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

Generated: 11/05/2022 11:57 am

Table of Contents

Overview

Splunk Add-on for Microsoft SCOM

Version	4.3.0
Vendors	Microsoft System Center Operations Manager 2019 Microsoft System Center Operations Manager 2022
Visible in Splunk Web	Yes. This add-on contains views for configuration.

The Splunk Add-on for Microsoft SCOM allows a Splunk software administrator to collect data from Microsoft System Center Operations Manager (SCOM). The add-on polls data from 54 built-in objects in SCOM, including alerts, events, tasks, network devices, management and performance settings. This add-on provides the inputs and **CIM**-compatible knowledge to use with other Splunk apps, such as Splunk Enterprise Security and the Splunk App for PCI Compliance and Splunk IT Service Intelligence.

This add-on uses the selected System Center Operations Manager scriptlets to collect the data. Since the scriptlets may not be performant enough for larger infrastructures, Splunk also provides a number of specialized SQL queries for collecting events, alerts and performance data.

Download the Splunk Add-on for Microsoft SCOM from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release notes for the Splunk Add-on for Microsoft SCOM.

For information about installing and configuring the Splunk Add-on for Microsoft SCOM, see Installation and configuration overview for the Splunk Add-on for Microsoft SCOM.

See the Splunk Community page for questions related to Splunk Add-on for Microsoft SCOM.

Source types for the Splunk Add-on for Microsoft SCOM

The Splunk Add-on for Microsoft SCOM divides data from Microsoft SCOM into thirteen source types. Each source type maps to one or more SCOM commands.

Source	Description	CIM compliance	ITSI compliance	Direct SQL available
`microsoft:scom:alert`	Get one or more alerts and their history. An alert is an indication of a significant event that requires your attention. Rules and monitors can generate alerts.	Alerts	None	Yes
`microsoft:scom:monitor`	Get monitors which define logic for determining the health of an object.	None	None	No
`microsoft:scom:diagnostic`	Get diagnostic tasks to discover the cause of a problem or provide you with additional information.	None	None	No
`microsoft:scom:task`		None	None	No

Source	Description	CIM compliance	ITSI compliance	Direct SQL available
	Get a list of tasks and their results. Task have a specific name or ID as well as tasks that are associated with specified user roles, class instances, management packs, or target classes.			
`microsoft:scom:recovery`	Get a list of recoveries.	None	None	No
`microsoft:scom:discovery`	Get a list of discoveries.	None	None	No
`microsoft:scom:override`	Get a list of overrides, and a resulting set of overrides.	None	None	No
`microsoft:scom:event`	Get one or more events which are collected by rules.	None	None	Yes
`microsoft:scom:rule`	Get one or more monitoring rules.	None	None	No
`microsoft:scom:internal`	Get some internal references such as SCOM class definitions, and class instances.	None	OS	No
`microsoft:scom:network`	Get some network configurations such as SCOM agent, connector, and proxy info.	None	None	No
`microsoft:scom:mgmt`	Get management configurations such as ManagementPack, group, and role.	None	None	No
`microsoft:scom:performance`	Get network performance such as CPU usage, memory, storage and network performance data.	Performance	OS	Yes

Configure Microsoft SCOM to send performance data

To collect performance data from Microsoft SCOM, you must import the System Center Management Pack in your Microsoft SCOM environment and enable rules to map to Splunk ITSI model.

Import System Center Management Pack

- Download the System Center Management Pack from the Microsoft website.
- Import the management pack in the Microsoft SCOM. See the System Center Management Pack Guide provided in your installation package for instructions.

Enable Rules in Management Pack Object

Each management pack has different rules for collecting performance data from metrics such as memory, processor, network or disk. To get the performance data and map to the ITSI Performance model, you must enable the rules manually if they are not enabled by default.
The table below describes the rules and the mapping to ITSI Performance data model.

Name (differs by OS version)	Enabled by default?	ITSI Object	ITSI Fields
Processor Information % Processor Time Total Windows Server 2016 and 1709+	True	Performance	cpu_user_percent

Name (differs by OS version)	Enabled by default?	ITSI Object	ITSI Fields
Processor Information % Processor Time Total Windows Server 2012 R2 Processor Information % Processor Time Total Windows Server 2008 R2 Processor % Processor Time Total Windows Server 2016 and 1709+ Processor % Processor Time Total Windows Server 2012 Processor % Processor Time Total Windows Server 2008			
System Processor Queue Length Windows Server 2016 and 1709+ System Processor Queue Length Windows Server 2012 R2 System Processor Queue Length Windows Server 2012 System Processor Queue Length 2008	True	Performance	wait_threads_count
Memory Available Megabytes Windows Server 2016 and 1709+ Memory Available Megabytes Windows Server 2012 R2 Memory Available Megabytes Windows Server 2012 Memory Available Megabytes 2008	True	Performance	mem_free
Percent Memory Used	True	Performance	mem_free_percent mem_used_percent
Memory Pages per Second Windows Server 2016 and 1709+ Memory Pages per Second Windows Server 2012 R2 Memory Pages per Second Windows Server 2012 Memory Pages per Second 2008	True	Performance	mem_page_ops
Cluster Disk - Total size / MB Cluster Shared Volume - Total size / MB	True	Performance	Storage
Cluster Disk - Free space / MB Cluster Shared Volume - Free space / MB Logical Disk Free Megabytes Windows Server 2016 and 1709+ Logical Disk Free Megabytes Windows Server 2012 Logical Disk Free Megabytes 2008	True	Performance	storage_free storage_used
Cluster Disk - Free space / % Cluster Shared Volume - Free space / % % Logical Disk Free Space Windows Server 2016 and 1709+ % Logical Disk Free Space Windows Server 2012 % Logical Disk Free Space 2008	True	Performance	storage_free_percent storage_used_percent
Network Adapter Bytes Total per Second Windows Server 2016 and 1709+ Network Adapter Bytes Total per Second Windows Server 2012	True	Performance	bytes

