

MoniK

Monitoring Kondor+

Product Description



May 20, 2011

Table of Content

1. OVERVIEW.....	3
1.1. Context.....	3
1.2. Readership	3
1.3. Executive summary.....	3
2. SUPERVISION IN REAL-TIME	5
2.1. Overall Description.....	5
2.2. Indicators	5
2.3. Business & Technical Processes	6
2.4. Alerts	7
3. LOGGING, INCIDENT ANALYSIS & REPORTING	7
4. ACTION AUTOMATION.....	9
5. ADVANCED GUI BUILDER.....	9
6. ARCHITECTURE & INTEGRATION	10
7. USAGE SCENARIOS	11
7.1. Deposit Position Failure.....	11
7.2. Back Office system not receiving trades.....	11
7.3. Kondor+ Slowing Down.....	12
7.4. Abnormal K+ Night Batch Duration.....	12
8. ROLES & SECURITY.....	12

1. *OVERVIEW*

1.1. *Context*

Kondor+ implementations are in general core to the activity of the organisation that uses it. However, the software has very limited functionality to monitor its status, understand its state, alert support teams in case of a problem, and provide them with all diagnostic information and most common remediation actions.

Of course, most organizations as a result have implemented solutions. Some rely on Technical Monitoring, which effectively links to low level indicators.

Few have implemented Business Activity Monitoring, and most of those that have, have not done it in a manner that deals with the system availability, but rather with the end result of the processes that the system supports, mostly towards Back Office operations, where manual processes can alleviate system unavailability.

Fewer still have found the budget to implement Business Services Monitoring (BSM).

Of course, as this requires mapping business processes all the way down to infrastructure, it represents a substantial effort, in a field too young to demonstrate return of investment.

But this begs the same question that initially prompted the purchase of a package rather than the internal development of the system: **shouldn't there be a standard solution to this problem, which can respond not only to your problem, but to the problem of the Kondor+ community as a whole?**

At 2LA, from our experience with the community, the organization of the yearly Kondor+ User Group, we have considered this need, and invested to provide an answer.

This document intends to present our solution, what it can do for you, how it can support you and free you from incident management to focus on problem management, capacity planning, or projects.

1.2. *Readership*

This document is intended for people who are effectively performing day to day support of a Kondor+ platform, and their managers.

Support Analyst expertise varies from application knowledge, database administrators and system administrators. Management varies from Support Management, Operation Management, and Application Management.

You do not need to know all aspects, functional, applicative and technical to read this document. That is the knowledge we have put in the software, to support you, in a way that makes it easy to understand and learn, so that using it should also make you more knowledgeable.

1.3. *Executive summary*

A Monitoring & Supervision system is used through the incident management process.

From a functionality perspective, we believe that such a product must demonstrate the following elements, and as such we have implemented:

- A wide variety of indicators at technical, application and business process level

This is important for several reasons: it allows defining the system behaviour as finely as possible, and become proactive, i.e. addressing issues before they have a business impact; it also helps in the diagnostic, making it faster to determine the extent of the problem and the system status to decide on the best remediation.

- User Interface

The user interface is a key element of the efficiency of the monitoring package; it must be accessible even remotely, have the information structured in a way that facilitates discovery of an issue, analysis of the system status, and diagnostic.

- A very flexible alerting mechanism

Alerts correspond not to the default implementation of the system, but the specificity of your implementation. It must be possible for you to define these alerts very precisely to reflect what abnormal system behaviour is and select the appropriate communication medium.

- Logging

During an issue, the support team is focused on restoring the system to acceptable operating parameters. However, once the issue is resolved, it is important to be able to revisit all the indicators, to conduct an appropriate post mortem that may uncover underlying issues, or feed problem root cause analysis. This relies on the fact that all values are logged with the right time stamp, allowing the review the situation as it happened.

- Incident Analysis & Reporting

It is important to produce accurate and effective communication about the system availability. Our solution allows this through a very flexible incident analysis and reporting module, where internally the system behaviour can be graphed over a period. Additionally, this analysis and reporting can be exported in Excel format to be included in your standard operational reporting.

