cockpit
IT Service Manager

Monitoring - Utilization guide

FAQ document

Table of contents

Introduction

I. Document objectives

- To process alerts collected by Cockpit IT Service Manager
- To process alerts pushed by third-party tools
- To check status of the engines
- To view equipment status

II. Definitions

Monitoring checks: Programs, commands, scripts, etc. running from a Cockpit IT Service Manager monitoring engine for the target equipment. The execution is triggered regularly according to a schedule. The result of the check is analyzed and can generate an alert for a target team based on conditions (alert thresholds).

Monitoring Alert: An alert message generated by a Cockpit IT Service Manager monitoring engine after a check is executed. Alerts are inserted into a queue and assigned to a target team.

External alert: An alert message generated by a third-party tool and inserted into a queue. The supported protocols are SNMP trap and emails. External alerts are not linked to a monitoring check or a team.

Overview

I. Dashboard

Menu: Monitoring > Overview > Dashboard

Objective: To provide a consolidated view of the monitoring indicators.

Operation:

- The data refreshes every minute.
- The number and status of the engines. Click on the boxes to display the list of engines:
  - The "Status" field indicates whether the engine is available (green dot = OK / red square = Not OK); an unavailable engine may no longer function, the controls, inventories and reports are not executed.
  - The "Last Signal" field indicates the date and time of the last synchronization between the engine and the portal. The engine synchronizes every 1 to 2 minutes.
- Number of alerts by criticality. Click on the boxes to display the list of alerts.
- Number of external alerts per protocol (Email, SNMP). Click on the boxes to display the list of alerts.

II. Views by structure and application

Menu: Monitoring > Overview > Structures / Monitoring > Overview > Applications

Objective: To view alert counters by element (structure, application, environment).

Operation:

- The number of alarms and the color of the highest criticality are indicated in the boxes.
- Alerts of "0 - Information" criticality do not change the color of the boxes which remain green.
- If all checks for an item are disabled, the corresponding box will remain green.
- Alerts in the lists are “Pending alerts”, the check may have changed status since.

III. Equipment

A. Status definitions

Equipment status definitions		
Status	**Color**	**Conditions**
Available	Green	The equipment availability check is successful. AND all the parents of the hierarchy on which it depends are available or not configured. AND the date of the check availability result is less than 10 minutes old.
Unavailable	Red	The availability check of the equipment is unsuccessful. AND the date of the check result is less than 10 minutes old.
Unreachable	Orange	At least one of the parent devices for this device is unavailable.

Unknown	Yellow	The date of the check availability result of the equipment is older than or equal to 10 minutes. AND the equipment does not have a parent OR the status of all parents is "Available".
Not configured	Gray	The equipment does not have an availability check selected.

> Important: When the status of a device is "unavailable", "unreachable" or "unknown", its checks - other than the availability check - as well as the checks of its child devices, are not executed.

B. Mapping

Menu: Monitoring > Overview > Equipment - Map

Objective: To view the status and dependencies of the equipment by structure.

Operation:

- The tree structure is established according to the equipment hierarchy.
- The color of the box of the structure is determined by the status of the devices, according to the following hierarchy:
    1. "Red": At least one device is unavailable
    2. "Orange": At least one device cannot be reached
    3. "Yellow": At least one device is unknown
    4. "Gray": At least one device does not have an availability check
    5. "Green": All devices have an availability check and are available

C. Status

Menu: Monitoring > Overview > Equipment - Status

Objective: To search for devices currently with "Unavailable", "Unreachable", "Unknown" or "Not configured" status.

Operation:

- The "Last availability check" field indicates the date and time of the last execution of the availability check for the device.
- The "Last known status" field indicates the status of the device during the last availability check.
- The "Current status" field indicates the status of the device when the menu is displayed.
- The "Last known status" and "Current status" fields may have different values.

  Example: In the case where the last availability check is successful (Last known status = Available) but is more than 10 minutes old (Current status = Unreachable). This case is possible if the parent of the device has an error, and thus the checks of the child devices are disabled.

I. Information on the alerts

A. List of alerts

Alerts are presented in the form of lists.
Each line corresponds to an alert with an execution counter. If a check generates a first alert, a row is added to the list, the counter is set to 1. If subsequent executions of the check still generate alerts no rows are added, the execution counter is simply incremented.
If a check passes from an "unsuccessful" status to a "successful" one and then back to an "unsuccessful" status, a new line is added to the list with a new counter.

B. Two types of alerts

1. Real alerts

Real alerts are generated as a result of a check that has completed successfully.
Example:

- A check of free disk space on the disk with a "if the free space is less than 10%" alert threshold.
- The check is executed and the free space on the monitored disk is 8%.
- An alert is generated. It concerns the disk. This is a real alert.

Real alerts can be acknowledged automatically when a check passes from an "unsuccessful" status to a "successful" one. This feature is optional.
In case of acknowledgment, the real alerts are kept in the history.

