IBM ECM System Monitor
Field Guides

Integration with Instana

March 04th, 2024
CENIT AG
Michael Wohland

Content

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 5.5.11.002. 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

- An Instana agent is running on the same system or namespace as the ESM agent is running. Basically, both Agents are monitoring same sources.
- The Instana agent modus must be set Infrastructure and not APM.
- The Instana agent must offer a REST API that allows JSON object to be posted. Typically "Instana" offers this option on port 42699 as an out of the box functionality.

Step by Step setup

1. Setup of the task in ESM

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

The URL where the JSON object will be sent to, is needed. The default URL in the task is specified as follows and usually fits where ESM agent and Instana agent is installed on the same system:

http://localhost:42699/com.instana.plugin.generic.event

If the Instana agent and the ESM agent are not installed on the same system or e.g. are deployed as containers, but they are monitoring the same sources, then you need to exchange localhost with the corresponding Instana agent name or address. Please make sure that the communication between the ESM agent and the Instana agent on the given port can be established.

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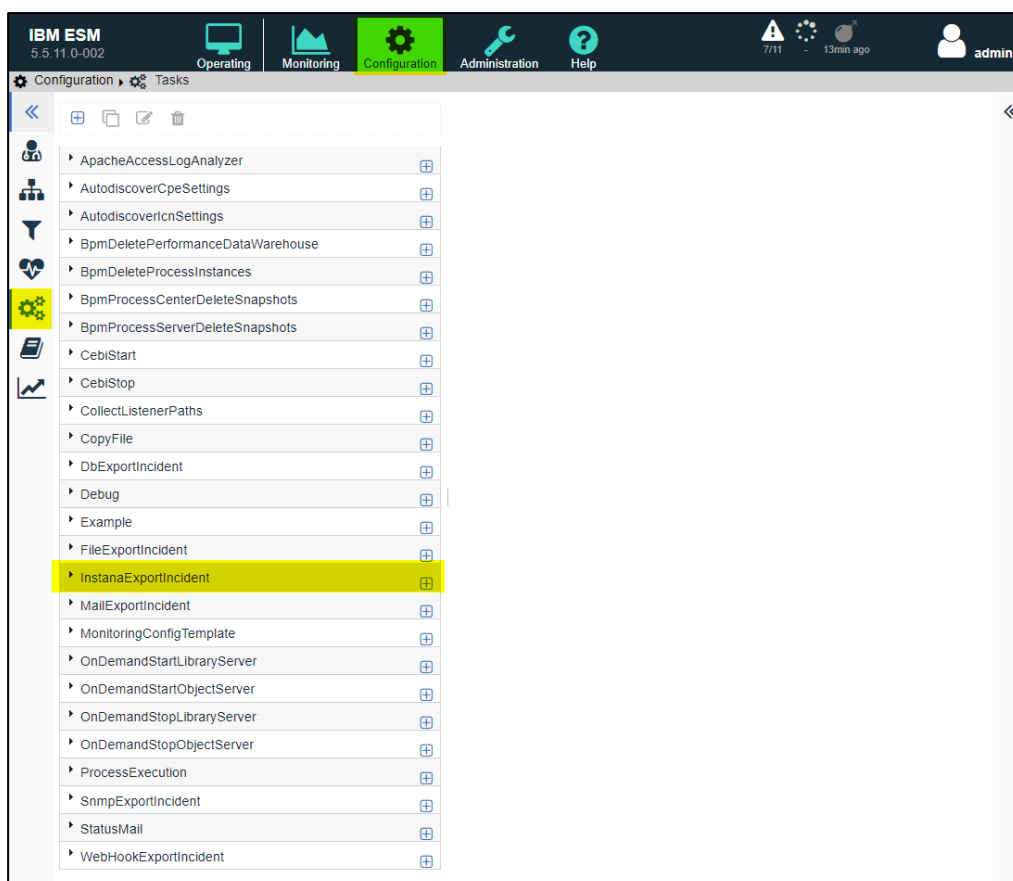
Click on the + on the right of the InstanaExportIncident task to open the task editor.

The editor looks like this:

- Specify a name for the task, e.g. Forward-Instana-CPE55
- Do not check the active button as the task will be triggered by an incident.
- Adjust the Endpoint URL if required. Make sure to address the matching Instana Agent to the below specified ESM agent for the execution. This will ensure that all incidents are getting displayed on the correct agent in Instana.
- As TLS Version select between TLS v1.2 and/or v1.3. When establishing the connection this will handle the version which is used.
- As Agent use the ESM agent that fits the Instana Agent → The task will be executed on the actual ESM agent.
- 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".

