Pourquoi superviser ?

Olivier Brand-Foissac

CNRS / Laboratoire de Physique Théorique - Orsay

ANGD Mathrice - Nov 2009

Plan

Plan

Monitoring et Supervision

Monitoring

Monitoring means the periodic inspection by [..] a directed function or activity and includes watching during performance, checking, and tracking progress, updating a supervisor of progress or accomplishment by the person monitored, and contacting a supervisor as needed for direction and consultation.

Supervision

"Supervision" means the guidance by a registered one for the accomplishment of a function or activity. The guidance consists of the activities included in monitoring as well as establishing the initial direction, delegating, setting expectations, directing activities and courses of action, critical watching, overseeing, evaluating, and changing a course of action.

Source [Minnesota Administrative Rules - 2008]

Monitoring et Supervision

En informatique, *monitoring* et *supervision* se distinguent par :

Monitoring

- local, proximité, courte portée
- précision
- temps réel
- attaché à la performance
- orienté diagnostic

Supervision

- regrouppement, global, longue portée
- concentration, concaténation, consolidation
- temps différé
- attaché au service
- orienté présentation *(reporting)*, pilotage

Monitoring et Supervision

En informatique, *monitoring* et *supervision* se distinguent par :

Monitoring

- local, proximité, courte portée
- précision
- temps réel
- attaché à la performance
- orienté diagnostic

Supervision

- regrouppement, global, longue portée
- concentration, concaténation, consolidation
- temps différé
- attaché au service
- orienté présentation *(reporting)*, pilotage

Supervision

- La supervision centralise le monitoring local.
- Peut effectuer du monitoring ciblé à distance

- Seront abordés ultérieurement :
  - Comment superviser ? Les protocoles mis en œuvre
  - Quelques outils de supervision ?
  - pas d'exhaustivité : plus de 1500 projets sur sourceforge . . .

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, mémoire, réseau, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (schéma en tuiles, remplacement à ...)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, mémoire, réseau, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (schéma en tuiles, remplacement à ...)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, mémoire, réseau, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (schéma en tuiles, remplacement à ...)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, mémoire, réseau, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente entre deux pannes / MTBF)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - en termes de ressources (CPU, stockage, fluides, ...)
  - en termes de capacités (accès et utilisation des ressources)
  - en termes de disponibilités (attente en files, contentions, HA)

Une nécessité ?

En quoi la supervision est-elle utile ?

- s'assurer du fonctionnement (bon, optimal) des ressources
- gagner du temps !
- gagner de la précision (fiabilité) !

En quoi la supervision est-elle nécessaire ?

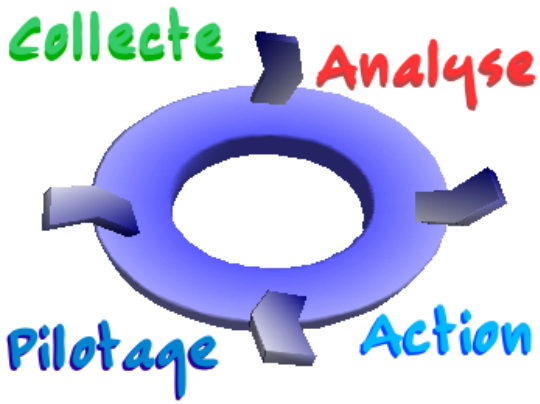
- contrôler la disponibilité des services/fonctions
- contrôler l'utilisation des ressources
- vérifier qu'elles sont suffisantes (dynamique)
- vérifier l'équilibrage de charge
- faciliter le diagnostic des pannes (pannes avérées)
- prévenir les pannes/défauts/débordements (pannes latentes)
- prévoir les évolutions (gestion de cluster)
  - > en termes de ressources (CPU, stockage, fluides, ...)
  - > en termes de capacités (accès et utilisation des ressources)
  - > en termes de disponibilités (attente en files, contentions, HA)