2. Parameter alerts

Parameter alerts are generated as a result of a check that has not completed successfully.
Example:

- A check of free disk space on the disk with a "if the free space is less than 10%" alert threshold.
- The check is executed, but the password to access the system is incorrect.
- An alert is generated. It concerns the access problem and not the free disk space. This is a parameter alert.

Parameter alerts are acknowledged automatically when a check passes from an "unsuccessful" status to a "successful" one.
In case of acknowledgment, the real alerts are kept in the history.
Parameter alerts are not taken into account by services forecast and calculation of availability rates.

C. Alert details

From the alert lists, it is possible to open the alert in order to display all information about it.

Main fields	
Field	**Information**
Alert counter	Number of "unsuccessful" executions
First / Last alert	Start and end dates of "unsuccessful" executions
Type of alert	Real / Parameter
Error code	Code and message returned by execution of the check
Check and execution schedule	Information about the check associated with the alert
Instructions	Information on the actions to be taken to deal with the alert
Logs	Result of each execution of the check Information collected on the target equipment
Manual test	Allows the check to be executed manually

II. Actions on the alerts

A. Acknowledge

- Send the alert from the menu “Alerts - New” to “Alerts - Acknowledge” menu.
- The acknowledgement date and identity of the operator making the acknowledgement are stored. A text message can be added to the alert when it is acknowledge.

B. Add a comment

- Add text to the “Comment” field of the alert for operators only.
- The comment is linked to the alert, if the alert is archived and a new alert appears, the comment will not be present.

C. Archive

- Deletes the alert from “Alerts - New” or “Alerts - Acknowledge” menu.
- Archived alerts are stored in the history with the archive date and identity of the operator making the archiving.

D. Edit

- Edits the check that generated the alert.
- A particular permission is required.

E. Execute

- Allows an immediate and one-off execution of the check.
- This execution does not affect the schedule of the check.

1. Instant controls

- An instant control raises a current value or status, examples:
  - Unix - Connection test
  - Unix - System Load

2. Differential controls

- Differential control checks what has changed since the last automatic (scheduled) execution of the control, the result is not always relevant for evaluating an alert. Examples of differential controls:
- When the differential check is run, the control period may be after the last alerts, these alerts will not raise up again, the check may be in success, but this does not mean that they are not to be processed. Thus the result of an immediate execution is not always relevant, examples:
  - Control with “Since the last check” parameter: When the check is run, the control period may be after the alerts, these alerts will not raise up again, but this does not mean that they are not to be processed.
  - “Log” type control: When a “log” type control such as “Unix - Log file” is run, the control period goes back to the last automatic execution of the control, the searched term may not be present and the control returns a success, but the term may well have been present before.

F. Create a ticket

- Creates a ticket with information about the alert.
- The ticket is created in the language of the structure and not in the language of the operator who creates the ticket.
- The created ticket is linked to the check and not to the alert. If a new alert is generated for this check, an indicator will signal that a ticket is already open for this check. When the ticket is closed, an option allows the pending alerts generated by the check to be acknowledged.
- Tickets can be created automatically for a check. If the ticket has been automatically created, if the status changes when the check is run (e.g. from "unsuccessful" to "successful"), the information is automatically added to the ticket.

G. Execute and acknowledge / archive

- These actions run the controls of selected alert individually before sending them to “Alerts - Acknowledged” or “Alerts - Archived” menu.
- The number of controls performed is limited for performance reasons.
- When an execution returns the message “Skipped – Execution impossible”, this means that the execution is technically possible, but that functionally it would not provide a relevant information

about the status of the control. It could be the case with differential controls, see the previous section “Execute”.

III. Pending alerts

Menu: Monitoring > Monitor > Alerts - New / Alerts - Acknowledge

Objective: To view the alerts pending processing by operator teams.

Operation:

- The data refreshes every minute. An option is available to disable automatic refresh.
- If no automatic acknowledgment is configured, the alerts remain pending until they are acknowledged manually. The "last alert date" is used to determine the age of an alert.
- A button allows simultaneous execution of several selected alerts and to acknowledge alerts whose check returns a "successful" status.

A. Alerts - New

Menu: Monitoring > Monitor > Alerts - New

Objective: To view the alerts pending processing and that have not seen by operator teams.

Operation:

- A “New” alert has not be seen by operator teams yet, the resolution is not in progress.
- When a check previously in success trigger an alert, the alert appears in this menu. The subsequent executions in error increment the first alert.
- The operator acknowledges the alert to indicate that it has been seen. The action “Execute and acknowledge” execute the selected checks and acknowledges alerts with a successful result.

B. Alerts - Acknowledge

Menu: Monitoring > Monitor > Alerts - Acknowledge

Objective: To view the alerts pending processing that have been acknowledged by operator teams.

