La gestion des notifications en supervision IT

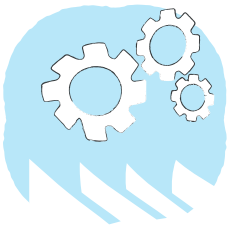
LIVRE BLANC

Sensor Factory

Feel your IT

La supervision :

LE PARADIGME DU GARÇON QUI CRIAIT AU LOUP



Fondée par des experts de la production informatique, SENSOR FACTORY™ est fournisseur de données sur l'état de santé du système d'information.

Nous accompagnons nos clients dans l'exploitation au quotidien de leurs outils de supervision ainsi que dans le maintien en condition opérationnelle de ceux-ci. C'est ce que nous appelons l'Intégration continue.

A l'instar d'un conte pour enfant bien connu, il est très fréquent de se retrouver dans la situation ou l'investissement dans un projet de supervision informatique se trouve rapidement perdu en raison de l'inondation des boites mails par des alertes plus ou moins pertinentes.

Une fois votre plate-forme de supervision déployée sur l'ensemble de votre système d'information, se pose la question suivante : comment s'organiser et traiter les informations remontées ?

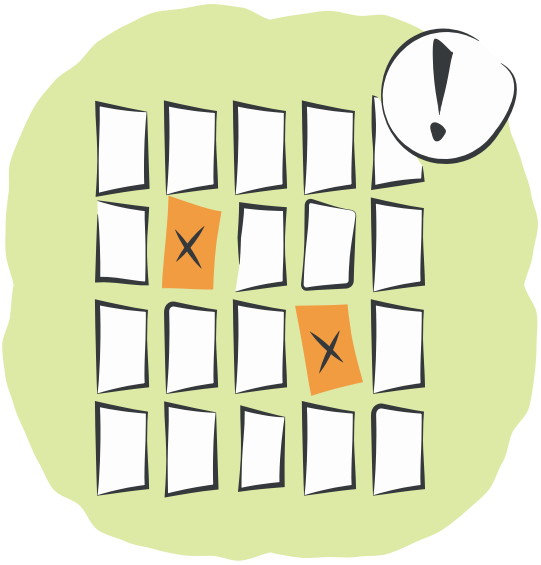
Pour vous aider à y répondre, nous allons aborder ensemble les problématiques induites, non seulement sous l'angle technique, mais également sous l'angle opérationnel humain.

Hibouvision

SENSOR FACTORY™ opère également HIBOUVISION™

Une solution de monitoring en cloud à haute résilience. Nous sommes basés à Nantes et intervenons partout où nos clients ont besoin de nous.

L'astreinte

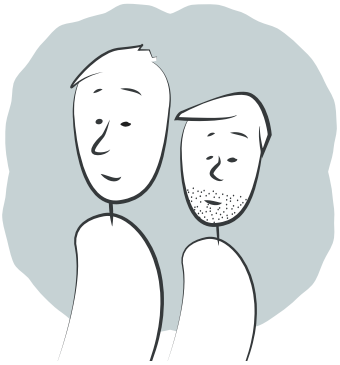


Évacuons tout de suite le cas particulier du traitement des alertes en astreinte. Tel que nous l'entendons dans la plupart des organisations, l'astreinte informatique a pour vocation d'intervenir techniquement en cas d'incident sur un système dont la disponibilité est attendue également en dehors des heures ouvrées de l'entreprise.

Ceci implique que la personne d'astreinte soit en capacité de résoudre l'incident soit parce que l'astreinte ne porte que sur son domaine de compétence soit parce que l'astreinte porte sur des domaines non maîtrisés à priori mais dont les référents ont fournis les procédures de diagnostic et de remédiation des incidents potentiels.

Dans tous les cas, il est souhaitable que l'astreinte ne soit sollicitée que pour des incidents avérés. La saturation d'un espace disque ou une surcharge ponctuelle de CPU ne sont sans doute pas des alertes suffisantes prises individuellement pour réveiller systématiquement la personne d'astreinte. Par contre, corrélées avec l'indisponibilité d'un service, ces informations se révéleront précieuses dans l'identification des origines de l'incident et sur les actions a effectuer pour y remédier, surtout par un opérationnel dont ce n'est pas le domaine de compétence.

Pour qui ?