- Standard remediation actions automation

During a crisis, reducing the operational risk is crucial, and having implemented most standard remediation actions helps tremendously. However it is important, it is not a fixed set, but an extensible one that can be applied to your implementation.

- Customisation and integration

We believe a good solution must be effective from the beginning, with its default configuration, and little configuration. However, each and every Kondor+ installation is unique, and in order to grow the solution must be flexible and allow customization of all the above elements.

2. SUPERVISION IN REAL-TIME

2.1. Overall Description

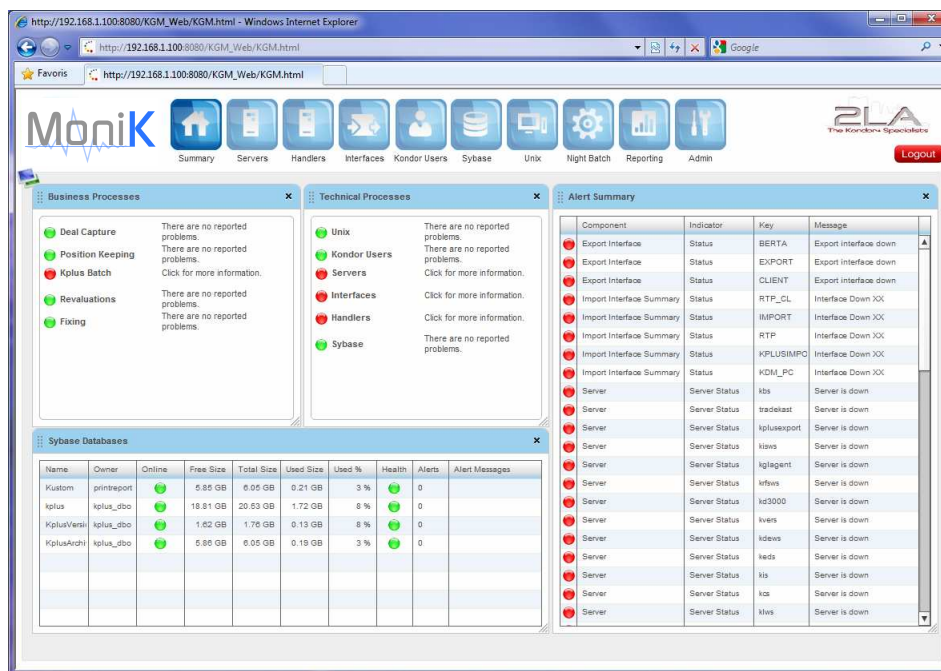
The Kondor+ world relies on the following components:

- Kondor+ Servers & Handlers
- Kondor+ Interfaces (incoming and outgoing)
- Kondor+ Users
- UNIX & Sybase
- Kondor+ Night Batch

where each has different characteristics.

A lot of the efficiency of the monitoring solution is the possibility for the interface to present the information in a manner that allows the support engineers to quickly assess the system status and diagnose the issue.

The first page should be the most important, and should concentrate all summary information.



As we have the experience of many Kondor+ implementations, we have implemented a default solution, but more importantly, we have made the user interface fully configurable, so that support analysts can create tailor made pages that make sense.

2.2. Indicators

There are two types of indicators: simple indicators, which reflect the monitoring of single value linked to a component, and synthetic indicators, that represent the combination of simple indicators.

Clicking on a specific indicator always provide a drill down, either to sub-indicators, if the indicator is synthetic, or to specific detailed information in a dedicated information pane.

The following table gives examples of areas and indicators for the monitoring of the Kondor+ world components:

Components	Areas & Features	Examples of indicators
Kondor+ Servers & Handlers	Hosts, Server list, Server parameters	Health, CPU, memory usage
Kondor+ Interfaces	Import & Export interfaces, interface queues, Trade workflow	Interface availability, waiting transactions, trades received by external systems
Kondor+ Users	List of users, associated Kondor+ processes	Number of K+ processes for a given user, memory and CPU used by this user
Unix	Hosts, disks partitions, processes	Availability, CPU, disk space, memory used
Sybase	Sybase setup, databases, processes	Database availabilities, number of used connections, available disk space per Kondor+ database
Kondor+ Night batch	Night batch status, job details, historical executions	Batch duration, average duration (overall and per job), errors, warnings

These can be combined to produce high level synthetic indicators from a business and a technical point of view.