Hint: The task will automatically match severities from ESM to Instana as follows:
ESM WARNING -> Instana WARNING
ESM CRITICAL or FATAL -> INSTANA CRITICAL
ESM Others than above -> INSTANA CHANGE

You should now see the saved task specified as "DEACTIVATED" below the InstanaExportIncident entry in the task list.
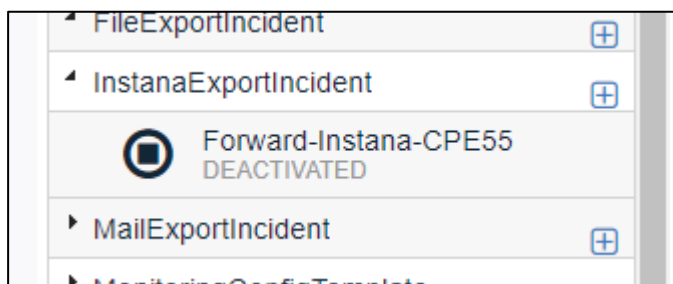
Repeat this step to create one task instance per matching Instana/ESM agent combination.

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

You have two possibilities to decide how the information should be forwarded to Instana.

2a. Standard way of triggering the task (Setup in task itself)

The trigger in this case is created within the task setup. It is only based on the situation for which the information should be forward. In this case all events/incidents from all severities (HARMLESS to FATAL) in ESM for the specified situations are getting forwarded.

