cockpit
IT Service Manager

Monitoring - Configuration guide

FAQ document

Table of contents

Introduction

I. Document objectives

- To set up monitoring checks
- To set up execution schedules
- To organize the hierarchy of checks
- To set up notifications
- To link the severity of checks to ticket priorities

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.

Principles

I. Operation

- Monitoring is done without installing an agent on the target servers.
- Access to equipment (servers, networks, etc.) and applications (databases, SAP instances, etc.) is configured in the "Infrastructure" module.
- The checks are configured in the "Monitoring" module of the Cockpit IT Service Manager portal.
- The checks are executed by the monitoring engines.
- A monitoring engine can monitor multiple devices and applications.
- Multiple monitoring engines can be used for a single Cockpit IT Service Manager portal.

II. Monitoring engines

A. Engine types

There are 2 types of engine:

- Local engines that connect directly to the database to exchange data and are used for Cockpit IT Service Manager "On Premise" instances.
- Remote engines that exchange data via the Cockpit IT Service Manager API:
  - The objective is to install a remote engine on a server on the same network as the equipment to be monitored. The engine connects locally to the equipment and applications to be monitored and sends the alerts to the portal via a secure connection.
  - The remote engine is autonomous; it executes the monitoring controls and sends the notifications.
  - The remote engine synchronizes with the portal regularly (every 1 to 2 minutes) to retrieve data (update of a check, of access, etc.) and to send other data (alerts, metrics, inventory, etc.).
  - The remote engine has an embedded database. If the connection to the API is temporarily unavailable, the data to be sent is stored in this database and synchronized as soon as the connection becomes operational again.

> Note: After creation or change of a check, it is necessary to wait for the engine to synchronize before testing the check.

B. Engine selection

It is possible to use several monitoring engines. This makes it possible to monitor equipment hosted on different physical sites or different networks. This also allows the load to be distributed across several engines when many devices are monitored.

The selection of the monitoring engine can be made:

- By structure (structure parameters): the engine is then proposed by default as the monitoring engine for all the equipment in the structure.
- By device (device parameters): it is possible to select a different engine from the default engine. All the checks for a particular device are executed by the same monitoring engine.

III. Infrastructure

A check must be associated with a device of the infrastructure.

The types of checks offered when editing differ according to:

- Type of equipment (Server, Network Element, etc.)
  Example: For "Network element" equipment, Windows type checks will not be offered.
- Operating system of the equipment (Windows, Linux, OS / 400, etc.)
  Example: Windows type checks will not be offered for a device with a Linux operating system.
- Applications associated with the equipment (SAP Instance, Database, etc.)
  Example: Creating an Oracle database on a device will show the "DB" and "Oracle DB" checks in the list of checks.

Check management

I. Definition

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).

II. Check parameters

Menu: Monitoring > Monitor > Management of checks

From the menu to create or edit a check.

The menu is divided into 3 tabs.

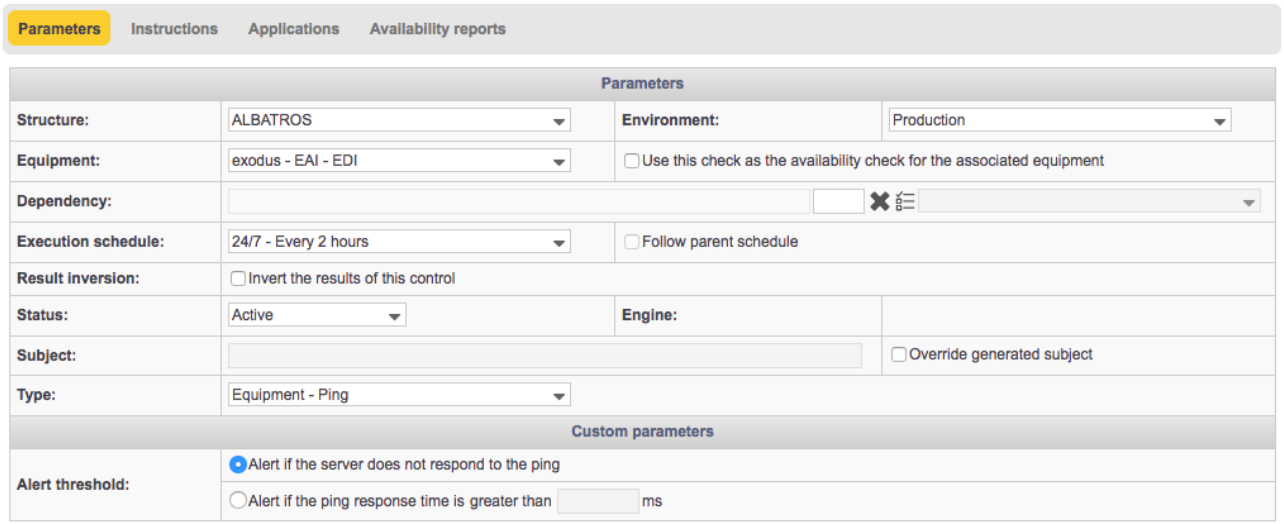
- Parameters
- Instructions
- Applications