2.3. Business & Technical Processes

The Business and Technical Processes, also called Services, are the combination of lower level indicators like Kondor+ servers, handlers, Sybase and UNIX processes, or interfaces.

The software by default comes preconfigured with some Business & Technical processes aggregating indicators and presented in the snapshot below:



The green light means that the Process is fully up and running whereas the red light warns that the Service is down.

Among the above Business Processes, here is the detail of the first two:

Deal Capture	Position Keeping
KMS server	Handlers
Sybase	KVS
UNIX	KRS
Kondor+ Licensing server (els server)	Sybase
	UNIX

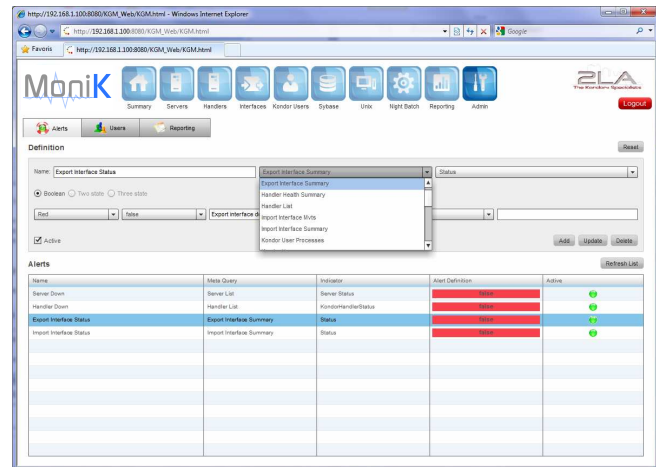
Additionally, this configuration can be modified, or even new business processes can be defined. This is for example very useful to configure monitoring of an End of Day process.

2.4. Alerts

It is key to implement versatility of alerts, of course to report efficiently system issues, but also to ensure not creating “false negative”, where alerts are raised when the system is perfectly fine.

As presented above, the software implements class of values, as varied as “Export Interfaces Summary”, “Kondor Users”, or “Sybase Databases”, but also measures and records the associated indicators.

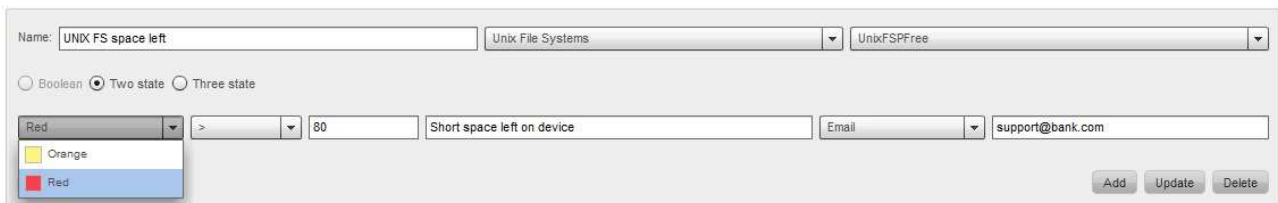
For example, for Unix Processes, some of the indicators are, the number of CPU, the amount of memory used, the percentage of memory used, the CPU used over a past period.



Alerts can be defined using a combination of tests on these values to define a Red or Orange status. Alerts can be Boolean if the value is Boolean, can use one or two event limits to define ranged alerts.

Ranges are defined using standard comparison operators ($>$, $<$, \leq , \geq , $=$).

Example: on the UNIX system, if the disk space used on a device is over 80 %, then we want an alert to be triggered and an email to be sent:



It is crucial that once alerts are raised, the information reaches supervising staff. To do this, a range of communication mechanism are used throughout organizations, and we have deemed important to implement the most common, SMS, email, but also email where a standard report is attached to provide already a view of the system status.