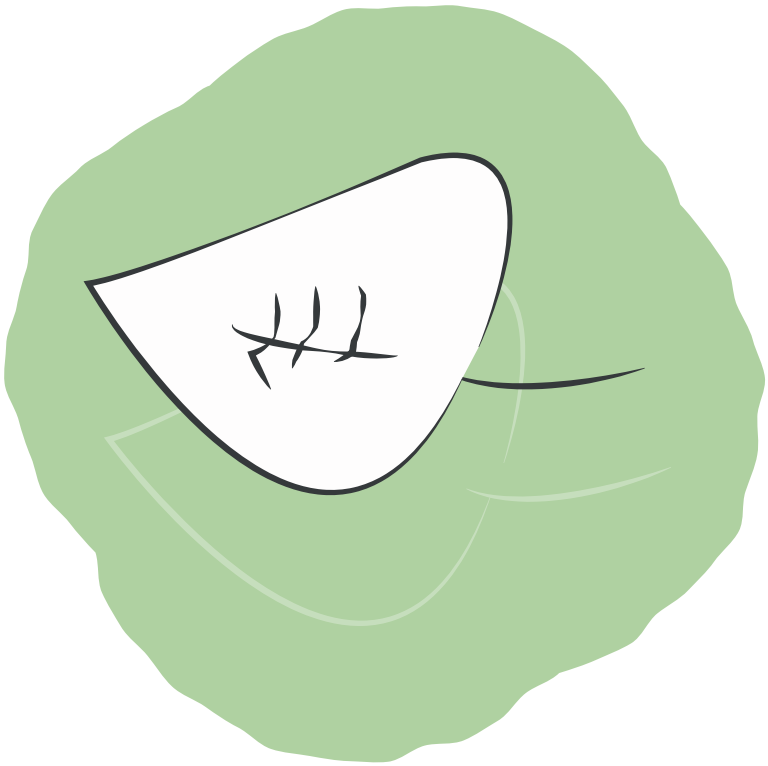
Qui a besoin des informations collectées par votre supervision ? Vos clients externes ou internes: l'information de disponibilité et/ou de performance des services que vous rendez peut leur être présentée directement par votre outil de supervision. Vos exploitants bien sûr, la plate-forme de supervision est leur outil de travail au quotidien. Vos développeurs, qui trouveront dans votre supervision une solution pour suivre dans le temps le comportement de leurs applications. Et enfin : vos décideurs qui s'appuieront sur des rapports de tendance afin d'anticiper les évolutions nécessaires de votre système d'information.

Comment alerter pertinemment ?

L'ennemi à combattre est l'inondation de messages et de notifications en tout genre. Noyés sous de nombreux mails d'alerte, la plupart des gens renoncent à les consulter voir finissent par créer une règle de messagerie les mettant directement dans leur corbeille.

Afin de ne pas en arriver là, il est essentiel de ne créer des règles de notifications qu'une fois vos processus internes de traitement définis.

Le mail est-il toujours le bon moyen de solliciter une personne ? Pas sûr, surtout si nous reprenons notre exemple de l'astreinte. Votre outil de supervision offre plusieurs alternatives que nous allons parcourir ensemble.



Objectif « Green »

Un système d'information en parfaite santé ne devrait remonter que du « vert » sur l'ensemble des capteurs. Or plus le système est vaste plus il est illusoire de vouloir y parvenir à chaque instant. Il est néanmoins important de s'organiser pour que le « rouge » soit pris en compte et traité dans les délais les plus bref (ie sous l'heure). Le « orange » doit, lui, être traité avant de passer au « rouge ».

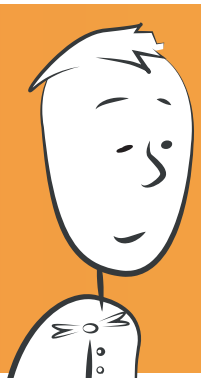
Un repère : Il n'est pas « normal » qu'un capteur remonte une erreur même ponctuellement. Par « normal », nous entendons le fait que si cette remontée est possible sans qu'il n'y ait de procédure de remédiation associée c'est que le seuil d'alerte n'est pas correctement configuré ou bien qu'un filtre doit être positionné pour effacer des franchissements de seuils ponctuels mais non significatifs. En respectant ce principe, on élimine à la source les notifications superflues. Plus le travail de définition des seuils aura pu être conduit finement, meilleure sera la pertinence des alertes remontées, moins les acteurs de la supervision seront inondés !

Définir vos processus internes de traitement des alertes

Nous n'avons pas la prétention de passer en revue de manière exhaustive tous les cas possibles d'organisation autour du traitement des alertes de votre système d'information. Nous vous donnons cependant quelques clés afin que vous vous posiez toutes les questions et que vous puissiez porter simplement la définition de vos processus dans la configuration de votre outil de supervision.

Quels acteurs autour de la plate-forme ?

