Guardium Administration

How to work out Alerting in Guardium

Scope

- **In General, an alerting system works by Raising** an alert and the alert stays up until someone fixes the issue and brings the alert down
- **Guardium alerting works differently,** as follows:
  - An event triggers the alert
  - The alert is sent as message, either as email, syslog, snmp trap
  - The alert is triggered on a frequency
  - The message is sent as long as the event keeps occurring
- **Exemple : MySql Disk Usage**
  - Alert set up for MySql Disk Usage over 80%
  - Alert set up to trigger every hour
  - Result : a message will be sent every hour as long as MySql Disk Usage is 80% or above

Types of Messages Sending Alerts

3 main ones :

- Most common : **email**
- Most integrated : **Syslog to a SIEM**
- Other : **SNMP trap**

By experience I know that **syslog** may be a no-no as it will generate extra license cost on the SIEM

SNMP is great but not very much used

It leaves **email**, which we will discuss here

The Challenges

- First,
  - It may generate a **sheer amount of emails**
  - The messages are **not centrally managed** as each team member will receive them and will have to handle them individually
  - Outlook Inbox becomes the main tool for managing potentially large volumes of alerts.
- Second,
  - Alerts do NOT provide **context** information
  - Context information is crucial to address the alerts. But you have to generate it each time you receive an alert
- Third
  - Even with an efficient management of Outlook, with rules and folders for example, you may experience the well-known **“Alert fatigue”**
  - Alert fatigue is dangerous as it will make more likely missing some alerts
  - Situation generating alert fatigue should therefore be avoided

There are 2 ways to Handle Alerts in guardium

1 : Efficient management and organization of Outlook but leaves you exposed to “Alert Fatigue”

2 : Use SonarG, Guardium Insights or “Context22 Add-on for Guardium” and replace Alerts by compact Dashboards. This is the best way to avoid “Alert Fatigue”

#1 : Setting up Outlook for Managing Guardium Alerts

#1.1 : Setting-up Alerts In a Way to make you proactive

Being Proactive is the KEY to be a successful Guardium Admin.

Alerts should not be set up to alert you only when the disaster has occurred or is about to.

An option I successfully used at a very large bank, is to set up a same alert with 3 levels of thresholds and frequency.

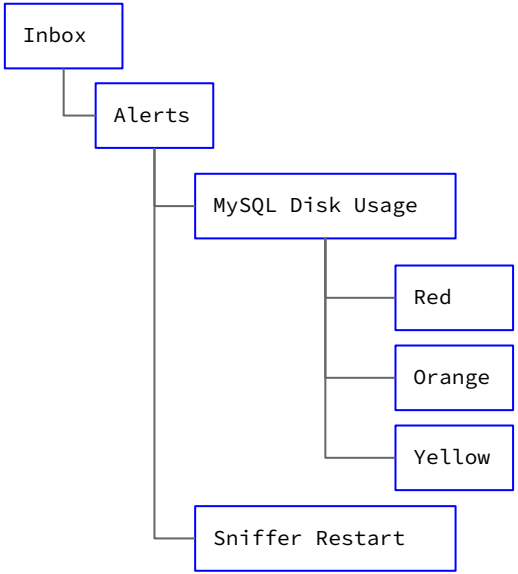
Let's take **MySql Disk Usage** as an example

- You define :
  - 3 levels of thresholds: 60%, 70% and 80% for example
  - Call them Yellow, Orange, Red
  - And corresponding frequencies :
    - 60% : once a day
    - 70% : twice a day
    - 80% : every hour
- You structure Outlook to mirror this, by :
  - A rule for each alert
  - A folder for each alert

