

IBM ECM System Monitor Field Guides

Integration with Instana

November 06th, 2023 CENIT AG Michael Wohland

Content

Introduction
Overview
Disclaimer
Purpose of this guide
Requirements 4
Step by Step setup 5
1. Find the description of the REST API and create the message template accordingly . 5
2. Setup of the actual task
3. Trigger the task (forwarding to Instana) once the incident is created
4. Output in Instana11
Contact Information

Introduction

Overview

This guide describes in detail, how IBM ECM System Monitor (ESM) can be integrated in an Application Performance Management Tool. Exemplarily we use "Instana" in this guide. For the integration an ESM task named WebHookExportIncident will be used.

Disclaimer

The content of this document is based on the latest ESM version. The descriptions and guidelines in this document are for informational purposes only. Up-to-dateness, content completeness, appropriateness and validity for all possible scenarios cannot be guaranteed. All information is provided on an as-is basis. The author is not liable for any errors or omissions in this document or any losses, injuries and damages arising from its use.

If you are planning to setup or configure ESM or to adjust an existing installation, it is necessary to consider current security whitepapers, release notes and announcements from the official IBM ECM System Monitor product documentation website.

Purpose of this guide

Many ESM users / customers want to integrate ESM with their Application Performance Management tool. ESM offers several possibilities for that. The WebHookExportIncident task offers a comfortable way to achieve that.

Requirements

- The Application Performance Management tool must offer a REST API that allows JSON object to be posted. For example "Instana" offers this option as an Agent REST API.

- An Instana Agent must be installed in the same location as the ESM Agent (Same container pod or same monitored server – one to one connection between ESM Agent and Instana Agent).

- The ESM Server must be able to access the URL to the REST API.

Step by Step setup

1. Find the description of the REST API and create the message template accordingly

Check for the description of the API on the vendor pages. Information about the Agent REST API from "Instana" can be found here: <u>https://www.instana.com/docs/api/agent</u>

The below is an example of a JSON object with one record at a time:

```
{
  "title": <string>,
  "text": <string>,
  "severity": <integer>,
  "timestamp": <integer>,
  "duration": <integer>,
.."incident": <boolean>,
  "path": <string>,
}
```

For a description of the object parts please have a look at the website.

The default template in the WebHookExportIncident task looks like this:

\$Timestamp: \$Severity: \$Value | \$Message | {"text" : "\$Timestamp: \$Severity: \$Value |
\$Message | \$Error "} +

Incident internal fields are used with the following notation: \$EntityType.FieldInCamelCase. They can be seen when double clicking on an incident. The field must be defined in CamelCase, meaning each word starts with a capital letter. E.g. SituationCfgId. Some of the fields e.g. Incident.ID might not be available at task execution since the entry is created when added to the DB.

The following EntityTypes are available:

- Incident (default used if nothing but FieldInCamelCase is specified)
- Situation
- Sample
- ProbeConfig
- Agent
- Subsystem

The information must be combined with the needed JSON object to the actual template. This is just an example and may not fit in your environment. Some JSON object variables have been removed as they are not needed:

```
"title": "ESM $ProbeConfig.Name",
"text": "Host: $Agent.Hostname,
Message:$Message,
Value: $Value,
Source: $Source,
Error: $Error",
"duration": 60000,
"severity": 5
```

The red highlighted parts are descriptive or information text parts – text starting with \$ like \$ProbeConfig.Name will be replaced with the corresponding content from the incident.

The template is completed, make sure to put it in a one line format after you have created it. We recommend to do that in an editor like notepad++ or vim.

```
{"title":"ESM $ProbeConfig.Name", "text": "Host: $Agent.Hostname ,
Message:$Message , Value: $Value , Source: $Source , Error: $Error",
"duration": 60000, "severity": 5}
```

The severity could not be replaced in this case by using the \$Severity info from the incident, as the information would be something like HARMLESS or CRITICAL. The object needs a number in this case. So depending on how many different severities for objects are needed in the Application Performance Management Tool, you might end up using several ESM tasks (one for each severity).

