



DAM YOUR ALERT FLOODS!

Rapid Deployment Approaches

for

Alerts & Message Management Solutions

BRIEFING PAPER
SEPTEMBER 2007

Alerts Management – DAM the Flood !

- This document provides a structured overview of the methodology adopted in enabling the consolidation, re-prioritisation and improved management control of all **alerts** that are generated within an IT infrastructure, irrespective of the number of differing monitors and technologies that may already be in use across the environment.



- PTC Alerts Manager can also be deployed alongside PTC Console to provide a comprehensive Message and Alert Management solution, replacing or integrating with other monitoring tools as appropriate.
- The strategy objectives are:-
 - To bring together all alerts from all monitors into a single repository.
 - Provision of software tools that can be easily used by existing IT staff, thereby reducing the need / dependency upon development resources from elsewhere in the organisation
 - Reformatting of all alerts into a single, common structure
 - Enable comprehensive browsing (through a common console) and management reports
 - Re-define alert status and most appropriate actions (no action – high priority – routing to most appropriate resource for action)
 - Guaranteed alert delivery, receipt, action, resolution and escalation
 - Ability to include 3rd party service providers within the alert management process
 - Systems, Event & Application Log file consolidation, alert creation and management
- The PTC Alerts Management solution allows customers to undertake a tactical approach to addressing the problem of alert floods on a case-by-case basis, whilst also offering a complete strategic solution that can be implemented over time to suit the available resources and budgets of each organisation.

DAM Your Alert Flood ~ A Structured Approach

Option 1 – Alert Consolidation & Browsing

- Provides customers with a simple and effective means to consolidate all of the alerts, created by any or all existing monitoring systems, into a single repository without impacting the existing alert management / workflow process.
- This is a common strategy step for those clients who would like to consolidate and standardise all alerts into a common, structured and more informed (or suppressed) format.



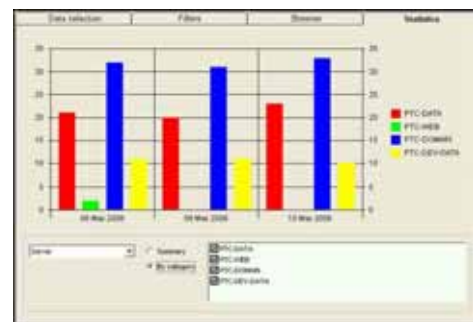
PTC Alerts - Browser

- PTC Alerts can be readily configured to capture e-mail alerts from all types of existing monitors.
- Each incoming email alert can be re-formatted into a standard e-mail format, including :-
 - Date / Time Stamp
 - Log Type – Incoming Alert
 - Severity – Information, Warning, Error
 - Server / Component Fault
 - Application – Sending Monitor
 - Message – Original Message content

- Once consolidated into the common format all alerts can be viewed through the Alert Browser using a number of differing selection criteria, including :- Server, Monitor, Severity or any other defined field.
- To initiate this consolidation process all alert emails can be 'copied' to PTC Alerts by MS Exchange or other mail server, or by using MS Outlook rules.
- For each email source, a transformation template can be developed in 5-15 minutes, using the unique PTC Charting RAD tool, which will convert emails from unstructured (or widely differing) alert content to the defined, fixed alert structure.
- This approach to structuring of alert management enables existing processes to remain unchanged whilst adding a consolidated, standardised and structured view of all alerts whatever their original source.

Option 2 – Simple Alert Reduction

- Delivers the functionality to review and re-prioritise all alerts that have been captured within the PTC Alerts data repository.
- The most common approach is to identify and select 'high priority' alerts and create a new alert with an appropriate 'urgency' status.
- Alert reduction is achieved through identification and selection of 'high priority' alerts and the creation of a 'new alert' which is sent to the designated recipient, whilst still providing a consolidated alert overview via the browser for additional information.



PTC Alerts - Statistics

- In reality, this means that alerts can be 'grouped and recognised' in a manner that enables the original recipient to receive only the 'selected' alerts, whilst still retaining the original alerts as required.
- Once again, the original alerting emails can be controlled through MS Exchange, other mail server or via MS Outlook rules.
- In turn, the incoming alert e-mails can be selected using the gathered alerts repository or directly from known alert formats and then forwarded to the designated recipient.
- Ultimately, this means that 'repetitive alerts' are captured within the alerts repository; an alert generated to the intended recipient; without further alerts being generated until the original problem has been acknowledged and resolved.
- By providing a level of functionality that can 'stem the flood' of repetitive alerts, PTC Alerts enables support personnel to concentrate on the task of resolving the original problem without having to respond to each of the repetitive calls to action for the same error situation.

Option 3 – Ensure Guaranteed 'Alert Delivery'

- Enables IT / User support departments to determine :-
 - WHO is available to receive the alert
 - WHAT action is to be taken
 - Associated escalation procedures in the even of a 'no response' within given parameters e.g. non availability of resource, time, etc...
- To maximise efficiency, effectiveness and productivity of IT support resources, it is essential that alerts are forwarded to the right resource; what ever time of day, night or weekend the problem occurs and through which communications medium (sound, email, mobile, pager) that is appropriate at the time of incident.



