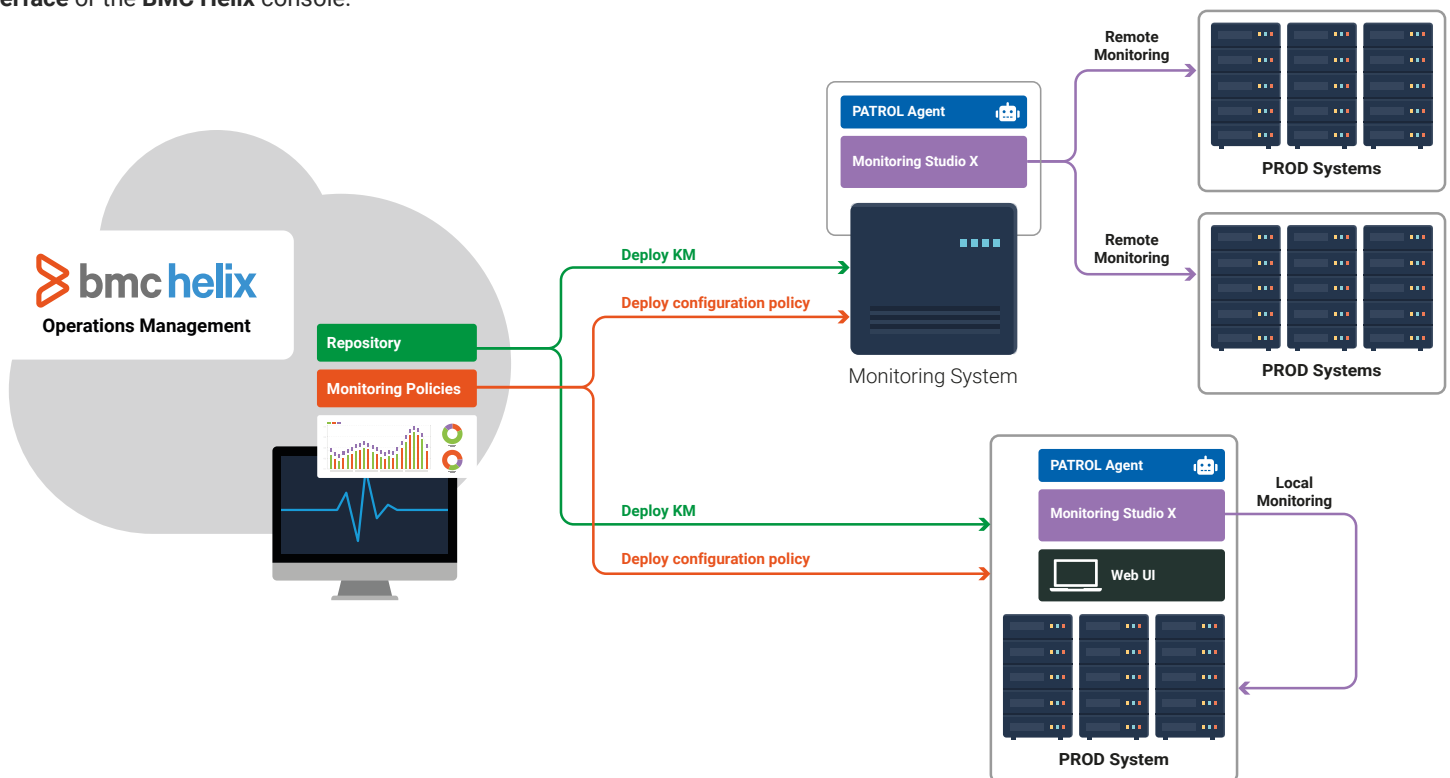


Monitoring Studio X

Monitoring Studio X simplifies agent management and troubleshooting in BMC Helix environments and extends monitoring to applications, systems, and devices without coding.

How Monitoring Studio X Works

Once **Monitoring Studio X** is installed on a server running a PATROL Agent, administrators can configure monitoring through the **Monitoring Studio X Web interface** or the **BMC Helix console**.



Administrators create a template containing the monitors required to discover, monitor, and collect information about the target technology, then apply it to one or more hosts. These monitors can execute commands, send HTTP requests, perform SNMP, SQL, WBEM, and WMI queries, or monitor processes, files, and file systems.

