Quels sont les outils d'aujourd'hui de supervision réseau LAN/WAN

TOME IV

Jean-François CASQUET
jfcasquet@yahoo.fr

Septembre 2004

Pourquoi superviser un réseau ?

TOME IV chapitre 1

Qu'est-ce qu'un Réseau ?

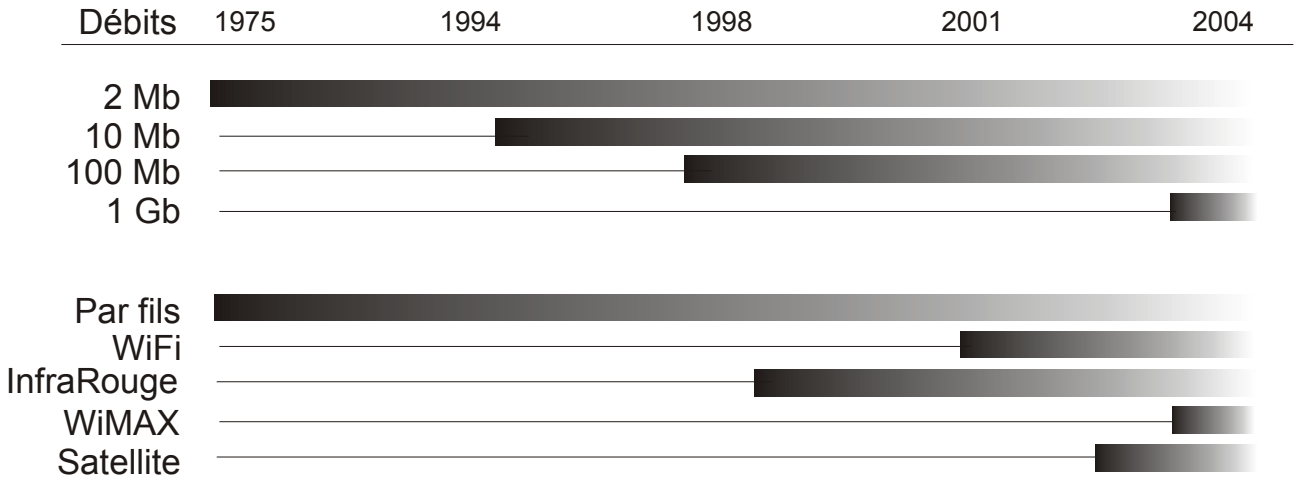
Les Origines du LAN

4.1.1

A quelle date a été inventé le LAN ?

Un réseau informatique = mise en communication entre machines informatiques dans le but de partager des informations (ressources).

Le support de communication dans le temps (grand-public)



IMPORTANT

Qui sait ce que seront les Réseaux de demain ?

CE QU'IL FAUT RETENIR

Bloc Note

Un réseau provoque la communication entre éléments informatiques - mais peut-être aussi à votre insu !

Que veut dire “Superviser” ?

4.1.2

Super = au dessus
Viser = regarder

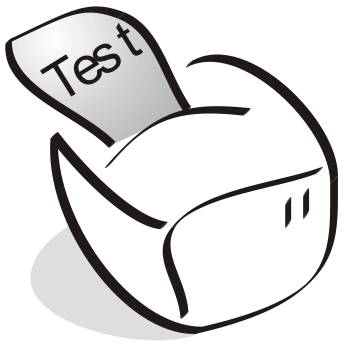
} Regarder au dessus ≠ regarder l’information

Regarder l’information = espionner
Regarder au dessus de l’information = surviser

Dans un Réseau informatique, que veut dire “superviser” ?

Il s’agit de regarder TOUT sauf l’information.

EXEMPLE



Espionner = on a imprimé “Test”

Superviser = on a imprimé 1 feuille

IMPORTANT

Superviser ne vous autorise pas à regarder l’information.

CE QU’IL FAUT RETENIR

Bloc Note

Il faut vérifier que la frontière entre superviser et espionner n’ a pas été franchie.

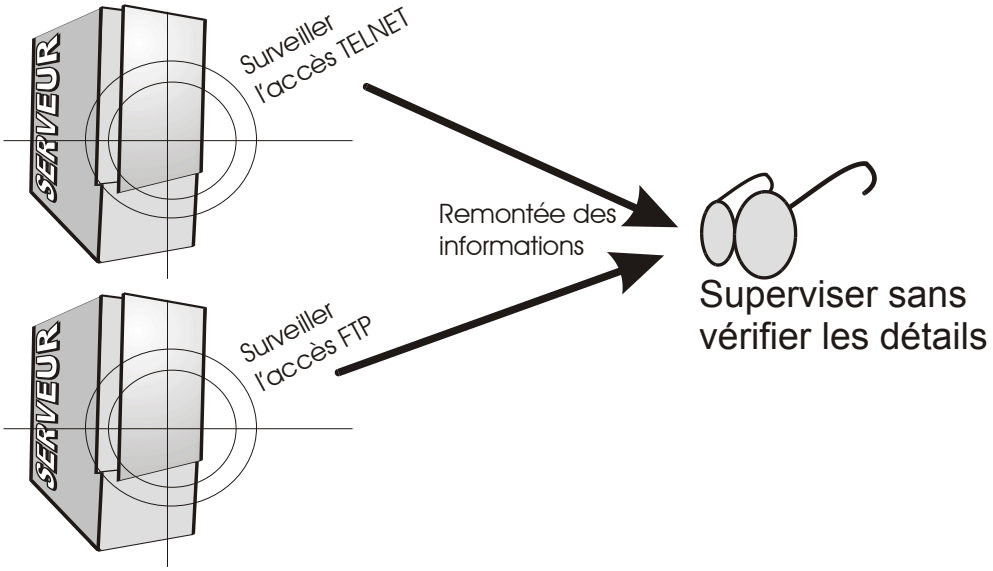
Différence entre superviser et surveiller

Surveiller = Veiller Sur
Superviser = Regarder au-dessus

La surveillance = Regarder quelque chose de précis.
Par exemple : surveiller la porte d'entrée (rien d'autre).

Superviser c'est, en réalité, surveiller plusieurs organes.

EXEMPLE



IMPORTANT

Superviser c'est veiller sur les organes en remontant les informations quantitatives

CE QU'IL FAUT RETENIR

Bloc Note

Avant de superviser, il faut que je sache ce que j'ai besoin de surveiller.

Pourquoi superviser ?

4.1.4

Je supervise dans le but d'être informé sur l'état de mon réseau ou de mes applications …

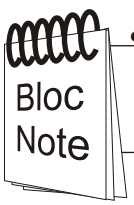
Je supervise pour ne pas tomber des nues !

Si je ne supervise pas :

- Je peux être piraté sans le savoir
- Mes serveurs peuvent être fatigués
- Mes performances peuvent tomber
- Les utilisateurs préviennent en cas de panne - je perds toute crédibilité
- Ma Direction se lasse : "l'informatique est toujours en panne" …

IMPORTANT

Je supervise pour ma tranquillité et ma crédibilité



CE QU'IL FAUT RETENIR

J'ai besoin de la supervision pour mon image.

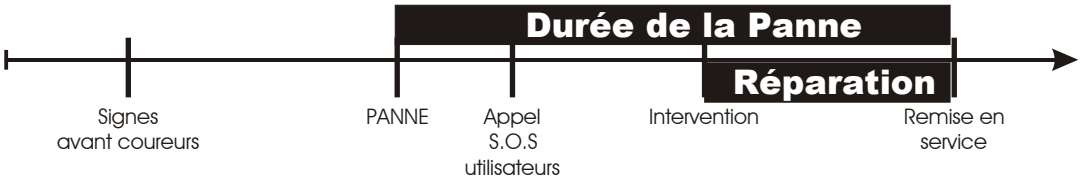
Pourquoi ne pas attendre la panne ?

Tout simplement

4.1.5

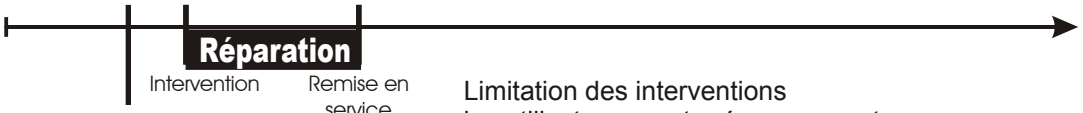
En plus de ma crédibilité - quels sont les enjeux de ma passivité ?

Si j'attends la panne



Si je supervise mal (post-panne)

Je supervise correctement (tolérance aux pannes)



Limitation des interventions
les utilisateurs sont prévenus avant pour que l'intervention puisse être planifiée
L'image de l'informatique s'améliore
Les motifs des pannes peuvent être trouvés pour améliorer les systèmes

IMPORTANT

Superviser sert aussi à prévenir des pannes.

CE QU'IL FAUT RETENIR

Bloc Note

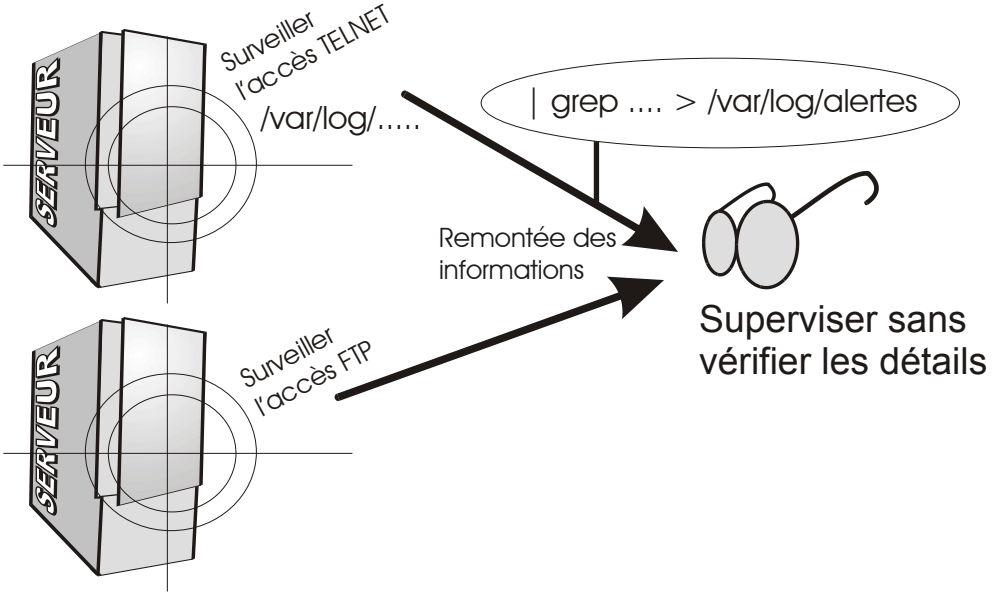
Plus les interventions sont courtes, plus on communique sur les actions préventives - plus les usagers travailleront en nous donnant la confiance et les crédits.

Oui mais : comment faire ?

Il faut trouver les tests à faire - savoir ce qu'il faut vérifier …

En face de chaque test à faire il faut trouver LA ou LES fonctions (commandes) de surveillance.
En face de chaque commande de surveillance il faut construire les trames de résultat qui permettront la supervision.

EXEMPLE



IMPORTANT

Préparer vos tests de surveillance en considérant tout de même la charge CPU - faire trop de tests tue le test !

CE QU'IL FAUT RETENIR

Bloc Note

Il est capital de vérifier que ce qui est surveillé remonte bien les 2 états : OK et KO - car un état intermédiaire peut cacher un problème...

Quels sont les impacts réels d'une défaillance ?

TOME IV chapitre 2

Qu’est-ce qu’une défaillance ?

4.2.1

Défaillance = passer d’un état normal à un état dégradé.

Niveaux de défaillance :

Légère : il s’agit d’un critère qui présente un état instable

Passagère : un élément défaille d’une manière prévisible et prévue (action de maintenance qui provoque une interruption de service)

Localisée : la défaillance ne provoque pas de problème de qualité de service

Grave : La défaillance affecte la qualité de service

IMPORTANT

Une défaillance peut être normale - lorsqu’elle est prévue.

CE QU’IL FAUT RETENIR

Bloc Note

Le niveau de gravité d’une défaillance DOIT ÊTRE évaluée avant qu’elle ne se produit - le niveau est défini et caractérisé par le choix technique de surveillance.

Suis-je responsable d'une défaillance ?

4.2.2

Puisqu'une défaillance peut intervenir sans "prévenir" - sans notre volonté … En serais-je responsable pour autant ?

Premier cas :Une défaillance grave est apparue avec des éléments annonciateurs (disque dur … ventilateurs ...)

J'en suis responsable

Second cas : Une défaillance sans éléments annonciateurs (alimentation ...)

Je n'en suis pas responsable
A condition, toutefois, de démontrer qu'aucun élément n'aurait pu l'annoncer.

Troisième cas : Une défaillance prévue et organisée (arrêt pour maintenance ...)

J'en suis responsable
à moins d'avoir communiqué suffisamment tôt

IMPORTANT

Si une défaillance était prévisible, je suis responsable de mon immobilisme.

CE QU'IL FAUT RETENIR

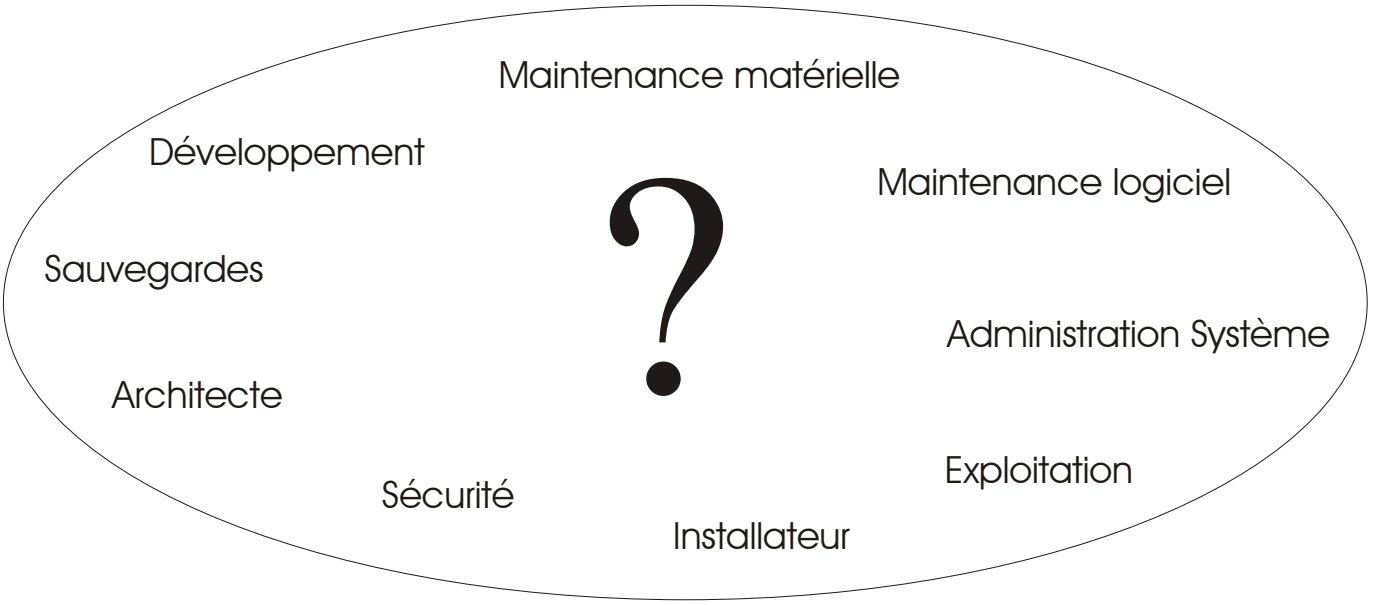
Bloc Note

Suivant le cas, la défaillance, même pour des opérations de "routine", peut entraîner notre responsabilité personnelle.