Name (differs by OS version)	Enabled by default?	ITSI Object	ITSI Fields
Physical Disk Average Disk Seconds per Transfer Windows Server 2016 and 1709+ Physical Disk Average Disk Seconds per Transfer Windows Server 2012 Physical Disk Average Disk Seconds per Transfer 2008 Collection Rule for Average Disk Seconds Per Transfer Windows Server 2016 and 1709+ Collection Rule for Average Disk Seconds Per Transfer Windows Server 2012 Collection Rule for Average Disk Seconds Per Transfer 2008	True	Performance	latency
Collection Rule for Average Disk Seconds Per Read Windows Server 2016 and 1709+ Collection Rule for Average Disk Seconds Per Read Windows Server 2012 Collection Rule for Average Disk Seconds Per Read 2008 Physical Disk Average Disk Seconds per Read Windows Server 2016 and 1709+ Physical Disk Average Disk Seconds per Read Windows Server 2012 Physical Disk Average Disk Seconds per Read 2008	False	Performance	read_latency
Collection Rule for Disk Reads Per Second Windows Server 2016 and 1709+ Collection Rule for Disk Reads Per Second Windows Server 2012 Collection Rule for Disk Reads Per Second 2008 Physical Disk Reads per Second Windows Server 2016 and 1709+ Physical Disk Reads per Second Windows Server 2012 Physical Disk Reads per Second 2008	False	Performance	read_ops
Collection Rule for Average Disk Seconds Per Write Windows Server 2016 and 1709+ Collection Rule for Average Disk Seconds Per Write Windows Server 2012 Collection Rule for Average Disk Seconds Per Write 2003 Physical Disk Average Disk Seconds per Write Windows Server 2016 and 1709+ Physical Disk Average Disk Seconds per Write Windows Server 2012 Physical Disk Average Disk Seconds per Write 2008	False	Performance	write_latency
Collection Rule for Disk Writes Per Second Windows Server 2016 and 1709+	False	Performance	write_ops

Name (differs by OS version)	Enabled by default?	ITSI Object	ITSI Fields
Collection Rule for Disk Writes Per Second Windows Server 2012 Collection Rule for Disk Writes Per Second 2008 Physical Disk Writes per Second Windows Server 2016 and 1709+ Physical Disk Writes per Second Windows Server 2012 Physical Disk Writes per Second 2008			
Network Adapter Bytes Received per Second Windows Server 2016 and 1709+ Network Adapter Bytes Received per Second Windows Server 2012	False	Performance	bytes_in
Network Adapter Bytes Sent per Second Windows Server 2016 and 1709+ Network Adapter Bytes Sent per Second Windows Server 2012	False	Performance	bytes_out

Other than the rules in the table, if you want to collect data on disk transfers per second, you must create a rule with the prefix Collection Rule for Disk Transfers Per Second. For example, Collection Rule for Disk Transfers Per Second Windows Server 2012. Then map the data to the `total_ops` field of ITSI Performance object.

Release notes for the Splunk Add-on for Microsoft SCOM

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM was released on October 17, 2022.

Compatibility

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.1.x, 8.2.x. 9.0.x
CIM	5.0.0
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2019 Microsoft System Center Operations Manager 2022

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Upgrade guide

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 4.2.0. All source types are the same and all inputs created using version 4.2.0 will continue to function.

New features

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Direct events processing using SQL queries instead of Powershell scriptlets.
- CIM enhancements for performance events.

Field Changes

Source-type	scom_command	Fields added	Fields removed
`['microsoft:scom:performance']`	get-scomallperfdata	cpu_load_percent, resource_type, scom_perf_category, mem, uptime	

Fixed issues

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 4.3.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a text file for download:
Splunk Add-on for Microsoft SCOM third-party software credits.

Release history for the Splunk Add-on for Microsoft SCOM

The latest version of the Splunk Add-on for Microsoft SCOM is version 4.3.0. See Release notes for the Splunk Add-on for Microsoft SCOM for the release notes of this latest version.

Version 4.2.0

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM was released on February 28, 2022.

Compatibility

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0.x, 8.1.x, 8.2.x
CIM	4.18.1
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2016 Microsoft System Center Operations Manager 2019

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Upgrade guide

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 4.1.1. All source types are the same and all inputs created using version 4.1.1 will continue to function.

New features

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Updated deprecated SCOM SDK functions for collecting performance data with newly supported Microsoft Functions.
- Added support for configuring filter parameters in performance data inputs.
- Added Server validation on server configuration page.
- Updated UI to show warning sign on inputs page for missing server/templates in the configured inputs.
- Updated behavior to allow deletion of servers that are being used by inputs.
- Minor Bug Fixes and UI enhancements.

This release introduces changes on the Inputs page, where a new field filter parameter has been added for performance based templates.

For more information about these changes and the configuration guide, refer to the Configure Inputs page.

.

Fixed issues

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 4.2.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2022-02-14	ADDON-48059	Data collection for all the inputs are getting triggered when any of the input is modified

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a PDF file for download:
Splunk Add-on for Microsoft SCOM third-party software credits.

Version 4.1.1

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM was released on July 30, 2021.

Compatibility

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0.x, 8.1.x, 8.2.x
CIM	4.18.1
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 Microsoft System Center Operations Manager 2019

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Upgrade guide

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 4.0.0. All source types are the same and all inputs created using version 4.0.0 will continue to function.

Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Fast and intuitive UI with an improved look and feel.
- Provides critical security fix by removing jquery2.
- Removal of python2 support. Only python3 is supported from now on.
- Changed add-on default landing page to configuration page.
- Changed default value of Start Time field to one day before current UTC time.

Fixed issues

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 4.1.1 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Some of the components included in this add-on are licensed under free or open source licenses. We wish to thank the contributors to those projects.

A complete listing of third-party software information for this add-on is available as a PDF file for download:
Splunk Add-on for Microsoft SCOM third-party software credits.

Version 4.0.0

Version 4.0.0 of the Splunk Add-on for Microsoft SCOM was released on February 17, 2021.

Compatibility

Version 4.1.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	8.0.x, 8.1.x, 8.2.x
CIM	4.18.1
Platforms	Windows

Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 Microsoft System Center Operations Manager 2019

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Upgrade guide

Version 4.1.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 4.0.0. All source types are the same and all inputs created using version 4.0.0 will continue to function.

Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 4.0.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- *Changed add-on default landing page to configuration page.

- Support for Microsoft System Center Operations Manager 2019
- Added a lookup for the "type" field of the Alerts CIM Data Model.
- Enhanced compatibility for the Common Information Model (CIM) by removing these field extractions from the alert events, since these fields are automatically provided by asset and identity correlation features using applications like Splunk Enterprise Security:
- `dest_bunit`
- `dest_category`
- `dest_priority`
- `src_bunit`
- `src_category`
- `src_priority`

Fixed issues

Version 4.0.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 4.0.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Version 4.0.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- configparser
- future
- select2
- six
- requests

Version 3.0.2

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM was released on June 30, 2020.

Compatibility

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.1.x, 7.2.x, 7.3.x, 8.0.0
CIM	4.14
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 R2

Upgrade guide

Version 3.0.x of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.3.0. All source types are the same and all inputs created using version 2.3.0 will continue to function.

> Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Enhanced python library structure.

Fixed issues

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Date resolved	Issue number	Description
2020-07-10	ADDON-26828	Addons unable to load UI or collect data on Splunk 8.0.4, 8.0.2004 and Splunk 8.0.5
2020-06-30	ADDON-26897, ADDON-26876	Fix UI and Data collection of Addon on Splunk 8.0.4 and 8.0.2004

Known issues

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Version 3.0.2 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- configparser
- httplib2
- future
- select2
- six

Version 3.0.1

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM was released on March 19, 2020.