Note: The advantage in doing it this way is that all events in Instana are getting updated -> CRITICAL events will be updated if a HARMLESS or WARNING update is sent for the same situation, so you do not have outdated critical alerts in the Instana Dashboard.
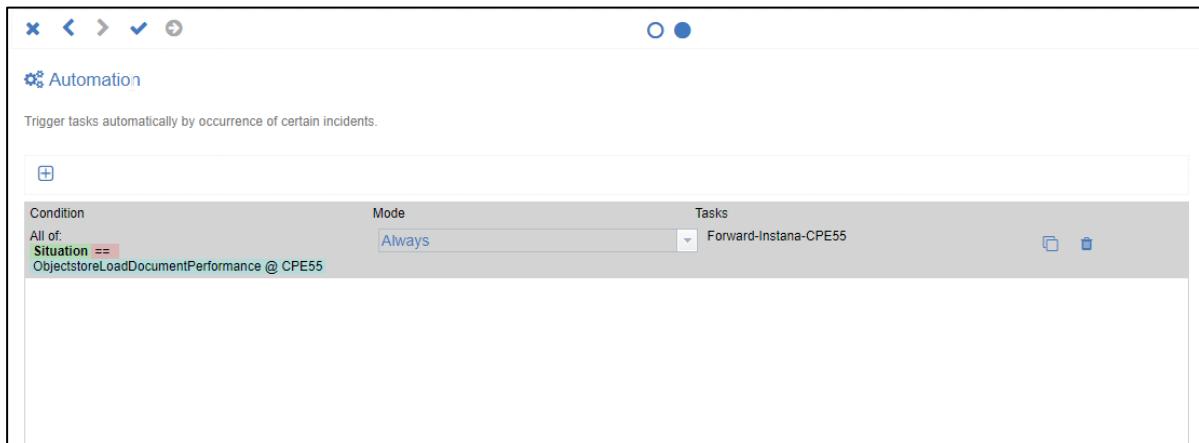
Edit the task(s) you have just created by opening it via double click or selecting it and using the edit button from above of the list.
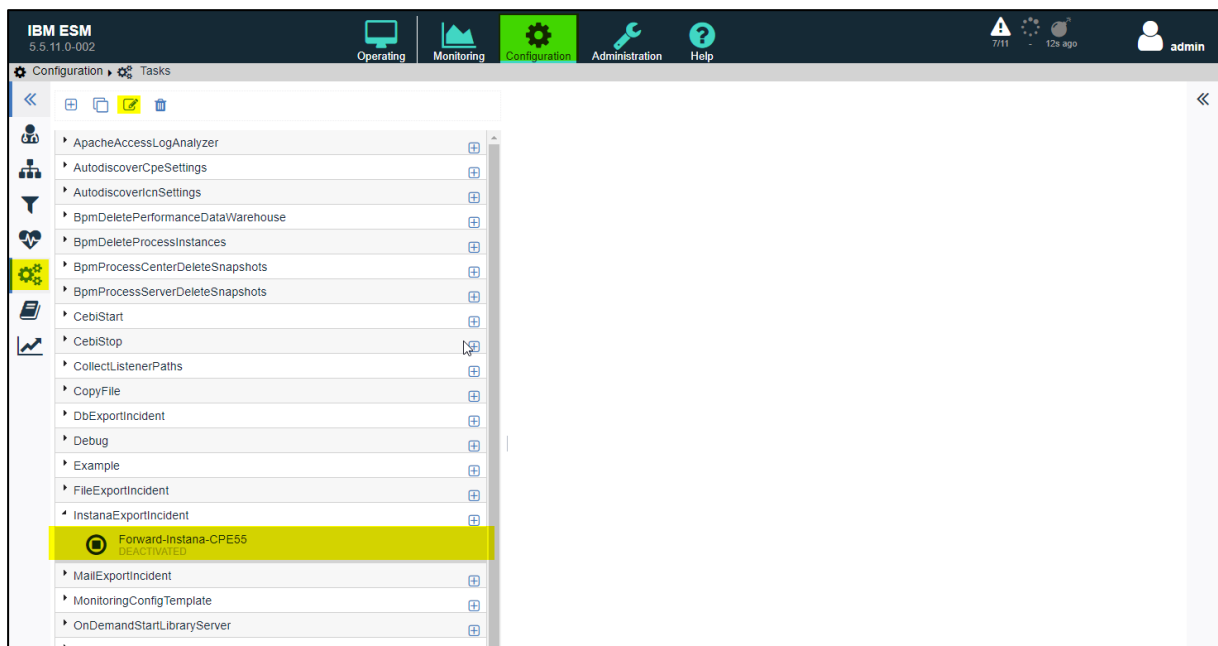
Switch to page two of the editor that opens using > or o and add a new trigger by clicking on the +.
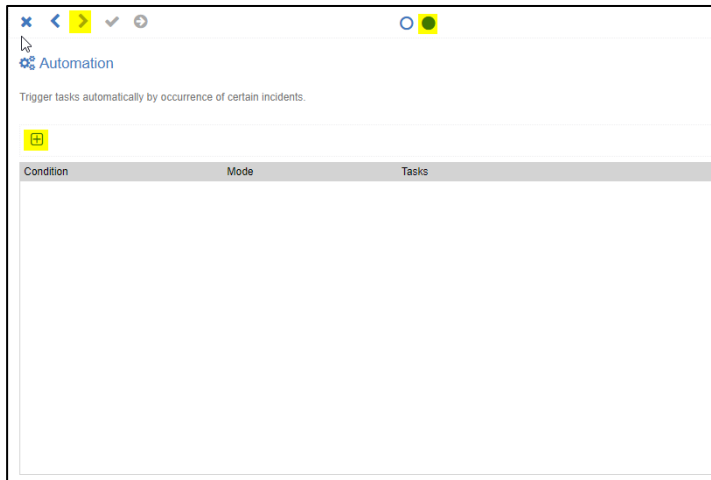
Adjust the trigger to read like this:

Condition:
As condition use Situation == XYZ where XYZ is any situation that you want to forward. You can add as many as you like here, just make sure these are the situations which monitor information on the system for which you trigger the task in this case. E.g. in the above task example the task will be executed on CPE55 System. So the probe for the situation getting forwarded here should also be executed on CPE55 system.

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.

Hint: You can copy an entry in the list of triggers by clicking on the copy button on the right and just select a new situation in the condition.

# 2b. Alternative way of triggering the task (Setup in situation)

In this case the trigger is defined within the situation setup and contains a severity condition. For each incident to be forwarded this must be done in the corresponding situation setup. As a simple example this is done with the "ObjectStoreLoadDocumentPerformance @ CPE55" situation here.