Plan

Mécanismes

Quatre phases de la chaîne monitoring-supervision :

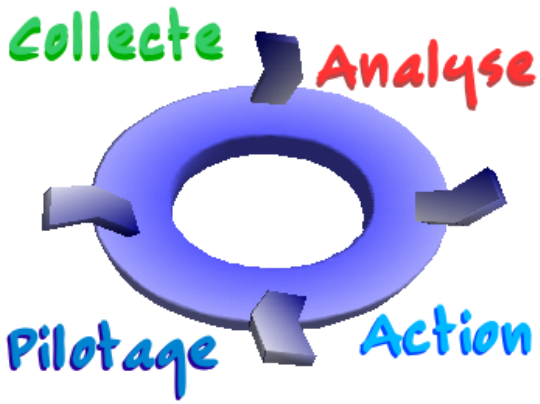
1. Collecte des données (acquisition).
   - ciblage (définir ce qui sera mesuré)
   - acquisition (faire la mesure)
     - comment la faire (quels outils)
     - d'où la faire (actif, passif)
   - stockage (où placer les métriques, dans quel format)
2. Analyse des données recueillies. (extraction/filtrage, synthèse)
   - immédiate (temps réel ou peu différé)
   - en différé (à posteriori, la nuit, ...)



Mécanismes

Quatre phases de la chaîne monitoring-supervision :

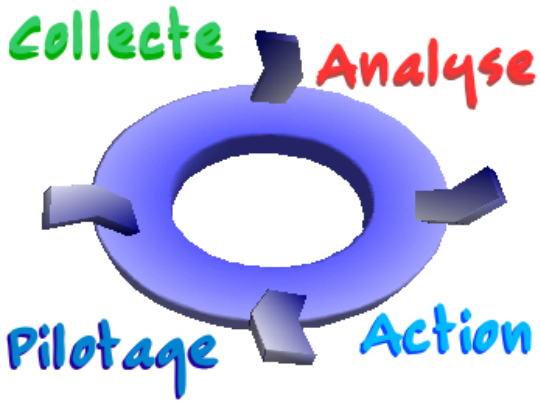
1. Collecte des données (acquisition).
   - ciblage (définir ce qui sera mesuré)
   - acquisition (faire la mesure)
     - comment la faire (quels outils)
     - d'où la faire (actif, passif)
   - stockage (où placer les métriques, dans quel format)
2. Analyse des données recueillies.
   (extraction/filtrage, synthèse)
   - immédiate (temps réel ou peu différé)
   - en différé (à posteriori, la nuit, ...)



Mécanismes

Quatre phases (suite) :

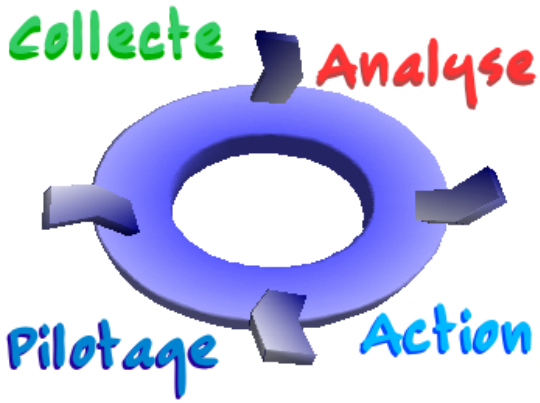
3. Actions (automatiques) déclenchées par l'analyse.
   - alertes (actif)
   - ré-actions (actif)
   - traitement (pré-conditionnement, visuels graphiques, passif)
4. Pilotage (actions de l'opérateur).
   - déclencher l'analyse (différée)
   - renouveler mesure/analyse
   - action sur l'objet de la mesure (ouverture/fermeture de ports réseaux, etc.)