3. LOGGING, INCIDENT ANALYSIS & REPORTING

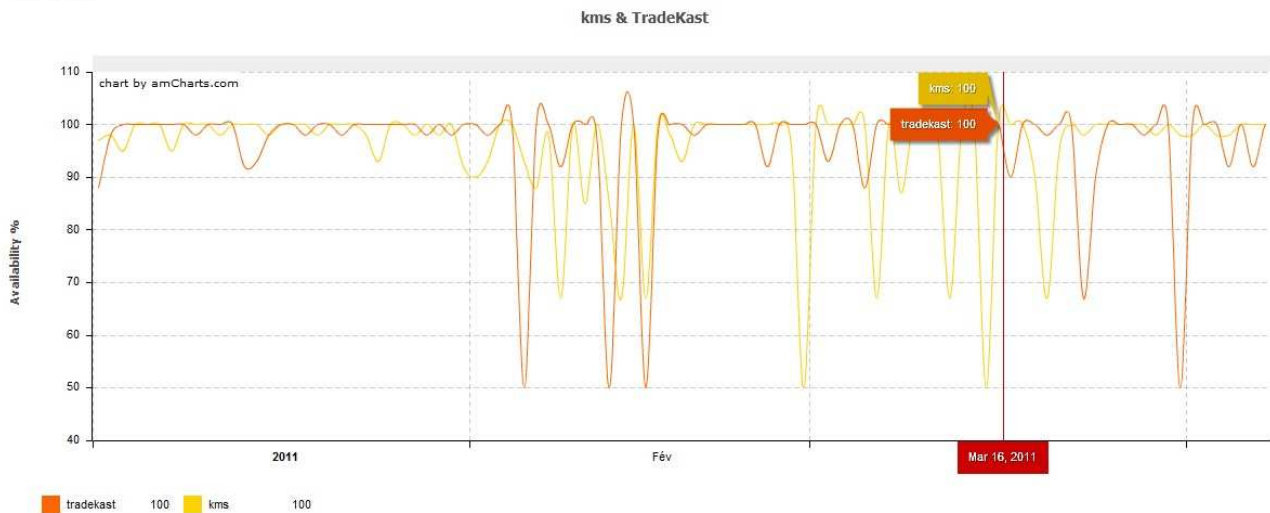
A very important feature of a Monitoring system is to record the exact sequence of events that led to the system issue.

This logging of events and actions must be exploitable immediately by the support analysis, and is a very important tool in the incident analysis, allowing validating hypothesis of root causes.

This analysis requires reporting the raw data, but also graphing it in simple modes, combining several indicators, displaying correlation.

Once the issue is resolved, the logging and reporting is useful “post-mortem” to perform problem analysis, and should also be available to be aggregated in standard operation reports, such as availability report, incident report or utilisation report.

Report Preview



The standard implementation comes with the following reports as standard (non-exhaustive list):

Components	Series	Filtering
Kondor+ Servers & Handlers	Number of start-ups, Downtime, Uptime, Availability (%), CPU (%), Memory (%)	All K+ servers & handlers
Kondor+ Interfaces	Number of start-ups, Downtime, Uptime, Availability (%), Number of processed movements, Waiting movements, Number of acknowledged movements	All Import & Export interfaces
Kondor+ Users	CPU (%), Memory (%)	All Kondor+ users
Unix	Availability, CPU usage (%), Memory usage (%), Disk space used (%), Disk space left (%)	All partitions
Sybase	Downtime, Uptime, Availability (%), Database space used (%), Database space left (%)	All databases
Kondor+ Night batch	Duration, Number of failed jobs, Number of errors, Number of warnings, Row processed	All Kondor+ jobs

When a report is selected, it can be manipulated; Indicator classes and the series, i.e. the indicator sought, can be selected as well as the reporting period but also a graph type, such as line or bar chart.

As presented above, the report is presented in a graphical format, but the data can also be extracted in an *Excel* format, to be incorporated in your standard operational reporting.

4. ACTION AUTOMATION

It is during the stress of a production incident that most errors occur in executing remediation actions. As such, we believe it is capital to script as much as possible the actions so they can be executed under stress without any risk of error.

For the Kondor+ Servers & Handlers, we have implemented a range of actions allowing to “start” or “stop” them but also to access to the corresponding parameter and log files. The parameter files can also be amended via our solution.

