Monitor the heartbeat of your critical business services with help from IncidentMonitor™

The service desk software and infrastructure monitoring tools have to be fully integrated to provide the greatest benefit to the business.

The Problem

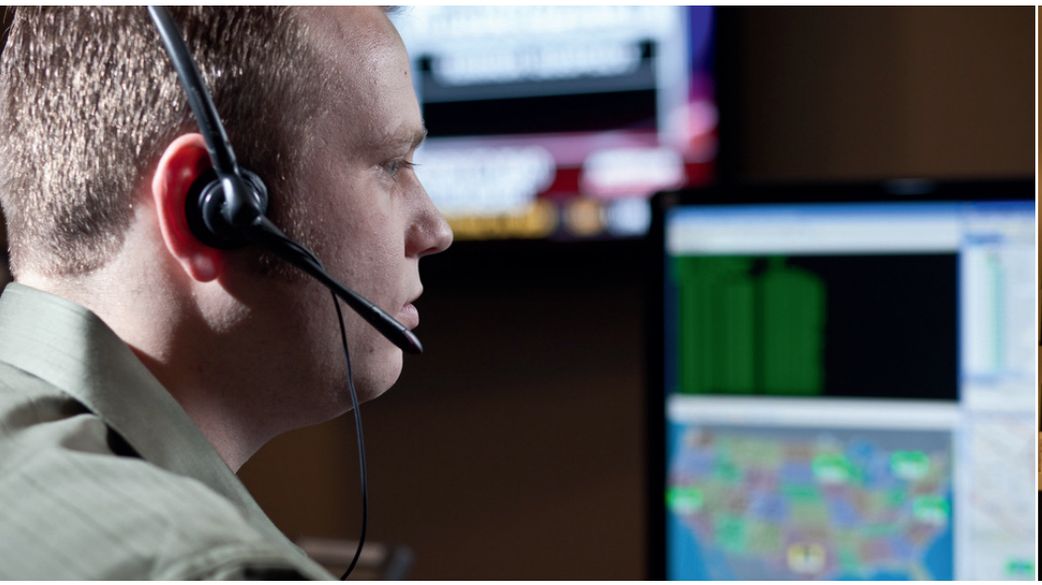
Integration of service desk software and infrastructure monitorig tools is often complex, expensive, sensitive to errors and subject to redevelopment when upgrades are necessary.

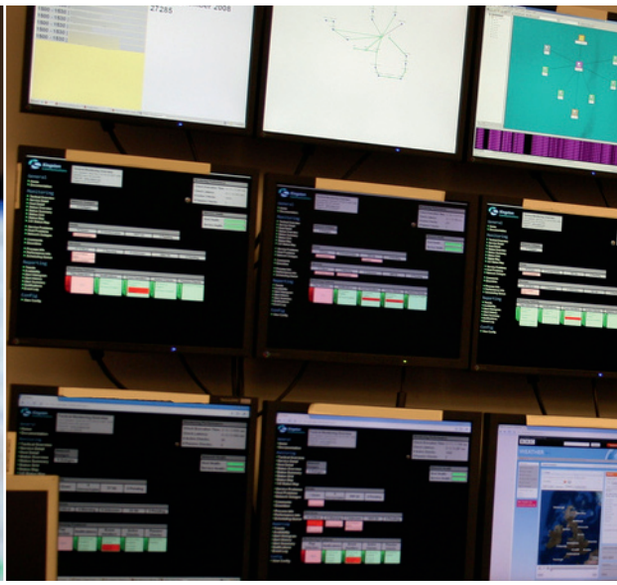
IncidentMonitor™'s Solution

An out of the box monitoring tool integration engine that allows for quick, robust integration to ANY monitoring solution. IncidentMonitor also ships with a bidirectional connector to Microsoft SCOM.

www.monitor24-7.com

Monitor the heartbeat of your critical business services with help from IncidentMonitor™





Many organizations monitor the health of business services using infrastructure management tools. Infrastructure management tools monitor and report on issues with the underlying hardware, software and networks supporting the services required by the business. In addition to management tools, most organizations have implemented service desk software to manage the logging and resolution of issues with the underlying infrastructure. Often the infrastructure management and service desk/technical support groups operate as silo departments.

Typically, the systems used by these departments are not tightly coupled because it requires extensive effort and cost to integrate. We believe that it is critical that these groups and systems are fully integrated so that the business benefits from a unified, end-to-end service management approach.

Providing end to end service management means that you need to be in control of all factors that may influence your service. What many organizations tend to overlook are the alerts which are triggered by infrastructure management tools. These alerts can throw your service management planning into chaos.

Defining Infrastructure Alerts

Alerts have a direct impact on your level of service. It is important to measure IT's performance in addressing these alerts and the impact it has on services provided to the organization. Many types of alerts are entered into Incident Management. Since most organizations do not properly identify alerts, they run the risk of not being able to track which incidents were created from management tools and which incidents were created by IT staff or end users. Recognizing the source of the incident will help organize the services that IT provides and ensure that normal day-to-day work does not suffer.

Following are examples of the types of alerts from most management systems:

1. **Alerts that require immediate attention**
   These alerts are the most important to your organization. For example, this could be a message saying that your server has gone down, possibly because a fan is not working (for example). If the server runs your organization's critical applications, once identified, all appropriate resources must immediately address the issue.