Où se trouve ma responsabilité ?

4.2.3

Chaque métier de l'informatique a sa responsabilité.
Il faut donc savoir où se trouve la nôtre : le périmètre de ma responsabilité est décrite par l'intéraction avec mes collaborateurs (et prestataires).



IMPORTANT

Dans l'organigramme de la Société, nous trouvons les autres intervenants afin de débusquer les métiers manquants : car, nous, l'Administrateur récupèrons ces fonctions d'une manière intuitive !

CE QU'IL FAUT RETENIR

Bloc Note

Il ne faut pas être laxiste en pensant que la défaillance pourrait être attribuée à quelqu'un d'autre.

Comment mesurer l'impact réel d'une défaillance ?

4.2.4

Recette de cuisine : Simuler la défaillance au pire des cas !

Par exemple : (pour ce qui concerne les sauvegardes) afin de connaître l'impact réel d'une défaillance, "disons qu'il y a eu le feu, les sauvegardes sont brûlées" …
Combien de temps faut-il pour tout refaire (si c'est possible) !
Mesurez le coût ....
A ce moment là, tout naturellement, le responsable apparaît à l'évidence - car "c'est le rôle de personne d'autre" !

Devant le coût et les conséquences : c'est à nous de mettre en place ce qu'il faut pour prévenir la panne, voire même, le sinistre …

IMPORTANT

Il faut simuler le sinistre pour que chacun se mouille vraiment.

CE QU'IL FAUT RETENIR

Bloc Note

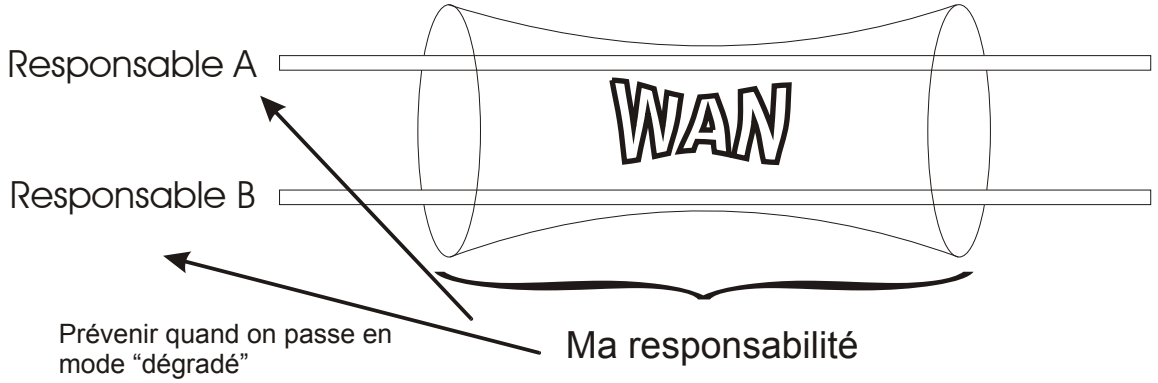
Veillez à ce que les conséquences d'une défaillance ne vous fasse pas tomber avec elle !

Comment répartir ma responsabilité sur les vrais acteurs ?

Recette de cuisine : Faites le schéma et écrivez ce que chacun fait en cas de sinistre.

Par exemple : Je suis responsable d'une liaison WAN.
Je dois donc me demander qui sera pénalisé en cas de défaillance.

Il faut donc noter les responsables et les éléments qui réclament une qualité de service.



IMPORTANT

Il faut trouver les intervenants qui dépendent de mes services afin de leur céder une part de responsabilité.

CE QU'IL FAUT RETENIR

Bloc Note

Répartir notre responsabilité permet de faire correctement notre travail.

Que dit la loi sur ma responsabilité ?

Salarié ou pas

4.2.6

Les devoirs d'un salarié :

Respecter le Code du Travail
Accéder au devoir d'Alerte
Ne pas mettre en péril la Société par notre négligence

Si votre Société est mise en péril à cause de votre négligence - elle peut non-seulement vous licencier pour faute grave mais aussi entreprendre des actions civiles sur le motif "a cherché à nuire" (dommages et intérêts) !

Que vous soyez Salarié ou pas (prestataire, consultant ...) vous avez un "Devoir d'Alerte".
En clair : ne pas alerter = laisser une faille qui peut nuire = il faudra en cas de poursuites, démontrer que les faits ne vous donneraient d'une manière ou d'une autre, aucun avantage (vous êtes considérés comme coupables !)

IMPORTANT

Notre métier est important / Soyons PRO !

CE QU'IL FAUT RETENIR

Bloc Note

Ne jamais rester sans rien dire devant des choses qui peuvent provoquer une panne.

Comment faire la frontière entre la supervision et la maintenance préventive ?

TOME IV chapitre 3

Qu'est-ce que la maintenance préventive ?

4.3.1

Maintenance en prévention
en prévention de panne éventuelle

La supervision permet de déterminer qu'une panne (bien souvent logicielle) arrive (la face cachée d'un Bug).

EXEMPLE

Un processus qui ne libère pas la mémoire correctement provoque une saturation - avec le temps.
Un reboot est bien souvent suffisant (tous les programmeurs ne sont pas forcément bons !)
Le problème arrive assez souvent avec les Routeurs.

EXEMPLE

Un fichier LOG qui gonfle trop peut entraîner un plantage

Ecouter un serveur (à nos oreilles) suffit bien souvent pour prévenir d'une panne matérielle (ventilateur / disques durs …)

IMPORTANT

Le but du dossier n'est pas de prévenir d'une panne matérielle.

CE QU'IL FAUT RETENIR

Bloc Note

La supervision sert aussi à prévenir de défaillance et donc de préparer les opérations de maintenance préventive.

Comment mesurer le coût d'une maintenance préventive ?

4.3.2

Maintenance préventive = maintenance **SANS PANNE**

Il est difficile de démontrer qu'une opération de maintenance préventive soit utile ! Puisque la panne n'a pas eu lieu - tout au moins : pas encore !

C'est pourquoi :

1. L'opération doit être organisée pour ne pas perturber les usagers
2. Il faut que le coût soit prévu et justifiable par rapport aux pannes actuelles.

Recette de cuisine : Pour justifier l'opération, il suffit de démontrer le coût du nettoyage / remplacement / reboot / archivage … face au coût de la panne.

IMPORTANT

Si la maintenance préventive doit être jusitifiée par "moins de panne", il faut bien quantifier les pannes AVANT.

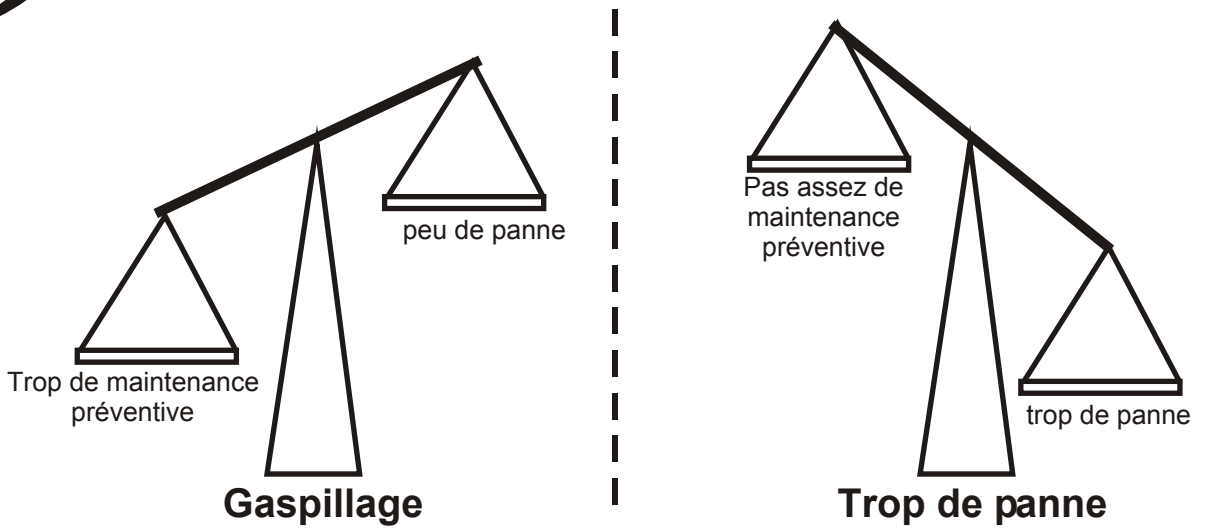
CE QU'IL FAUT RETENIR

Bloc Note

La maintenance préventive est très importante / mais trop de maintenance préventive sera considérée comme du gaspillage !

Juger de l'opportunité de la Maintenance préventive

4.3.3



L'opportunité = à chaque signe annonciateur il y a une durée "d'avant panne" - durant laquelle il faut intervenir.

EXEMPLE

archiver les Logs tous les jours = perte de temps = inutile = coûte cher

IMPORTANT

Prévoir une maintenance préventive même éloignée permet de crédibiliser notre métier - même si la panne arrive dans l'entre temps.

CE QU'IL FAUT RETENIR

Bloc Note

La maintenance préventive doit être prévue sur le calendrier pour juger à ce moment-là si l'opération est à prévoir.

Comment se servir de la supervision ?

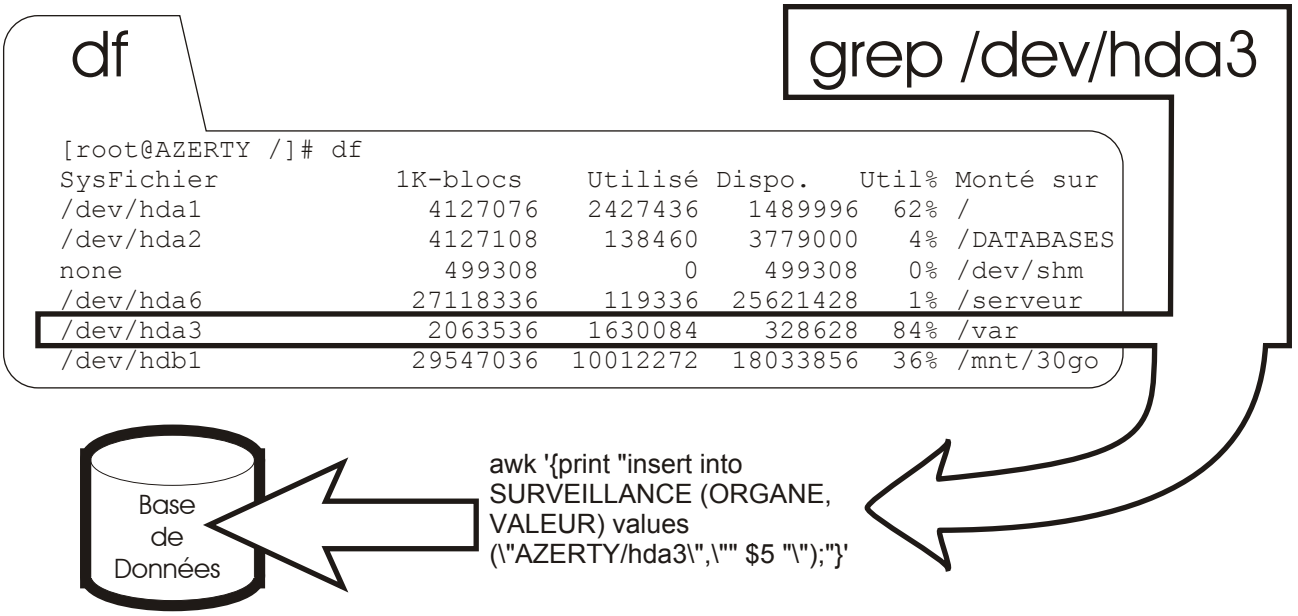
Prévenir des pannes

Avant tout : il faut se demander quelles opérations sont à vérifier.

EXEMPLE

```
df | grep /dev/hda3 | awk '{print "insert into SURVEILLANCE
(ORGANE, VALEUR) values (\"AZERTY/hda3\",\"" $5 "\");"}' >
/tmp/addSurveillance

mysql -e "\. /tmp/addSurveillance" STATISTIQUES_AZERTY
```



IMPORTANT

La supervision logiciel ne permet QUE de surveiller les logiciels. La surveillance matérielle est faite par l'équipe "exploitation".

CE QU'IL FAUT RETENIR

Bloc Note

La supervision doit être bien faite pour servir à la maintenance. Prévoir de remonter une information synthétique pour qu'elle puisse être utile.

Dans un monde de supervision et de continuité de service

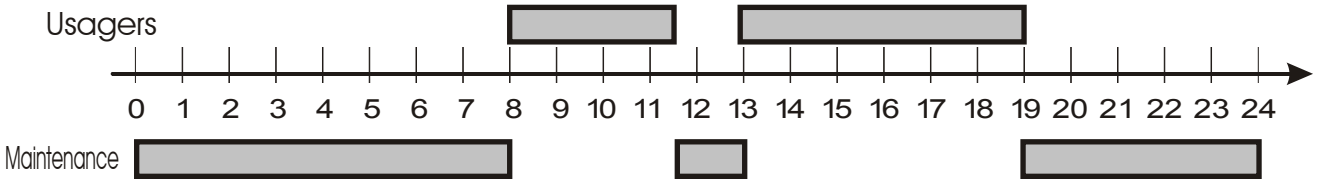
Une nouvelle notion : la “continuité de service”
= service continu pour les usagers

EXEMPLE

Je dois me renseigner sur les services qui doivent continuer …
ex: *“est-ce que CRON doit avoir une continuité de services? … pour les usagers”*

Il faut donc identifier les services qu’il ne faut pas interrompre (”ODBC”, “Telnet”, “Oracle”, ...)

Il suffit de placer les plannings de présence des usagers avec celui de la maintenance => continuité de service



IMPORTANT

Il faut que tout ce qui peut être fait, le soit durant les périodes de maintenance.

