

Platform : Enterprise 9.0

This add-on was working well on 8.x version. But, This add-on was not working on 9.0 version.

<July 13 issue>

	Desc
Add-on	"Microsoft Office 365 Reporting Mail Add-on for Splunk" (https://splunkbase.splunk.com/app/3720/)
The	process of collecting data using continuously_monitor mode From the time when millisecond is added to the time value in , it is repeatedly confirmed that the log is not properly collected.
Example	Settings Start Time - 2022-07-11T06:00:00 Cycle - 10 minutes

Example Related Logs

Time	Source	Filter
95 2022/07/12 18:01:27.447	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
96 2022/07/12 17:51:27.035	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
97 2022/07/12 17:41:27.323	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
98 2022/07/12 17:31:26.944	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
99 2022/07/12 17:21:27.332	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
100 2022/07/12 17:11:27.214	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:27:03.115648Z'20and20EndDate20eq20datetime'2022-07-11T07:37:03.27:03.115648Z
101 2022/07/12 17:01:27.584	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:20:00Z'20and20EndDate20eq20datetime'2022-07-11T07:30:00Z'20and20EndDate20eq20datetime'2022-07-11T07:30:00Z'
102 2022/07/12 16:51:27.147	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:10:00Z'20and20EndDate20eq20datetime'2022-07-11T07:20:00Z'20and20EndDate20eq20datetime'2022-07-11T07:20:00Z'
103 2022/07/12 16:41:27.890	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T07:00:00Z'20and20EndDate20eq20datetime'2022-07-11T07:10:00Z'20and20EndDate20eq20datetime'2022-07-11T07:10:00Z'
104 2022/07/12 16:31:27.320	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T06:50:00Z'20and20EndDate20eq20datetime'2022-07-11T07:00:00Z'20and20EndDate20eq20datetime'2022-07-11T07:00:00Z'
105 2022/07/12 16:21:27.562	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T06:40:00Z'20and20EndDate20eq20datetime'2022-07-11T06:50:00Z'20and20EndDate20eq20datetime'2022-07-11T06:50:00Z'
106 2022/07/12 16:11:27.396	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T06:30:00Z'20and20EndDate20eq20datetime'2022-07-11T06:40:00Z'20and20EndDate20eq20datetime'2022-07-11T06:40:00Z'
107 2022/07/12 16:01:27.670	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T06:20:00Z'20and20EndDate20eq20datetime'2022-07-11T06:30:00Z'20and20EndDate20eq20datetime'2022-07-11T06:30:00Z'
108 2022/07/12 15:51:27.372	ta_ms_o365_reporting_ms_o365_message_trace.log	StartDate20eq20datetime'2022-07-11T06:10:00Z'20and20EndDate20eq20datetime'2022-07-11T06:20:00Z'20and20EndDate20eq20datetime'2022-07-11T06:20:00Z'

< July 26 issue in detail >

First of all, in the previous inquiry email, micro second was added to the Start Time when collecting logs, and it was confirmed that there was an abnormal operation of the app.

And today, as below, it was additionally confirmed through internal log analysis.

The problem occurs as the Start Time value when the app attempts to collect logs is changed (attached 2) to the time of the last log collected (attached 1), ignoring the Interval value. This means that the same log is collected every time.

Based on the attached and confirmed contents below, a bug in the collection window of the app is suspected and we wondering how the conditions of the window change.

Additionally, the log cannot collect additional logs after a certain period (after the start time is fixed).

That's why it seems like it should be resolved as quickly as possible.

Attachment 1>

Interval : 10 sec

Time window: 60 min

This is events.

Start time converted the time as same with “Received” time of event. Why?

이벤트	
2022-07-26 14:54:39,128 DEBUG pid=40515 tid=MainThread file=base_modinput.py:log_debug:288 _Splunk_	Start date: 2022-07-26 01:17:06.856689, End date: 2022-07-26 02:17:06.856689
host = [REDACTED] source = [REDACTED] var/log/splunk/ta_ms_o365_reporting_ms_o365_message_trace.I...	sourcetype = ta_ms_o365_reporting_ms_o365_message_trace-3
2022-07-26 14:54:29,133 DEBUG pid=40428 tid=MainThread file=base_modinput.py:log_debug:288 _Splunk_	Start date: 2022-07-26 01:17:06.856689, End date: 2022-07-26 02:17:06.856689
host = [REDACTED] source = [REDACTED] var/log/splunk/ta_ms_o365_reporting_ms_o365_message_trace.I...	sourcetype = ta_ms_o365_reporting_ms_o365_message_trace-3
2022-07-26 14:54:19,196 DEBUG pid=40344 tid=MainThread file=base_modinput.py:log_debug:288 _Splunk_	Start date: 2022-07-26 01:10:00, End date: 2022-07-26 02:10:00
host = [REDACTED] source = [REDACTED] var/log/splunk/ta_ms_o365_reporting_ms_o365_message_trace.I...	sourcetype = ta_ms_o365_reporting_ms_o365_message_trace-3