2. Setup of the actual task

Note: For each monitored ESM Agent where information should be forwarded to Instana, you will need at least one task instance. This step must be repeated for all of them.

Once the template is created, the URL where the JSON object will be sent to, is needed. In case of "Instana" an example is given on the above specified web page again.

http://<agent ip>:42699/com.instana.plugin.generic.event

The actual task setup is done in the ESM console. Browse to the Configuration Console and on the left to the navigation item "Tasks". There you will find the WebHookExportIncident task.

IBN 5.5.7	I ESM 7.0-000	Monitoring Configuration	Administration Help	👬 🖊 🍏 6/13 161x 9sago	admin
Cor	figuration , 😋 Tasks				
«	• • • •				*
e	AutodiscoverCpeSettings	Ð			
	BpmDeleteProcessInstances	Ŧ			
-	BpmProcessCenterDeleteSnapsh	ots 🕀			
T	BpmProcessServerDeleteSnapsh	ots 🕀			
?	CebiStart	Ē.			
100	CebiStop	Œ			
245	CleanupDebug	Œ			
	ConfigureDebugSettings	Œ			
~	CopyFile	Œ			
<u> </u>	DbExportIncident	Œ			
	• Debug	Œ			
	• Example	(F)			
	FileExportIncident	(H)			
	MailExportIncident	Œ			
	MonitoringConfigTemplate	Œ			
	• OnDemandStart	Œ			
	OnDemandStop	(F)			
	ProcessExecution	Œ			
	SnmpExportIncident	Œ			
	StatusMail	(F)			
	WebHookExportIncident	Đ			

Click on the + on the right of the WebHookExportIncident task to open the task editor.

The editor looks like this:

📽 Task Configuration	Stask Configuration
Select the type of the task and enter its configuration data.	Select the type of the task and enter its configuration data.
*Name active	*Name Webhook-Instand
Task: WebHookExportIncident Template: {'text' : "\$Timestamp: \$Severity: \$Value \$Message \$Er Webhook URL: https://hooks.slack.com/services/ <t>//<x> Authorization Header: apJToken</x></t>	Task: WebHookExportIncident Template: ["title":"ESM \$ProbeConfig.Name", "text": "Host: \$Agent.He Webhook URL: http://instana-agent-instana-agent.cenit-eim-ocp-2-35dd50 Authorization Header:
& Agent Select the location where the Task should run.	Select the location where the Task should run.
[Run on Server]	[Run on Server]
🛗 Schedule	🛗 Schedule 🕞
If active when and how often should the Task be executed?	If active when and how often should the Task be executed?
Interval Cron Start: End: Interval: 10 Minute(s)	Interval Cron Start: End: Interval: 10 Minute(s)

- Specify a name for the task, e.g. Webhook-Instana.
- Do not check the active button as the task will be triggered by an incident.
- Copy the template that has been created in the template section.
- Copy the REST API URL in the Webhook URL.
- As Agent use [Run On Server] → The task will be executed on the actual ESM Server which is what we want.
- Because the task is triggered, the schedule part will not be used at all.
- Save the task by clicking on the hook button above the "Task Configuration".

You should now see the saved task specified as "DEACTIVATED" below the WebHookExportIncident entry in the task list.



Repeat this step for tasks of this particular Agent that use other severities, e.g. two more tasks for severities -1 and 10.

3. Trigger the task (forwarding to Instana) once the incident is created

For forwarding the incident to the Application Performance Management tool a task trigger must be defined. This is done in the situation editor. For each incident to be forwarded this must be done in the corresponding situation setup. As a simple example this is done with the "ProcessCount @ Server_Agent" situation here.

Select the Configuration Console and switch to the "Situation Groups" on the left. Open the situation editor by double clicking on the situation for which you want to add the trigger.