Mécanismes

Quatre phases (suite) :

3. Actions (automatiques) déclenchées par l'analyse.
   - alertes (actif)
   - ré-actions (actif)
   - traitement (pré-conditionnement, visuels graphiques, passif)
4. Pilotage (actions de l'opérateur).
   - déclencher l'analyse (différée)
   - renouveler mesure/analyse
   - action sur l'objet de la mesure (ouverture/fermeture de ports réseaux, etc.)



Acquisition

- Sélection des objets des mesures et des quantités associées
  (taux de charge, valeur/taux remplissage, présence/absence, etc.)
- Choix des fréquences de collecte
  - granularité et précision des données
  - influence sur le volume
- Choix des outils de collecte
  - avec agent (permanent)
    (process permanent local (démon), mesures en continu ou temporisées, influence sur les performances de l'hôte)
  - sans agent (ou agent non-permanent)
    (déclenchement à distance ou local (cron, ...), influence sur la qualité des mesures)
- Stockage et format des données
  - lieu du stockage, format (nécessité ou non d'un décodage)
    (local et/ou distant, historique, cumulatif, redondance, ...)
  - date et lieu de l'événement → synchronisation des horloges !

Acquisition

- Sélection des objets des mesures et des quantités associées
  (taux de charge, valeur/taux remplissage, présence/absence, etc.)
- Choix des fréquences de collecte
  - granularité et précision des données
  - influence sur le volume
- Choix des outils de collecte
  - avec agent (permanent)
    (process permanent local (démon), mesures en continu ou temporisées, influence sur les performances de l'hôte)
  - sans agent (ou agent non-permanent)
    (déclenchement à distance ou local (cron, ...), influence sur la qualité des mesures)
- Stockage et format des données
  - lieu du stockage, format (nécessité ou non d'un décodage)
    (local et/ou distant, historique, cumulatif, redondance, ...)
  - date et lieu de l'événement → synchronisation des horloges !

Acquisition

- Sélection des objets des mesures et des quantités associées
  (taux de charge, valeur/taux remplissage, présence/absence, etc.)
- Choix des fréquences de collecte
  - granularité et précision des données
  - influence sur le volume
- Choix des outils de collecte
  - avec agent (permanent)
    (process permanent local (démon), mesures en continu ou temporisées, influence sur les performances de l'hôte)
  - sans agent (ou agent non-permanent)
    (déclenchement à distance ou local (cron, ...), influence sur la qualité des mesures)
- Stockage et format des données
  - lieu du stockage, format (nécessité ou non d'un décodage)
    (local et/ou distant, historique, cumulatif, redondance, ...)
  - date et lieu de l'événement → synchronisation des horloges !

Acquisition

- Sélection des objets des mesures et des quantités associées
  (taux de charge, valeur/taux remplissage, présence/absence, etc.)
- Choix des fréquences de collecte
  - granularité et précision des données
  - influence sur le volume
- Choix des outils de collecte
  - avec agent (permanent)
    (process permanent local (démon), mesures en continu ou temporisées, influence sur les performances de l'hôte)
  - sans agent (ou agent non-permanent)
    (déclenchement à distance ou local (cron, ...), influence sur la qualité des mesures)
- Stockage et format des données
  - lieu du stockage, format (nécessité ou non d'un décodage)
    (local et/ou distant, historique, cumulatif, redondance, ...)
  - date et lieu de l'événement → synchronisation des horloges !

Analyse

Extraire les informations utiles et exploiter les données recueillies

(comparaison de valeurs seuils, recherche de mot-clés, calculs, ...)

- à destination de concaténation, de regroupement, de filtrage
- à destination d'actions automatiques (déclenchement d'alertes, ...)
- à destination visuelle (éléments de tableau de bord, graphiques)
- en pré-conditionnement (reformatage avec ou sans pertes, consolidation)

Analyse

Extraire les informations utiles et exploiter les données recueillies

(comparaison de valeurs seuils, recherche de mot-clés, calculs, ...)