CE QU’IL FAUT RETENIR

Bloc Note

La supervision me permet de préparer mes opérations de maintenance sur les plages d’absence des usagers.

Equilibrer continuité de service et maintenance

4.3.6

Comment faire pour que la maintenance soit en équilibre avec la continuité de service ?

Recette de cuisine

La supervision me permet de voir une défaillance qui peut arriver.. Je vais donc écrire ce qu'il se passe pour me faire un "retour d'expérience" et donc : de prévoir l'opération de maintenance avant même un symptôme = maintenance préventive.

Pour trouver l'équilibre, il suffit de planifier les opérations de maintenance préventive hors horaire des usagers.

Aucun usager n'est présent environs 15 heures par jours ! et ceci sur 5 jours.

Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche
15 h de libre	15 h de libre	15 h de libre	15 h de libre	15 h de libre	24 h de libre	24 h de libre

IMPORTANT

Prévoir d'aménager les horaires de travail afin de tester les procédures de maintenance préventives (ré-indexer les bases de données, vérifier les logs, sauvegarde système ...)

CE QU'IL FAUT RETENIR

Bloc Note

L'équilibre ne se trouve pas en 5 minutes. Des années d'expérience / des années de supervision permettent de trouver l'équilibre dans votre Entreprise.

A quoi sert le protocole SNMP ?

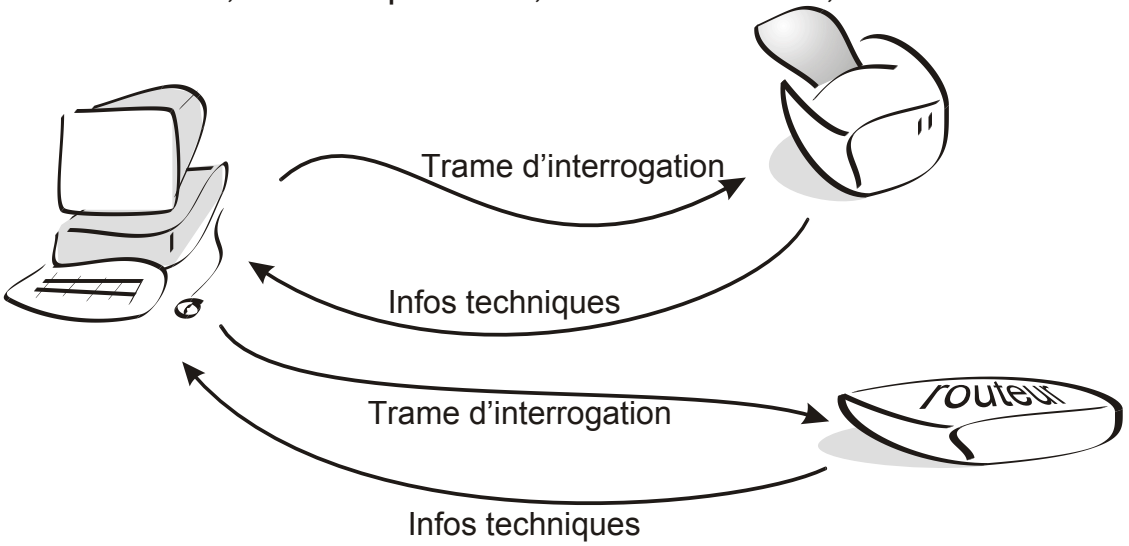
TOME IV chapitre 4

Un moyen standard de supervision

4.4.1

Existe-t-il un moyen standard de superviser presque tous les organes d'un réseau ?

Et s'il existait une norme pour connaître les informations internes d'un routeur, d'une imprimante, de certains HUB, de serveurs …



Effectivement, il existe plein de moyens pour superviser automatiquement les organes d'un réseau.
L'un des moyens actuels standard = SNMP (ne pas confondre avec SMTP = messagerie)

IMPORTANT

SNMP me permet de surveiller des organes réseaux (imprimantes, routeurs, hub, serveurs, station …)

CE QU'IL FAUT RETENIR

Bloc Note

Les appareils à superviser n'ont pas forcément l'option SNMP / dans ce cas il faut choisir autre chose.
On utilise l'outil fourni avec l'appareil.

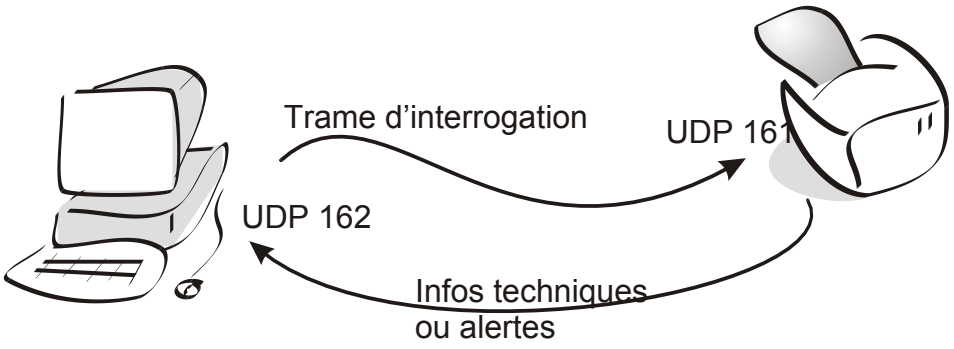
Un protocole de supervision

4.4.2

Pourquoi un Protocole de supervision ?

La raison est simple : elle est économique. L'élément n'a pas besoin d'être complexe pour avoir un agent SNMP. La complexité est renvoyée à la console de surveillance.

Qu'est-ce que je peux faire avec ? :
Connaître l'état d'un appareil => en lui envoyant une question
Avec une vue sur les données locales => nb paquets passés …
Configurer => en donnant un ordre, l'élément peut changer sa conf
Alerter => dans le protocole, un port est réservé aux alertes



IMPORTANT

SNMP est un protocole en 2 morceaux : la définition de la structure (MIB) et les trames elles-mêmes.

CE QU'IL FAUT RETENIR

Bloc Note

Chaque élément possède sa propre liste d'ordres et de résultats à une trame SNMP.

La M.I.B.

Management Information Base (MIB), en clair ?

Il s'agit d'un pseudo langage qui permet de définir les données à envoyer à l'élément pour obtenir le résultat voulu.

Ce langage possède même une aide que le constructeur nous donne pour mieux comprendre le résultat binaire de l'appareil.

En SNMP, les requêtes partent sous forme de code auquel l'appareil répond.

```
sysServices OBJECT-TYPE
   SYNTAX      INTEGER (0..127)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
         "A value indicating the set of services that this
         entity potentially offers.  The value is a sum.  This
         sum initially takes the value zero. Then, for each layer, L,
         in the range 1 through 7, that this node performs
         transactions for, 2 raised to (L - 1) is added to the sum.
         For example, a node which performs only routing functions
         would have a value of 4 (2^(3-1)).  In contrast, a node
         which is a host offering application service would have a
         value of 72 (2^(4-1) + 2^(7-1)).  Note that in the context
         of the Internet suite of protocols, values should be
         calculated accordingly:

            layer     functionality
              1       physical (e.g., repeaters)
              2       datalink/subnetwork (e.g., bridges)
              3       internet (e.g., supports the IP)
              4       end-to-end  (e.g., supports the TCP)
              7       applications (e.g., supports the SMTP)

         For systems including OSI protocols, layers 5 and 6 can also
         be counted."
   ::= { system 7 }
```

IMPORTANT

Un élément compatible SNMP n'est exploitable qu'avec sa MIB. Attention à l'ordre des bits !

CE QU'IL FAUT RETENIR

Bloc Note

L'agent SNMP de LINUX permet de créer une MIB sur mesure !

Eplucher les informations

4.4.4

Qu'est-ce qui est réellement utile ?

La MIB contient des informations techniques que le constructeur a jugé importantes - pas forcément intéressantes - pas forcément pertinentes dans le cadre de la supervision.

Par ailleurs, d'autres informations qui ne se trouvent pas dans le SNMP sont capitales pour la supervision (ex. état d'une base de données).

D'un autre coté, des informations qui semblent être sans importance reflètent des critères de supervision / par exemple : le nombre de pages qui évolue vite peut refléter une surcharge du serveur d'impression.

Des trames importantes sortantes du Serveur Proxy (internet) peuvent nous diriger vers une recherche de virus (spyware) dans le réseau.

IMPORTANT

Toutes les informations ne sont pas utiles - il faut non seulement les trier mais aussi les agrémenter d'autres données.

CE QU'IL FAUT RETENIR

Bloc Note

Il faut chercher les données utiles là où elles sont / SNMP ou autre.

SNMP et les autres protocoles

4.4.5

Il existe beaucoup d'outil d'aide à la gestion d'actifs informatiques (Gestion de parc) … quelques uns ont été sélectionnés.

Soft	Avantages	Inconvénients
SNMP	STANDARD Fonctionne avec presque tous les appareils réseaux	Ne fonctionne pas avec les applications (logiciels)
NSM	Fonctionne sur l'état des ressources + événements systèmes Paramétrable directement sur le système client (UNIX, NT, ...).	Ne s'adapte pas aux applications internes (ex. bases de données)
TIVOLI	Gamme de logiciels qui part de la gestion des ressources jusqu'à l'inventaire de parc. Bases de données centralisées.	Ne s'adapte pas aux applications internes (ex. bases de données)
MOM	Donne une vue sur l'état des services Micro$oft.	Compatible qu'avec Micro$oft
CGS	Fonctionne sur toutes les plateformes et ouvert aux développeurs qui veulent créer leur propre surveillance (ex. surveillance des ressources d'une application propriétaire). S'adapte au Bloc alarme ALRM2v5.	Ne sera commercialisé qu'en 2ième trimestre 2005

NSM : marque déposée par Computer Associates www.ca.com
TIVOLI : marque déposée par IBM www.tivoli.fr
MOM : marque déposée par Microsoft www.microsoft.fr
CGS : marque déposée par AZERTY MicroSystem gp.azerty.fr

IMPORTANT

Chaque Logiciel a son protocole préféré. Pour les appareils : SNMP. Pour les Stations : Agents locaux propriétaires.

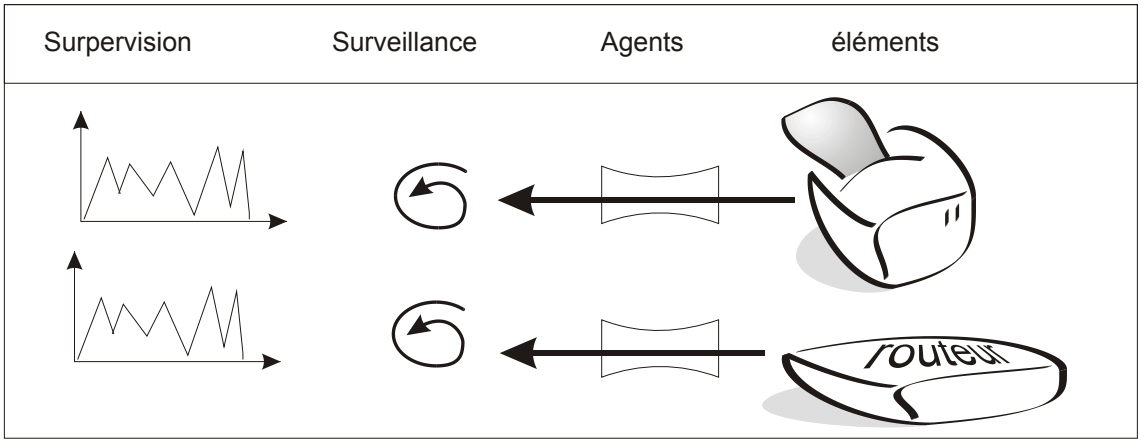
CE QU'IL FAUT RETENIR

Bloc Note

A chaque élément à contrôler (de VOTRE réseau), il faut choisir le Logiciel adapté pour superviser.

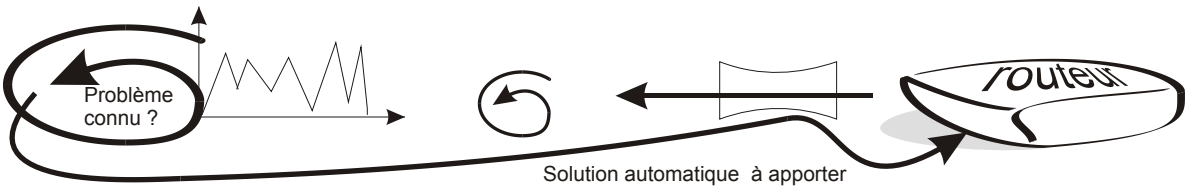
Vers quel type de protocole va-t-on ?

Attention, notre but est de parler “supervision”.



Mais que veut-on réellement ?

Bien plus que de la surveillance, en réalité, c’est, en cas de problème, d’automatiser la solution (autant que possible).



IMPORTANT

Les constructeurs et les éditeurs vont vers des protocoles bi-directionnels.

CE QU’IL FAUT RETENIR

Le choix du logiciel de surveillance prend donc toute son importance (base de connaissance des pannes ...).

Vers un protocole universel ?

4.4.7

Les constructeurs vont là où il y a de la rentabilité. Donc, ils vont tous dans des directions différentes.

En effet, pour parler des imprimantes, les constructeurs vendent de plus en plus leurs manageurs et leurs outils d'inventaires (CANON, HP, LexMark ...).

Aujourd'hui, uniformiser est très difficile.

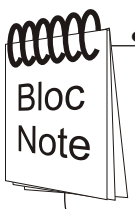
Le leader aujourd'hui est SNMP.

D'autant plus que les ordres de configurations font partie de son vocabulaire maintenant.

On le trouve sur les imprimantes réseaux, les Hubs, les routeurs, les serveurs (NT, UNIX, LINUX, As400, Switch ...)

IMPORTANT

Les constructeurs poussent vers des protocoles persos tout en maintenant une compatibilité SNMP.



CE QU'IL FAUT RETENIR

Les constructeurs font leurs normes. Personne ne les vérifie ! Et "eux", ils ne sont pas "OpenSources" - d'où le danger pour demain.

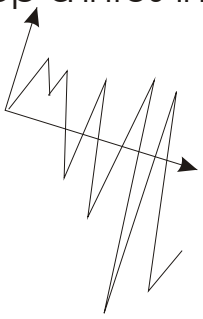
Comment choisir mes appareils ?

