

[Procedure] Microsoft Sentinel for SAP

Last updated by | Alexandru Panait | Mar 31, 2023 at 8:39 AM CDT

Microsoft Sentinel for SAP

Section/ Landing Page Description

This wiki will address the situation when connection to Sentinel SAP connectors drops frequently and we've got a lot of RFC_COMMUNICATION_FAILURE errors.

Contents

- How the issue is listed:
 - To see more details of the issue, run the following query o...
- Update Aget to the latest version
 - Manual Agent Update:
 - Automated Agent Update
 - Location where the latest agent version can be checked:
 - Official Documentation for Troubleshooting Microsoft Sent...
 - IcM

How the issue is listed:

Configuration			
Search by agent name or SID			
Agent Name ↑↓	SID ↑↓	Health ↑↓	System role ↑↓
09e97a5c-1005-4121-a171-a4c47ad0ce26	A4U-100	System healthy	test
97a2ff58-1e4c-4fa6-8bfa-366376f419fa	CAF-001	RFC_COMMUNICATION_FAILURE	Customizing
9a68cb3f-1983-4d24-bcbc-6558468afd6c	CTA-001	RFC_COMMUNICATION_FAILURE	Customizing
9bac01423156_10.40.145.136	C05-001	System unreachable for over 1 day	Production
a2a08c3e4661_10.40.146.132	C0A-001	System unreachable for over 1 day	Production
a3dde4262f07_10.40.146.68	C0P-001	RFC_COMMUNICATION_FAILURE	Production
c1710d00-945d-4b26-bbb6-69691bafcc55	S40-100	NOT_AUTHORIZED	Unknown (Production)
c3da55eb-b6e6-4b6f-88ae-b607bcd61333	P70-100	RFC_COMMUNICATION_FAILURE	Production

To see more details of the issue, run the following query on the Workspace:

```
SAP_HeartBeat_CL
| where system_id_s contains "CAF-001"
```

Sample

LOCATION CPIC (TCP/IP) on local host with Unicode ERROR partner '10.40.157.68:3300' not reached TIME
Fri Mar 10 13:24:40 2023 RELEASE 753 COMPONENT NI (network interface) VERSION 40 RC -10 MODULE /bas/753_REL/sr

Update Aget to the latest version

Usually, this issue is related to the fact that the latest agent is not in use.

Manual Agent Update:

The following Command has to be run on the Container:

```
wget -O sapcon-instance-update.sh https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/SAP/
```

Automated Agent Update

The following set-up has to be done on All the Containers:

Auto-Update script

```
wget -O sapcon-sentinel-auto-update.sh https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Solutions/SAP/sapcon-sentinel-auto-update.sh && bash ./sapcon-sentinel-auto-update.sh
```

Auto-update-registration log

```
cat /var/log/sapcon-sentinel-register-autoupdate.log Auto-update log
```

```
cat /var/log/sapcon-sentinel-auto-update.log
```

Update log

```
cat /var/log/sapcon-update.log
```

config

```
cat /etc/crontab or cat /etc/anacrontab
```

Location where the latest agent version can be checked:

<https://mcr.microsoft.com/v2/azure-sentinel/solutions/sapcon/tags/list> 

Official Documentation for Troubleshooting Microsoft Sentinel solution for SAP

<https://learn.microsoft.com/en-us/azure/sentinel/sap/sap-deploy-troubleshoot> 

IcM

<https://portal.microsofticm.com/imp/v3/incidents/details/376182301/home> 

Contributor Name	Details	Date
Alex Panait	Created this section	03/31/2023
Dvir Naim	Approved Wiki Content	