Compatibility

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.0
CIM	4.14
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 R2

Upgrade guide

Version 3.0.x of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.3.0. All source types are the same and all inputs created using version 2.3.0 will continue to function.

> Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Restmap.conf updated to provide a flag that, by default, directs Splunk to run this add-on in Python3.

Fixed issues

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Version 3.0.1 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- configparser
- httplib2
- future
- select2
- six

Version 3.0.0

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM was released on December 17, 2019.

Compatibility

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	7.0.x, 7.1.x, 7.2.x, 7.3.x, 8.0.0
CIM	4.14
Platforms	Windows

Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 R2

Upgrade guide

Version 3.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.3.0. All source types are the same and all inputs created using version 2.3.0 will continue to function.

> Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Support for Splunk 8.0.x
- Support for Python3

Fixed issues

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2019-10-18	ADDON-23985	Issue in Data collection for all inputs when user gets "Permission Error" in 1 data input
2019-10-16	ADDON-23967	Data Collection restarts for all enabled scripts once disabled script is enabled in Microsoft-SCOM addon

Third-party software attributions=

Version 3.0.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- configparser
- httplib2
- future
- select2
- six

Version 2.3.0

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM was released on August 06, 2019.

Compatibility

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x, 7.3.x
CIM	4.12
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 R2

Upgrade guide

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.2.0. All source types are the same and all inputs created using version 2.2.0 will continue to function.

> Some events might be duplicated when you upgrade the Splunk Add-on for Microsoft SCOM on Splunk 7.3.x while the modular input script is running.

New features

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Support for Splunk 7.3.x

Fixed issues

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues.

Date resolved	Issue number	Description
2019-06-11	ADDON-22162	Input-Stanza name is not logging in ta_scom.log with Splunk PinkiePie
2019-06-07	ADDON-22050	"Description" field is getting override with a NULL value and not getting extracted for most of the source types
2019-06-06	ADDON-21394	Performance issue on SCOM
2019-05-13	ADDON-21913	Fieldalias behavior changed for SCOM "dest" field as mentioned in SPL-164505

Known issues

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2019-10-18	ADDON-23985	Issue in Data collection for all inputs when user gets "Permission Error" in 1 data input

Third-party software attributions

Version 2.3.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- select2

Version 2.2.0

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM was released on June 21, 2018.

Compatibility

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.6.x, 7.0.x, 7.1.x, 7.2.x
CIM	4.4
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2 Microsoft System Center Operations Manager 2016 R2

Upgrade guide

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.1.0. All source types are the same and all inputs created using version 2.1.0 will continue to function.

New features

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

- Support for Microsoft SCOM 2016
- Improved date support for various locales. Date inputs and *datetime* parameters are properly indexed.

Fixed issues

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM fixes the following issues.

Date resolved	Issue number	Description
2018-06-13	ADDON-18067	Data is not getting indexed into Splunk for Microsoft SCOM as 'request was aborted: Could not create SSL/TLS secure channel'
2018-05-10	ADDON-16305	The command Get-SCOMMonitoringObject' is an alias for 'Get-SCOMClassInstance' and is called twice
2018-05-10	ADDON-8632	Splunk Add-on for Microsoft SCOM only does a one-time pull of data

Known issues

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2019-06-06	ADDON-22162	Input-Stanza name is not logging in ta_scom.log with Splunk PinkiePie
2019-05-26	ADDON-22050	"Description" field is getting override with a NULL value and not getting extracted for most of the source types
2019-05-01	ADDON-21913	Fieldalias behavior changed for SCOM "dest" field as mentioned in SPL-164505
2019-02-25	ADDON-21394	Performance issue on SCOM
2018-03-30	ADDON-17594	Event ingestion latency grows until the collection process ceases entirely
2016-08-17	ADDON-10936	DATA lost when SCOM spends a long time to sample it
2016-04-21	ADDON-8910, SPL-118489	interval does not support cron expression "0 0/5 * * * *"
2016-04-11	ADDON-8687	Request takes a long time to return
2015-04-23	ADDON-3876	500 error message upon failed input configuration is vague and unfriendly
2015-04-15	ADDON-3726	inputs will not be updated when the template is modified/deleted from UI

Third-party software attributions

Version 2.2.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- select2

Version 2.1.0

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM was released on September 21, 2016.

Compatibility

Splunk platform versions	6.3, 6.4, 6.5, 6.6
CIM	4.3, 4.4, 4.5

Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2

Upgrade instructions

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM is backwards compatible with version 2.0.0. All source types are the same and all inputs created using version 2.0.0 will continue to function.

Since Splunk platform version 6.3 and higher contains a native PowerShell modular input, if you upgrade the Splunk platform version from 6.2 or earlier to 6.3 or later, you need to delete the Powershell add-on which was installed to collect data.

New features

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

Date	Issue number	Description
2016-09-20	ADDON-9067	Mapping to ITSI OS data model.
2016-09-20	ADDON-9318	Support to collect performance metrics from monitors configured in Microsoft SCOM.
2016-09-20	ADDON-10405	Support to set the start date of data collection.
2016-09-20	ADDON-10983	Support to change the start time later than the time in the existing checkpoint file.

Known issues

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM contains the following known issues.

Date Filed	Issue number	Description
2016-08-17	ADDON-10936	There will be some data loss if Microsoft SCOM takes more than 15 minutes to add the data in the database.
2016-04-25	ADDON-8910 /SPL-118489	If an input is created with an interval using a cron expression of `0 0/5 * * * *`, no data is collected. Workaround: Change interval to `0 */5 * * * *` to create a similar schedule.
2016-04-11	ADDON-8687	Requests take a long time to return on Windows.
2015-04-24	ADDON-3876	Error messages displayed in the UI are vague.
2015-04-15	ADDON-3726	Inputs are not updated when a template is modified or deleted. Workaround: When you need to modify or delete a collection template, delete any tasks that use that template and recreate the tasks with the modified or new set of templates.

Fixed issues

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM has the following fixed issues.

Date	Issue number	Description
2016-09-07	ADDON-9694	The input and configuration page will be decrypted if you set the proxy in `splunk-launcher.conf`.
2015-09-09	ADDON-8740	

Date	Issue number	Description
		Duplicate events are indexed when a short crontab interval is used. When Splunk first starts, it may invoke the PowerShell inputs twice. These two running instances may overlap and duplicated events may be indexed. Afterwards, the Powershell modular input will run in sequence and will not generate duplicated events.

Third-party software attributions

Version 2.1.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- select2

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Microsoft SCOM is compatible with the following software, CIM versions and platforms.

Splunk platform versions	6.3 or later
CIM	4.1 or later
Platforms	Windows
Vendor Products	Microsoft System Center Operations Manager 2012 R2

New features

Date	Issue number	Description
2016-03-22	ADDON-8082	Add support for separate console and management servers so that Splunk admins can pull data from SCOM environments where the console server and SCOM management servers are on separate machines.
2016-03-22	ADDON-6772	Add support to collect data from nodes in a SCOM failover cluster.
2016-03-22	ADDON-6233	UI updates for a better configuration experience.
2016-03-22	ADDON-4290	Use Splunk platform 6.3 native PowerShell modular input rather than rely on the Splunk Add-on for Microsoft PowerShell.