Parameters

The menu is divided into 2 sections:

- A "Parameters" section that is common to all types of check.
- A "Custom parameters" section which is different depending on the type of check selected.

Overview:



Main parameters	
Fields	**Information**
Equipment (Mandatory)	Selection of the equipment on which the check will be carried out.
Availability check	Enable this option to have the status of the equipment match the status of the check:

	Successful check = equipment available Unsuccessful check = equipment unavailable Only one check per device can indicate the status of the equipment. Select a check which can distinguish the status of the equipment, examples: "Equip. - Ping » "Equip. - Port " "Web - HTTP request" etc. When equipment is unavailable, no check of this equipment is executed until the availability check is successful.
Dependence	Select the parent check: By directly indicating the ID of the check Or by selecting it from the checks of that equipment via the "Modify" button Select the condition for execution of the check: Execute if the parent's result is successful Execute if the parent's result is in unsuccessful For more details on parent checks, see the "Hierarchy" section.
Execution schedule (Mandatory)	Selection of the execution schedule The check will be executed at the times indicated in the schedule
Follow scheduling of the parent	Can only be selected if a parent check has been chosen. Selected: the check runs at the same frequency and after the parent check. Unselected: the check runs according to its own schedule. Example of this feature: Parent check: "Windows - Connection Test" runs every 10 minutes Child checks: - CPU, memory, disk, etc. Indicate that these follow the parent check, so only one connection to the equipment will be used for all these checks (efficiency gain and resource saving for the engine). - "Windows - File - Number" executed every day at 06:00: lets the check follow its own schedule. Note : When the equipment where the controls are deployed has the option “Cluster – This server is the logical node of a cluster” checked, each control generates a connection to the target equipment event if the control follows the parent's schedule. The objective is to always perform control over the equipment where the resources are.
Status (Mandatory)	Selects status of the check: "Active": the check is executed. "Under test": the check is executed but in case of error the alerts are visible in the menu "Test alerts" and the notifications are not applied. Child checks run normally. Use this feature when you want to observe the behavior of a check without interfering with production check alerts. "Inactive": No execution, no child check is executed.
Engine	Information field Indicates the monitoring engine entered in the equipment sheet
Object	Filled by default according to type of check and alert threshold. Check "Specific object" to customize this field. The object is part of the alert email body sent by the notifications.
Type (Mandatory)	Selection of the type of check to run. The list varies depending on the equipment selected.

Why assign a check to the availability status of a device?

When the check used to obtain the availability status of the equipment is unsuccessful (e.g. a ping on a server), none of the other checks for the equipment execute, thus avoiding the generation of many unnecessary alerts.

Equipment can also have a hierarchy, with parent and child equipment. When parent equipment is considered unavailable, the checks associated with child equipment are not performed.