Note: During this setup a severity is used in the condition by default. If that is above HARMLESS, the events in Instana will not get updated with harmless information -> This can be a wished behavior.
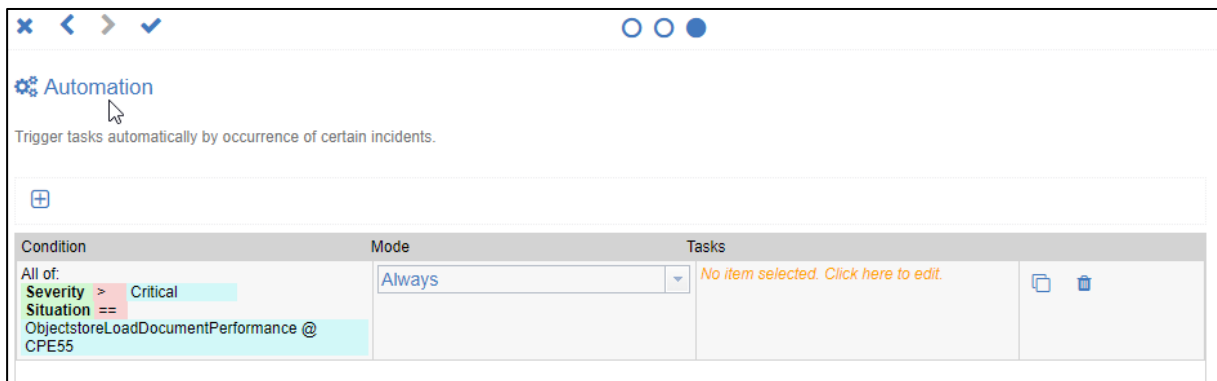
Select the Configuration Console and switch to the "Situation Groups" on the left. Open the situation editor by double clicking on the situation for which you want to add the trigger.
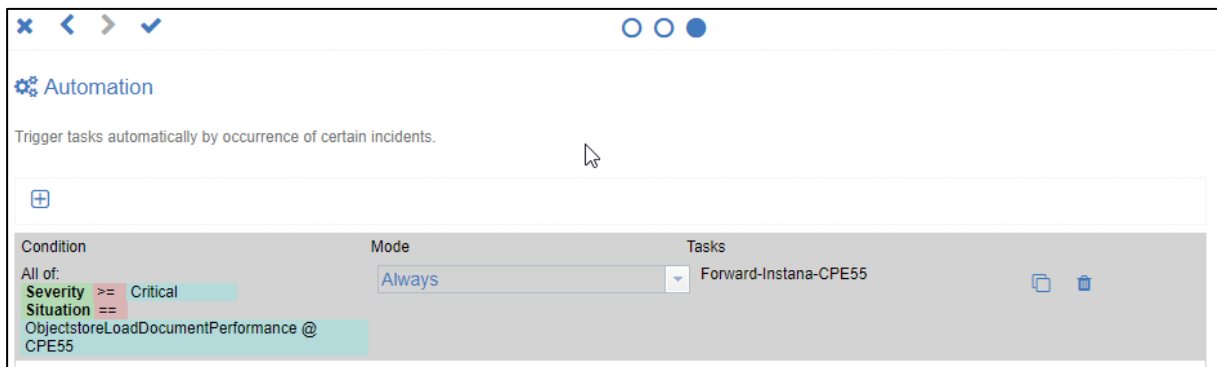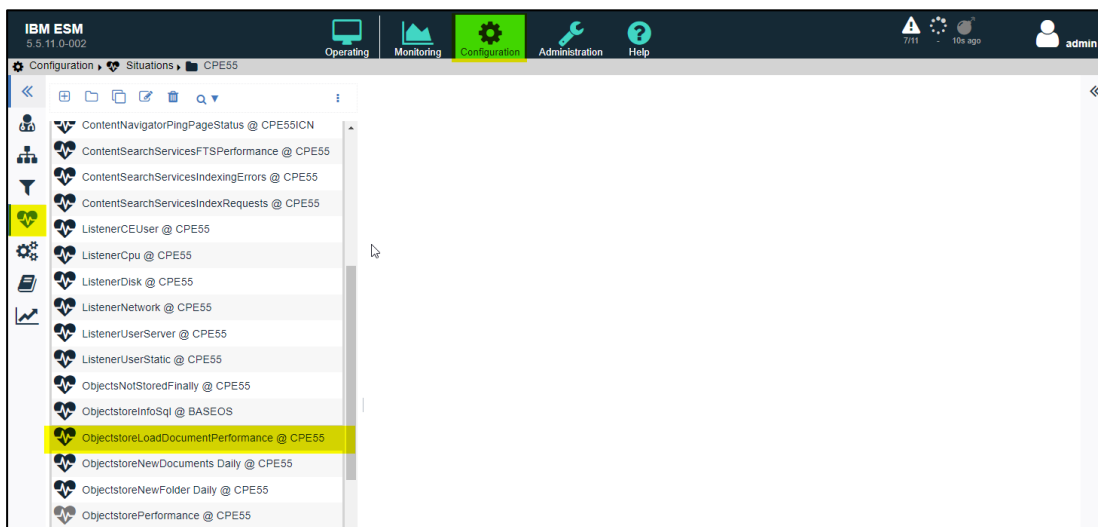