Fixed Issues

Date	Issue number	Description
2016-03-22	ADDON-7050	Ingest timestamp problems. In Splunk Add-on for Microsoft SCOM 2.0.0, the time is stored in the checkpoint file as UTC time to resolve problems.
2016-03-23	ADDON-8397	UI cannot show when using base URL via reverse proxy.
2015-06-10	ADDON-4214	Check that objects exist before querying them.
2016-04-12	ADDON-8673	splunk_powershell.ps.log reports error "script exception:module OperationsManager not found".
2015-04-16	ADDON-3733	404 error logged in ta_util log each time a user creates a new template/task. Can be safely ignored.
2015-04-15	ADDON-3716	UI allows you to create a template with no metrics.

Known Issues

Date Filed	Issue number	Description
2016-04-25	ADDON-8910 /SPL-118489	If an input is created with an interval using a cron expression of `0 0/5 * * * *`, no data is collected. Workaround: Change interval to `0 */5 * * * *` to create a similar schedule.
2016-04-19	ADDON-8740 /SPL-118488	Duplicate events are indexed when a short crontab interval is used. When Splunk first starts, it may invoke the PowerShell inputs twice. These two running instances may overlap and duplicated events may be indexed. Afterwards, the Powershell modular input will run in sequence and will not generate duplicated events.
2016-04-11	ADDON-8687	Requests take a long time to return on Windows.
2015-04-24	ADDON-3876	Error messages displayed in the UI are vague.
2015-04-15	ADDON-3726	Inputs are not updated when a template is modified or deleted. Workaround: When you need to modify or delete a collection template, delete any tasks that use that template and recreate the tasks with the modified or new set of templates.

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- select2

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Microsoft SCOM has the same compatibility specifications as version 2.0.0.

New features

Version 1.0.0 of the Splunk Add-on for Microsoft SCOM has the following new features.

Date	Issue number	Description
2015/04/16	ADDON-435	New Splunk-supported add-on.

Known issues

Version 1.0.0 of the Splunk Add-on for Microsoft SCOM has the following known issues.

Date	Issue number	Description
2015/04/24	ADDON-3876	Error messages displayed in the UI are vague.
2015/04/16	ADDON-3733	404 error logged in ta_util log each time a user creates a new template/task. Can be safely ignored.
2015/04/15	ADDON-3726	Inputs are not updated when a template is modified or deleted. Workaround: When you need to modify or delete a collection template, delete any tasks that use that template and recreate the tasks with the modified or new set of templates.
2015/04/15	ADDON-3716	UI allows you to create a template with no metrics.

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Microsoft SCOM incorporates the following third-party components.

- Bootstrap
- Bootstrap table
- jqBootstrapValidation
- select2

Hardware and software requirements for the Splunk Add-on for Microsoft SCOM

Splunk admin requirements

You must be member of the `admin` or `sc_admin` role.

Microsoft SCOM requirements

To collect data, the Splunk Add-on for Microsoft SCOM must be installed on a Splunk Enterprise forwarder or single instance Splunk Enterprise that is installed on the same machine as your Microsoft System Center Operations Manager 2019 Operations console. All of the hardware and software requirements for your Microsoft SCOM instance apply to this add-on when it is installed on the data collection node. Configuration tasks that depend on Microsoft Windows and SCOM components may not work when the add-on is not installed on Windows.

The Splunk Add-on for Microsoft SCOM supports distributed deployments of SCOM in which management servers are installed separately from the operations console. If you have management servers for which you want to collect SCOM data installed on separate machines from your operations console, you must have an administrator account, or another account that has read permissions for the commands you use to collect SCOM data, on your management server in order for the Splunk Add-on for Microsoft SCOM to collect the metrics from the remote server.

The Splunk Add-on for Microsoft SCOM version supports Microsoft SCOM clustered environments. You can collect metrics from more than one node in a SCOM cluster.

PowerShell and .NET framework requirements

The following software must be installed on the same machine as your Microsoft System Center Operations Manager 2019:

- PowerShell v3 or later
- Microsoft .NET framework v4.0 or later

You do not need to install the Splunk Add-on for Microsoft PowerShell with this version of the Splunk Add-on for Microsoft SCOM, because Splunk platform versions 6.3 and later contain a native PowerShell modular input.

Splunk platform requirements

Because this add-on runs on the Splunk platform, all of the system requirements apply for the Splunk software that you use to run this add-on.

- For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise *Installation Manual*.
- If you plan to run this add-on entirely in Splunk Cloud, there are no additional Splunk platform requirements.
- If you are managing on-premises forwarders to get data into Splunk Cloud, see System Requirements in the Splunk Enterprise *Installation Manual*, which includes information about forwarders.

For information about installation locations and environments, see Install the Splunk Add-on for Microsoft SCOM.

Sizing guidelines and performance data

A single-instance deployment of Splunk Enterprise performed data collection at the rates and volumes listed below.

Events per second	Average CPU usage	Max memory usage	Average event size
66.8	8.23	3.1 GB	1.25 KB

Performance impact with the Splunk Add-on for Microsoft SCOM 2.3.0 on Splunk 7.3.x

The Splunk Add-on for Microsoft SCOM 2.3.0 on Splunk 7.3.x has the following performance impact:

- Events are ingested immediately after the Add-on script is executed
- Events per second is lower because serialization happens immediately after the Add-on script is executed instead of after all objects are collected
- Memory consumption is improved

Trial 1

No. of events	Add-on version	Splunk version	Script execution time	Execution vs ingest time [1]	Average CPU usage	Max memory usage	Events per second
50000	2.3.0	7.2.x	61 min	61 min	25.925	991.91 MB	35.88
50000	2.2.0	7.2.x	61 min	61 min	27.9	1.49 GB	30.49
50000	2.3.0	7.3.x	91 min	1 sec	25.7	117.48 MB	12.06
50000	2.2.0	7.3.x	94 min	60 min	30.4	740 MB	30.83

1. The approximate time between the execution of the Add-on command and ingesting the first event index into Splunk.

Trial 2:

No. of events	Add-on version	Splunk version	Script execution time	Execution vs ingest time [1]	Average CPU usage	Max memory usage	Events per second
50000	2.3.0	7.2.x	65 min	65 min	27	1 GB	33.67
50000	2.2.0	7.2.x	65 min	65 min	26.5	1.45 GB	32
50000	2.3.0	7.3.x	82 min	5 sec	28	230 MB	11.2
50000	2.2.0	7.3.x	95 min	61 min	32	750 MB	33

1. The approximate time between the execution of the Add-on script and ingesting the first event index into Splunk.

Installation and configuration overview for the Splunk Add-on for Microsoft SCOM

Direct event processing for Microsoft SCOM

One known limitation of the scriptlets used by the Splunk Add-on for Microsoft SCOM is time range filtering - Splunk always receives a complete set of available data and then filters out already processed events. This might affect performance for larger installations.

