cockpit
IT Service Manager

Monitoring - External alert configuration

FAQ document

Table of contents

Introduction

I. Principles

The "external alerts" menu allows to receive and manage messages generated by third parties (equipment, applications, scripts, etc.) via different protocols:

- Sending emails
- Sending SNMP TRAPS
- Sending API messages

II. Objectives of the document

- To set up mailboxes.
- To set up engines to receive SNMP TRAPS.
- To set API access and explain how to inject a message.

Mailboxes

Menu: Monitoring > External alerts > Inboxes

Principe: Cockpit IT Service Manager regularly checks for the presence of new emails in a mailbox, each email matching the search criteria is used to generate an alert in the "Monitoring / External Alerts / Pending Alerts" menu.

Operation:

- On the first check (upon creation of the mailbox), all the emails for the day (day starting from 00:00) are reported.
- At the following checks, Cockpit IT Service Manager verifies the presence of new emails after the previous check.
- Reported emails are sent to pending alerts in the "External alerts" menu.
- The reported emails are not marked as read in the mailbox.
- When a mailbox is reactivated after a period of inactivity, all emails received during that period of inactivity are reported.

Main parameters	
Fields	**Information**
Organization	Select an organization: the alerts are displayed to the operators who access to the organization. Select “No organization”: the alerts are not associated to an organization, all the operators view the alerts.
Status	Unselected: emails are not uploaded Selected: emails are uploaded
Protocol	Selection of the protocol for connecting to the mailbox: POP3 POP3 (SSL) IMAP IMAP (SSL)
SHA-1 SSL certificate thumbprint	SHA-1 SSL certificate thumbprint. The certificate thumbprint must be filled in for self-signed or expired certificates.
Server	Mail server Example: pop.myserver.com
Port	Mail connection port
User / Password	Identifiers
Subject terms	Indicate the terms that will be searched for in the subject of the emails, only the emails containing these terms will generate an alert. For a distinct search on several terms, separate the terms by a "; ". Field empty: all emails are taken into account
Options	Select the options to activate them: Delete the emails loaded from the server Ignore messages marked as read

Menu management:

- Deleting a mailbox does not impact the generated alerts.
- Testing the manual connection to the mailbox does not affect the monitoring of emails, it just checks the connection availability.

SNMP TRAPS

Menu: Administration > Configuration > Engine

Principle: SNMP TRAPS can be sent to an engine (remote or local); all received TRAPS generate an alert in the "Monitoring / External alerts / Pending Alerts" menu.

Configuration: Select an engine, click on "Configure", go to the "Functional settings" tab, "Monitoring and Infrastructure" section:

- Status: Port listening status (active / inactive). When the status is inactive, no SNMP TRAP is loaded.
- Port: Listener port for receiving SNMP TRAPS (16100 by default). Ensure that equipment sending the SNMP TRAPS access the engine's port.
- Versions:
  - V1 / V2c: The "community string" is used for authentication for SNMPv1 and SNMPv2c. By convention, the devices send SNMP TRAPS using the "community string" "public" but it may be different, it is necessary to verify which "community string" is used by the SNMP agents sending the SNMP TRAPS.
  - V3: The SNMPv3 uses an authentication, fill in Protocols, Username and Authentifications fields.

Example:

It is possible to use an SNMP TRAP generation tool to check the configuration, for example SnmpTrapGen detailed in the link below:

https://snmpsoft.com/shell-tools/snmp-trap-gen/

Using the following command:

SnmpTrapGen.exe -r:127.0.0.1 -p:162 -t:10 -v:2c -c:"public" -to:.1.3.6.1.2.1.1.4.0

- "-r": IP address of the device
- "-p": port, by default SNMP TRAPS are sent on port 162
- "-v": version, by default version 1 is used
- "-t": timeout in seconds (1 - 600)
- "-c": community string, by default "public" is used, only applies to SNMP v1 / v2c
- "-to": OID sent by the SNMP TRAP

API

I. Principles

Messages can be sent to the portal API via an URL. Each message is injected into the external alert pending list.

II. API access

Menu: Monitoring > External alerts > API access

Configuration:

In order to create an API access, just click on "New".

- The API key is generated automatically.
- It is possible to associate an access to an organization, all received messages will be associated with this organization.
- Once the access is created, it is possible to perform a message injection test.

It is possible to modify an existing access by modifying the key, in this case it will be necessary to update the key of all the external elements which use the access.

III. Injecting a message

HTTPS protocol is used to inject a message via the API. Just call an URL with the correct parameters to inject a message.

When the message is injected, the API returns "OK".

URL parameters are listed in the following table.

Paramètres	
Paramètre	**Informations**
URL	Portal URL followed by « /alert-api » https://portal_adress/alert-api
key	API access key. Mandatory parameter.
message	Message to inject. Mandatory parameter. 255 characters maximum.
sender	To indicate the message source. Optional parameter. 255 characters maximum.
structure	Organization name linked to the message. Optional parameter. If the API access is already linked to an organization, this parameter will not be re-spected.
environment	Environment name linked to the message.

	Optional parameter.

Examples :

Inject « hello » message without parameters :

https://support.cockpit-itsm.com/alert-api?key=598ksoze5-35b8-4ef4-b280-a605faf04d91&message=hello

Inject « hello world! » message with the next parameters :

- Source : My script
- Organization : ALBATROS
- Environment : Production

https://support.cockpit-itsm.com/alert-api?key=598ksoze5-35b8-4ef4-b280-a605faf04d91&message=Hello%20world!&sender=My%20script&structure=ALBATROS&environment=Production

Document end