Server	Status	Health	CPU	Mem	Started At	Host	Alerts	Alert Messages	logfile	params
<input checked="" type="checkbox"/>	kms	●	0 %	1 %	08/04/2011 03:33	THOR	0		logfile	params
<input type="checkbox"/>	tradekast	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kols	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kplusexport	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kiws	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kglagent	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	krfws	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kd3000	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kvers	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kdevs	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	keds	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kis	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kcs	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kiws	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kbs	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kctds	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kpsclient	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kts	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kps	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kfis	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kconsos	●	0 %	0 %			1	Server is down	logfile	params
<input type="checkbox"/>	kts	●	0 %	0 %			1	Server is down	logfile	params

5. ADVANCED GUI BUILDER

The Graphical User Interface is based on the concept of workspace. The banner on the top lists all the workspaces available:

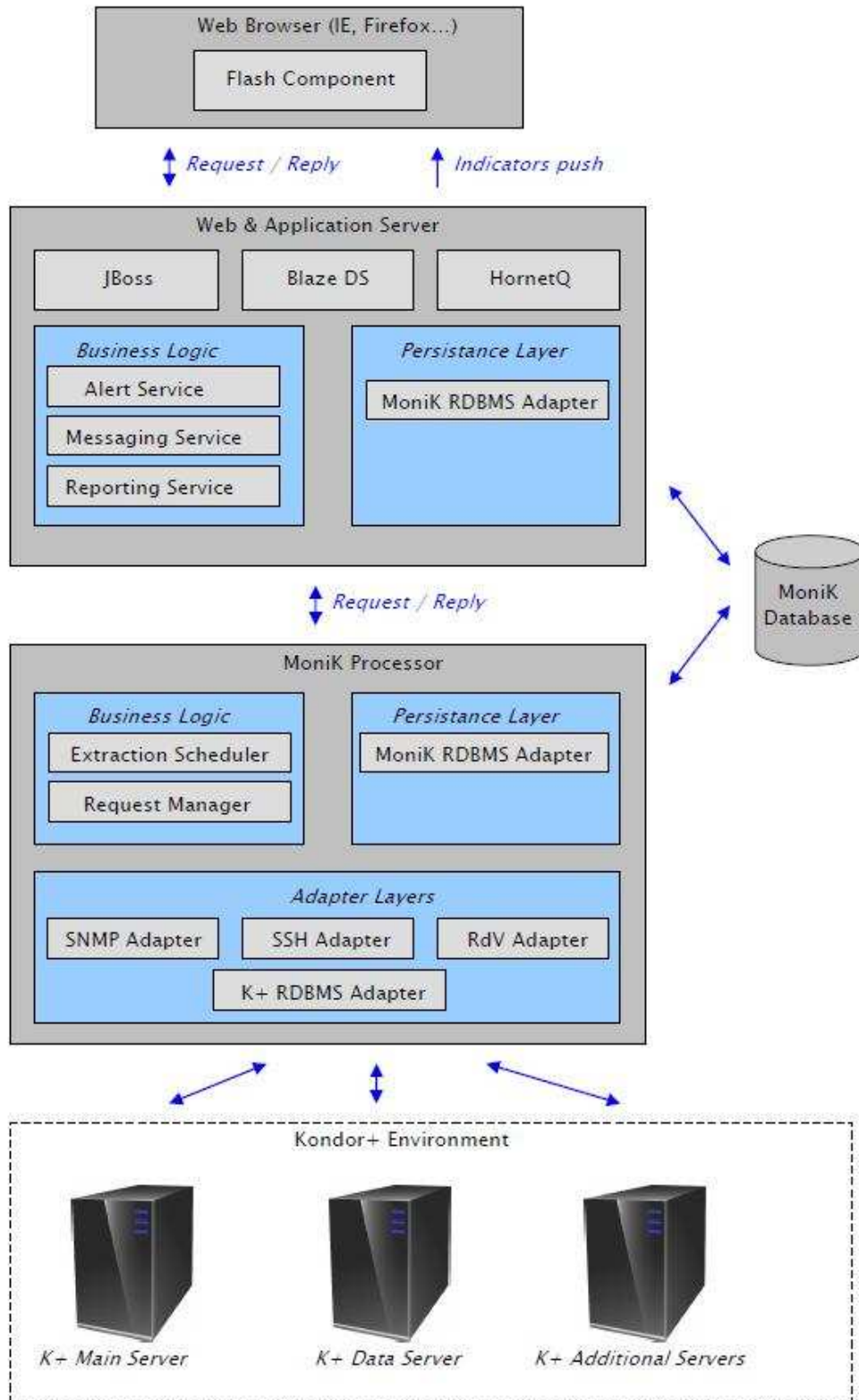


Each of these workspaces is configurable per user, in the sense that widgets can be removed from a workspace, new one can be added, they can be freely moved on the workspace, and different views can be combined using the workspace builder.

