hosts that run Exchange Server and hold the Client Access role.

3. Add all Exchange Server hosts that hold the Mailbox Server role to this server class.
4. Push the add-on to all hosts in this server class.

Example inputs.conf

The following `inputs.conf` listing is an example of how you should configure the TA-Windows-Exchange-IIS add-on for installation on a Windows Server 2008 R2 host that runs Exchange Server 2010 and holds the Client Access role. In this example, the Windows Server 2008 R2 block has had its input stanza changed from `disabled = true` to `disabled = false`. All other data input blocks have not been changed.

Remember to save the inputs.conf file after editing it, as changes do not take effect until the file has been saved and the add-on has been pushed to Exchange Server hosts.

```
##################################################################################################
#User should enable the stanza specific to the exchange server version by setting disabled=false #
##################################################################################################

####Common Stanzas - Start####

[WinHostMon://Processes]
index = windows
interval = 10
disabled = false
type = process

[WinHostMon://Services]
index = windows
interval = 10
disabled = false
type = service

[perfmon://Total_Processor_Time]
index=perfmon
object=Processor
counters=% Processor Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Processor]
index=perfmon
object=Processor
counters=% User Time; % Privileged Time
instances=_Total
interval=10
disabled=false
useEnglishOnly=true

[perfmon://System]
index=perfmon
object=System
counters=Processor Queue Length
instances=*
interval=10
disabled=false
useEnglishOnly=true
```

```
[perfmon://Available_Memory]
index=perfmon
object=Memory
counters=Available MBytes
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Memory]
index=perfmon
object=Memory
counters=Pool Nonpaged bytes; Pool Paged bytes; Cache Bytes; Committed Bytes; %Committed Bytes in Use;
Transition Pages Repurposed/sec; Pages/sec; Pages Input/sec; Pages Output/sec
interval=10
disabled=false
useEnglishOnly=true

[perfmon://DotNET_CLR_Memory]
index=perfmon
object=.NET CLR Memory
counters=% Time in GC; # Bytes in all Heaps
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://Network_Utilization]
index=perfmon
object=Network Interface
counters=Bytes Total/sec; Packets Outbound Errors
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv4]
index=perfmon
object=TCPv4
counters=Connections Established; Connections Reset
interval=10
disabled=false
useEnglishOnly=true

[perfmon://TCPv6]
index=perfmon
object=TCPv6
counters=Connection Failures
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_Control_Panel]
index=perfmon
object=MSExchange Control Panel
counters=Outbound Proxy Requests - Average Response Time; Requests - Average Response Time; ASP.Net Request
Failures/sec; Explicit Sign-On Inbound Proxy Requests/sec; Explicit Sign-On Inbound Proxy Sessions/sec;
Explicit Sign-On Outbound Proxy Requests/sec; Explicit Sign-On Outbound Session Requests/sec; Explicit
Sign-On Standard RBAC Requests/sec; Explicit Sign-On Standard RBAC Sessions/sec; Inbound Proxy Requests/sec;
Inbound Proxy Sessions/sec; Outbound Proxy Requests - Average Response Time; Outbound Proxy Requests/sec;
Outbound Proxy Sessions/sec; PowerShell Runspaces - Activations/sec; PowerShell Runspaces - Average Active
Time; PowerShell Runspaces/sec; RBAC Sessions/sec; Requests - Activations/sec; Requests - Average Response
```

```
Time
interval=10
disabled=false
useEnglishOnly=true

[perfmon://ASP_NET]
index=perfmon
object=ASP.NET
counters=Requests Current; Request Wait Time; Application Restarts; Worker Process Restarts
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://ASP_NET_Applications]
index=perfmon
object=ASP.NET Applications
counters=Requests in Application Queue
instances=*
interval=10
disabled=false
useEnglishOnly=true

[perfmon://RPC_HTTP_Proxy]
index=perfmon
object=RPC/HTTP Proxy
counters=Number of Failed Back-End Connection attempts per Second; Current Number of Incoming RPC over HTTP
Connections; Current Number of Unique Users; \RPC/HTTP Requests per Second
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchange_RpcClientAccess]
index=perfmon
object=MSExchange RpcClientAccess
counters=RPC Averaged Latency; RPC Operations/sec; RPC Requests; Active User Count; Connection Count; User
Count
interval=10
disabled=false
useEnglishOnly=true

[perfmon://MSExchangeAB]
index=perfmon
object=MSExchangeAB
counters=NSPI RPC Browse Requests Average Latency; NSPI RPC Requests Average Latency; Referral RPC Requests
Average Latency; NSPI Connections Current; NSPI Connections/sec; Referral RPC Requests/sec
interval=10
disabled=false
useEnglishOnly=true

####Common Stanzas - End####

###From Exchange app/add-on version 3.5.2,support for Windows Server 2003 has ended.###
####Windows Server Version 2003 - Start####

[monitor://C:\WINDOWS\system32\LogFiles\W3SVC1\W3SVC1\*.log]
sourcetype=MSWindows:2003:IIS
queue=parsingQueue
index=msexchange
disabled=true

####Windows Server Version 2003 - End####
```

```
####Windows Server Version 2008R2 - Start####

[monitor://C:\inetpub\logs\...\W3SVC1\*.log]
sourcetype=MSWindows:2008R2:IIS
queue=parsingQueue
index=msexchange
disabled=false

####Windows Server Version 2008R2 - End####

####Windows Server Version 2012 - Start####

[monitor://C:\inetpub\logs\LogFiles\W3SVC1\*.log]
sourcetype=MSWindows:2012:IIS
queue=parsingQueue
index=msexchange
disabled=true

####Windows Server Version 2012 - End####

####Exchange Server Version 2010 - Start####
[monitor://C:\Program Files\Microsoft\Exchange Server\V14\Logging\Ews]
whitelist=\.log$|\.LOG$
sourcetype=MSWindows:2010EWS:IIS
queue=parsingQueue
index=msexchange
disabled=false
initCrcLength=8192
####Exchange Server Version 2010 - End####

####Exchange Server Version 2013/2016/2019 - Start####
[monitor://C:\Program Files\Microsoft\Exchange Server\V15\Logging\Ews]
whitelist=\.log$|\.LOG$
sourcetype=MSWindows:2013EWS:IIS
queue=parsingQueue
index=msexchange
disabled=true
initCrcLength=8192
####Exchange Server Version 2013/2016/2019 - End####
```