2. **Wake up alerts**
   Messages from your system to warn you that you need to act on something, which is less important but must be done.

3. **Awareness alerts**
   Messages that just inform you how the systems are doing, what the status is, etc…

Typically, these alerts are managed by different priorities and different SLA's, which will have a different impact on the service of your organization. And managing the service of your organization is something that needs to be supported by your service desk software solution.

Monitor the heartbeat of your critical business services with help from IncidentMonitor™

Service Desk Software Configuration and Integration with Monitoring Tools

The organization has to ensure that when an alert is generated by the management tool, a ticket is immediately logged in the service desk software solution. The service desk software must be configured so that it is able to recognize the type of messages and automatically assign the ticket to the appropriate group or individual. Service thresholds and service rules can be defined to manage the resolution of the ticket over its lifecycle.

Running reports and setting Key Performance Indicators (KPIs) against the alerts and the time to resolve will help you to improve your service instantly and help you keep control of all aspects that impact your service, using one single front end solution which is already there: Your Service Desk

In order to provide end-to-end service management you have to integrate your service desk software with infrastructure management tools. One popular application is Microsoft System Center Operations Manager (SCOM). SCOM will be configured to monitor the infrastructure for specific alerts. When a configured alert occurs the 'event' is forwarded to a central SCOM server, where a database is held which includes a history of alerts.

The ease of integration with popular software products has often been a moot subject, however this has now been resolved.

IncidentMonitor™ Service Desk Software and Microsoft SCOM

Next to the standard Network Management interface in IncidentMonitor™, Monitor 24-7 has developed an easy to setup, out of the box solution for a robust, bi-directional integration with Microsoft SCOM.
The IncidentMonitor™ SCOM connector leverages the IncidentMonitor™ Network Management subsystem.
The IncidentMonitor™ SCOM connector and the IncidentMonitor™ Network Management subsystem are provided out of the box at no additional cost.

"The SCOM interface, simply put, exemplifies the power of integration capabilities for the IncidentMonitor™ as whole." said Scott Walling, Managing Consultant at Monitor 24-7. "This connector was developed with absolutely no changes to our service management framework and provides a working example of how powerful this framework is. The SCOM connector provides an out-of-the-box, easy to install, low maintenance approach to an integration that is, traditionally, difficult to accomplish without a published object interface on both sides. It's great that Microsoft stepped up their interface to enable third parties to integrate seamlessly with SCOM."

IncidentMonitor™ SCOM Connector, How It Works

Event Message Configuration

The IncidentMonitor™ Network Management subsystem provides a simple interface that allows you to define the request properties (process, categorization, urgency, etc.) and associated whiteboard, for each event message, or network trap, that has to be configured within IncidentMonitor™.

The IncidentMonitor/SCOM integration utility adds an additional layer of simplicity to the integration; this utility will access the SCOM Management Pack Catalog and display all network traps configured within SCOM. Using a right-click menu item on the network trap, a window is displayed with the configuration items for the request and whiteboard item. You simply define the properties of the request; click OK and the IncidentMonitor™ SCOM Connector will create the consumable message within the IncidentMonitor™ Network Management system. All network traps configured in IncidentMonitor™ will be listed in the utility UI with the IncidentMonitor™ logo next to it.

In cases where several messages have to be configured within IncidentMonitor™, you can export the messages from the SCOM database into a delimited file. This file can be imported into the IncidentMonitor™ Network Management Import Utility, which will then import and create all messages within IncidentMonitor™.

Bi-Directional Integration

When a configured SCOM event occurs within the infrastructure, SCOM will trap the event and it will be displayed within the SCOM interface. The event will be passed to the IncidentMonitor™ SCOM Connector, which will then create the request within IncidentMonitor™ using the properties configured for this SCOM event. A request will be created using the configured project, folder, categorization, urgency, priority and additional information from SCOM, such as severity, message ID, node ID, etc.

Once the request is created within IncidentMonitor™, it will be managed by your process, such as SLAs, notifications, escalations, workflow, serviceable times, skills-based routing, etc. In addition, the asset that generated the event will be linked to the request, which provides the resource with all asset properties including an impact analysis view, showing all downstream assets that can be affected. When the resource accesses the request, all information required to quickly assess and resolve the issue is all tracked within the request.

The IncidentMonitor™ SCOM Connector will then retrieve the request number, assigned resource and assigned activity level from the request and update the alert in SCOM. This provides the infrastructure/SCOM administrators with a view into the service desk regarding the management and resolution of the alert using your corporate policies.

As the request is updated during its lifecycle, such as re-assignment to another resource or activity level, the IncidentMonitor™ SCOM Connector will update the alert in SCOM, thereby keeping the infrastructure/SCOM administrators updated.

When the alert is resolved in SCOM, the request in IncidentMonitor™ will be updated and closed. Similarly, if the request is closed in IncidentMonitor™, the alert in SCOM will be updated and closed.

Conclusion

The IncidentMonitor™ SCOM Connector provides a simple, yet powerful integration between two critical infrastructure management components—service desk and monitoring solutions. The IncidentMonitor™ SCOM Connector allows the systems to be integrated with NO PROGRAMMING required to configure and manage, thereby reducing the time to implement and almost a zero-effort ongoing administration.

If you want to learn more check our website to view the movie or contact our sales team

IncidentMonitor SCOM Connector Overview