A. Instructions

Main parameters	
Fields	**Information**
Team (Mandatory)	Selection of the team to receive the alerts. In case of double threshold this field can be found in the "Parameters" tab and a different team can be selected for each threshold.
Criticality (Mandatory)	Selection of the criticality of the alert: Information, Low, Medium, High, Extreme
Document related to the action	Selection of a reference document in the "Knowledge" module. The document must belong to the same structure as the check.
Document related to the escalation	Selection of a reference document in the "Knowledge" module. The document must belong to the same structure as the check.
Message	Inserted in emails sent by notifications and in tickets created from the alerts. In case of double threshold this field can be found in the "Parameters" tab and a different message can be entered for each threshold.
Notification	Selection of a notification and conditions for generation: For real alerts only Or for all alerts (real and parameter alerts) In case of double threshold this field can be found in the "Parameters" tab and a different notification can be selected for each threshold.
Comments	Visible at portal alert level. Not inserted in the emails sent by the notifications or the tickets created from the alerts.

B. Applications

- Allows selection of the applications affected by the status of the check.
- At least one application must be selected.

III. Actions related to the checks

List of actions	
Actions	**Information**
Display	Displays details of the check
Modify	Edits the check The Structure, ID, and Type of check are not editable
Copy	Copies the check and creates a new one, all fields are modifiable.

Delete	Deletes the check
Disable	Disables execution of the check and alls its children
Execute	Requests immediate execution of the check This execution does not affect the check's schedule
Scheduling information	Displays detailed information about: The characteristics of the check and the execution schedule Execution statistics (result of last execution, execution time, counters, etc.)
Open check audit	Allows all executions of a check to be viewed
Equipment information	Displays the sheet for the equipment to which the check is related

IV. Views by structure and application

Menu: Monitor > Configuration > View by equipment / Monitor > Configuration > View by application

Objectives: To display the checks by equipment and by application and to view the status of the checks.

A. Status of the checks

The status of the checks is indicated by 2 fields:

- Last message: Date and time of last execution of the check, there is no execution after this date.
- Error code:
  - 0 – Success
  - 1 – Error (real alert)
  - 2 – Temporary failure (parameter alert)

> Note: If these 2 fields are empty the check has never been executed.

B. View by equipment

- Select a structure, an "Environment > Type of equipment > Equipment" tree appears, navigate the tree to a device to display its checks.
- The "Type" field indicates the hierarchy of the checks. The types of checks are located under the parent check and offset to the right. Aligned check types have the same hierarchical level.

C. View by application

- Select a structure, the list of applications of the structure appears, click on an application to display all the checks related to this application.

> Note: Two checks of a single device related to different applications do not appear in the same view.

V. Deletion

It is possible to delete a check. All its alert history will also be deleted; however the tickets created for this check are kept.

Scheduling

I. Definition

The execution schedule defines when the monitoring checks must be executed; this must be created before the check.

A check can be associated directly with a schedule or can follow the schedule of the check on which it depends (parent).

The hierarchy of the checks does not affect their scheduling. For example:

- The parent check is run every 5 minutes except from 00:00 to 07:00.
- The child check is run every day at 05:00 if the status of the parent is success.
- The 2 checks will follow their respective schedule. The child check will run the parent check at 05:00 to ensure that its status is success.

Schedules are not impacted by the hierarchy of checks, for example:

- A period of inactivity in a continuous schedule does not stop the child checks.
- Parent and child checks may have different schedules.

The execution schedule can be multi-structured.

Continuous and weekly schedules are affected by holidays in the structure:

- Multi-structure scheduling takes into account holidays in the monitoring checks structure.
- When setting schedules, check the presence of holidays in the structure in order to predict the behavior of the check.

II. Settings

Menu: Monitor > Configuration > Schedules

A. General parameters

Parameters	
Fields	**Information**
Description (Mandatory)	Name of the schedule. Used to select it from a monitoring check.
Time zone (Mandatory)	The checks are executed at the times of the selected time zone. Selecting a different time zone from the default one does not affect the other schedules of the structure or the schedules of the child or parent checks.
Structures (Mandatory)	All structures: default value, the schedule can be used by all structures Selected structures: the schedule appears only for the structures selected.