Troubleshoot TA-Windows-Exchange-IIS

The TA-Windows-Exchange-IIS add-on should install on your Exchange Server hosts without problems as long as you configure it for the version of Windows Server you run before you deploy it.

If you do not configure the add-on for your version of Windows Server before you deploy it, then the add-on only collects data inputs that are common to all supported versions of Windows Server. This results in missing data that is specific to your version of Windows Server. See Configure TA-Windows-Exchange-IIS for the procedure to configure the add-on and distribute it to your Exchange Server Client Access Server hosts.

If you upgrade from an earlier version of the Splunk App for Microsoft Exchange, complete the upgrade instructions in the Splunk App for Microsoft Exchange manual to ensure that the add-on collects all Windows Server data for the version of Windows Server that you run.

TA-SMTP-Reputation

Overview of TA-SMTP-Reputation

The TA-SMTP-Reputation add-on comes with the Splunk Add-on for Microsoft Exchange package. E-mail sender reputation requires a server that has an outbound connection to the Internet. It supports a collection of data from Exchange Server 2010, Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019.

Install the add-on on a universal forwarder that has been installed on the Exchange Server host. Because the add-on collects data for all supported versions of Exchange Server by default, when you install the add-on you must configure it to collect only the data for the version of Exchange Server that you run. Use a deployment server to manage the distribution of this add-on to your Exchange Server hosts.

TA-SMTP-Reputation inputs

E-mail sender reputation requires a server that has an outbound connection to the Internet.

See Configure TA-SMTP-Reputation to learn how to configure the add-on for the version of Windows Server that your Exchange Server SMTP-Reputation Server host runs prior to deploying it to Exchange Server hosts.

Data Inputs

The add-on includes the following data inputs:

Data inputs for Linux and Windows OS:

```
[script://.\bin\check_my_reputation.py]
[script://./bin/check_my_reputation.py]
```

Configure TA-SMTP-Reputation

The Splunk Add-ons for Microsoft Exchange must be configured before you can deploy them to Exchange Server hosts. This is because you must specifically enable support for the version of Exchange Server and Windows Server that you run.

Each add-on within the Splunk Add-ons for Microsoft Exchange package includes an `inputs.conf` file that has all of the data inputs that are necessary to get Exchange Server data. These inputs are disabled by default.

To get a reputation for a particular VM then the user has to add VM IP in `reputation.conf`.

Download and unpack the TA-Exchange-SMTP-Reputation add-on

1. Download the Splunk Add-ons for Microsoft Exchange package from Splunkbase.
2. Unpack the add-on bundle to an accessible location.

Create and edit `inputs.conf`

1. Open a PowerShell window, command prompt, or Explorer window.
2. Create a local directory within the `TA-SMTP-Reputation add-on`.
3. Copy inputs.conf from the `TA-SMTP-Reputation\default` directory to the `TA-SMTP-Reputation\local directory`.
4. Use a text editor such as Notepad to open the `TA-SMTP-Reputation\local\inputs.conf` file for editing.
5. Modify the `inputs.conf` file so that the common data inputs that you run are enabled. Do this by changing `disabled = true to disabled = false for all input stanzas`. See the example `inputs.conf` later in this topic.
6. After you update the `inputs.conf file`, save it and close it.

Distribute the add-ons

If you do not have a deployment server to distribute apps and add-ons, set one up. A deployment server greatly reduces the overhead in distributing apps and add-ons to hosts. You can make one change on the deployment server and push that change to all universal forwarders in your Splunk App for Microsoft Exchange deployment. The Splunk App for Microsoft Exchange manual uses deployment server extensively in its setup instructions.

1. Copy the TA-SMTP-Reputation add-on to the `%SPLUNK_HOME%\etc\deployment-apps` directory on the deployment server.
2. Push the add-on to all hosts in this server class.

Troubleshoot TA-SMTP-Reputation

The TA-SMTP-Reputation add-on should install on your Exchange Server hosts without problems as long as you configure it for the version of Windows Server you run before you deploy it.

If you do not configure the add-on for your version of Windows Server before you deploy it, then the add-on only collects data inputs that are common to all supported versions of Windows Server. This results in missing data that is specific to your version of Windows Server.

See Configure TA-SMTP-Reputation for the procedure to configure the add-on and distribute it to your Exchange Server SMTP-Reputation Server hosts.

If you upgrade from an earlier version of the Splunk App for Microsoft Exchange, complete the upgrade instructions in the Splunk App for Microsoft Exchange manual to ensure that the add-on collects all Windows Server data for the version of Windows Server that you run.

Third-party software attributions

Some of the components included in Splunk App for Microsoft Exchange are licensed under free or open source licenses. We wish to thank the contributors to those projects.

These attributions are in addition to the attributions we give for third-party vendors whose components the Splunk Enterprise software uses and redistributes. You can find those credits in the Release Notes.

We wish to thank the contributors to these projects:

- **dnspython 1.16.0** (https://www.dnspython.org/) - ISC license

ISC License

Copyright (C) Dnspython Contributors

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2001-2017 Nominum, Inc. Copyright (C) Google Inc.