The editor will open and look like this:
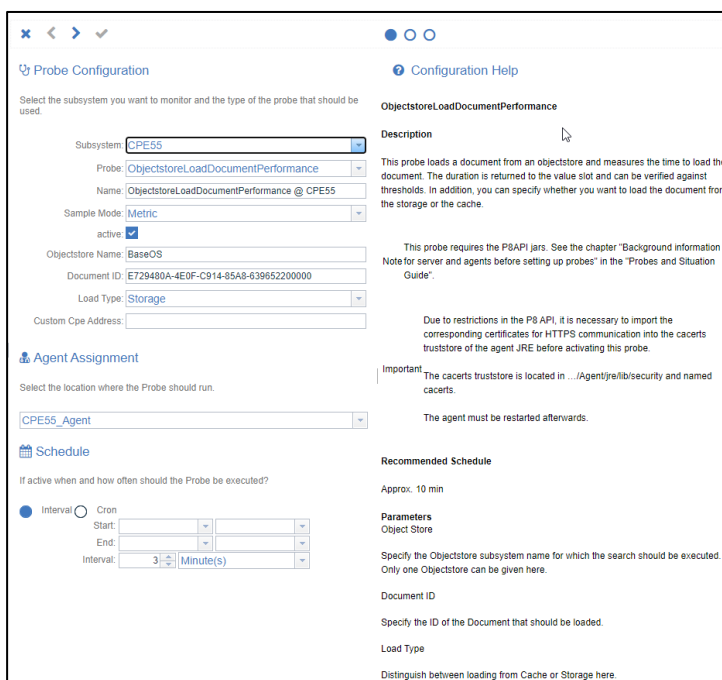
Switch to page 3 (Automation) of the editor. Per default no entry is given there. Click on the + to add a new automation task.

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.

Hint: You can also use the 2a procedure for this setup – just keep the severity in the condition.

3. Output in Instana

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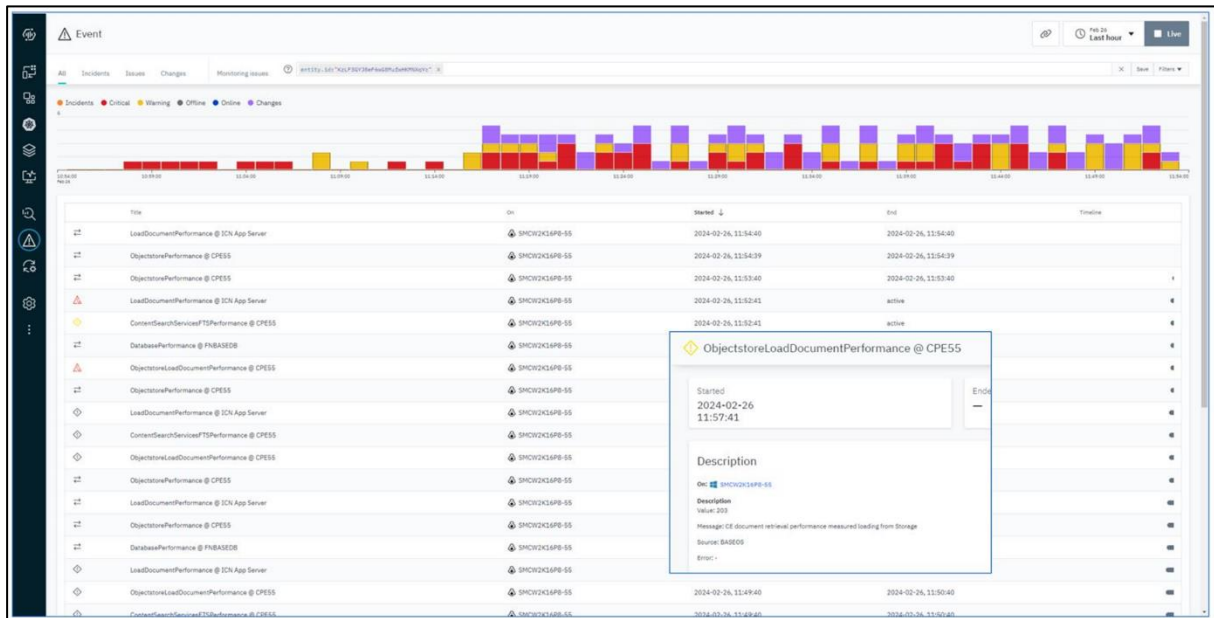
Contact Information

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

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