Nous proposons communément plusieurs catégories d'acteurs autour de la plate-forme de supervision et qui peuvent se décliner naturellement en groupe de traitement dans votre outil de supervision :



L'exploitant

Opérationnel en première ligne sur le front du traitement des incidents, cet acteur a besoin d'être alerté rapidement. La plate-forme de supervision doit lui fournir en première lecture la nature et l'importance des impacts afin qu'il adapte la communication auprès des utilisateurs et puissent dérouler les procédures prédéfinies de remédiation sans avoir à analyser finement les causes des dysfonctionnements.

L'expert

Lorsque les procédures standard de remédiation prédéfinies ne sont pas efficaces, c'est à l'expert de prendre le relais. Par définition, l'origine de l'incident qui lui est escaladé n'est à priori pas complètement identifiée. Il est donc important que la plate-forme de supervision lui fournisse les métriques nécessaires au diagnostic.

Le manager

Responsable en charge du capacity planning de la production, la plate-forme de supervision lui permet de compiler dans le temps les données nécessaires à la perception de l'évolution de la charge sur la production. Elle lui permet également, à partir de l'historique des incidents, de dégager les axes d'évolutions nécessaires à l'amélioration de la stabilité de la production.

Le développeur / architecte

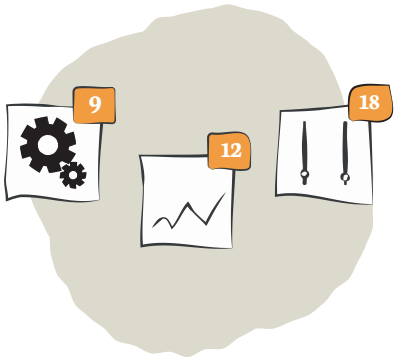
Bien qu'il puisse être associé à la résolution d'incident, les seules données issues de la plate-forme de supervision ne sont que rarement suffisantes pour lui permettre de résoudre un incident. Cet acteur peut par contre trouver dans la plate-forme de supervision les données qui vont lui permettre de suivre la vie de l'architecture et ou de l'application dont il a la charge et d'améliorer ainsi les performances de son code.

Il est bien sûr possible de combiner ces rôles et de les adapter à votre propre organisation.
Suivant sa taille, les rôles d'exploitant et d'expert peuvent être confondus par exemple.
Il reste cependant essentiel que la plate-forme de supervision réponde techniquement à tous les besoins liés aux fonctions définies ci-dessus. Elle doit donc monitorer de manière exhaustive tous les équipements de la production mais également fournir les tableaux de bord incluant les points de contrôle combinant l'état des capteurs clés facilitant ainsi la lecture du niveau de disponibilité de chacune de vos applications.

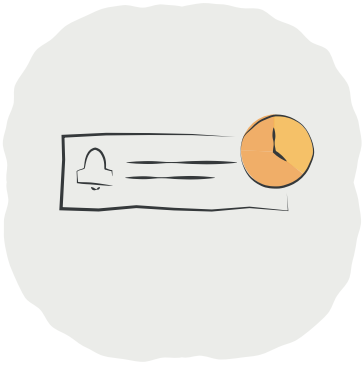
Chaque fonction-type peut se décliner par domaine de compétence (réseau, système, stockage, DBA ...).

Quand notifier ?

Est-ce que tous les groupes de traitement doivent être notifiés tout le temps ? A priori, il n'est pas utile d'inonder les messageries de vos collaborateurs en dehors de leurs heures ouvrées. De retour au bureau, un rapport généré automatiquement sur les incidents survenus en leur absence et sur le périmètre les concernant leur fera gagner beaucoup de temps. Inutile également de leur envoyer des SMS si vos collaborateurs ne sont pas en astreinte. On comprend donc qu'il est essentiel de maîtriser les plages horaires d'envoi des notifications afin de ne pas surcharger les acteurs d'informations dont ils n'auront que faire après coup.



Que faire des alertes ?



Si une alerte remonte et « qu'il n'y a rien à faire », elle ne doit logiquement pas donner lieu à une notification. Inutile de prévenir qui que ce soit dans ce cas. L'alerte en tant que tel apparaîtra dans les rapports de tendance et pourra être prise en compte dans le cadre de l'amélioration de la stabilité du système d'information. Mais ce cas devrait être finalement plutôt rare. En effet, même un franchissement de seuil provoquant
un « warning » doit à minima déclencher une procédure de surveillance de l'évolution de la situation dans le cadre d'une exploitation proactive. Autre exemple, une erreur non traitée dans le délai imparti par l'exploitation doit donner lieu à une escalade vers les managers afin que ceux-ci puissent organiser la réponse de leurs collaborateurs.