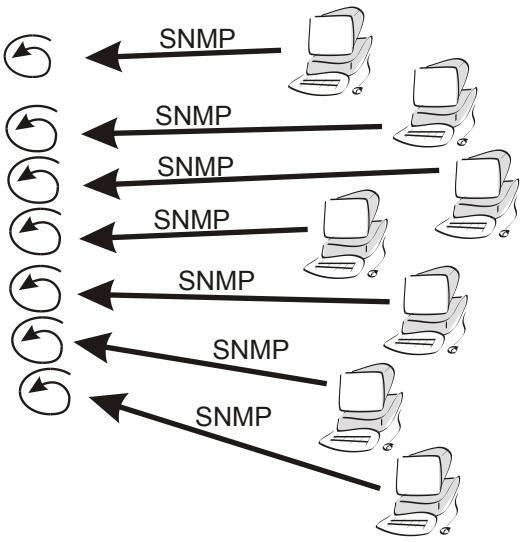
Soyons francs !

Les appareils que nous ne souhaitons pas surveiller n'ont pas besoin d'agent interne (SNMP ou autre).
Ex : un HUB vers les connexions internet
Ex : un agent SNMP sur les PC de bureautique

Par contre, dès lors où l'on veut surveiller, il nous faut un protocole qui soit compatible avec le reste de notre infrastructure.

Alerte !
Trop d'infos inutiles !





IMPORTANT

Je choisis des éléments administrables à condition de les administrer !?!

CE QU'IL FAUT RETENIR

Bloc Note

Les appareils avec un agent (SNMP) coûte plus cher / il faut donc mesurer la pertinence de nos choix.

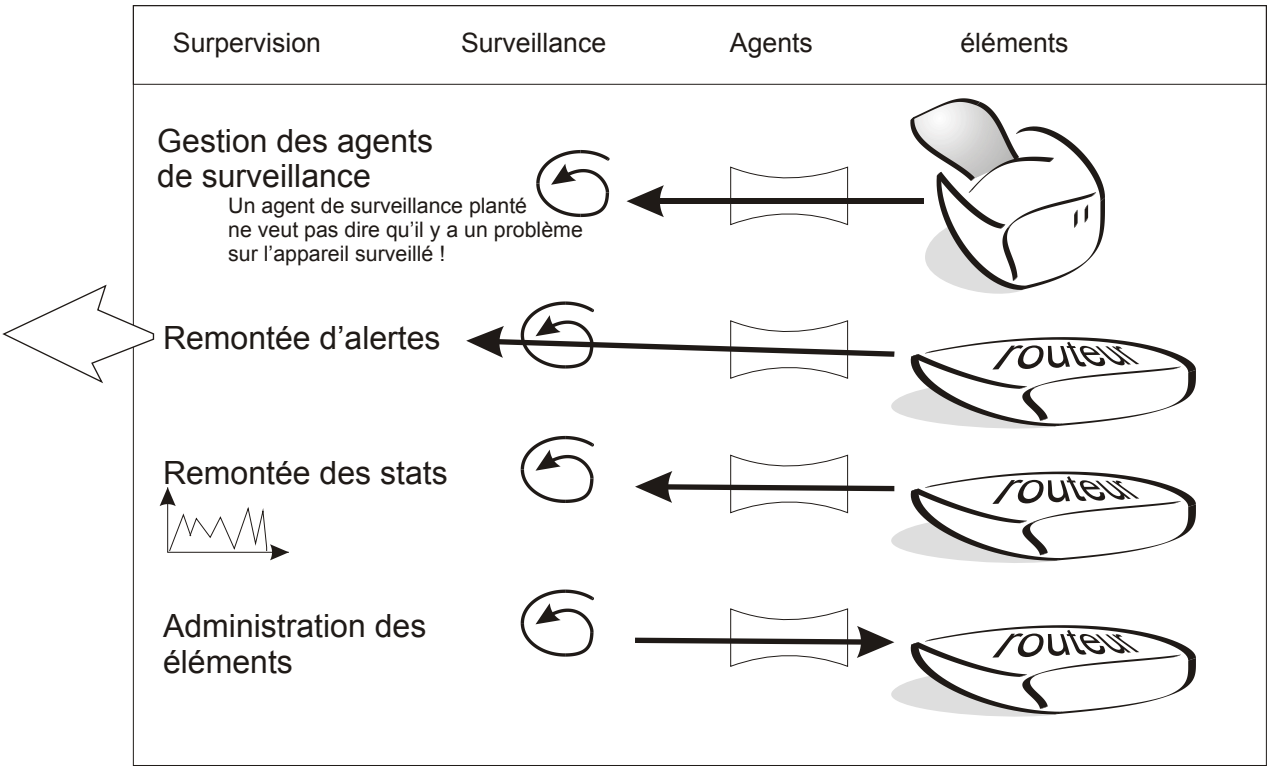
Quels outils de supervision NSM / TIVOLI / CGS ?

TOME IV chapitre 5

Outil de supervision

4.5.1

Qu'est-ce qu'un outil de supervision ? Quelles sont ces fonctions ?



IMPORTANT

Il ne faut pas multiplier les outils de supervision / car l'administration devient trop lourde.

CE QU'IL FAUT RETENIR

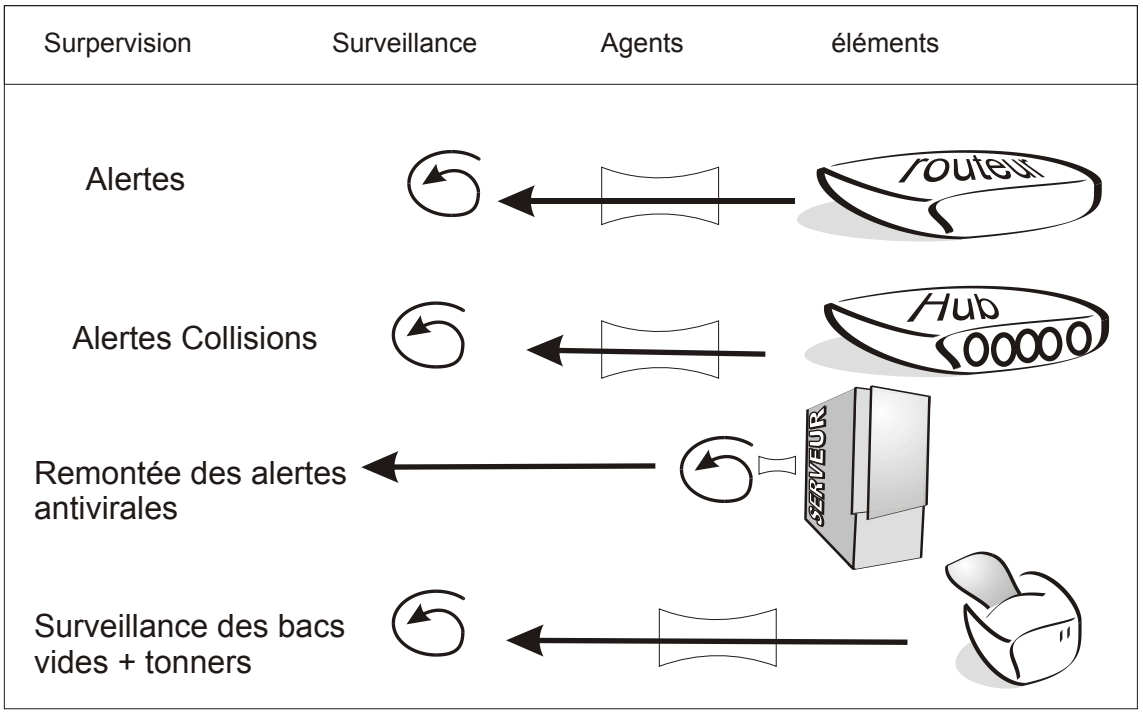
Bloc Note

Il faut choisir mon outil par rapport à ce que j'attends de lui.

Le rôle de l'administateur Réseau

4.5.2

Qu'est-ce qu'un outil de supervision ? Quelles sont ces fonctions ?



Le rôle de l'administrateur est de définir les organes à surveiller / ce qu'il faut surveiller et trouver ce qu'il faut faire à chaque alerte.

IMPORTANT

Après la remise en service, il faut trouver le motif de la panne pour qu'elle ne se reproduise pas (si possible) - pour certains routeurs le reboot régulier est nécessaire (le sachant, nous prévoyons alors de la maintenance préventive régulière.

CE QU'IL FAUT RETENIR

Bloc Note

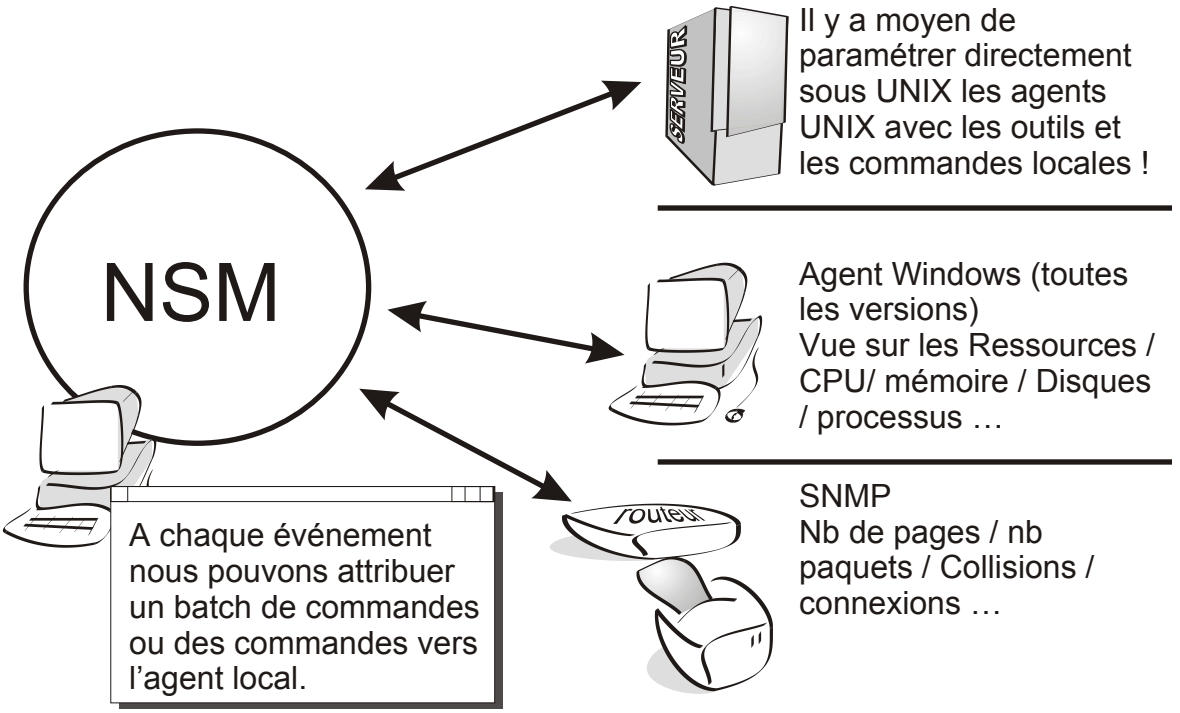
La définition de notre périmètre nous montre ce qu'il faut surveiller / il faut lister chaque élement.

NSM : atouts et faiblesses

4.5.3

Computer Associates a travaillé pour proposer une console de surveillance avec ses agents “multi plate-forme”.

En effet, la vraie problèmatique, c’est qu’il peut y avoir des centaines de choses à vérifier, et chacune avec des fréquences différentes (toutes les minutes, les heures ...).



IMPORTANT

Avantage : NSM possède plein d’autres fonctions (ordonnancement)
Inconvénient : Son prix / documentation incompréhensible

CE QU’IL FAUT RETENIR

Bloc Note

NSM est un produit qui tient la route / il s’appelait TNG.

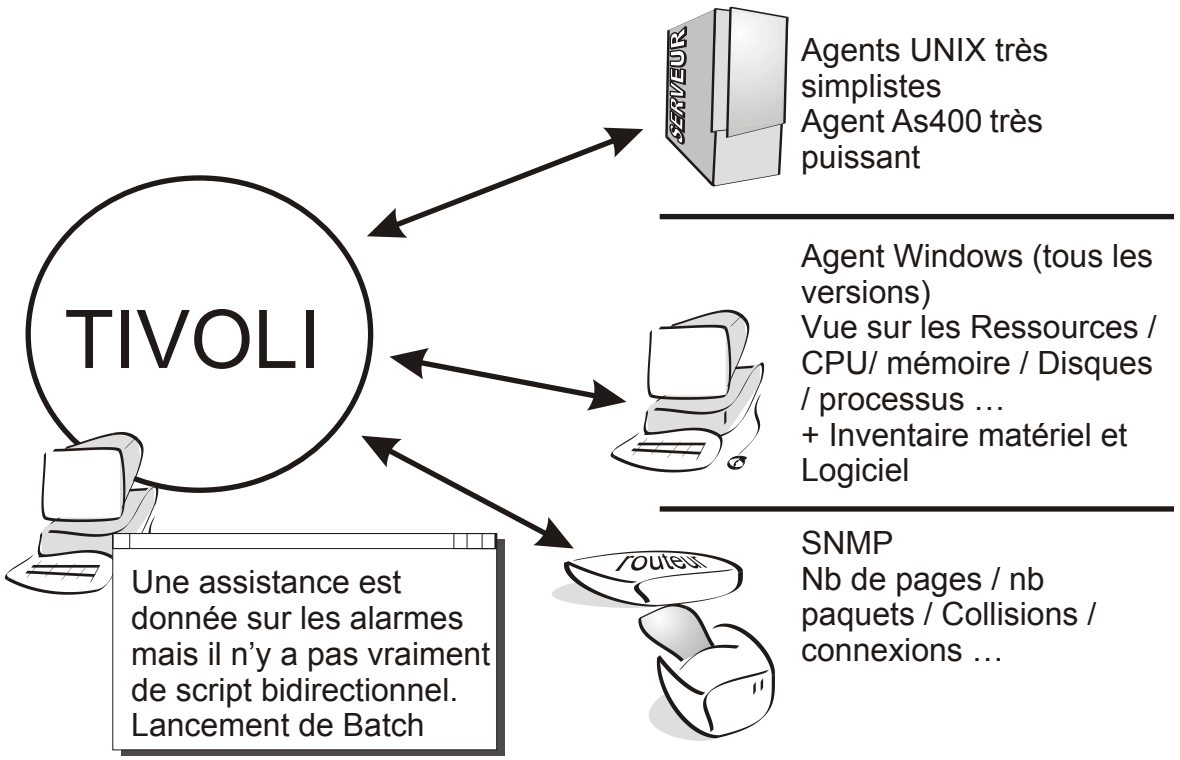
TIVOLI : atouts et faiblesses

4.5.4

IBM a voulu répondre à plusieurs problèmatiques en même temps :

- découverte automatique d'un réseau UNIX / Windows / SNMP / As400...

- Mise en base de données des informations d'inventaire pour la gestion de parc.



IMPORTANT

Avantage : Les données sont traitées et placées dans une base de référence (Gestion de parc)
Inconvénient : Ne résout pas la problèmatique de réponse automatique à une alerte.