B. Continuous scheduling

The continuous schedule executes the check according to:

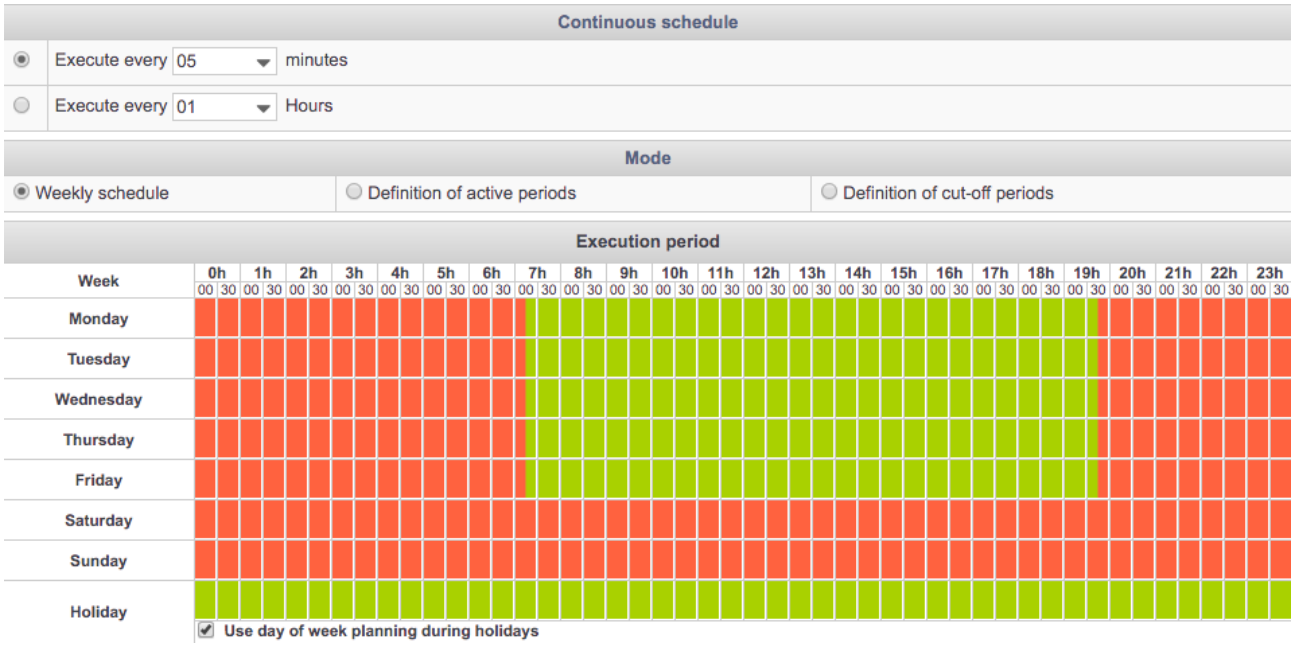
- A frequency, for example: every 5 minutes.
- A time slot, for example: every day from 06:00 to 18:00 except Saturdays and Sundays.

The reference execution (or first execution) is:

- After saving the check (after creation or modification).
- After the engine is restarted.

Parameters	
Fields	**Details**
Frequency	Every 5 to 55 minutes Or every 01/02/03/04/08/12 hours
Weekly scheduling	Click on the schedule to define the execution periods for the checks: In green: the schedule is active, the check is executed. In red: the schedule is inactive, the check is not executed. The granularity of the periods is in increments of 15 minutes, for example: 15:00 - 15:15 / 15:15 - 15:30, etc.
Using the daily schedule (holidays)	Selected: The check follows the daily schedule without taking into account the structure's holidays. Unselected: The check follows the "Holiday" line schedule during the structure's holidays.
Definition of active periods	The check is executed only at the indicated periods
Definition of inactive periods	The check is executed at all times except during the periods indicated

Overview:



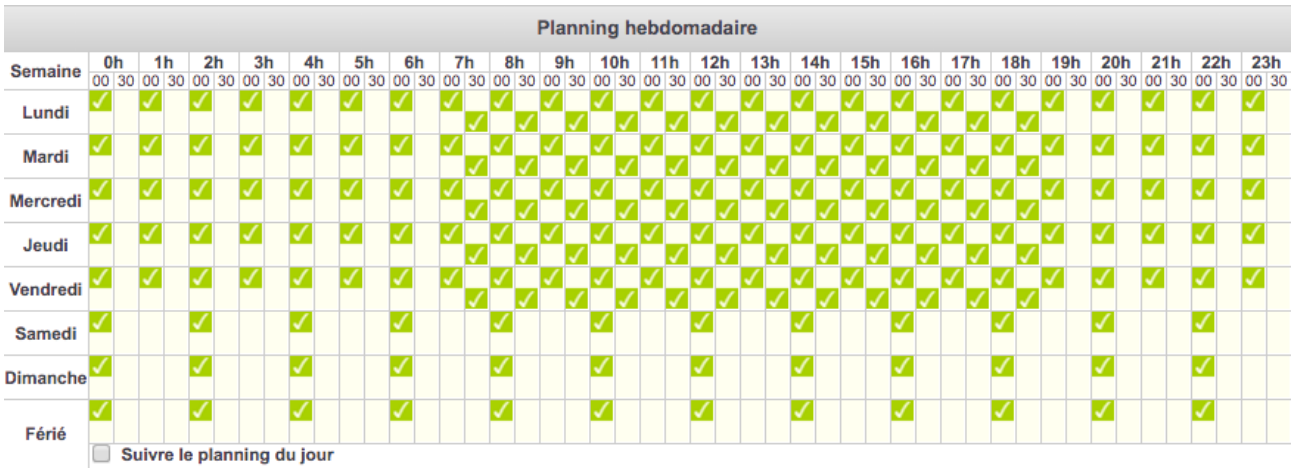
C. Weekly schedule

The weekly scheduling executes the check:

- At the times indicated by a green box, the granularity is 15 minutes, example: 15:00 / 15:15 / 15:30, etc.

- "Using the daily schedule" option:
  - Selected: The check follows the daily schedule without taking into account the structure's holidays.
  - Unselected: The check follows the "Holiday" line schedule during the structure's holidays.

Overview:



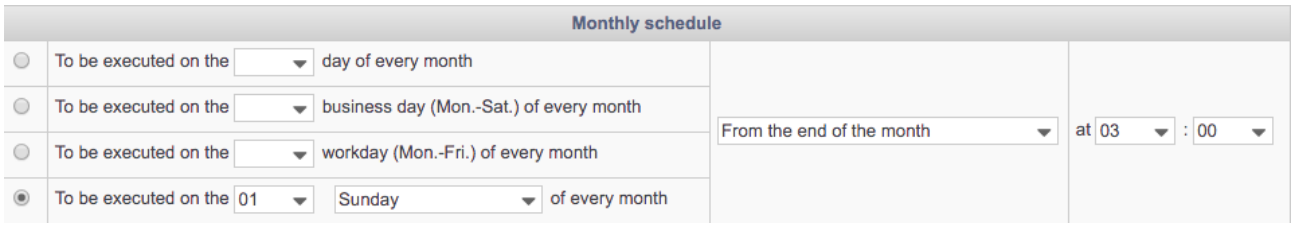
D. Monthly schedule

The monthly schedule performs the check every month at a fixed date and time:

- By selecting a calendar day (0 to 31)
- By selecting a business day (Monday to Saturday) or workday (Monday to Friday)
- By selecting a day of the week (Monday to Sunday)

> Note: as not all months have the same number of days or full weeks, select the option "From the end of the month" for all month end dates (last day of the month, last Sunday of each month, etc.).

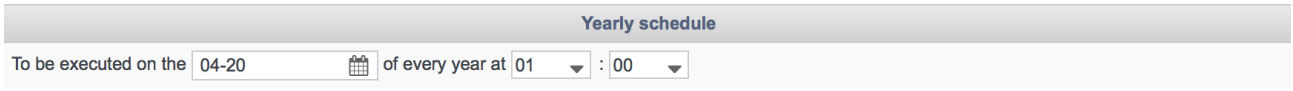
Overview:



E. Yearly schedule

The yearly schedule executes the check every year at a fixed date and time.