All the data of the Management Group is stored in the Operational Database. It is hosted on a SQL Server instance and accessed by Management Server and PowerShell cmdlets. The "Direct event processing" feature lets you collect data directly from the database and provides a more flexible and performant solution by having a direct SQL connection.

Still, a scriptlet-based solution shall be the default choice. The SCOM Database Schema isn't formally documented and can be changed without notice. Moreover - due to possible additional post-processing in PowerShell scriptlets - the results may slightly differ between both sources.

See these steps to install and configure this add-on, including direct event processing:

1. Install the Splunk Add-on for Microsoft SCOM.
2. (Optional) Configure direct events collection using the Splunk Add-on for Microsoft SCOM.
3. Configure inputs for the Splunk Add-on for Microsoft SCOM.

Installation and Configuration

Install the Splunk Add-on for Microsoft SCOM

1. Get the Splunk Add-on for Microsoft SCOM by downloading it from http://splunkbase.splunk.com/app/2729 or browsing to it using the app browser within Splunk Web.
2. Determine where and how to install this add-on in your deployment, using the tables on this page.
3. Perform any prerequisite steps before installing, if required and specified in the tables below.
4. Complete your installation.

If you need step-by-step instructions on how to install an add-on in your specific deployment environment, see the installation walkthroughs section at the bottom of this page for links to installation instructions specific to a single-instance deployment, distributed deployment, or Splunk Cloud.

Distributed deployments

Use the tables below to determine where and how to install this add-on in a distributed deployment of Splunk Enterprise.

> This add-on must be installed on a Windows instance of Splunk Enterprise for data collection. The add-on is platform independent for indexers and search heads.

Where to install this add-on

This table provides a quick reference for installing this add-on to a distributed deployment of Splunk Enterprise or any deployment for which you are using forwarders to get your data in. Depending on your environment, your preferences, and the requirements of the add-on, you may need to install the add-on in multiple places.

Splunk instance type	Supported	Required	Action Required/Comments
Search Heads	Yes	Yes	Install this add-on to all search heads where Microsoft SCOM knowledge management is required. Splunk recommends that you turn add-on visibility off on your search heads to prevent data duplication errors that can result from running inputs on your search heads instead of (or in addition to) on your data collection node.
Indexers	Yes	No	Not required as parsing and data collection operations occur on the heavy forwarders.
Heavy Forwarders	Yes	Yes	Best practice: Using the Splunk Add-on for Microsoft SCOM configuration UI to configure your inputs speeds configuration and helps prevent errors. The Splunk Add-on for Microsoft SCOM and the Heavy forwarder must be installed on the same machine as the SCOM Operations console.
Universal Forwarders	No	No	Not supported because the add-on requires Python.

Distributed deployment feature compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features.

Distributed deployment feature	Supported	Comments
Search Head Clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but only configure inputs on forwarders to avoid duplicate data collection. Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the `inputs.conf` file.
Indexer Clusters	Yes	Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the `inputs.conf` file.
Deployment Server	No	Supported for deploying unconfigured add-on only. Using a deployment server to deploy the configured add-on to multiple forwarders acting as data collectors causes duplication of data.

Installation walkthroughs

The *Splunk Add-Ons* manual includes an Installing add-ons guide that helps you successfully install any Splunk-supported add-on to your Splunk platform.

For a walkthrough of the installation procedure, follow the link that matches your deployment scenario:

- Single-instance Splunk Enterprise
- Distributed Splunk Enterprise
- Splunk Cloud

Configure inputs for the Splunk Add-on for Microsoft SCOM

Configure inputs on the node responsible for data collection. The Splunk Add-on for Microsoft SCOM supports three different methods for configuring inputs:

1. Use the Splunk Add-on for Microsoft SCOM configuration UI.
2. Use the PowerShell scripted input UI.
3. Use the configuration files.

Regardless of the method you use, switching to a different method to update data inputs later may cause inconsistencies in data collection. Splunk recommends that you configure inputs through the Splunk Add-on for Microsoft SCOM configuration UI.

Splunk recommends that you do not override the source types in this add-on. In all cases where the input collects data using a group metric (a collection of individual SCOM commands), the modular input code sets the source type based on the group from which the event originated, regardless of any custom source type you attempt to set in the configuration files or the UI configuration screens. You can override the source type for any input configured to collect metrics consisting of individual SCOM commands, but this can cause inconsistencies and errors in CIM mapping, dashboard displays, and workflow actions.

The first time when you configure the inputs to collect performance data from Microsoft SCOM, it may take a long time (about 20 minutes) to get data in.

Configure inputs through the Splunk Add-on for Microsoft SCOM configuration UI

1. Access Splunk Web on the node responsible for data collection.
2. Go to the Splunk Add-on for Microsoft SCOM configuration page by clicking on the Microsoft SCOM add-on in the left navigation banner on the Splunk platform home page. You can also go to **Manage Apps**, then click **Launch App** in the row for Splunk Add-on for Microsoft SCOM.
3. Review the configured inputs. The templates that are assigned to each input provide the metrics to be collected.
4. Click the **Configuration** tab to review the configured templates on the Template tab and see the metrics each template collects.
    1. To add or remove metrics from a template, click **Edit** under the **Actions** menu next to a template.
    2. You can select a metric group to automatically run all the related commands in that group, or choose individual SCOM commands.
    3. To create a new template, click **Add**. Give your template a name and select a set of metrics. You can select a metric group to automatically run all the related commands in that group, or choose individual SCOM commands.
5. If you have management servers for which you want to collect SCOM data installed on separate machines from your Operations console, click the **Server** tab to provide information about the remote management servers.
    1. Go to **Microsoft SCOM Server** and Click **Add**.
    2. Provide a name, host (for example, scom-management) and a username and password that the add-on can use to connect to this server.
    3. For Host, you can provide the hostname, IP address, or fully qualified domain name.
    4. For Username and Password, use an Admin account or another account that has read permissions for the commands you are using to collect SCOM data. If you are using a domain user account, use the format `<domain>\<username>` in the Username field.
    5. Do not edit an existing server to add a new remote server. The checkpoint is correlated to the server name so editing an existing remote server's host, username, and password will reuse the checkpoint file which can cause event data loss.
6. Click the **Logging** tab to set the logging level to use. You can select WARN, DEBUG, or ERROR. The default is WARN.
7. Review or add inputs by clicking **Inputs** tab at the top.
    1. Click **Edit** under the **Action** menu to adjust a configured input. You can add or remove **templates**, change the server to a remote server if necessary, set a different **interval** by entering a different cron expression, set the **start time** or select a custom **index**.
    2. If the input settings match your use case, you can leave them unchanged and click the **Status** toggle button to enable it as a data input.
8. If you prefer to create a new input, click **Create New Input**.
    1. Give your input a name and select one or more collection templates.
    2. If you are collecting data from a remote server, select the server name from the list of remote servers you previously added under the **Server** tab or select **localhost** if the server is local.
    3. Provide a schedule by entering a cron expression in the **Interval** field and the **Start Time**.
9. If a template is selected which has performance command (Metrics as cmd=Get-SCOMAllPerfData), then a field filter parameter will be visible:
    1. By default the value will be "CounterName IS NOT NULL", this will fetch all the performance data. This is also applicable when this field is kept empty.
    2. Users can also add filter parameters as per their requirements to fetch specific data.
    3. The filter parameter should be in SCOM defined syntax of criteria expression.
    4. The property name which can be used in criteria expression can be found on https://docs.microsoft.com/en-us/dotnet/api/microsoft.enterprisemanagement.monitoring.monitoringperformanceda page and the expression should be formed as per criteria expression syntax defined on https://docs.microsoft.com/en-us/previous-versions/system-center/developer/bb437603%28v=msdn.10%29?redire page.