CE QU'IL FAUT RETENIR

Bloc Note

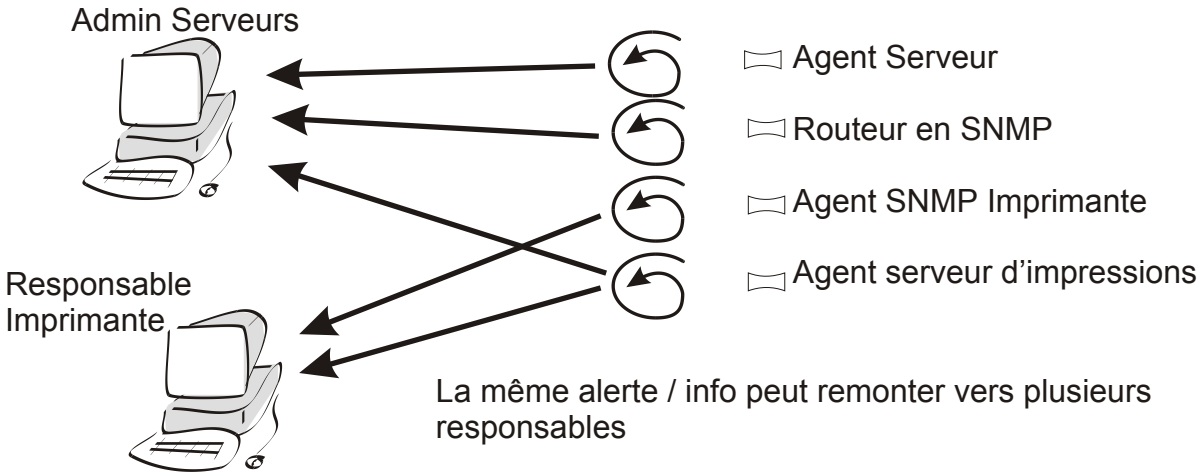
TIVOLI n'est pas vraiment un concurrent de NSM car ses fonctions d'inventaire le cloisonne à des clients de Gestion de Parc.

CGS : atouts et faiblesses

4.5.5

AZERTY MicroSystem a voulu répondre à une problèmatique d'ouverture au monde en faisant de l "opensource".

Une hiérarchie de serveurs et de consoles permet à chaque administrateur d'empièter sur le terrain des autres - sans y interagir.



IMPORTANT

Avantage : Les données sont traitées et placées dans une base de référence (Gestion de parc) + réponse automatique aux événements.
Inconvénient : Ne sera commercialisé qu'en juin 2005.

CE QU'IL FAUT RETENIR

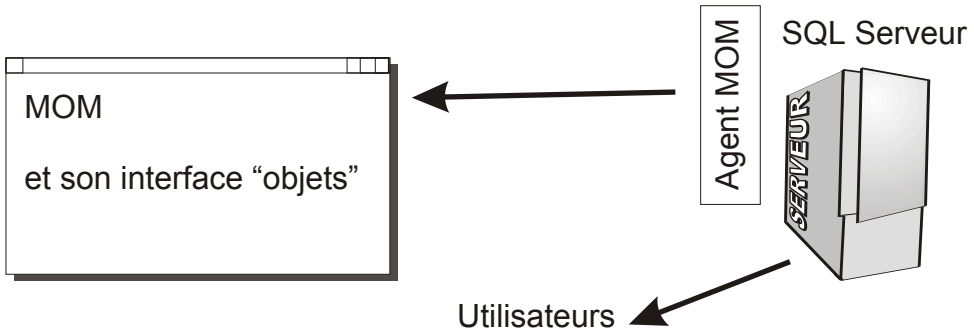
Bloc Note

CGS (SoftsCheckers) ouvre ses informations internes de fonctionnement afin que les administrateurs puissent créer eux-même un agent compatible avec tous les autres.

Les autres outils du marché

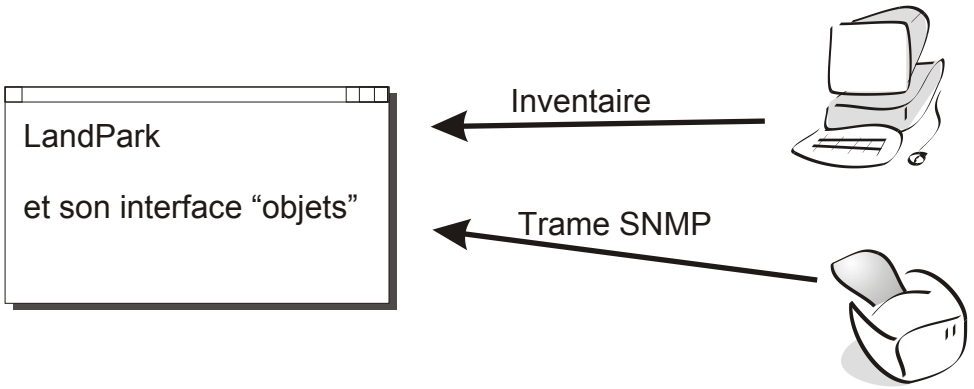
MOM de Micro$oft : le nombrilisme à grande échelle !

MOM vous permet de savoir si les applications microsoft qui tournent sur des serveurs microsoft, fonctionnent correctement ou pas.
Les agents de surveillance ne traitent que les informations délivrées par le service … donc, nous ne pouvons pas savoir réellement si les services fonctionnent correctement pour les usagers !



CERUS Informatique a développé LandPark.

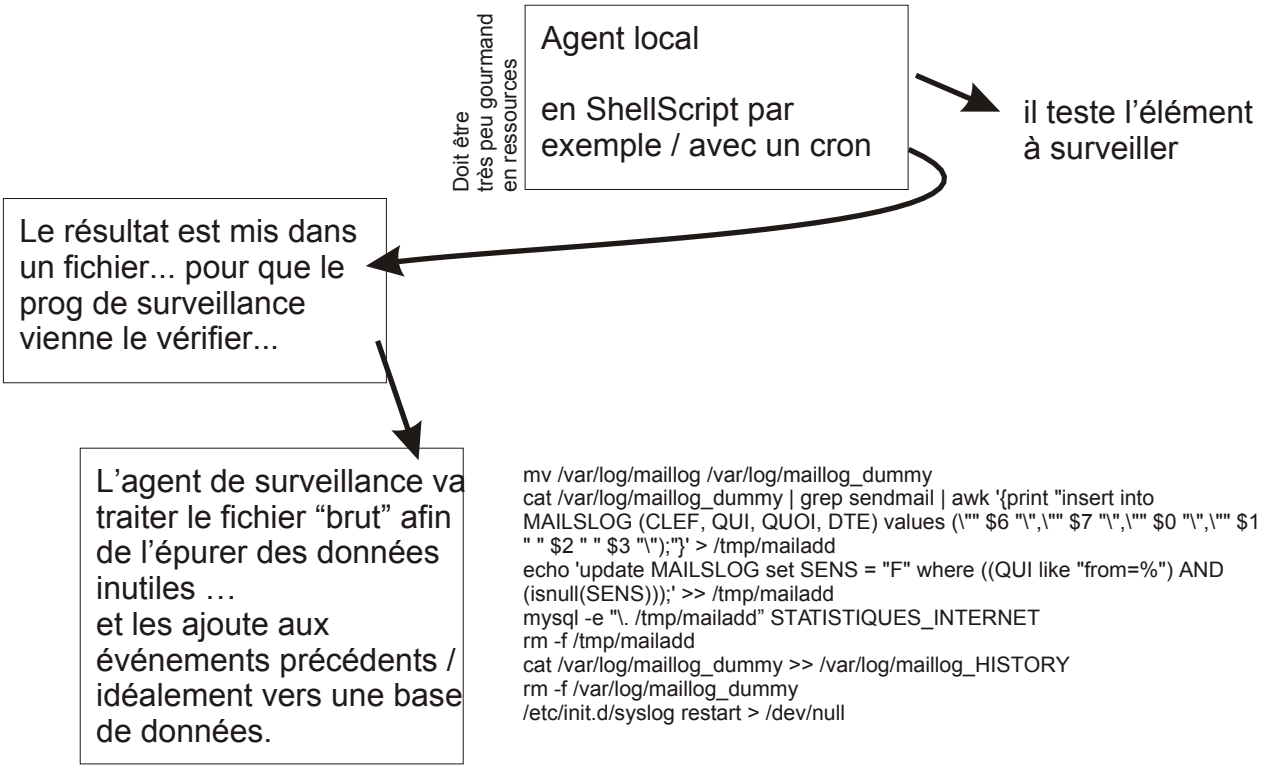
Il s’agit d’un logiciel de gestion de parc qui migre doucement doucement vers la supervision... (qu’avec SNMP et son agent d’inventaire).



Nous sommes prévenus s’il manque des feuilles dans l’imprimante … cool !
Mais il faut que nous regardions la fiche de l’imprimante dans le logiciel pour le savoir .... pas cool .....

Créer son propre outil de surveillance

Il faut se créer notre agent local (CRON par exemple).



L'outil de supervision ouvre la base de données afin d'y voir les informations linéaires et sous forme de requête afin d'avoir une visibilité claire.
L'outil de supervision peut être fait en PHP par exemple.

IMPORTANT

Attention, l'agent local doit être rapide et sans blocage car il pourrait engendrer des soucis involontaires.

CE QU'IL FAUT RETENIR

Bloc Note

Créer notre propre outil a l'avantage de répondre exactement à nos besoins.

Qu'est-ce qu'un Help-Desk
&
un WorkFlow ?

TOME IV chapitre 6

Qu'est-ce qu'un Help-Desk ?

4.6.1

Jusque là, nous avons vu comment repérer des pannes afin d'y remédier …
Mais savoir qu'il y a un problème : c'est bien

le référencer : c'est Mieux !

Imaginons que les incidents ne soient pas notés / comment trouver alors une récurrence aux pannes ?

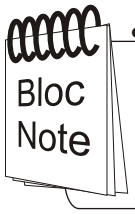
Un Help-Desk permet de noter les incidents et d'y indiquer la résolution.
Au début, c'est un bloc note de ce qu'il se passe …
C'est, à vrai dire, assez peu réjouissant et fastidieux ...

Rapidement, il devient un allier car, lorsqu'une panne ou un soucis apparaît, ces informations (du passé) nous aide à résoudre le problème du moment !
Toutes les informations s'appellent : une "base de connaissance"
ou un "Help-Desk".

Bien sûr, la méthode de rangement des informations est capitale !
Il faut ranger les données par thème et sous forme d'arbre logique.

IMPORTANT

Un Help-Desk est obligatoire / n'oublions pas qu'il est notre allier - d'autant plus lorsqu'on est plusieurs informaticiens.



CE QU'IL FAUT RETENIR

Avoir une base de connaissance permet aussi de mesurer le taux d'incidents afin d'être transparent.

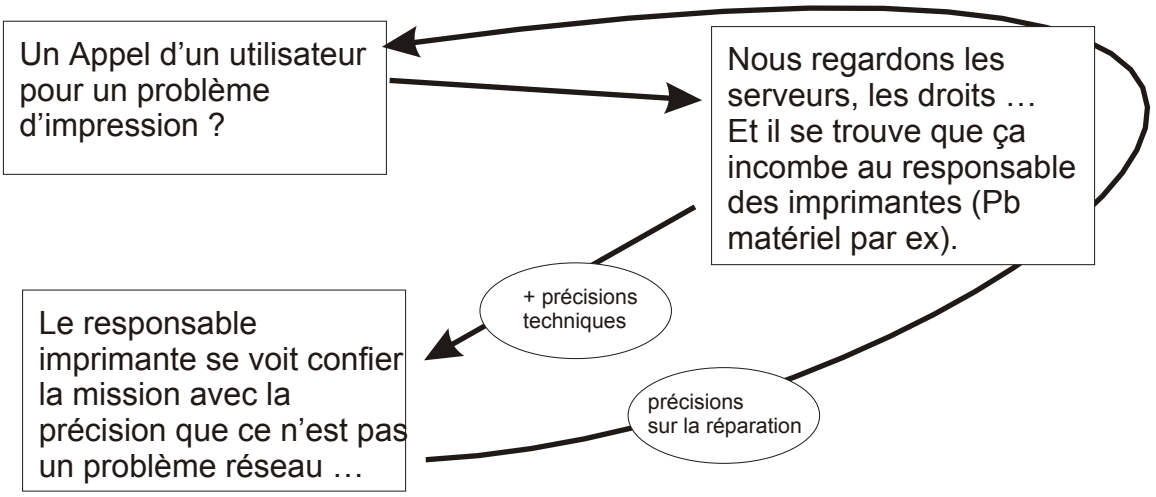
Qu'est-ce qu'un WorkFlow ?

Avoir une base de connaissance (Help-Desk), c'est capital !

Mais si un incident ne nous concerne pas ?

Ne serait-il pas intéressant de pouvoir transmettre (un peu comme un Email) les données techniques + infos du problème à la personne responsable ?

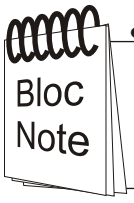
Et bien, un tel logiciel s'appelle un WorkFlow !



Le WorkFlow est un logiciel assez facile à mettre en place (ou en l'achetant) / il permet de mêler les compétences et le flux d'information entre services. Un peu comme un Mail, mais visible des autres intervenants.

IMPORTANT

Un WorkFlow permet à chaque intervenant de faire correctement son travail en le documentant.



CE QU'IL FAUT RETENIR

L'utilisateur est notre "client" (baromètre), veillons à ce qu'il ait le maximum d'informations.

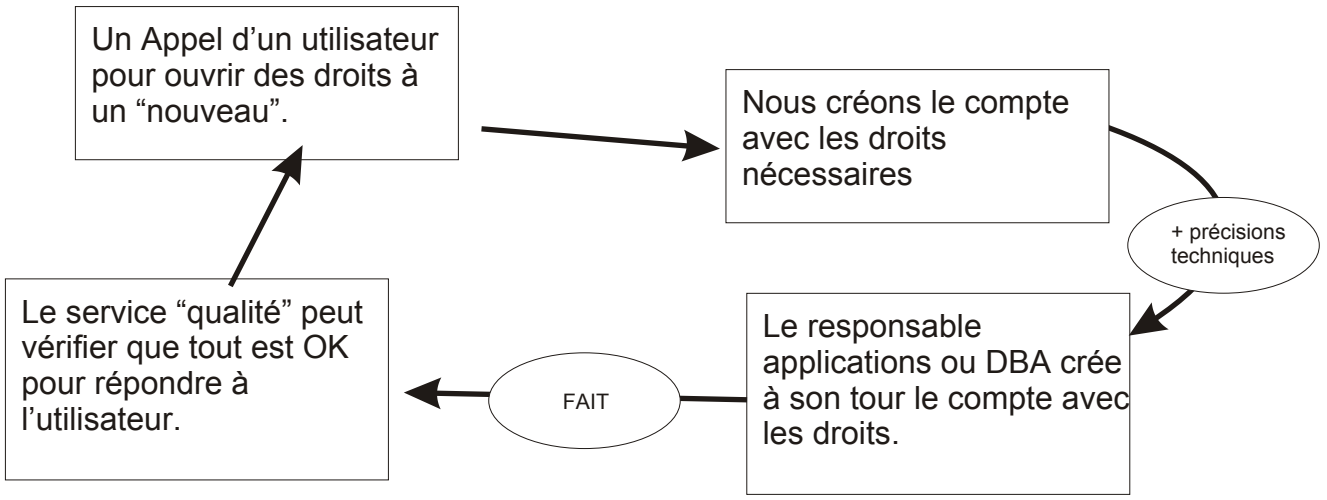
Faire jouer les acteurs ensemble

4.6.3

Bien sûr, il se pose la question de “comment faire travailler les acteurs ensemble” ?