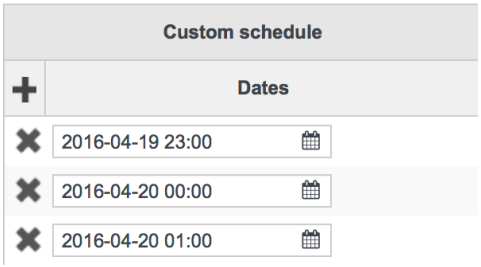
Overview:



F. Custom schedule

The custom schedule executes at the indicated dates and times, once these have passed the check is is no longer executed.

Overview:



III. Deletion

It is possible to delete a schedule, but first it is necessary to remove all the checks which use it. When the deletion is forced the checks are also deleted.

Check hierarchy

I. Definition

The hierarchy makes it possible to organize the checks in the form of a tree.

Each check can have:

- A single parent check
- Several children checks

The status of the parent check is a condition of the execution of its children checks:

- Check is inactive: all checks in this tree dependent on this check do not execute (even if they retain their own "active" status).
- Check is active: Child checks are set to execute according to the result of the parent check (Successful or Unsuccessful).

The hierarchical links between checks are limited to within the same device.

> Important: It is not mandatory to organize checks under a hierarchy for the operation of the checks, but is strongly recommended.

II. Settings

Menu: Monitoring > Monitor > Configuration > Hierarchy of the checks

Objective: To configure the hierarchy of checks within the devices

Operation:

The hierarchy of checks is presented in the form of a list, with each line corresponding to a check:

Details of the view	
Formats	**Details**
Offsets in the "ID" column	The ID column displays the checks tree. The IDs of the child checks are located under the parent check ID and offset to the right. The check IDs with the same offset are at the same hierarchical level.
The characters of the line are in normal font	The check is active
The characters of the line are in italic	The check is inactive
The check ID is green	The check runs if its check parent is successful. This is the most common use, for example: the check "DB - Connection Test" runs if the parent check "Equip. - Ping" is successful. If the ping is unsuccessful, there is no need to perform the children checks.
The check ID is orange	The check runs if its parent check is unsuccessful. More rarely used, this functionality can be useful in some spe-

	cial cases, for example with a clustered organization where processes can switch from one device to another: process check A depends on process check B, it runs if process B is in unsuccessful (absent or stopped).

Handling:

- The dependencies between the checks can be modified by dragging and dropping.
- All changes of dependency must be validated by the "Save" button
- Any changes of dependency can be canceled with the "Cancel" button
- All checks can be viewed and edited; if a check is modified and saved, any hierarchy changes made previously are canceled.

III. Good practices

In the majority of cases a tree of 2 or 3 levels is sufficient:

1. Ideally a device has a unique parent check at the root of the tree:
- When this root check is disabled, all monitoring of the device is lifted, without the need to disable other checks.
- In most cases the root check is used as the availability check for the equipment.

Depending on the options (ping permission, port opening, etc.) the most common root checks are: "Equip. - Ping", "Equip. - Port", connection test checks (OS, databases, etc.).

2. The second level contains the connections to the applications or operating systems: "Unix - Connection test", "Windows - Connection test", "DB - Connection test", "SAP - Connection test", "ESX - Connection Test", etc.
3. The third level contains the checks linked to the second level checks: the checks of a database will be children of the "DB - Connection test" check of this database, checks of the disks will be children of the "Windows - Connection Test" check, etc.

> Note: Not all checks fit this schema and can be placed elsewhere in the tree as required: "SNMP - Query", "Web - HTTP request", "Email receipt", etc.