    5. Some of the examples of the valid expressions are:
        1. ObjectName MATCHES 'Health Service'
        2. CounterName = 'NumberAgents'
        3. MonitoringClassId = 'ab4c891f-3359-3fb6-0704-075fbfe36710'

Default value for **Start Time** field is one day before current UTC time.

1. 1. You can also select a custom **index** for the data.
2. You can also copy an existing input by selecting **Clone** from the **Action** link of the input to start with the settings of the input.
3. Enable the inputs to start collecting data. No restart is required.
4. Click the **Search** tab at the top and perform the following search to verify the Splunk platform is indexing the data you expect.

   ```
   sourcetype=microsoft:scom*
   ```
5. If you encounter problems or do not see the data you expect, see the Troubleshooting suggestions.

To prevent the Splunk platform from indexing duplicate data, do not enable more than one input that collects the same metric more than once. For example, if you enable one input configured to use a template that collects the Alerts group and another input configured to use a template that collects data using individual alert commands, the Splunk platform indexes the alert command data twice. Verify that each input that you enable invokes templates that do not have overlapping metrics. To see how the groups and commands are related, see the source types table.

Configure inputs through the PowerShell scripted input UI

Prerequisite: If you are collecting data from a remote management server with this script, you must first add the remote management server using the Splunk Add-on for MS SCOM configuration user interface or in the `microsoft_scom_servers.conf` file before creating the PowerShell scripted input.

1. Access Splunk Web on the node responsible for data collection. Click **Splunk** in the upper left to start from the home screen.
2. Go to **Settings > Data inputs**, then select **PowerShell v3 Modular Input**.
3. Click **New**.
4. Enter a name for your input.
5. In the **Command or Script Path** field, enter `& "$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1"` followed by one or more metrics expressed as groups or commands. For example: `& "$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1" -groups override` or `& "$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1" -commands Get-SCOMAlert, Get-SCOMEvent`
6. If you are collecting data from a remote management server with this script, you need to specify the `-server` parameter and the stanza name for the remote server from the `microsoft_scom_servers.conf` file. For example: `& "$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1" -groups task -server remote_management_server`
7. You can also specify the `-starttime` and `-loglevel` parameter. For example: `& "$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1" -groups task -server remote_management_server -loglevel DEBUG -starttime "2021-01-02T00:00:00Z"`
8. You can also specify the `-performancefilter`. For example:

   ```
   &"$SplunkHome\etc\apps\Splunk_TA_microsoft-scom\bin\scom_command_loader.ps1" -commands
   "get-scomallperfdata" -server "abcd" -loglevel WARN -starttime "2022-02-21T07:21:02Z"
   -performancefilter "CounterName IS NOT NULL"
   ```
9. For more information about the group and individual command metrics, see the source types table.
10. Enter a cron expression in the **Cron Schedule** field to specify how often the data should be collected.

11. Optionally, check **More settings** to configure a custom source type, host or index value.
12. Click **Next** to save and enable the input.
13. Go to the Search & Reporting app and search for `sourcetype=microsoft:scom*` to verify the Splunk platform is indexing the data you expect.
14. If you encounter problems or do not see the data you expect, see the Troubleshooting suggestions.

To prevent the Splunk platform from indexing duplicate data, do not create multiple inputs using the same metrics. For example, if you enable one input using the Alerts group and another input using individual alert commands, the Splunk platform indexes the alert command data twice. To see how the groups and commands are related, see the source types table.

Configure inputs through the configuration files

If you want to collect SCOM data from management servers that are installed on separate machines from your Operations console, you need to provide information about the remote management servers in the `microsoft_scom_servers.conf` file before you configure your inputs in the `inputs.conf` file.

Configure remote servers in `microsoft_scom_servers.conf`

If the management server and the Operations console are installed on the same machine, you do not need to perform the steps in this section.

1. Open `%SPLUNK_HOME%\etc\apps\Splunk_TA_microsoft-scom\default\microsoft_scom_servers.conf`.
2. Copy the contents to `%SPLUNK_HOME%\etc\apps\Splunk_TA_microsoft-scom\local\microsoft_scom_servers.conf`. The contents look like this:

   ```
   [localhost]
   host = localhost
   password = ********
   username =
   ```
3. Change the `[localhost]` stanza name to a name that describes the remote server, then type the name of the host and a username and password for an account on that server. Do not use / or \ characters in the stanza name. For Host, you can provide the hostname, IP address, or fully qualified domain name.
4. For username and password, use an Admin account or another account that has read permissions for the commands you are using to collect SCOM data. If you are using a domain user account, use the format `<domain>\<username>` for username. For example:

   ```
   [remote_management_server]
   host = <your SCOM host>
   password = <your SCOM server password>
   username = <your SCOM server username>
   ```
   The password will be encrypted upon reloading the configuration page.
5. Create a stanza for each remote management server you want to collect metrics for, then save the file.

If you need to add a new remote server, do not edit an existing server's host, username and password. The checkpoint is strongly correlated to the server's stanza name. Editing an existing stanza will reuse the checkpoint file which can cause event data loss.

Configure local `inputs.conf`

1. Open `%SPLUNK_HOME%\etc\apps\Splunk_TA_microsoft-scom\default\inputs.conf.template`.
2. Copy the contents to `%SPLUNK_HOME%\etc\apps\Splunk_TA_microsoft-scom\local\inputs.conf`.

3. Enable the inputs for one or more of the predefined stanzas by changing `disabled = 1` to `disabled = 0`.
4. If you would like to customize your own input, customize the final stanza `[powershell://scom_commands]` with your desired settings and enable it. Follow the instructions in the file.
5. Go to the Search & Reporting app and search for `sourcetype=microsoft:scom*` to verify the Splunk platform is indexing the data you expect.
6. If you encounter problems or do not see the data you expect, see the Troubleshooting suggestions.