Chaque intervenant peut être “missionné” par un autre - en lui donnant des informations techniques et personnelles sur la situation à son niveau.

Pour que les acteurs travaillent ensemble, il faut démontrer aux autres informaticiens que le WorkFlow répond à la communication, à la perte de temps et à la transparence pour l’utilisateur.



IMPORTANT

Avec un tel schéma, nous ne perdons plus de temps / et les utilisateurs sont contents aussi !

CE QU’IL FAUT RETENIR

Bloc Note

Bien plus que tout ça, le travail en WorkFlow permet de garder en historique les interventions ou les missions.

Organisation & Sérieux

A chaque demande du genre “changer les droits” / “créer un compte”, il nous faut noter QUI, QUAND, QUOI et POURQUOI nous le faisons.

Bref, il nous faut ces données (d’une manière ou d’une autre).
Le Help-Desk, aussi simpliste soit-il, répond à notre soucis de se souvenir pourquoi on a créé un compte le 10 janvier 2092 pour “cocolapin” ?!?

Certaines sociétés exigent des traces papiers.

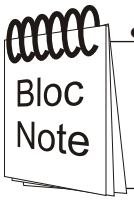
quand	qui	quoi	pourquoi	fait le

+ jusque quand

+ jusque quand

IMPORTANT

A chaque mission d’administration / pensez à documenter le pourquoi, qui, quand, quoi … et **jusque quand**



CE QU’IL FAUT RETENIR

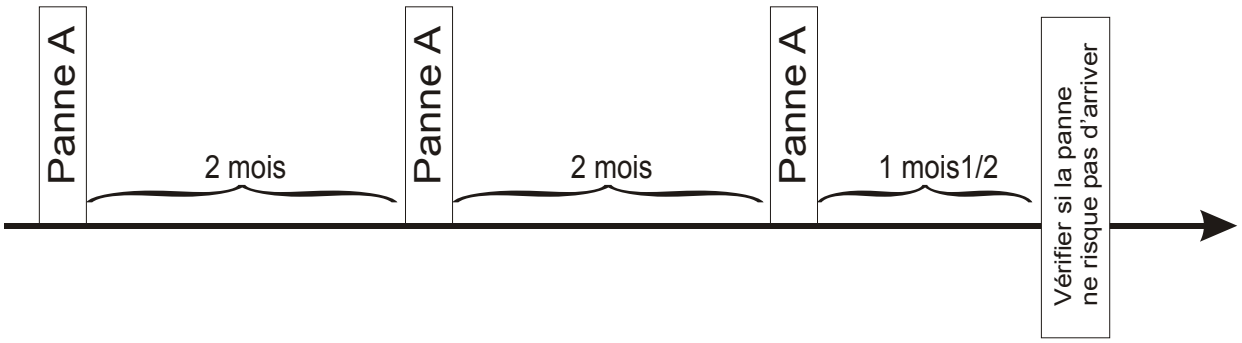
On oublie souvent le “jusque quand” - cette information est capitale pour un accès de sécurité.

Alertes bien gérées

4.6.5

Avec le Help-Desk, nous pourrons “voir” les cyclicités des problèmes (la récurrence).
Donc, entre le Help-Desk et le WorkFlow, nous pourrons facilement faire un planning des opérations de maintenance préventive pour anticiper les pannes.

Nous ne pouvons pas penser à tout. Donc il faut noter tout ça dans le Help-Desk.
Gràce à cette base de connaissance, nous pourrons faire des requêtes pour trouver les pannes récurrentes et les anticiper.



IMPORTANT

C’est avec le temps que nous améliorerons notre qualité d’administrateur.

CE QU’IL FAUT RETENIR

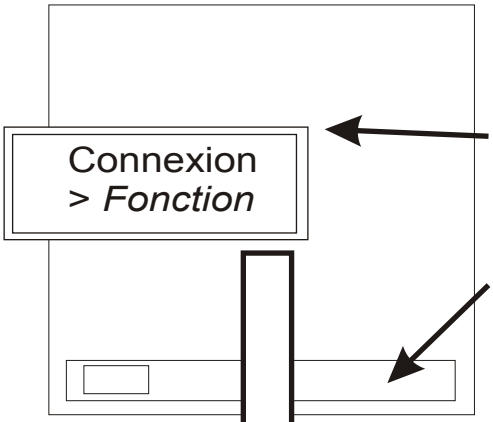
Bloc Note

Il s’agit d’un travail long et peu pationnant, mais il est notre force de demain.

Comment développer un WorkFlow

4.6.6

Il s'agit d'un logiciel qui permet de se passer les fiches entre responsables.



Le logiciel est conçu avec une partie haute : les données communes
Il s'agit là que de données d'une base de données.

et la partie basse : les boutons de circulation de la fiche / à envoyer vers …
ce qui peut changer l'état de la fiche (?!)

FONCTIONS

code	Libellé
1	D.I.
2	Resp. Impr.
3	Adm.Réseau

WorkFlow

Pos	EtatCourant	EtatSuivant	EtatCourant	InfoBouton de celui qui m'a mis ds cet état
1	1	1	Entrée infos	
2	2	3	Chez l'Adm Réseau	Envoyer à AdmRéseau
3	3	2	Chez le Resp. Impr.	Envoyer à Resp.Impr.
4	2		Clôturée	Envoyer à AdmRéseau
5	3		Clôturée	Clôturée par AdmRéseau
6	1		Avortée	Clôturée par D.I.

Interventions

IT	Date	Pos
40	..	1
41	..	5
42	..	2
43	..	3
45	..	2
46	..	4

Lors du Login de "Cocolapin" => groupe "Adm.Réseau"

Il se positionne sur la fiche en cours pour Lui :
une liaison entre Interventions.Pos == WorkFlow.Pos
Et ne liste que ceux pour EtatCourant == "3" (Adm.Réseau)
La liste des fiches pour Cocolapin : 42, 45 et 46

Dès que la fiche s'affiche / les boutons sont rafraîchis en bas :
exemple la fiche 42 :
Pos = 2 , EtatSuivant de Pos 2 = 3 donc nous listons tous les boutons qui ont un EtatCourant == 3 en mettant InfoBouton dans le bouton de WorkFlow / dès que l'on clique, la "Pos" du Bouton met à jour la Fichier Interventions.
Bien sûr, il est conseillé d'avoir un historique des actions en y mettant une zone commentaire pour le suivant.

Interventions

IT	Date	Pos
40	..	1
41	..	5
42	..	2
43	..	3
45	..	2
46	..	4

WorkFlow

Pos	EtatCourant	EtatSuivant	EtatCourant	InfoBouton de celui qui m'a mis ds cet état
1	1	1	Entrée infos	
2	1	3	Chez l'Adm Réseau	Envoyer à AdmRéseau
3	3	2	Chez le Resp. Impr.	Envoyer à Resp.Impr.
4	2		Clôturée	Envoyer à AdmRéseau
5	3		Clôturée	Clôturée par AdmRéseau
6	1		Avortée	Clôturée par D.I.

Bloquée à la réception

Boutons pour cette fice

Comment développer un Help-Desk

Il s'agit d'un logiciel qui de noter des infos classées sur thème avec les résolutions (base de connaissance).

THEMES

code	Libellé	Thème parent
1	HUB	
2	Routeurs	
3	Serveurs	
4	Linux	3
5	NetGear	2

Les thèmes sont rangés comme un arbre de pointeurs.

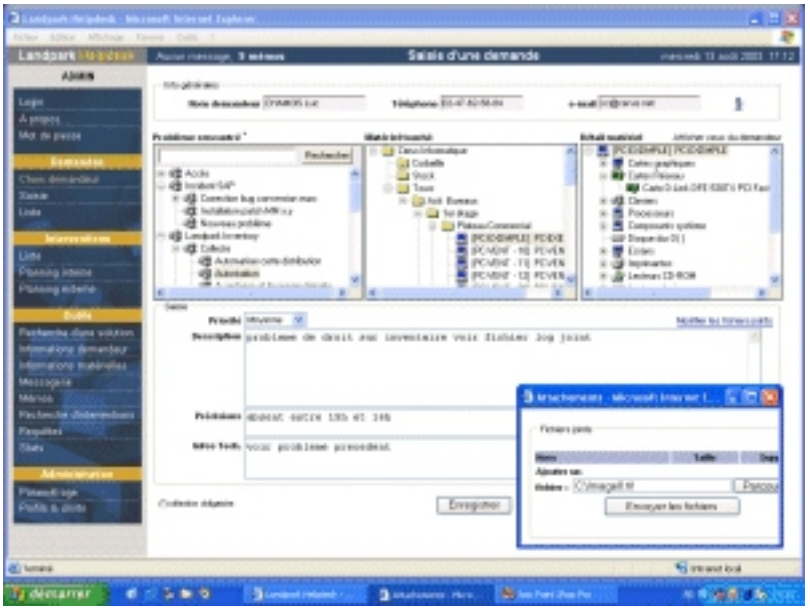
D'une manière linéaire, nous reconstruisons très simplement l'arbre.

FICHES

N°	Thème	Motif	Solutions apportés
1	1	fil débranché	rebrancher
2	5	SNMP tombé	rebooter le routeur
3	4	Créer un compte	adduser …
4	5	Ajouter une trame	interface HTTP://...
5	5	faire un test	connexion WIFI …

autres infos

Le Help-Desk doit avoir une interface la plus simple possible, sinon, nous n'y rentrerons pas grand chose.



Exemple d'écran sur LANDPARK

Comment gérer les escalades ?

TOME IV chapitre 7

Qu’est-ce qu’une Escalade ?

4.7.1

Toujours dans l’esprit du service à l’utilisateur, il faut pouvoir mesurer le délais d’intervention et la montée dans les alertes.

C’est ce qu’on appelle une “escalade”.

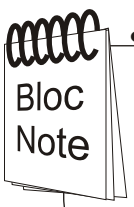
Si l’intervenant met trop de temps à résoudre le problème, le principe de l’escalade veut que la personne au dessus soit prévenue. (pas forcément hiérarchiquement)

Ce concept ne permet non pas de fliquer les délais (quoique), mais de ne pas mettre trop de temps à régler les problèmes.

En général, on s’en sert pour refaire une relance par Mail à la même personne à qui le dossier a été passé.

IMPORTANT

L’escalade est utile, voir nécessaire, lorsqu’il y a plusieurs intervenants - ça évite les dossiers bloqués.



CE QU’IL FAUT RETENIR

Ca demande une bonne entente dans le groupe de travail afin que l’escalade ne soit pas mal vécue.

Comment gérer les escalades ?

4.7.2

A chaque type de demande, il suffit de déterminer le délais après lequel la demande passe au suivant de l'escalade.

Dossiers
date … date d'arrivée chez l'acteur actuel numéro de l'acteur actuel

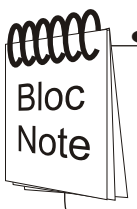
Escalades
Numéro acteur actuel Délais pour passer au suivant Numéro acteur suivant

Si "date d'arriver chez l'acteur actuel" + "délais pour passer au suivant"
Where "numéro de l'acteur actuel" = "Numéro acteur actuel"

Alors
"Numéro de l'acteur actuel" = "Numéro acteur suivant"
"date d'arrivée chez l'acteur actuel" = now()

IMPORTANT

Il ne s'agit que de requêtes SQL / beaucoup de logiciels de Help-Desk gérent les escalades.



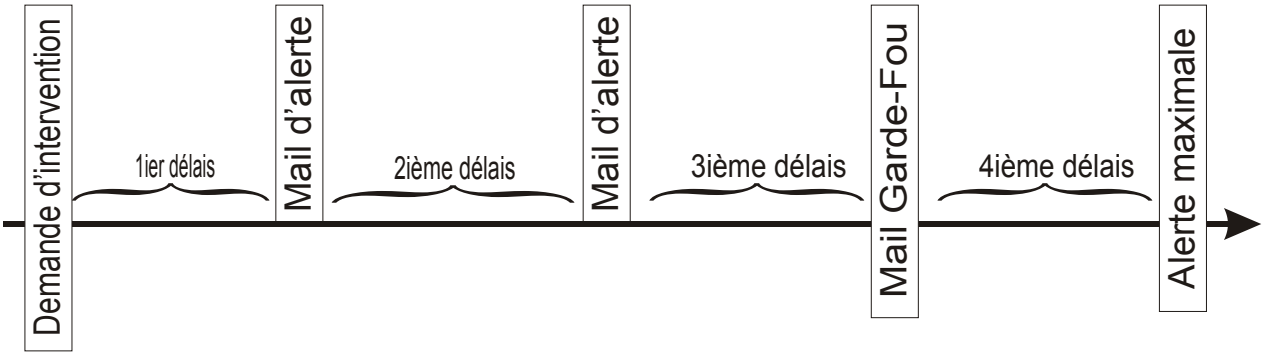
CE QU'IL FAUT RETENIR

La gestion des escalades n'apporte généralement pas de solution / elle ne fait que transmettre à l'autre les interventions à effectuer.

Pas d'escalades Maximales !

4.7.3

Une bonne gestion du suivi des demandes d'intervention permet d'éviter de faire traîner des demandes.
Afin d'éviter que les demandes n'arrivent en "haut" de l'escalade, il faut se mettre des gardes-fous.



Généralement, l'alerte maximale part vers notre supérieur ou vers l'utilisateur …

IMPORTANT

Il faut toujours prévoir quelque chose avant que les délais ne sortent du raisonnable.