Each of the small windows in a workspace is fully resizable, new can be added on the page.

6. ARCHITECTURE & INTEGRATION

Our solution relies on the following architecture where any communication between all MoniK modules is encrypted.



As mentioned before, many organisations have implemented technical monitoring solutions, including overnight operator teams, and any monitoring solution must allow leveraging this.

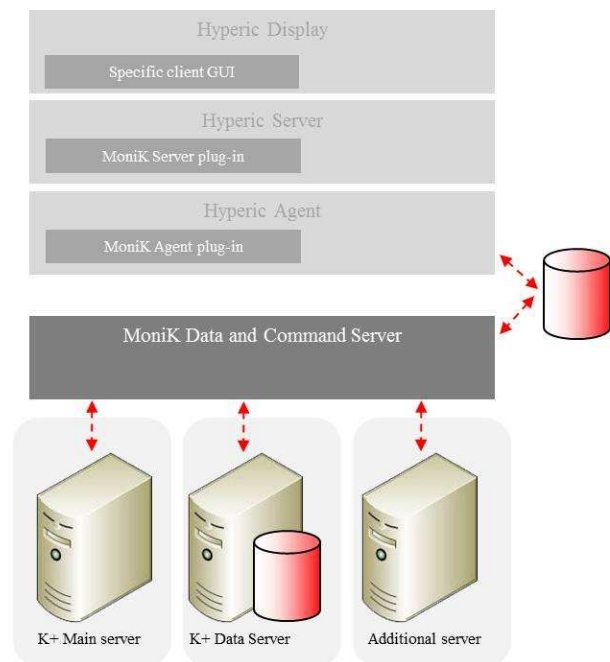
Through its architecture, our solution is interoperable with most market solutions, which will result in surveillance teams being able to capture, report and escalate on alerts you have established, as well as the application reporting on all indicators monitored by the standard solution. Below is an example of integration with a market solution.

Hyperic Display is used to surface all indicators and Alerts, possibly with a specific GUI for Kondor+ parameters.

The Hyperic Server has a specific plug-in, allowing it to retrieve and exploit all Kondor+ indicators and alerts.

These are extracted by a specific Hyperic Agent, linked through our database of indicators and alerts.

MoniK performs the indicators capture and surveillance.



7. USAGE SCENARIOS

The following sub-sections aim at providing examples of issues occurring in Production and how our solution helps in:

- saving time in isolating the issue and its cause
- preventing issues before they happen and they have an impact on the end users

7.1. Deposit Position Failure

Monitoring: the “Position Keeping” and “Handlers” lights are red in the Summary workspace.

Alert: a standard alert is defined to track a server or handler failure.

Diagnostic: Near the “Handlers” light, you can see an alert message telling you that the Deposit Position Handler is down. Click on one of these red lights which will bring you top the Handlers workspace. You can see that the *kdeposithdl* status is red with an alert message stating that it is down. Click on the “LogFile” button to investigate the issue.

Remediation: you can modify the handler param file if necessary by clicking on the “Params” button and launch it using the “Start” button.

Reporting: A standard report can be launched to have an overview of the handler activity intraday or over the last week to check if this behaviour is recurrent.

7.2. Back Office system not receiving trades

Monitoring: the “Interfaces” light is red in the Summary workspace.

Alert: standard alerts are defined for the Interfaces, dealing with the number of processed messages

Diagnostic: Click on the “Interfaces” light which will move you to the Interfaces workspace. There, you could see that the number of processed messages by the Destination System (back office) is far lower (or even equal to zero) than the number of messages processed by *TradeKast* and the adapter (*TradeKast* client for the back office system). This would mean that the Back Office system could be down or very slow in the messages processing.