- à destination de concaténation, de regroupement, de filtrage
- à destination d'actions automatiques (déclenchement d'alertes, ...)
- à destination visuelle (éléments de tableau de bord, graphiques)
- en pré-conditionnement (reformatage avec ou sans pertes, consolidation)

Analyse

Extraire les informations utiles et exploiter les données recueillies

(comparaison de valeurs seuils, recherche de mot-clés, calculs, ...)

- à destination de concaténation, de regroupement, de filtrage
- à destination d'actions automatiques (déclenchement d'alertes, ...)
- à destination visuelle (éléments de tableau de bord, graphiques)
- en pré-conditionnement (reformatage avec ou sans pertes, consolidation)

Analyse

Extraire les informations utiles et exploiter les données recueillies

(comparaison de valeurs seuils, recherche de mot-clés, calculs, ...)

- à destination de concaténation, de regroupement, de filtrage
- à destination d'actions automatiques (déclenchement d'alertes, ...)
- à destination visuelle (éléments de tableau de bord, graphiques)
- en pré-conditionnement (reformatage avec ou sans pertes, consolidation)

Actions Informatives

Dans le but de diffuser l'information, selon une criticité établie

- alerte par eMail (listes ciblées, différents niveaux de destinataires)
- alerte par action locale (trap d'agent, création de fichier, etc.)
- alerte par action distante (dépôt de fichier, télé-alarme, appel de page web)

→ garder les traces d'alertes

Actions Informatives

Dans le but de diffuser l'information, selon une criticité établie

- alerte par eMail (listes ciblées, différents niveaux de destinataires)
- alerte par action locale (trap d'agent, création de fichier, etc.)
- alerte par action distante (dépôt de fichier, télé-alarme, appel de page web)

→ garder les traces d'alertes

Actions Informatives

Dans le but de diffuser l'information, selon une criticité établie

- alerte par eMail (listes ciblées, différents niveaux de destinataires)
- alerte par action locale (trap d'agent, création de fichier, etc.)
- alerte par action distante (dépôt de fichier, télé-alarme, appel de page web)

→ garder les traces d'alertes

Actions Informatives

Dans le but de diffuser l'information, selon une criticité établie

- alerte par eMail (listes ciblées, différents niveaux de destinataires)
- alerte par action locale (trap d'agent, création de fichier, etc.)
- alerte par action distante (dépôt de fichier, télé-alarme, appel de page web)

$\longrightarrow$ garder les traces d'alertes

Actions Opératives

Dans le but de provoquer des modifications

- Auto-action (pare-feu, ...)
- Auto-extinction (seuil de température, ...)
- Nettoyages/rotations divers (caches, historisation, fichiers temporaires, ...)
- Relance d'acquisition

Actions Opératives

Dans le but de provoquer des modifications

- Auto-action (pare-feu, ...)
- Auto-extinction (seuil de température, ...)
- Nettoyages/rotations divers (caches, historisation, fichiers temporaires, ...)
- Relance d'acquisition

Actions Opératives

Dans le but de provoquer des modifications

- Auto-action (pare-feu, ...)
- Auto-extinction (seuil de température, ...)
- Nettoyages/rotations divers (caches, historisation, fichiers temporaires, ...)
- Relance d'acquisition

Actions Opératives

Dans le but de provoquer des modifications

- Auto-action (pare-feu, ...)
- Auto-extinction (seuil de température, ...)
- Nettoyages/rotations divers (caches, historisation, fichiers temporaires, ...)
- Relance d'acquisition

Pilotage

Contrôles par l'opérateur :

- sans action (visuels, tableaux de bord)
- avec action
  - recherche ponctuelle (dans les traces)
  - recherche statistique (fréquence des défauts, émergeance de problèmes, ...)

Pilotage

Contrôles par l'opérateur :

- sans action (visuels, tableaux de bord)
- avec action
  - recherche ponctuelle (dans les traces)
  - recherche statistique (fréquence des défauts, émergeance de problèmes, ...)

Attention

- Confidentialité (certaines données, traces, peuvent faire l'objet d'un accès limité)
- Veiller au respect de la législation

Protocoles d'interrogation/transmission

La supervision s'appuie sur des protocoles standardisés (voire normalisés)

Il seront détaillé dans l'exposé suivant.