CE QU'IL FAUT RETENIR

Bloc Note

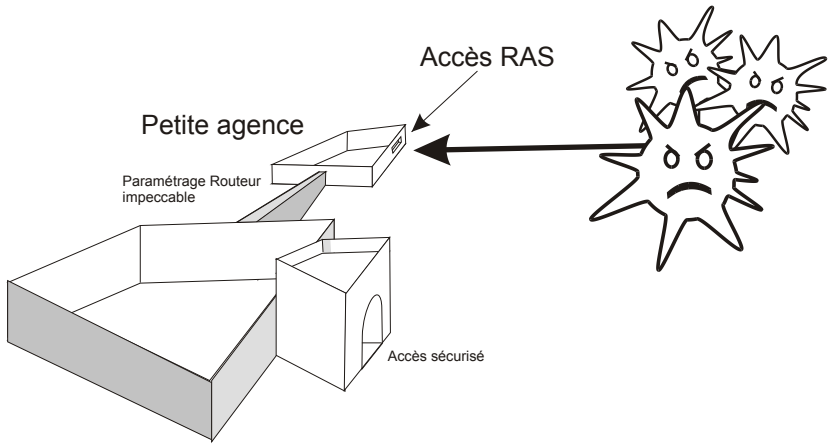
Pensez à déterminer des délais raisonnables pour chaque action / c'est la frontière entre la transparence et le professionnalisme.

Le rôle de l'Adminstrateur

4.7.4

L'Administration système est au centre du réseau de l'Entreprise.
Et c'est pour cela que nous en parlons aujourd'hui.
Car effectivement, dans toutes les Grandes Entreprises, il y a une Hot-Line (interne) qui "route" les appels au travers d'un WorkFlow (ou d'un organigramme).

Quelque soit l'Entreprise (voire même la nôtre), nous sommes au centre des escalades. A nous donc d'être exigeant car le moindre appel peut cacher une faille importante de la sécurité.



IMPORTANT

Même un administrateur ne peut pas connaître tous les accès extérieurs !
Un simple portable avec un Modem … Maintenant du WIFI …
Mais grâce aux appels (qu'il ne faut pas laisser monter en escalade) - nous construisons le ***VRAI*** réseau.

CE QU'IL FAUT RETENIR

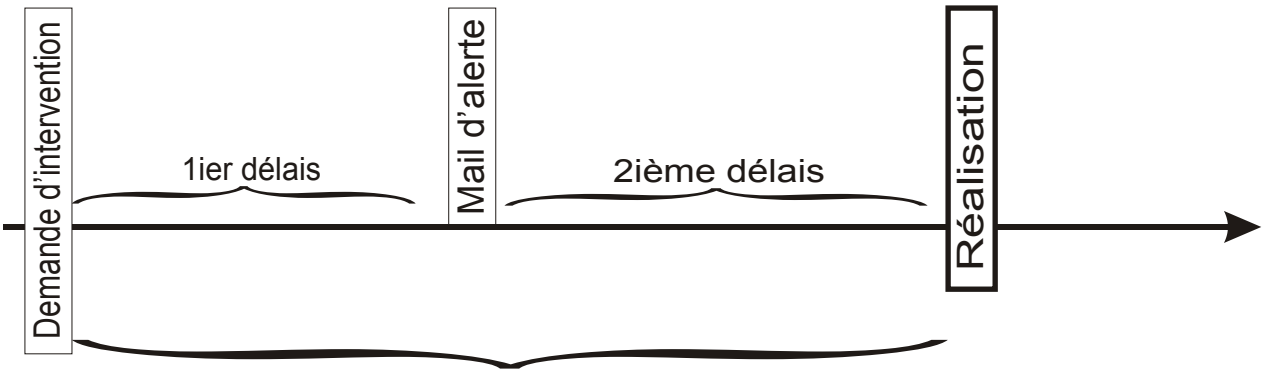
Bloc Note

L'écoute et la réponse aux utilisateurs est notre seule chance lorsqu'on entre dans une Entreprise (PME).

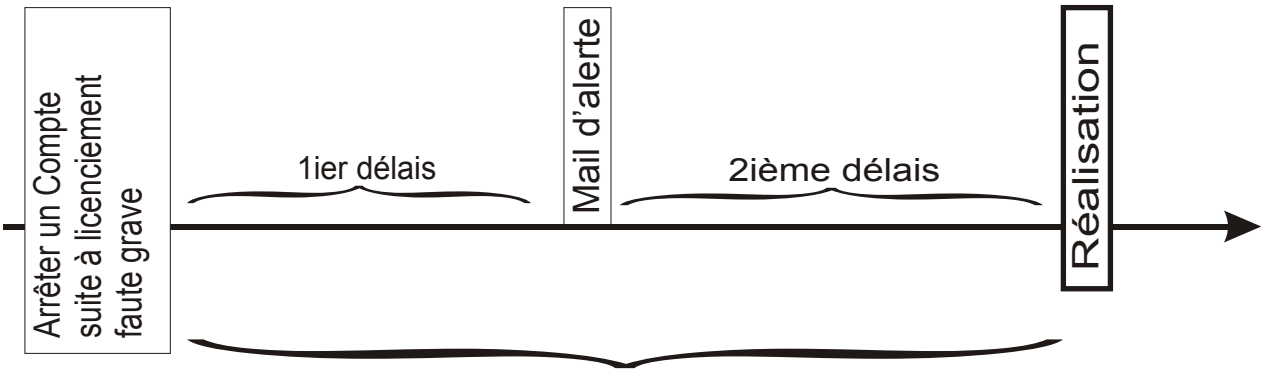
Le rôle de la sécurité dans l'escalade

4.7.5

A chaque type de demande, il suffit de déterminer le délais après lequel la demande passe au suivant de l'escalade.



Durée durant laquelle, si votre collaborateur ne fait pas vite son travail, il peut y avoir des conséquences sur la sécurité !



Délais durant lequel le réseau est vulnérable / d'autant plus avec un accès RAS !!!

IMPORTANT

En tant qu'agent de sécurité, nous devons être attentifs à **toutes** les demandes des utilisateurs / même si ça ne nous concerne pas (à priori).

CE QU'IL FAUT RETENIR

Bloc Note

Malheureusement, les Entreprises n'ont pas encore compris que l'agent de sécurité est "le passage obligé" pour toutes les demandes … *non pas pour y répondre !*

Mes escalades sont-elles correctes ?

4.7.6

Comment s'assurer que notre fonction n'est pas en péril à cause des escalades ?

L'exemple précédent est un peu la preuve qu'une escalade mal implémentée peut provoquer des soucis sérieux de sécurité !

Avec l'usage, les ajustements à réaliser nous sauterons à la figure / à condition d'y être attentif.

Grâce aux outils tels que le Help-Desk, WorkFlow et Supervision, nous limitons sérieusement les imprévus et les "on ne pouvait pas l'éviter" *(Bouyues Telecom Nov.2004)*

IMPORTANT

Rien ne peut, à priori, nous dire que la définition des escalades est correcte / c'est pourquoi "regarder" les délais de réalisation permet bien souvent de limiter la casse en relançant "humainement" l'acteur en retard ou laxiste.

CE QU'IL FAUT RETENIR

Le meilleur administrateur passera pour quelqu'un d'inutile puisque tout va bien...
Le même administrateur qui utilise le Help-Desk et le WorkFlow passera pour un expert car il résolve tous les soucis !
A nous de choisir !

Mise à jour de l'Organisation

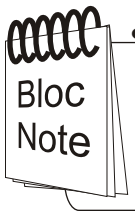
Autant ces méthodes pseudo-techniques sont indispensables, autant, ne rien changer dans l'Organisation malgré les anomalies, nous lasse !

Comme indiqué juste avant, ces outils nous permettent non seulement de valoriser notre travail mais aussi de pouvoir améliorer nos recherches de pannes au niveau de la supervision.

ex: IIS (de Micro$oft) tombe souvent en rade … il y a de nombreux appels pour cela.
Il nous suffit de créer un agent de surveillance du type "HEAD / HTTP/1.1" sur le port 80 sur serveur.
Le délais de réponse nous donne sa "santé" instantanée.
Notre supervision nous permet alors de prévenir une défaillance avant même les appels et réaliser nos opérations de maintenance préventive afin que le soucis ne paraisse plus quand les usagers sont là (Reboot du service pour IIS / *Micro$oft oblige*).

IMPORTANT

Ne pas croire que les appels puissent cacher un autre problème est souvent le reflet d'un manque d'organisation.



CE QU'IL FAUT RETENIR

Toujours être attentif à l'utilisateur / il est le thermomètre des applications informatiques !

Une supervision centralisée ou décentralisée ? Que choisir ?

TOME IV chapitre 8

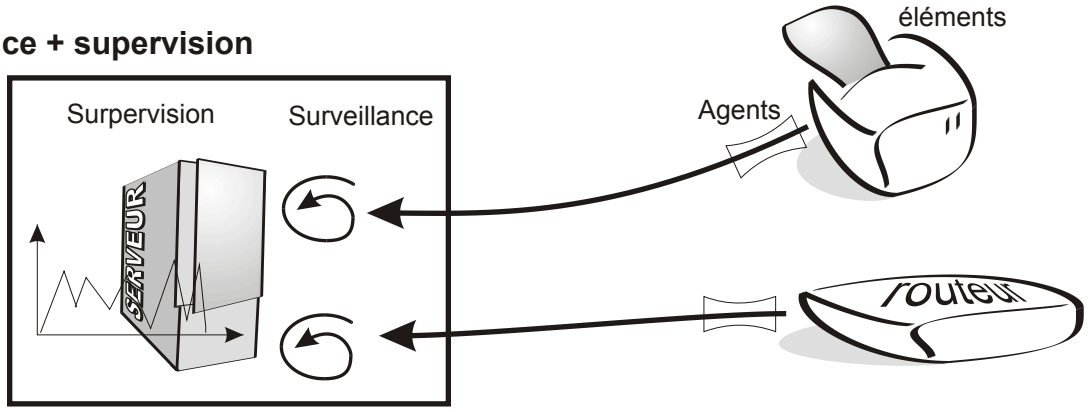
Qu'est-ce que la Centralisation

4.8.1

Centralisation = Mettre au centre / tout mettre ensemble

Merci monsieur De Lapalisse !

Surveillance + supervision ensemble



Bien souvent l'outil de supervision contient les agents de surveillance.
Inutile de dire que le CPU de la console doit tenir la route !

IMPORTANT

Ce type d'architecture répond bien à une supervision de taille humaine … (PME)

CE QU'IL FAUT RETENIR

Bloc Note

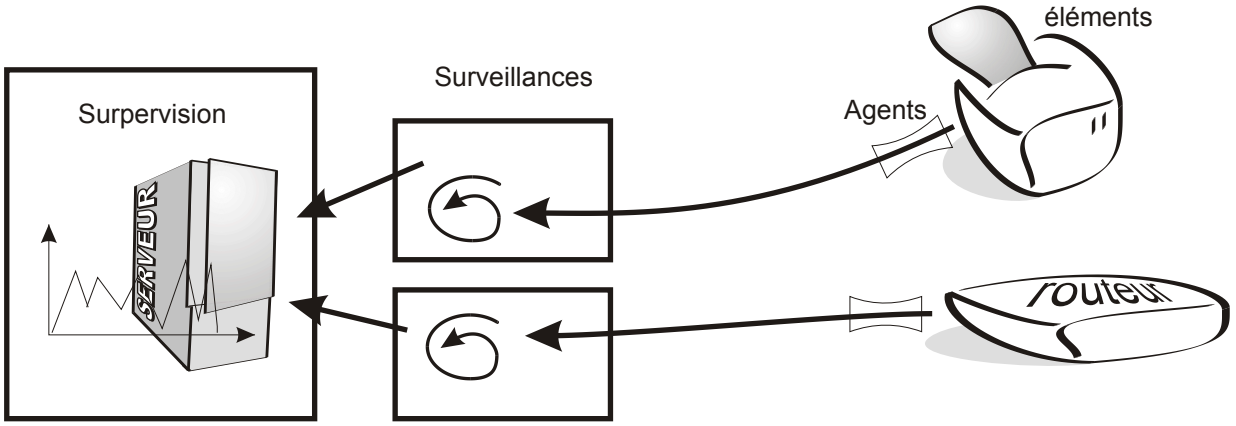
Tout est sur la même machine / les sauvegardes sont uniques / en cas de crash : plus rien n'est surveillé.

Qu'est-ce que la Décentralisation

4.8.2

Décentralisation = ne rien mettre au centre

Merci monsieur De Lapalisse !



Bien souvent, la supervision s'appelle "une console".
Les agents de surveillance sont sur d'autres machines, si possible le plus éparpillés possible afin de répartir la charge CPU du traitement des informations (épurations).

IMPORTANT

Ce type d'architecture répond bien à une supervision de Grande dimension (plusieurs centaines d'agents).

CE QU'IL FAUT RETENIR

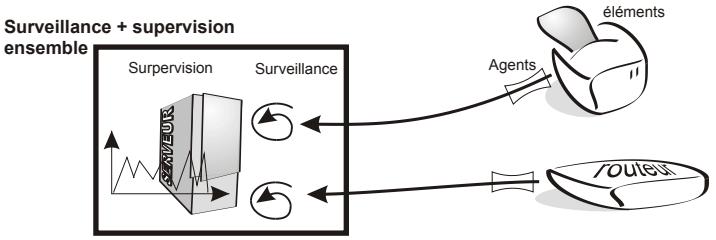
Bloc Note

Seules les informations traitées sont stockées en base de données. Les infos données aux agents de surveillance ne sont pas stockées.

Avantages des 2 approches

4.8.3

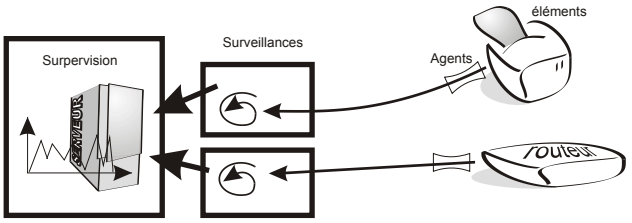
Centraliser ou Décentraliser ? les Avantages des 2 solutions ?



Avantages de la centralisation :

Le coût (1 seule machine)

La gestion des agents, puisqu'ils sont sur le serveur



Avantages de la décentralisation :

Le CPU est épargné sur la console

Chaque Agent est autonome

Les agents ne consomment presque rien sur les stations "clientes"

IMPORTANT

Chaque architecture a ses avantages ! Le choix viendra très certainement de la taille de votre Réseau.

CE QU'IL FAUT RETENIR

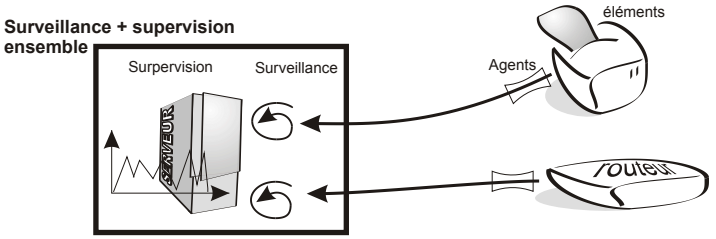
Bloc Note

Attention : tous les logiciels ne permettent pas le choix d'architecture …C'est pourquoi il faut choisir le logiciel de surveillance en rapport avec la taille du Réseau.