To prevent the Splunk platform from indexing duplicate data, do not create more than one input using the same metrics. For example, if you enable one input using the Alerts group and another input using individual alert commands, the Splunk platform indexes the alert command data twice. To see how the groups and commands are related, see the source types table.

Configure direct events collection using the Splunk Add-on for Microsoft SCOM

Prerequisites

You need Splunk DB Connect to utilize direct events processing for Microsoft SCOM.

Migration from scriptlet-based events collection to a direct SQL-based approach

Complete these steps to migrate from scriptlet-based events collection to a direct, SQL-based approach. Splunk best practice is to first exercise the migration in a test environment.

1. Go to "Apps" -> "Splunk Add-on for Microsoft SCOM" -> "Inputs"
2. Note the Index name and (optionally) the Interval
3. Change the status of the selected input to "Disabled"
4. Go to the search page, find last event, and note it's "scom_timestamp" value

Configure Microsoft SCOM Database to send data

Work with your local Database admin to create the least-privileged account for collecting data from the database. At a minimum, the account can open a database connection from the machine with the add-on installed to the machine with the database. It can be a local account for collocated services, or a domain user account if the instances are separated. This account needs read-only ("select") access to the "OperationsManager" database, "OperationsManager.dbo.__MOMManagementGroupInfo__" table and Tables/Views (depending of data types to be collected).

Source Type	Table/View Name
Alert	dbo.AlertView
Alert History	dbo.AlertHistory
Performance	dbo.PerformanceDataAllView, dbo.PerformanceCounterSignatureView, dbo.RuleView
Event	dbo.EventView, dbo.RuleView, dbo.LocalizedText

Configure DB Connect v3 inputs

This topic presents the instructions for DB Connect Version 3.6 and above. For previous versions follow the instructions that correspond to the version of DB Connect that you have installed.

To prepare your environment and configure your inputs, follow these steps.

1. Download Splunk DB Connect from Splunkbase.
2. Set up the database connection
3. Download and install the Microsoft JDBC driver for SQL Server. To enable Microsoft SQL Server connections, download and install the Microsoft JDBC Driver for SQL Server as described in the Install database drivers section of the Deploy and Use Splunk DB Connect manual.
4. Create an identity in the Splunk platform. See steps on how to Create an identity from the Splunk DB Connect manual.

Configure inputs

Complete these steps to utlize Direct events processing SQL queries as templates in Splunk DB Connect.

1. Select "Splunk DB Connect" from Apps menu
2. In Splunk DB Connect, click Data Lab > Inputs and then New Input.
3. Select defined database connection in left-hand menu dropdown: "Choose Table" -> "Connection"
4. Select one of "Splunk Add-on for Microsoft SCOM" templates from "Settings" right-hand menu

Template Name	Template Description
msscom:alerts	Collect alerts data from MS SCOM
msscom:alertshistory	Collect alerts history data from MS SCOM
msscom:allperformance	Collect all performance data from MS SCOM
msscom:events	Collect audit event data from MS SCOM

Leave "Input Mode" and "Input Type" ("Event" / "Rising") as is

1. Press the "Execute SQL" button next to "Settings" menu. Note: this initial execution is used to validate the query and download metadata. If you examine the query you notice a query filter similar to `where ah.TimeAdded > '2022-09-01 06:51:29.413'`. You may replace the date with any other date from the past to get the results faster (remember about proper format!)
2. After successful query execution make sure that "scom_timestamp" column is selected as a rising column (the column to differentiate between events from past and events that should be picked up)
3. Checkpoint Value: depending on scenario - for fresh installations it can be any date (but usually SCOM Operational Database stores the information up to two weeks); for migration scenario adequate scriptlet input shall be disabled first and timestamp of the latest collected event shall be used (to avoid gaps and duplicated events)
4. Timestamp (which column shall be used as an event timestamp): Click the "Choose Column" button, scom_timestamp column shall be selected from dropdown below
5. Query Timeout: consult your DBA to select optimal value, the default is 30 seconds if you leave it blank
6. Scroll back to the top of the page. Note that step 3 of "Follow these steps:" procedure shall be marked green. If you press "Execute SQL" button at this moment you shall see following error `com.microsoft.sqlserver.jdbc.SQLServerException: The index 1 is out of range.`

It means that the query is sent with a single variable (defined in "Checkpoint Value" field), but there is no place to inject this value.

1. Navigate to the bottom of the query. Locate line similar to `where ah.TimeAdded > '2022-09-01 06:51:29.413'` (it may be â â ah.TimeAdded, av.TimeAdded, pdav.TimeAdded or ev.TimeAdded depending on selected template)
2. Replace quoted timestamp with single question mark. Line `where ah.TimeAdded > '2022-09-01 06:51:29.413'` shall now look like this: `where ah.TimeAdded > ?`
3. Press the "Execute SQL" button again. The query shall be executed successfully. In case of the issues contact your DBA
4. Once all the steps of "Follow these steps" procedure is marked green press green "Next" button at the top of the page
5. Select descriptive name, feel free to modify the description, we suggest to leave the application as it is
6. We suggest to leave "Max Rows to Retrieve" blank unless you are ready to drop some events
7. Fetch size: Feel free to consult this value with your DBA
8. Execution Frequency: it purely depends on your usage scenario but we suggest to start with default values and tune it later. More frequent executions result in additional overload to database server while less frequent execution create bigger data packages to be processed at once and increased delay
9. Metadata: Predefined source type is required for valid Data model mapping. In case of the migration - Index value shall match "scriptlet" input.

Follow Create a database input procedure from Deploy and Use Splunk DB Connect manual in case of unexpected issues.

Troubleshooting

Troubleshoot the Splunk Add-on for Microsoft SCOM

General troubleshooting

For helpful troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

Custom source types

If you attempt to override the default source types set by this add-on, be aware that some functionality may fail, including CIM mapping, prebuilt panels, checkpoints, and timestamps. For all inputs configured using group metrics, source type overrides are not accepted to preserve this functionality.

Missing data

If your Splunk platform search results are missing data for certain objects in your SCOM that you expect based on the inputs you enabled, consult with your Microsoft SCOM administrator to ensure that SCOM is configured so that these objects are created. The Splunk Add-on for Microsoft SCOM uses only GET commands to return lists of objects. In some cases, the SCOM admin must create the objects first by using ADD commands manually. For example, if you have configured an input to use the `Get-SCOMNotificationChannel`, the input only produces data if a SCOM admin has previously called the command `Add-SCOMNotificationChannel` manually.

Add-on logs

The Splunk Add-on for Microsoft SCOM has a log located at `%SPLUNK_HOME%\var\log\splunk\ta_scom.log`.