시간	이벤트
22/07/26 10:17:06.856	<pre>{ [-] FromIP: null Index: 0 MessageId: <7[REDACTED]> MessageTraceId: 35[REDACTED]# Organization: [REDACTED],com Received: 2022-07-26T01:17:06.856689 RecipientAddress: [REDACTED].com SenderAddress: MicrosoftExchange[REDACTED] Size: 155805 Status: Delivered Subject: [REDACTED]이 메시지를 보냈습니다. ToIP: [REDACTED]41 }</pre> 원시 텍스트로 표시 host = [REDACTED] source = ms_o365_message_trace sourcetype = ms:o365:reporting:messageatrace

Attachment 2>

Internal log

pid=40515

2022-07-26 14:54:39,355 DEBUG pid=40515 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.002830

2022-07-26 14:54:39,355 DEBUG pid=40515 tid=MainThread

file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "POST

/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpoint/batch_save HTTP/1.1" 200 26

2022-07-26 14:54:39,352 DEBUG pid=40515 tid=MainThread file=binding.py:post:750 | POST request to

https://127.0.0.1:8089/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpoint/batch_save (body: {'body': '{"_key": "test2_obj_checkpoint", "state": {"max_date\\": "\\2022-07-26 01:17:06.856689\\\"}}'})

2022-07-26 14:54:39,352 DEBUG pid=40515 tid=MainThread

file=base_modinput.py:log_debug:288 | **_Splunk_ max date after getting messages: 2022-07-26 01:17:06.856689**

2022-07-26 14:54:39,352 DEBUG pid=40515 tid=MainThread

file=base_modinput.py:log_debug:288 | **_Splunk_ max date before getting message: 2022-07-26 01:17:06.856689**

2022-07-26 14:54:39,350 DEBUG pid=40515 tid=MainThread

file=connectionpool.py:_make_request:437 | <https://reports.office365.com:443> "GET

/ecp/reportingwebservice/reporting.svc/MessageTrace?\$filter=StartDate%20eq%20datetime'2022-07-26T01:17:06.856689Z'%20and%20EndDate%20eq%20datetime'2022-07-26T02:17:06.856689Z' HTTP/1.1" 200 629

2022-07-26 14:54:39,129 DEBUG pid=40515 tid=MainThread

file=connectionpool.py:_new_conn:959 | Starting new HTTPS connection (1):

reports.office365.com:443

2022-07-26 14:54:39,128 INFO pid=40515 tid=MainThread file=setup_util.py:log_info:117 | Proxy is not enabled!

2022-07-26 14:54:39,128 DEBUG pid=40515 tid=MainThread

file=base_modinput.py:log_debug:288 | Endpoint URL:

[https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?\\$filter=StartDate eq datetime'2022-07-26T01:17:06.856689Z' and EndDate eq datetime'2022-07-26T02:17:06.856689Z'](https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?$filter=StartDate eq datetime'2022-07-26T01:17:06.856689Z' and EndDate eq datetime'2022-07-26T02:17:06.856689Z')

2022-07-26 14:54:39,128 DEBUG pid=40515 tid=MainThread

file=base_modinput.py:log_debug:288 | **_Splunk_ Start date: 2022-07-26 01:17:06.856689, End date: 2022-07-26 02:17:06.856689**

2022-07-26 14:54:39,128 DEBUG pid=40515 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.002103

2022-07-26 14:54:39,127 DEBUG pid=40515 tid=MainThread

file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "GET

/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpoint/test2_obj_checkpoint HTTP/1.1" 200 115

2022-07-26 14:54:39,125 DEBUG pid=40515 tid=MainThread file=binding.py:get:677 | GET request to

https://127.0.0.1:8089/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpoint/test2_obj_checkpoint (body: {})

2022-07-26 14:54:39,124 DEBUG pid=40515 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.002395

2022-07-26 14:54:39,124 DEBUG pid=40515 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "GET
/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/config/?count=-1&offset=0&search=TA_MS_0365_Reporting_checkpointer HTTP/1.1" 200 7417

2022-07-26 14:54:39,122 DEBUG pid=40515 tid=MainThread file=binding.py:get:677 | GET request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/config/
(body: {'count': -1, 'offset': 0, 'search': 'TA_MS_0365_Reporting_checkpointer'})

2022-07-26 14:54:39,121 DEBUG pid=40515 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.007915

2022-07-26 14:54:39,121 DEBUG pid=40515 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "GET
/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/config/TA_MS_0365_Reporting_checkpointer HTTP/1.1" 200 5562

2022-07-26 14:54:39,114 DEBUG pid=40515 tid=MainThread
file=connectionpool.py:_new_conn:959 | Starting new HTTPS connection (1): 127.0.0.1:8089