IBM ESM 5.5.7.0-000	Monitoring Configuration	Administration Help	6/13 170x 11s ago	admin
🔅 Configuration , 😍 Situations , 🖿 All S	Situations			
	1			*
🔒 💌				
PortReachable @ CPE55_Ag	gent			
PpmoildleRequestHandlers @	₫ IS42			
PpmoiNoProcOccurence @ I	S42			
PpmoiPercentageTotalByMax	x @ IS42			
🗱 💎 PrintQueueStatistics @ IS42				
PrintQueueStatus @ IS42				
Process @ CMoD105_Agent	E	N		
Process @ CMoD105_Agent	1	13		
ProcessCount @ Server_Age	ent			
Processinstances @ CMoD1	05_Agent			
Prometheus @ Prometheus				
RejectedUsers @ IS42				
ResourceManagerHeartbeat	@ CM86LS			
ResourceManagerServices @	a CM86RM			
ResourceManagerVolumeSp	ace @ CM86RM			
ResourceManagerWebStatus	s @ CM86LS			
RPC Put Request Failed @ 1	ocall istener			
	50004			

The editor will open and look like this:

x < > ~	• 0 0
양 Probe Configuration	 Configuration Help
Select the subsystem you want to monitor and the type of used.	e probe that should be ProcessCount Description
Subsystem: Server_Agent	This probe counts the number of running instances for the given processes and
Probe: ProcessCount	 services. It returns one sample for each process or service with the corresponding
Name: ProcessCount @ Server_Agen	count
active: 🗸	Recommended Schedule
Process List: karaf	Approx. 5 min
Service List	Darametere
Agent Assignment Select the location where the Probe should run.	routes Les Comma-separated list of case-insensitive process names to check. Service List Comma-enarated list of case_insensitive Windows service names to check
Server_Agent	
🛗 Schedule	The entries in both Process List and Service List are treated as regula expressions.
If active when and how often should the Probe be execute Interval Cron Stat: End: Interval: 2 Minute(s)	This means that you can include valid regular expression patterns in the process or service name. Leading and trailing ' are added automatically to make sure that the whole process name including the path and any parameters are matched. It also means that backslashes in process and service names must be doublet to create valid regular expressions (e.g. specify bin \jav to check for Windows process that have bin \java in their proce name).

Switch to page 3 (Automation) of the editor. Per default no entry is given there. Click on the + to add a new setup.

🌣 Automation				
Trigger tasks automatically by occurrence of certain incidents.				
Ŧ				
Condition	Mode	Tasks		
All of: Severity > Critical Situation == ProcessCount @ Server_Agent	Always	No item selected. Click here to edit.	© •	
		Л		
Automation				
Trigger tasks automatically by occurrence of certain incidents.				
Ð				
Condition	Mode	Tasks		
All of: Severity >= Harmless Situation == ProcessCount @ Server_Agent	Always	 Webnook-instana 	6	

Condition:

You should adjust the condition to your needs, but you should keep the entry "Situation == XYZ" at this point. Otherwise the condition will match all situations and the task is trigged from each incident that matches the condition.

Mode:

Select from the drop down between "First" or "Always".

- First: will trigger the task only once once the condition changes to a first match so if the incident is currently having this condition already, nothing will be triggered.
- Always: Each time the condition matches the currently created incident, the task will be triggered.

Tasks:

Select the task you want to trigger once the condition matches from the drop down.

Save the situation setup by clicking on the hook button above the "Automation". Repeat this for all incidents that must be forwarded. The integration is now complete.

4. Output in Instana

Once a Webhook task was triggered by an incident the Event that is created in Instana will look like this:

△ ESM ProcessCount @ Server_Agent					
Started 2021-12-22 12:43:23	Ended	Duration 30s	Severity Warning		
Description On:					

Contact Information

If you have any questions, please contact us at <u>ECM.SystemMonitor@cenit.com</u>.

CENIT AG Phone: +49 711 7825 30 Email: <u>ECM.SystemMonitor@cenit.com</u>