Once monitoring is enabled, collected metrics are available in the **BMC Helix console** and in the **Monitoring Studio X Web interface**.

The **Monitoring Studio X Web interface** also allows administrators to configure and troubleshoot the PATROL Agent, while the **REST API** provides programmatic access to the agent and its main components.

Requirements

- ✓ Any supported version of **BMC Helix Operations Management**
- ✓ A **Sentry Bundle for BMC Helix Operations Management** license
- ✓ Access to **BMC Helix Operations Management** with **Tenant Administrator** rights
- ✓ Java Runtime Environment (JRE) 1.8 or higher, installed on the server running the PATROL Agent
- ✓ Network access from the PATROL Agent to the target systems, with the credentials required by the selected monitors

Monitoring Capabilities

Basic Monitors

File System

- Monitor file system usage and growth
- Report on the available capacity, the percentage of available Inodes, and the consumed capacity growth (speed and percentage)

Process

- Verify the presence of processes on:
 - Windows
 - UNIX
 - Linux
- Verify the:
 - number of processes, handles, page faults, threads
 - page file used by the process
 - processor time
 - process status
 - working set

SNMP Trap

- Listen for SNMP traps
- Be informed when SNMP Trap is received
- Report on the number of matching SNMP traps

Content-Parsing Monitors

String Search

Search for a specific string in the information sources previously configured (flat or log files, output of a Web request or a database query, OID content, etc.)

Numeric Value Extraction

Extract a number from the information sources previously configured.

Windows Events

- Monitor Windows Event logs posted by your technology
- Report on the number and rate of matching Windows events
- List all matching events

Windows Performance Counter

- Monitor any commercial Windows based technology or any custom technology relying on a Windows based middleware
- Collect information about objects (processors, threads, processes, memory, etc.) present on a Windows server

Windows Service

- Monitor Windows services
- Verify their status and details

Value Map

Extract values from result outputs generated by other Monitors and map up to 25 of these values to user-defined statuses.

Dynamic Objects

Dynamically create Monitor objects based on the Result generated by a Monitor with Content and create an instance for each line found in the Result parameter

Monitors with Content*

Command Line

- Execute commands and scripts on:
 - Windows
 - UNIX
 - Linux systems
- Analyze their output
- Verify their execution time and status

Database Query (SQL)

- Execute SQL queries on:
 - Microsoft SQL Server
 - MySQL Server
 - Oracle Database server
 - PostgreSQL databases
- Analyze their output
- Verify their execution time and status

File

- Monitor log and flat files
- Keep an eye on their content, growth, and timestamp
- Be informed when critical files go missing

Folder

- Monitor folders usage, size, growth, and flow
- Be informed when folders go missing
- Verify the age of the newest and oldest file

HTTP Request

- Send HTTP requests to Web servers (HTTP GET, HTTP POST, or Web service methods)
- Specify the information to be retrieved from the Web page
- Analyze HTTP requests output
- Verify their execution time and status

Nagios Plugin

- Integrate and monitor Nagios Plugins execution results directly in BMC Helix Operations Management
- Import an entire Nagios configuration and extend your monitoring experience in a few clicks

Parameter Combination

- Monitor all the KMs loaded in the PATROL Console
- Extract parameters' values, compute them, and perform additional operations (units conversion, correlation, etc.)

PSL Script

- Run any PSL command on the local PATROL Agent system
- Analyze their output
- Verify their execution time and status

SNMP Polling

- Poll SNMP agents and retrieve data from single OIDs or SNMP tables
- Verify execution time and status

WBEM Query

- Execute WBEM queries on a system
- Analyze their output
- Verify their execution time and status

WMI Query

- Execute WMI queries on a system
- Analyze their output
- Verify their execution time and status

* The results obtained with the Monitors with Content can be analyzed with Content-Parsing Monitors



About Sentry Software

Sentry Software develops solutions that extend BMC Helix with deep visibility into hardware, storage, and custom technologies. Organizations across industries rely on Sentry Software to monitor heterogeneous infrastructure, optimize storage resources, and reduce operational complexity. Learn more: sentrysoftware.com



About BMC Helix

BMC Helix is an enterprise software company specializing in IT service and operations management. Its solutions help organizations manage IT services, monitor complex environments, automate workflows, and use AIOps and agentic AI to improve operational efficiency and service availability. Learn more: helixops.ai