PTC Alerts – Contact Availability

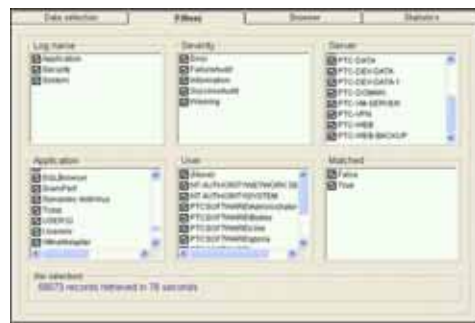
- Equally important, is that each alert is tracked to ensure that action is taken - from initial confirmation of alert receipt through to ultimate closure. Escalation procedures and alternate action can be built in to guarantee action is taken in the appropriate and prescribed manner.
- By harnessing the 'Contact Availability' function within PTC Alerts, it is possible to define who is available and when, thereby catering for holidays and shift patterns, training courses, etc..
- The contact diary defines the rules on availability hours and holidays for each member of the IT and/or User support teams, hence ensuring that alert messages are only sent to those people who are available to action them.
- Alert management can be configured to accept 2-way communications, including support personnel acknowledging responsibility for the alerts and closing the alert once it has been dealt with.
- Also, PTC Alerts can both send and receive SMS Text Messages through use of a GSM modem. Replies to alerts, via SMS text messages, can easily be accomplished.
- Additionally, escalation procedures can be configured for critical alerts that are not 'accepted' within defined timescales. Escalation can use different methods of alerting, e.g. e-mail to SMS, or from the support team to supervisors and ultimately through to management.
- Through contact diaries defining support availability, detailed management reporting and via a master console showing full alerts status, PTC Alerts provides IT departments with a comprehensive Alerts Management solution that ensures that alerts are fully tracked from inception through to completion.

Option 4 – Event & Log File Monitoring

- IT infrastructures evolve over time and nowadays most contain differing hardware and operating systems, manufacturer supplied monitoring products and 3rd party offerings – all of which are (individually) designed to aid productivity.
- However, in reality we often face a complex mix of technologies in order to integrate the many system, event, security and application log files that are inherent on each server environment. Controlling alerts across these differing environments can become a nightmare.



- PTC Console enables the capture, reformatting and consolidation of event and fault logs across Microsoft, Unix and Linux environments, generating and managing the alerts as appropriate.
- PTC Console can be deployed to either replace or complement existing monitors and has the ability to monitor log files of various types for important events, which can be turned into alerts and then follow the procedures outlined in any of the options above.
- MS Windows event logs and UNIX / Linux system logs are automatically reformatted to a standard structure, so that browsing can be carried out on either the original log entries or on the alerts that have been generated.
- User logs can also be monitored, with transformation from the native log file format to the PTC structured log entries and are easily defined by the user.
- Through PTC Console systems administrators can set 'watches' on any log file that contains entries of interest.
- The next step would be to define how to transform non-standard log file entries into the structured PTC format for storage on the database.



PTC Console - Filters

- This could vary from being as simple as : any line in the log file being the same format e.g.
 - Characters 1-10 = Entry Type
 - Characters 12-15 = Alert Severity
 - Characters 20-60 = Relevant Message1
- Or as complex as :
 - if a line appears that says 'xxxxxx STARTED' we can wait for a line that say 'xxxxxx FINISHED – STATUS OK' before adding it to the database.
- By using the PTC Charting tool it is then possible to rapidly develop and deploy a whole array of message filters and transformers which will dramatically increase control and auditability of error message delivery, alerts management and subsequent problem resolution.

Summary

- The Alerts and Message Management solution from PTC Software provides IT Departments and Solutions Providers with a fully scalable, powerful yet easy to use solution that enables the consolidation, re-prioritisation and management of alerts, together with the delivery of improved alerting and escalation mechanisms to ensure issue resolution.
- Whether your objective is simply to provide a single, common repository for alert capture and review, or to commence the strategic process of alert consolidation and management, reducing the alerts flood from existing monitors / log files across the enterprise to a manageable trickle, PTC Software delivers an initial tactical approach that can be extended into a enterprise wide strategic solution in a fraction of the time and a fraction of the cost of other solutions.
- The PTC Software Suite enables our customers to address multiple tactical issues to improve the productivity, effectiveness and efficiency of the resources available to them, whilst delivering components that can evolve into an end-to-end strategic solution.
- We have organised a number of Webinars to enable you to review a demonstration of our solutions from the comfort of your desk. You can register for the webinar at http://www.ptc.co.uk/am/request_form.asp . Alternatively, get in touch to arrange for a one to one discussion with our technical consultants by calling us on **01480 479090** or by registration on our website <http://www.ptc.co.uk/am/requestinfo.asp> .



PTC Suite is an integrated toolset of co-operative point software solutions designed specifically to assist both IT Departments and Solution Providers alike in the rapid deployment of :-

- **Service Availability & IT Infrastructure Management**
- **Alerts & Message Management**
- **Workflow & Scheduling Management**
- **Business Intelligence & Performance Management**



PTC Software Ltd.
Phoenix house
2 Phoenix Park
Eaton Socon
Cambs.
PE 19 8EP

01480 479090