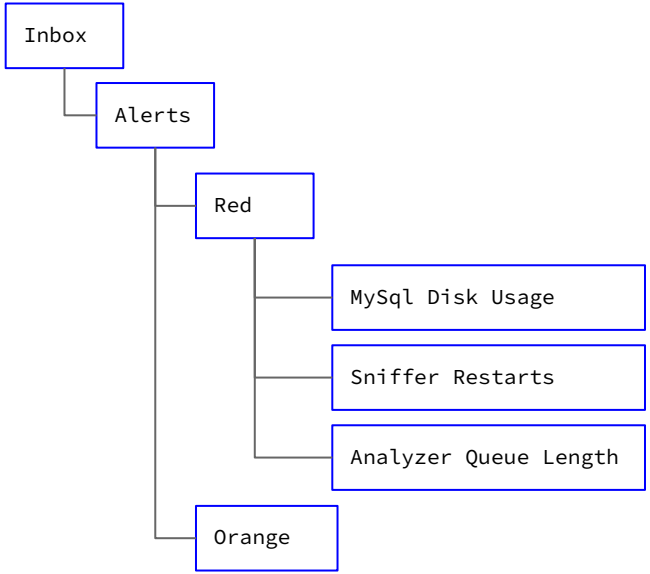
#1.1 : Organizing Outlook Efficiently

2 ways of managing Outlook folders : folder by Alerts and subfolder per Color or the opposite

Alerts then colors



Colors then alerts



#1.2 : How to Act on Alerts set up that way

2 ways of managing Outlook folders : folder by Alerts and subfolder per Color or the opposite

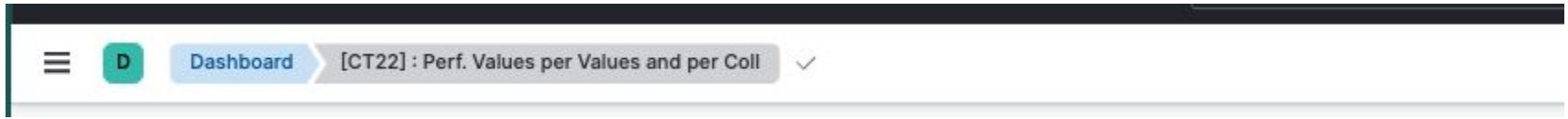
- **ALWAYS start with the Red ones** : they are the most urgent
- But you MUST end up with few or **NO Red ones.** Having Red ones is a sign of not being proactive enough.
- Pay particular attention to the **Orange ones.** Some structural changes in the Traffic pattern may be occurring and you act already by redirecting some STAPs to other collectors or by dividing the traffic of an agent among several Collectors.
  Develop a Plan in case the Collector goes to Red level
- IBM has introduced Alerts based on growth rate. This is an nice evolution of this Alert system. BUT it still doesn't protect from Alert Fatigue and is still far from a standard Alerting system.

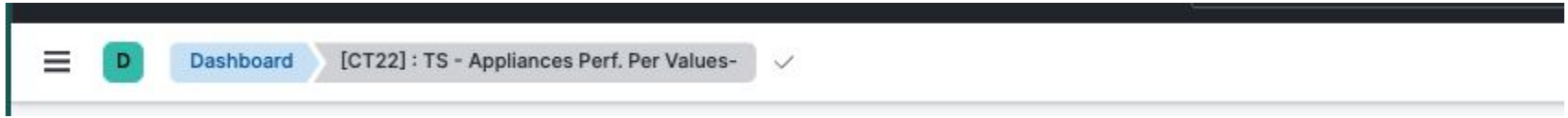
#2 : Replacing Alerts by Dashbord using SonarG, Guardium Insights or our "Context22 Add-on"

Option #2 : Using SonarG, Insights or Context 22 Add-on

- Based on the **BUM centrally ingested** in those systems, you can develop compact and meaningful **Dashboards**
- No strenuous management of your Outlook.
- Dashboards are WAY more efficient than emails and Outlook
- You get contextual information by default : for example a on **Full SQL** Count is built-in, simple and fast, giving you the right information soon enough
- But of course, you need to watch those Dashboards frequently, which means you have to be proactive, on the lookout and constantly poking around to find potential issues
- **No more Alert Fatigue**
- **How to implement such Dashboards:**
  - See my Videos on the topic

Demo


D
Dashboard
[CT22] : Perf. Values per Values and per Coll


D
Dashboard
[CT22] : TS - Appliances Perf. Per Values-

How to contact us

info@context22.com
Support@context22.com
LinkedIn
www.context22.com
(under construction)