For errors regarding invalid commands, params, or other exceptions, search for

```
index=_internal source=*ta_scom.log
```

For remote management server connection errors, search for

```
index=_internal source=*ta_scom.log New SCOMManagementGroupConnection Fail
```

For server validation related errors, search for

```
index=_internal sourcetype=ms:scom:log:server_validation
```

For input validation related errors, search for

```
index=_internal sourcetype=ms:scom:log:input_validation
```

For performance filter parameter validation related errors, search for

```
index=_internal sourcetype=ms:scom:log:performance_filter_parameter_validation
```

Logging Levels

The Splunk Add-on for Microsoft SCOM allows you to configure logging levels in the configuration UI or in `microsoft_scom.conf`. Allowed log levels are DEBUG, WARN, and ERROR. The default is WARN. To configure logging using the UI:

1. Go to Splunk Web on your data collection node.
2. Click **Splunk Add-on for Microsoft SCOM** on the left side to access the Splunk Add-on for Microsoft SCOM configuration UI.
3. Click **Configuration**, then **Logging** and select a logging level from the drop-down menu.

PowerShell logs

A PowerShell log is provided here: `%SPLUNK_HOME%\var\log\splunk\splunk-powershell.ps1.log`.

For errors that occur when PowerShell calls the SCOM scripts, search for

```
index=_internal source=*powershell*.log
```

Cron expression format

The add-on is configured to expect cron expressions in the Quartz Scheduler format rather than the Unix standard.

See the Quartz documentation for complete documentation.

Re-indexing events

The Splunk Add-on for Microsoft SCOM saves checkpoints for some commands to preserve the last indexed date. If you want to index events again, remove all the files in `%SPLUNK_HOME%\var\lib\splunk\modinputs\scom`.

Reference

PowerShell command/timestamp reference

During data collection, if the objects returned from the PowerShell command have a timestamp field such as `TimeAdded` or `LastModified`, the Splunk Add-on for Microsoft SCOM saves a checkpoint file using this timestamp to preserve the last indexed date. When a checkpoint file exists, only data after this date is collected the next time data collection occurs. If the objects returned from the PowerShell command have no timestamp field, the add-on cannot save a checkpoint file and all events are collected every time data collection occurs.

The table below lists all the PowerShell commands used by the add-on for data collection and indicates the timestamp field, if one is available, that is used to create the checkpoint. The commands with no timestamp field do not have a checkpoint.

Template	Group	PowerShell command	Timestamp field
Performance	None	Get-SCOMAllPerfData	TimeSampled
Events	Alert	Get-SCOMAlert	TimeAdded
		Get-SCOMAlertHistory	TimeAdded
	Monitor	Get-SCOMMonitor	LastModified
	Diagnostic	Get-SCOMDiagnostic	LastModified
	Task	Get-SCOMTask	LastModified
		Get-SCOMTaskResult	LastModified
	Recovery	Get-SCOMRecovery	LastModified
	Discovery	Get-SCOMDiscovery	LastModified
	Override	Get-SCOMOverride	LastModified
		Get-SCOMOverrideResult -Instance (Get-SCOMClassInstance) -Monitor (Get-SCOMMonitor)	None
	Event	Get-SCOMEvent	TimeAdded
	Rule	Get-SCOMRule	LastModified
Network	Network	Get-SCOMConnector	Last Modified
		Get-SCOMAgent	LastModified
		Get-SCOMAgentlessManagedComputer	LastModified
		Get-SCAdvisorProxy	None
		Get-SCOMParentManagementServer -Agent (Get-SCOMAgent)	Last Modified
		Get-SCAdvisorAgent	LastModified
		Get-SCOMADAgentAssignment	None
		Get-SCOMGatewayManagementServer	LastModified
Management	Management	Get-SCOMManagementPack	LastModified
		Get-SCOMRunAsAccount	LastModified

Template	Group	PowerShell command	Timestamp field
		Get-SCOMRunAsProfile	LastModified
		Get-SCOMRunAsDistribution	None
		Get-SCOMHeartbeatSetting	None
		Get-SCOMManagementGroup	None
		Get-SCOMManagementServer	LastModified
		Get-SCOMUserRole	LastModified
		Get-SCOMAlertResolutionSetting	None
		Get-SCOMAlertResolutionState	None
		Get-SCOMManagementGroupConnection	None
		Get-SCOMAccessLicense	None
		Get-SCOMDatabaseGroomingSetting	None
		Get-SCOMDataWarehouseSetting	None
		Get-SCOMErrorReportingSetting	None
		Get-SCOMReportingSetting	None
		Get-SCOMResourcePool	LastModified
		Get-SCOMRMSEmulator	LastModified
		Get-SCOMGroup	LastModified
		Get-SCOMWebAddressSetting	None
		Get-SCOMAgentApprovalSetting	None
		Get-SCOMLocation	LastModified
		Get-SCOMTieredManagementGroup	None
		Get-SCOMNotificationChannel	None
		Get-SCOMNotificationSubscriber	None
		Get-SCOMNotificationSubscription	None
		Get-SCOMMaintenanceMode	LastModified
		Get-SCOMPendingManagement	LastModified
		Get-SCOMTieredManagementGroup | Get-SCOMTierConnector	None
Internal	Internal	Get-SCOMClass	LastModified
		Get-SCOMClassInstance	LastModified
		Get-SCOMRelationship	LastModified
		Get-SCOMRelationshipInstance	LastModified
		Get-SCOMMonitoringObject	LastModified

Lookups for the Splunk Add-on for Microsoft SCOM

The Splunk Add-on for Microsoft SCOM has the following **lookups** that map fields from Microsoft SCOM systems to CIM-compliant and Splunk IT Service Intelligence values in the Splunk platform. The lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_microsoft-scom/lookups`.

Filename	Description
`ms_scom_alert_severity.csv`	The SCOM alert severity lookup maps the severity from SCOM alert to a CIM-compliant string.
ms_scom_countername_to_datamodel_4.3.0.csv	Applies to performance data. Lookup uses the value of the "countername" field to map event to the appropriate performance category in CIM.
`ms_scom_alert_type.csv`	The SCOM alert type lookup uses the severity value from SCOM events to map to the "type" CIM field from the Alerts Data Model with a CIM-compliant string.
`ms_scom_datamodel.csv`	Data Model Association for RuleNames

SQL queries for SCOM direct events processing reference

> The SQL queries provided with the Splunk Add-on for Microsoft SCOM might overload your SCOM Server or Splunk instances.

Splunk support may not be able to assist in cases where you modified your SQL queries. Splunk best practice is to exercise extreme caution during modification of provided SQL queries.

1. Number of columns are modified at the SQL level for compatibility with scriptlet based source types (All the invocations of `ISNULL` and `LOWER` methods).
2. Number of hard coded columns (splunk_scom_group, scom_command) looks redundant but are required for valid Data Model mapping.
3. Removal of double quotes from search results: this operation is required to alleviate a known Splunk DB Connect issue: Incomplete field values are extracted when the value contains double quotes