2022-07-26 14:54:39,113 DEBUG pid=40515 tid=MainThread file=binding.py:get:677 | GET request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/config/TA_MS_0365_Reporting_checkpointer (body: {})

2022-07-26 14:54:39,113 INFO pid=40515 tid=MainThread
file=splunk_rest_client.py:_request_handler:105 | Use HTTP connection pooling

pid=40344

2022-07-26 14:54:19,480 DEBUG pid=40344 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.002540

2022-07-26 14:54:19,480 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "POST
/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpointer/batch_save HTTP/1.1" 200 26

2022-07-26 14:54:19,478 DEBUG pid=40344 tid=MainThread file=binding.py:post:750 | POST request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_0365_Reporting/storage/collections/data/TA_MS_0365_Reporting_checkpointer/batch_save (body: {'body': '[{"_key": "test2_obj_checkpoint", "state": "{\"max_date\": \"2022-07-26 01:17:06.856689\"}"}]'})

2022-07-26 14:54:19,478 DEBUG pid=40344 tid=MainThread
file=base_modinput.py:log_debug:288 | **_Splunk_ max date after getting messages: 2022-07-26 01:17:06.856689**

2022-07-26 14:54:19,477 DEBUG pid=40344 tid=MainThread
file=base_modinput.py:log_debug:288 | **_Splunk_ max date before getting message: 2022-07-26 01:10:00**

2022-07-26 14:54:19,476 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://reports.office365.com:443> "GET
/ecp/reportingwebservice/reporting.svc/MessageTrace?\$filter=StartDate%20eq%20datetime'202

2-07-26T01:10:00Z'%20and%20EndDate%20eq%20datetime'2022-07-26T02:10:00Z' HTTP/1.1" 200 1313

2022-07-26 14:54:19,197 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_new_conn:959 | Starting new HTTPS connection (1):
reports.office365.com:443

2022-07-26 14:54:19,196 INFO pid=40344 tid=MainThread file=setup_util.py:log_info:117 | Proxy is not enabled!

2022-07-26 14:54:19,196 DEBUG pid=40344 tid=MainThread
file=base_modinput.py:log_debug:288 | Endpoint URL:
[https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?\\$filter=StartDate eq datetime'2022-07-26T01:10:00Z' and EndDate eq datetime'2022-07-26T02:10:00Z'](https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace?$filter=StartDate eq datetime'2022-07-26T01:10:00Z' and EndDate eq datetime'2022-07-26T02:10:00Z')

2022-07-26 14:54:19,196 DEBUG pid=40344 tid=MainThread
file=base_modinput.py:log_debug:288 | _Splunk_ Start date: 2022-07-26 01:10:00, End date: 2022-07-26 02:10:00

2022-07-26 14:54:19,195 DEBUG pid=40344 tid=MainThread file=connectionpool.py
:_make_request:437 | <https://127.0.0.1:8089> "GET
/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/data/TA_MS_O365_Reporting_checkpoint/test2_obj_checkpoint HTTP/1.1" 404 140

2022-07-26 14:54:19,193 DEBUG pid=40344 tid=MainThread file=binding.py:get:677 | GET request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/data/TA_MS_O365_Reporting_checkpoint/test2_obj_checkpoint (body: {})

2022-07-26 14:54:19,192 DEBUG pid=40344 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.002389

2022-07-26 14:54:19,191 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "GET
/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/config/?count=-1&offset=0&search=TA_MS_O365_Reporting_checkpoint HTTP/1.1" 200 7417

2022-07-26 14:54:19,189 DEBUG pid=40344 tid=MainThread file=binding.py:get:677 | GET request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/config/
(body: {'count': -1, 'offset': 0, 'search': 'TA_MS_O365_Reporting_checkpoint'})

2022-07-26 14:54:19,189 DEBUG pid=40344 tid=MainThread file=binding.py:new_f:73 | Operation took 0:00:00.007881

2022-07-26 14:54:19,189 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_make_request:437 | <https://127.0.0.1:8089> "GET
/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/config/TA_MS_O365_Reporting_checkpoint HTTP/1.1" 200 5562

2022-07-26 14:54:19,182 DEBUG pid=40344 tid=MainThread
file=connectionpool.py:_new_conn:959 | Starting new HTTPS connection (1): 127.0.0.1:8089

2022-07-26 14:54:19,181 DEBUG pid=40344 tid=MainThread file=binding.py:get:677 | GET request to
https://127.0.0.1:8089/servicesNS/nobody/TA-MS_O365_Reporting/storage/collections/config/TA_MS_O365_Reporting_checkpoint (body: {})

2022-07-26 14:54:19,181 INFO pid=40344 tid=MainThread
file=splunk_rest_client.py:_request_handler:105 | Use HTTP connection pooling