Stockage des métriques

Stockage des mesures :

- fichiers de logs (bruts, concaténés, filtrés, ...)
- stockages en bases de données (RRD, Round-Robin Database, SQL, ...)
- formats spécifiques d'outils

Stockage des métriques

Stockage des mesures :

- fichiers de logs (bruts, concaténés, filtrés, ...)
- stockages en bases de données (RRD, Round-Robin Database, SQL, ...)
- formats spécifiques d'outils

Gestion du stockage des métriques :

- locale ou distante
- avec ou sans historisation (logrotate, durée de conservation ...)
- centralisée ou non
- redondante ou non (disponibilité, intégrité)

  $\longrightarrow$ le volume du stockage doit être estimé et surveillé !

Présentation

Interfaces de présentation des tableaux de bord

- vue(s) synthétique(s) (souvent en pages web)
- plus ou moins de détails, de profondeur de visualisation
- historisation et consolidation statistique (avec ou sans perte d'information)
- textes et/ou graphiques (RRDtool)

Présentation

Interfaces de présentation des tableaux de bord

- vue(s) synthétique(s) (souvent en pages web)
- plus ou moins de détails, de profondeur de visualisation
- historisation et consolidation statistique (avec ou sans perte d'information)
- textes et/ou graphiques (RRDtool)

Présentation

Interfaces de présentation des tableaux de bord

- vue(s) synthétique(s) (souvent en pages web)
- plus ou moins de détails, de profondeur de visualisation
- historisation et consolidation statistique (avec ou sans perte d'information)
- textes et/ou graphiques (RRDtool)

Présentation

Interfaces de présentation des tableaux de bord

- vue(s) synthétique(s) (souvent en pages web)
- plus ou moins de détails, de profondeur de visualisation
- historisation et consolidation statistique (avec ou sans perte d'information)
- textes et/ou graphiques (RRDtool)

Plan

Sondes actives / passives

Sondes actives

Avantages	Inconvénients
✓ proximité, indépendance	• influence sur l'hôte
✓ pas d'influences extérieures	• stockage
✓ grain fin	
✓ mesures plus fréquentes	

Sondes actives / passives

Sondes actives

Avantages	Inconvénients
✓ proximité, indépendance	• influence sur l'hôte
✓ pas d'influences extérieures	• stockage
✓ grain fin	
✓ mesures plus fréquentes	

Sondes passives

Avantages	Inconvénients
✓ moins (non) intrusives	• portée limitée (accès)
✓ alerte pas absence	• sécurité
✓ stockage volumineux	• fréquence des mesures limitée

Stockage des mesures

Stockage local

Avantages	Inconvénients
✓ immédiat	• influence sur l'hôte
✓ flux élevé	• accès/intégrité (crash)
	• volume limité
	• capacité d'alertes limitées

Stockage des mesures

Stockage local

Avantages	Inconvénients
✓ immédiat	• influence sur l'hôte
✓ flux élevé	• accès/intégrité (crash)
	• volume limité
	• capacité d'alertes limitées

Stockage distant

Avantages	Inconvénients
✓ plus disponible	• dépendant du réseau
✓ alertes	• veiller à la sécurité
	• flux limité
	• influence sur réseaux

Précision vs performance

Souvent choisir entre précision des mesures et performance de la machine :

Bonne précision :

- fréquence élevée des mesures
- sonde embarquée
  → impacte CPU et disque de l'hôte

Bonne performance :

- fréquence des mesures plus étagée
- sonde distante
  → impacte le réseau

L'idéal dépend certainement de la situation :

> routine : performance
> crise : précision

Précision vs performance

Souvent choisir entre précision des mesures et performance de la machine :

Bonne précision :

- fréquence élevée des mesures
- sonde embarquée
  → impacte CPU et disque de l'hôte

Bonne performance :