Operation:

- An “Acknowledge” alert has be seen by operator teams and the resolution may in progress.
- When an alert is acknowledged, the subsequent executions in error increment the row in “Alerts - Acknowledge” menu.
- When the control of an acknowledged alert is back to success, then falls in error again, the new alert is added in the menu "Alerts - News" on a new line. The alerts already acknowledged do not change.

IV. Test alerts

Menu: Monitoring > Monitor > Alerts - Under test

Objective: To display the alerts pending processing by the operator teams, where the status of the check is "under test".

Operation:

- Checks whose status is "under test" run like other checks but generate alerts to a specific list. The goal is to run these checks without interfering with the production checks.
- During acknowledgment, alerts generated by "under test" checks are not retained in the history, they are deleted.
- When a check passes from "under test" to "active" status, any alerts present in the "Alerts under test" list migrate to the "Alerts - New / Acknowledge" lists.

V. Alert history

Menu: Monitoring > Monitor > Alerts - Archived

Objective: To search for archived alerts.

Operation:

- Archived alerts (real or parameter) are stored in the history with the archiving date and the identity of the operator who performed the archiving.
- The dates taken into account for the search are the dates of the alerts and not the dates of the archiving.
- Alerts acknowledged by the operator "ADM KOALY" are alerts that have been acknowledged automatically.

VI. Current status

Menu: Monitoring > Monitor > Checks - Current status

Objective: To display the checks – and not the alerts – when the last execution is unsuccessful. These checks are currently unsuccessful.

External alerts

I. Pending alerts

Menu: Monitoring > External alerts > Pending alerts

Objective: To display the pending external alerts.

Operation:

- "Email" alerts are emails collected in inboxes. Each line is an email.
- "SNMP" alerts are SNMP TRAPS sent to the monitoring engine by the devices. Each line is a TRAP for sent from an equipment with an OID. If several TRAPS are sent from the same equipment with the same OID, there is only one line in the list but the alert count is increased.
- "API" alerts are messages sent by external items (applications, scripts, etc.) to the API. Each line is a message.
- The data refreshes every minute. There is an option to disable automatic refresh.

Actions:

- Show details of the alert
- Acknowledge the alert
  - It is possible to add a comment when acknowledging.
  - The alert is kept in the history with the date of acknowledgment and the identity of the operator who acknowledged it.
- Create a ticket or add information to an existing ticket
    - Information about the alert is included in the ticket.

II. Alert history

Menu: Monitoring > External alerts > Alert history

Objective: Search for acknowledged alerts.

Operation:

- The dates taken into account for the search are the dates of the alerts and not the dates of the acknowledgments.

FAQ

A. Why does the "Execute" function not always appear in the context menu of an alert?

Some checks cannot be run manually if they were never run automatically. For example, for "Log file" type checks, manual execution of the check is based on the previous execution to verify changes in the log file, if this first execution has never occurred, the check cannot be started manually.

B. Why does the "Display graphic" feature only appear in the context menu of some alerts?

An option allows the execution results of certain checks to be stored (for example: the response time of a URL). If this option is enabled, the "Display graphic" functionality appears in the context menu of the alert.

C. What are the different return codes for the alerts?

List of alert return codes	
Code	**Message**
-1	UNDEFINED
0	SUCCESS
1	ERROR
100	INTERNAL_SERVER_ERROR
101	INTERNAL_SERVER_ERROR_CHECK_TYPE_MISMATCH
102	INTERNAL_SERVER_ERROR_MISSING_CHECK_REGISTRY
103	INTERNAL_SERVER_ERROR_MISSING_DP_REGISTRY
104	INTERNAL_SERVER_ERROR_MISSING_DATA_PROVIDER
105	INTERNAL_SERVER_ERROR_DATA_PROVIDER_NO_DATA
106	INTERNAL_SERVER_ERROR_DATA_PROVIDER_INVALID_DATA_TYPE
107	INTERNAL_SERVER_ERROR_DATA_PROVIDER_REQUEST_FAILURE
108	INTERNAL_SERVER_ERROR_NO_CHECK_EXECUTOR
109	INTERNAL_SERVER_ERROR_MISSING_BEAN
110	INTERNAL_SERVER_ERROR_EXCEPTION
1000	INVALID_RESULT
1001	RESULT_OUT_OF_RANGE
1002	COULD_NOT_EXTRACT_VALUE
1003	TIMED_OUT
1004	CANCELLED
1005	INTERRUPTED
1006	FAILURE

1007	NO_RESULT
1008	INVALID_CARDINALITY
1009	EMPTY_RESULT
1010	NO_SUCH_FUNCTION
1011	ILLEGAL_ARGUMENT
1012	EXCEPTION
1013	CONNECTION_ERROR
1014	QUERY_ERROR
1100	FILE_DOES_NOT_EXIST
1101	FILE_NOT_READABLE
1200	INVALID_EXIT_CODE
1300	ERROR_NO_SUCH_FUNCTION
1301	JCO_ERROR_MISSING_MANDATORY_PARAMETER

Document end