Les vecteurs de notification

Nous partons du principe ici que votre outil de supervision est l'outil qui doit avertir les acteurs de la supervision. Chaque vecteur présente des avantages qu'il s'agît d'adapter et d'utiliser au mieux des besoins et des habitudes de travail de chaque population d'utilisateurs de la plate-forme.

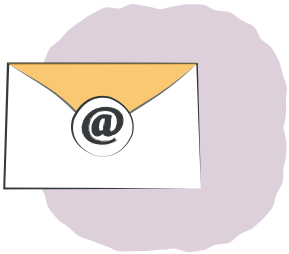
L'écran de supervision

Recommandé pour : l'exploitant, l'expert

Dès lors que plusieurs opérationnels sont dans le même bureau, l'écran de supervision devient complètement pertinent. Il est possible pour ceux qui sont devant cet écran d'être alertés presque instantanément d'un incident, à partir du moment où l'on a pris le temps de créer un visuel adapté. Le changement d'état d'un capteur peut aussi s'accompagner d'un son d'alerte.

L'envoi de mail

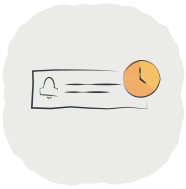
Recommandé pour : l'exploitant, l'expert, le développeur, le manager



Notification la plus classique. C'est la première méthode à laquelle on pense lorsque l'on met en place des notifications. On peut vite être inondé de mails, il devient alors difficile de ne pas passer à côté d'informations importantes.
Les outils de supervision les plus évolués proposent un contenu HTML avec des liens directs vers des actions de réaction à l'alerte (ex: acquittement de l'alarme, redémarrage d'un service...)

Les notifications PUSH

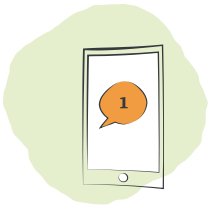
Recommandé pour : l'expert, le développeur, le manager



Ce canal est le plus adapté pour les opérationnels qui ont d'autres tâches que le pupîtrage classique à effectuer. Moins envahissant que le mail, l'information nous parvient instantanément à condition bien sûr de disposer d'un smartphone.

L'envoi de SMS

Recommandé pour : l'expert, le développeur, le manager



Encore largement utilisé, cette fonctionnalité présente l'intérêt d'être compatible avec n'importe quel mobile. Cette solution implique un surcoût puisqu'il faut s'appuyer sur un broker SMS ou un modem avec abonnement pour l'envoi des messages. Elle tend à être remplacée par la solution de PUSH.

L'exécution du programme

Recommandé pour : l'exploitant, l'expert

A partir de ce vecteur, tout ou presque est possible. SENSOR FACTORY™ le recommande pour une solution en particulier : le réveil en astreinte. En effet, toutes les autres méthodes que nous avons vu ensemble ne présentent pas de solution technique satisfaisante pour réveiller un opérateur humain en astreinte. Il est donc indispensable de pouvoir jouer à l'aide d'un SVI sortant une alerte qui appellera sur son téléphone la personne d'astreinte. Ce SVI doit prévoir un mécanisme d'acquittement.

En résumé

C'est simple ! Pour tirer la quintessence de votre outil de supervision il faut donc :

1. **Identifier les groupes de traitement (fonction et domaine)**
2. **Leur appliquer les périodes de notification adaptées**
3. **Identifier les SLAs de prise en charge d'incident et d'escalade**
4. **Définir les procédures de remédiation pour incident faisant l'objet d'une notification**

Vous l'aurez compris, un projet de supervision ne s'arrête pas à l'installation et à la configuration de l'outil technique. C'est toute une organisation qu'il vous faudra prendre le temps de penser et mettre en place si vous voulez être sûr que cet investissement soit rentable. Tout comme il est essentiel que votre équipe s'organise pour que votre plate-forme de supervision soit toujours exhaustive et opérationnelle. Si ce n'est pas le cas, vous ne pourrez pas vous y fier. Quoi de plus délicat à gérer pour une société qu'un incident remonté par ses clients ?

Merci de votre attention

Vous souhaitez de plus amples renseignements sur nos activités :

NOUS APPELER

+33 2 57 48 00 13

PASSER NOUS VOIR :

3, chemin du Pressoir Chênaie
44100 Nantes

Matthieu Noirbusson
ASSOCIÉ

matthieu.noirbusson@sensorfactory.eu

Nicolas Jançon
ASSOCIÉ

nicolas.jancon@sensorfactory.eu