- fréquence des mesures plus étagée
- sonde distante
  → impacte le réseau

L'idéal dépend certainement de la situation :

> routine : performance
> crise : précision

Précision vs performance

Souvent choisir entre précision des mesures et performance de la machine :

Bonne précision :

- fréquence élevée des mesures
- sonde embarquée

  → impacte CPU et disque de l'hôte

Bonne performance :

- fréquence des mesures plus étagée
- sonde distante

  → impacte le réseau

L'idéal dépend certainement de la situation :

> routine : performance
> crise : précision

Précision vs performance

Souvent choisir entre précision des mesures et performance de la machine :

Bonne précision :

- fréquence élevée des mesures
- sonde embarquée
  → impacte CPU et disque de l'hôte

Bonne performance :

- fréquence des mesures plus étagée
- sonde distante
  → impacte le réseau

L'idéal dépend certainement de la situation :

> routine : performance
> crise : précision

Précision vs performance

Souvent choisir entre précision des mesures et performance de la machine :

Bonne précision :

- fréquence élevée des mesures
- sonde embarquée
  → impacte CPU et disque de l'hôte

Bonne performance :

- fréquence des mesures plus étagée
- sonde distante
  → impacte le réseau

L'idéal dépend certainement de la situation :

> routine : performance
> crise : précision

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines

(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines

(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines

(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines

(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau du fonctionnement des machines
(serveurs, stations, équipements réseaux)

- l'utilisation système (%cpu, nbre de cores utilisés, chgt de contextes)
- nombre de processus (contentions, zombies)
- utilisation de la mémoire (cache, swap, fautes)
- utilisation des disques (lectures/écritures, wait sur I/O, remplissage, pannes, t^o)
- utilisation des réseaux (débits, latences, bande passante utilisée, taux d'erreurs)
- température processeurs, température du boîtier
- vitesse de rotation des ventillateurs
- sécurité (nbre d'authentifications, tunnels, nbre de tentatives échouées de login, scans)
- disponibilité des services (files d'attente batch, interfaces, DHCP, DNS, LDAP, ...)
- compteurs hardware si disponibles et pertinents (mcelog, collectd, ...)
- sabordage de runs (atteinte de limite de temps, plantages, bouclages)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Que contrôler ?

Quelques exemples au niveau environnemental ou périphérique

- température de salle (climatiseurs)
- niveau d'eau (innondation, fuites, hygrométrie, ...)
- état des onduleurs (% capacité, temps de disponibilité, état des batteries)
- utilisation des ressources (remplissage des disques, temps de calculs, ...)
- intrusions logiques (login d'utilisateur sur des systèmes restreints, ...)
- intrusions réseaux (correspondance adresses MAC-IP, scans)
- intrusions personnelles (salle système, bâtiment)
- statistiques (taux d'utilisation par utilisateur/groupe, ...)
- ...

Cas particuliers

Les périphériques spécialisés qui intègrent leur propre système de supervision :

- systèmes de stockage : cartes/baies de RAID (3Ware, PERC, ...)
- switches manageables
- périphériques : imprimantes, scanners, ...

Comment intégrer ces moniteurs dans le tableau de bord ?

Choix d'un superviseur

Quelques critères de choix d'un superviseur :

- capacité d'analyse et de restitution
- offre et variété des dispositifs d'alerte
- notoriété, pérennité
- souplesse de configuration et de déploiement
- nombre et type de 'sondes' existant (celles dont j'(aur)ai besoin !)
- protocoles utilisés / supportés
- possibilité / complexité d'extensions (plugins, . . .)
- architecture générale (multi-site, limites de capacités)
- look and feel
- impact local/distant
- capacité à collaborer avec d'autres moyens de supervision / monitoring
- . . .

Conclusion

- le monitoring/supervision est nécessaire
- beaucoup d'outils disponibles
- choix adapté en fonction des configuration/contraintes
- adopter une démarche qualité : évolutivité de la solution