Overview:

ID		Team	Type	Subject	Environment
▾ 292		SEED	Equipment - Ping		DEVELOPPEMENT
▾ 293		SEED	Windows - Connection test		DEVELOPPEMENT
294		SEED	Windows - Disk free space	All (< 10/5 %)	DEVELOPPEMENT
295		SEED	Windows - Swap usage	(> 30/40 %)	DEVELOPPEMENT
296		SEED	Windows - Processor usage	(> 80/90 %)	DEVELOPPEMENT
297		AVENGERS	Windows - Up-time	Reboot impromptu	DEVELOPPEMENT
▾ 298		SEED	Windows - Service status	SERVICEWINDOWS (Service Windows)	DEVELOPPEMENT
▾ 299		SEED	Windows - Process status	kompressor.exe (< 1)	DEVELOPPEMENT
512'		*SEED*	*Windows - Process status*	*orakeul (< 1)*	*DEVELOPPEMENT*

Notifications

I. Definition

Notifications are linked to the checks, they are optional and allow:

- messages to be sent (email, SMS) to Cockpit IT Service Manager users or to external recipients,
- automatic creation of an incident in the Cockpit IT Service Manager Ticket module,
- execution of a command from the monitoring engine (script, etc.) when a check runs or when it generates an alert.

II. Settings

Menu: Monitoring > Configuration > Notifications

Main parameters	
Fields	**Information**
Team (mandatory)	Target team.
Description (mandatory)	Will be displayed in drop-down menus.
Status (Email, SMS, Command)	Status of notification type (active / inactive). An inactive notification generates no messages.
Automatically create a ticket in the event of an alert (Ticket)	Automatic creation of an "incident" ticket when an alert is generated. Only real alerts trigger creation of a ticket, setup alerts do not. When a check changes status (unsuccessful / successful): the information is added to the ticket. When a check generates an error and a ticket is already open for this check, information is added to the ticket.
Addressees (Email)	To e-mail: e-mail addresses separated by "," or "; ". The field is 255 characters long. To an operator: Selects an operator belonging to the team, the email address is the one entered in the operator sheet. To all the team's operators: All the operators belonging to the selected team, the email addresses are those indicated in the operators' sheets.
Addressees (SMS)	To phone number: enter only one telephone number, the character "+" and spaces are accepted. To an operator: Operator belonging to the selected team, the number is the one entered in the "Mobile phone" field of the operator's sheet. To all the operators of the team: All the operators of the selected team, the numbers are those entered in the "Mobile phone" field of the operators' sheets.
Confidentiality (Email)	Selected: Email recipients are not visible.
Command	Used to enter the command to be executed on the monitoring engine.

	On a Windows engine the command is executed via the command prompt (cmd.exe). Example: Enter "C:\Path\script.bat" to run "script.bat". On a Linux engine the command is executed with the shell of the user starting the engine. If this user does not have a shell, the command is executed with the default Linux distribution shell. It is possible to use the alert information with variables in the format "${VARIABLE_NAME}".
Frequency (Email, SMS, Command)	With each execution of a check: The execution of all checks, whatever the result, generates a notification. Example (Emails): A check that runs every 5 minutes will send an e-mail every 5 minutes. Every time the check reports an alert: The execution of all checks that results in an error generates a notification. Example (Emails): If a check runs every 5 minutes and generates an error for one hour, a dozen emails will be sent. During the first alert reported by the check and upon return to a normal situation. Example: If a check runs every 5 minutes and generates an error for one hour, two emails will be sent: one to signal the raising of the alert, and one hour later a second to signal the return of a successful check.
Format (Email, SMS)	Allows to customize the format of the message sent by notification. It is possible to use the alert information with variables in the format "${VARIABLE_NAME}". Use the “Preview” button to preview the notification that will be sent.
Check status (Email, SMS, Command, Ticket)	Select the check status for which the notification is to be triggered: “Active” / “Testing” / “Active or Testing”.
Alert type (Email, SMS, Command, Ticket)	Select the alert type for which the notification is to be triggered: “Real” / “False” / “Real or settings”.
Alert counter (Email, SMS, Command, Ticket)	Number of consecutive alerts required to trigger notification (1 to 5).

Ticket properties

Menu: Monitoring > Configuration > Ticket priorities

Principle: To associate a ticket priority to each alert severity that will be used by default when creating a ticket from an alert.

The priorities for the "Incident" tickets must be configured before creating the link.

Settings:

- Only one management of priority can be created per structure.
- Creation: Click on "New", select the structure and then a priority per level.
- Edit: Click directly on the priority to edit it.

Document end