Remediation: contact the Back Office team to check what is going on.

Reporting: A standard report can be launched to have an overview of the Interfaces activity intraday or over the last week to check if this behaviour is recurrent.

7.3. *Kondor+ Slowing Down*

Monitoring: the “UNIX” light is red in the Summary workspace

Alert: standard alerts are defined for the UNIX Hosts, dealing with the CPU usage

Diagnostic: Click on the “UNIX” light which will move you to the UNIX workspace. There, you could see that the CPU usage is over 90% for the last 5 to 15 minutes.

Remediation: You can drill down to the process causing this issue in the UNIX Processes component and take the relevant decision.

Reporting: A standard report can be launched to have an overview of the UNIX system intraday or over the last week to check if this behaviour is recurrent.

7.4. *Abnormal K+ Night Batch Duration*

Monitoring: the “Kondor Batch” light is red in the Summary workspace

Alert: standard alerts are defined for the Kondor+ Night Batch and the associated jobs, dealing with duration.

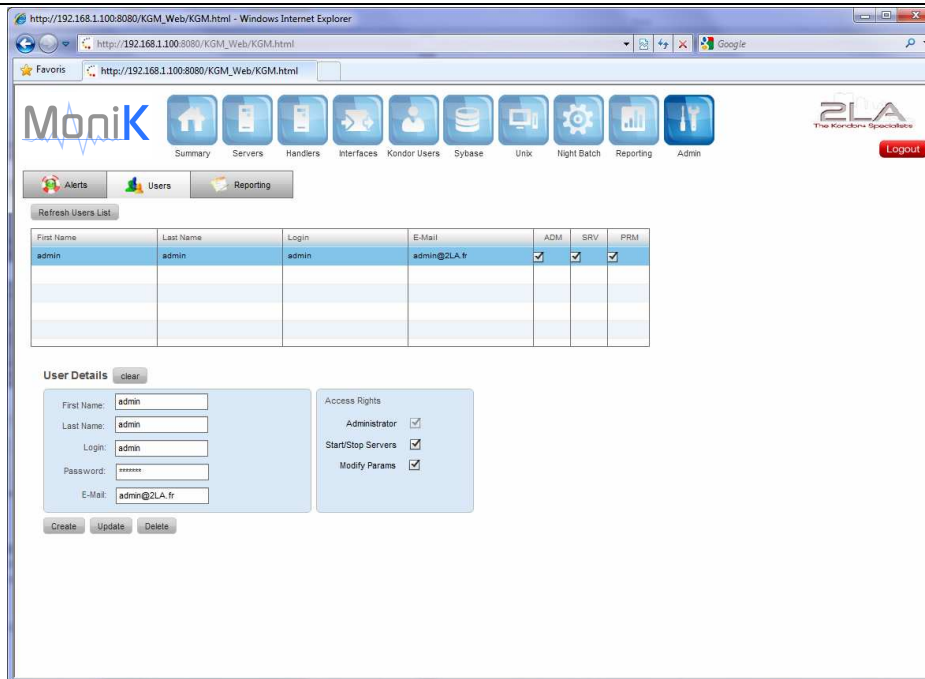
Diagnostic: Click on the “Kondor Batch” light which will move you to the Night Batch workspace. There, you could see that the last Night Batch duration was 4 hours whereas the average duration is 2 hours and the previous run duration was 1 hour 50 minutes.

Remediation: You can drill down to the Job(s) which caused this issue by seeing the average durations and previous run duration for all the night batch jobs. When the jobs are identified you could also see that some errors or warnings may have been raised by our solution when we analysed the log files. Some dead locks may have occurred which would have produced such a long overall batch duration.

Reporting: A standard report can be launched to have an overview of the Kondor+ Night Batch behaviour over the last week to check if this behaviour is recurrent.

8. *ROLES & SECURITY*

Users of our monitoring solution can have various roles like, support analysts, support managers or application managers. Therefore, the tool manages authentication and rights defining these roles.



The privileges can allow to:

- Be Administrator of the tool
- Start/Stop Kondor+ Servers or Handlers
- Modify the Servers & Handlers parameter files

The tool authentication is performed via a login and a password per user.