Trouver un équilibre

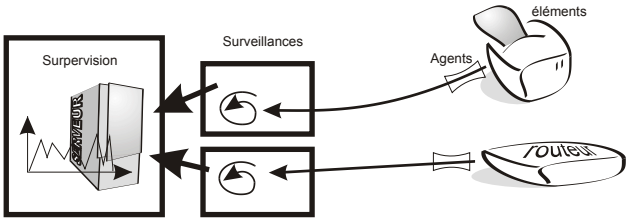
4.8.4

Centraliser ou Décentraliser ? Les Inconvénients des solutions...



Inconvénient de la centralisation :

Le CPU de la console ne sert plus qu'à ça.
Lors d'une panne / nous sommes aveugles
Les bases de données sont immenses car elle enregistrent, bien souvent, tous les événements



Inconvénient de la décentralisation :

Lorsque qu'une station où se trouve un agent, plante / nous devenons aveugles sur ce qu'elle surveillait.
Nous ne pouvons pas voir le détail des trames de surveillance.

IMPORTANT

Toutes les solutions ont leurs inconvénients / il faut les connaître pour s'y préparer.

CE QU'IL FAUT RETENIR

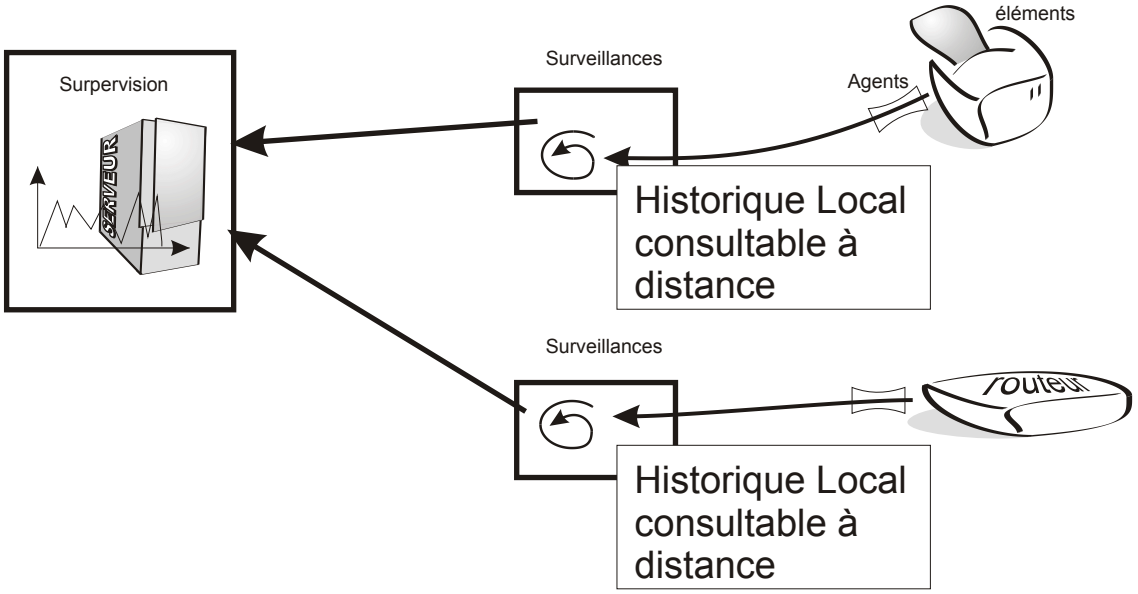
Bloc Note

Attention : tous les logiciels ne permettent pas le choix d'architecture …C'est pourquoi il faut choisir le logiciel de surveillance en rapport avec la taille du Réseau.

Gestion semi centralisée

En ne laissant pas un serveur “seul” faire toutes les surveillances mais en étalant les agents de surveillance sur le parc, notre gestion semble plus rationnelle.

Pourtant, il faut trouver comment avoir tous les avantages en même temps.



IMPORTANT

Attention, cette solution demande bien souvent des agents propres à la plate forme !

CE QU’IL FAUT RETENIR

Bloc Note

Il n’y a pas de solution magique. Mesurez d’abord l’impact de vos choix sur votre planning car il est bien souvent préférable de démarrer par une solution centralisée pour partir peu à peu vers une solution décentralisée en s’arrêtant lorsque l’équilibre CPU est atteint.

Que dit la Presse ?

4.8.6

Je pense que l'on appelle la "presse" parce que les gens qui y travaillent sont des "pressés" !

Pressés d'écrire, on écrit n'importe quoi !

Suivant l'humeur du jour, on vous dit que la gestion centralisée est la meilleur ... Demain, elle n'a que des failles …

Chaque éditeur propose sa solution … suivant l'humeur du moment, la presse loue les qualités de telle architecture, ou telle autre …

Soft	Solutions
NSM	Centralise ses agents de surveillance Décentralise ses agents bi directionnels
TIVOLI	Centralise tous ses agents (même ceux en multi plate-forme !)
MOM	Décentralise complètement / la console n'est qu'une supervision.
CGS	Semi centralisé et permet les rebonds de trames (routages encapsulés)
CERUS	Centralise tous ses agents

IMPORTANT

Ne pas se jeter sur ce que dit la presse - même celle de Linux / ils mélangent souvent Bidouille & professionnalisme.

CE QU'IL FAUT RETENIR

Bloc Note

Lisons la presse car elle dénote les tendances pour se remettre en question … avec les nouveaux outils.

Comment faire son choix ?

4.8.7

Si nous avons déjà un Logiciel : nous n'avons plus le choix !
Il faut se soumettre à la politique de l'éditeur …

Si je reste libre (outils perso) je m'inspire des réflexions de la presse et des éditeurs pour que ma supervision réponde à ce que j'attends d'elle !

IMPORTANT

Dans tous les cas : Attention aux défauts cachés !

- Les mails d'alerte ne partent QUE si notre serveur de messagerie fonctionne (et internet) !

- Les SMS d'alerte ne partent QUE si Internet fonctionne

- Les alertes écrans ne sont utiles que si vous êtes devant l'écran (pas de RTT).

CE QU'IL FAUT RETENIR

Bloc Note

Je prévois toujours de prévenir quelqu'un d'autre en cas d'absence / une console sur une seconde station.

Ca vous semble bête aujourd'hui ?
Ca le sera moins demain !
Pensez à tous ceux qui ont placé leur sécurité sur le téléphone portable quand BOUYGUES est tombé !!!

Depuis, AZERTY MicroSystem commercialise un boîtier electro-informatique de surveillance / alarme...

Comment garantir que ma supervision est correcte et complète ?

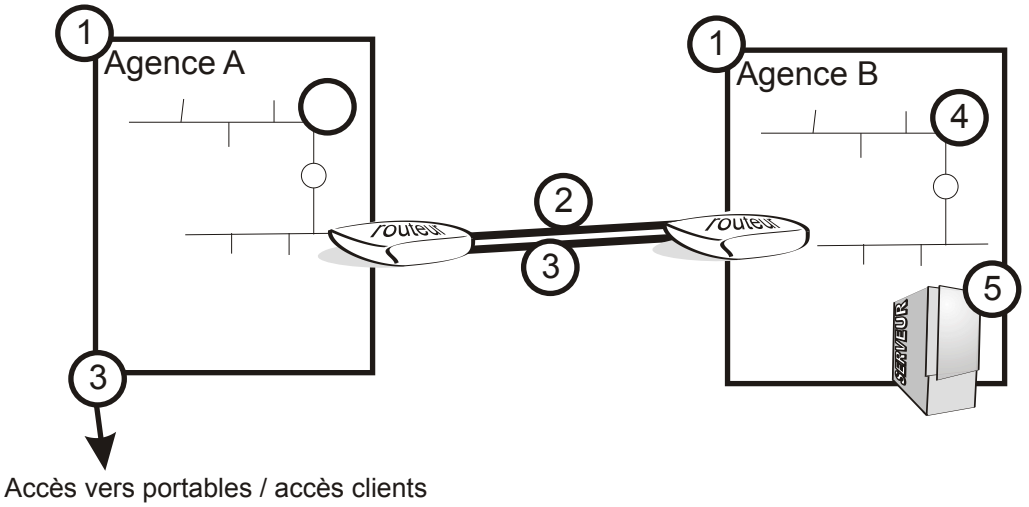
TOME IV chapitre 9

Périmètre d'action / méthode

4.9.1

Avant tout, il faut définir notre périmètre d'action …
Pour y parvenir facilement, voici une méthode :

1. définir les agences
2. définir les relations entre elles (routeurs, pont, WIFI ...)
3. trouver les relations de backup (+ accès externes RAS)
4. définir les réseaux et sous- réseaux
5. définir les plate formes de communication pour circulation des flux de supervision



IMPORTANT

Nous n'avons pas le droit à la "bidouille" ! L'approche doit être méthodique afin de ne rien oublier (autant que possible).

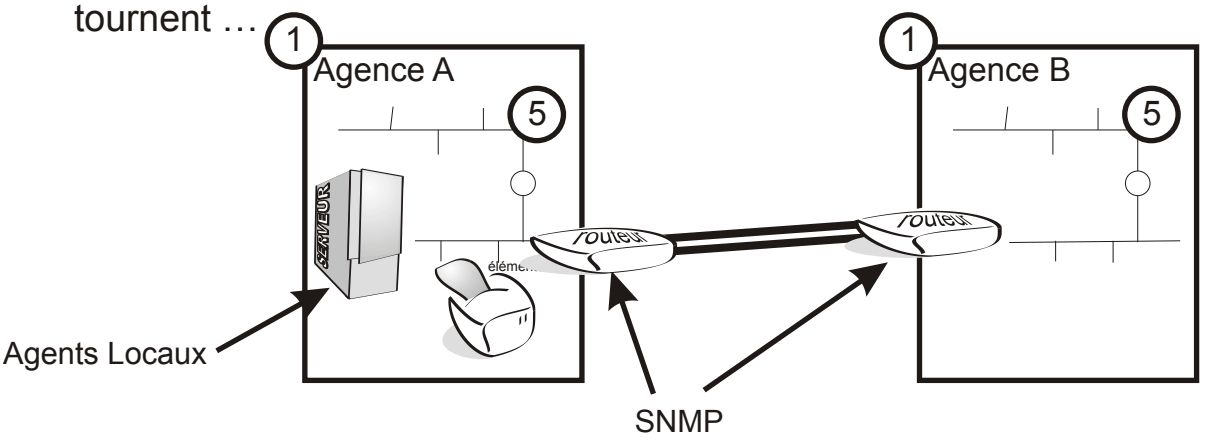
CE QU'IL FAUT RETENIR

Bloc Note

Après avoir fait le schéma, il faut le faire valider, car les anciens en savent toujours plus que nous (en arrivant).

Mettre en place les moyens techniques

Avant tout, il faut lister les éléments à surveiller + sur quel OS ils tournent …



Petit rappel (qui ne fait pas de mal) :
Un routeur possède plusieurs adresses IP. Donc, pour connaître le motif de la panne, voici un petit tableau simple.

ip WAN	ip LAN	SNMP	ip WAN	ip LAN	Motif
Routeur externe			Routeur Interne		
ok	ok	ok	ok	ok	tout va bien
ok			ok	ok	Routeur externe a un problème
			ok	ok	Liaison FT en rade
				ok	routeur en rade ? Ma station n'a pas la bonne passerelle FT en rade
ok		ok		ok	je ne vois pas le bon réseau

IMPORTANT

La méthode de DEBUG fonctionne à condition de laisser l'ICMP sur les routeurs (ping).

CE QU'IL FAUT RETENIR

Bloc Note

A chaque élément, vérifions bien que nous avons l'Agent de surveillance adapté (SNMP, ICMP, UDP ...)

Préparer les escalades

4.9.3

Il est facile de dire qu'il faut "escalader" - mais comment fait-on réellement ? (sans logiciel qui le fait)

En face de chose qui nécessite une escalade, il faut déterminer les responsables à prévenir (Email par exemple).

Prenons un exemple : tester une ligne LS entre 2 routeurs.
La méthode du "ping" est la plus simple et la plus rapide (à condition de ne pas avoir inhibé les trames ICMP sur les routeurs).

Si 3 fois ping sans réponse avec un intercalaire d' 1 minute => mail admin
Si 10 fois ping sans réponse avec un intercalaire d' 1 minute => mail SMS

En réalité, il s'agit de
2 opérations différentes :
L'un vérifie le Ping
L'autre compte et envoie le mail

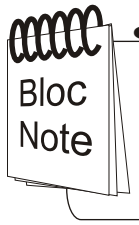
```
OK=`ping -c 1 www.tf1.fr | grep "1 packets received" | awk '{print $2}'`

case "_$OK" in
      _packets*)
            # Connexion OK
            # effacer l'augmentation de nombre d'alertes
            ;;
      *)
            # Connexion tombee
            # il faut incrémenter puis, si 3 => envoyer un mail
            ;;
esac
```

```
cat /etc/HOSTNAME > /tmp/mailOK
date >> /tmp/mailOK
mail -s `cat /etc/HOSTNAME`   jfcasquet@yahoo.fr < /tmp/mailOK
```

IMPORTANT

EN préparant mes escalades - je prépare aussi l'organisation qui doit y faire face (ici mes "collègues").



CE QU'IL FAUT RETENIR

Grâce au Help-Desk, même si je suis en vacances, mes collègues pourront consulter la base de connaissance afin de faire ce qu'ils doivent (tests à faire, appeler FT ...)

Répartir les rayons d'action

4.9.4

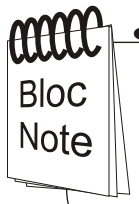
Maintenant que j'y suis, certaines alertes peuvent être transmises à d'autres personnes.

Bien souvent, l'administrateur est considéré comme un hermite - la supervision va permettre aussi de provoquer des échanges constructifs de collaboration avec des BDA, programmeur, équipe déploiement applicatifs …

Exemple :
Nous sommes administrateur LAN en multisite.
SI la liaison WAN tombe, ce n'est pas de notre responsabilité mais, sans cette liaison, notre supervision tombe et les utilisateurs sont gênés.
Donc, dans nos tests, ça ne nous coûte pas grand chose de vérifier la liaison WAN (si son responsable ne le fait pas), afin de se rassurer sur **nos** installations et de prévenir le "vrai" responsable.

IMPORTANT

Nous sommes au coeur du Système d'information.
Si une partie de l'entreprise ne va pas bien, nous sommes les premiers impliqués / pensons donc, avec nos outils et nos idées, à ce qui peut faire que le monde tourne mieux.



CE QU'IL FAUT RETENIR

Les outils persos peuvent être Netstat, ping, ssh, cat / grep, awk …

Une organisation Normale

conditions normales

4.9.5

Grâce encore une fois, au Help-Desk, nous mesurons quand ça va …

Bien souvent, on entend (de la part des services informatiques) “on courre toujours”...

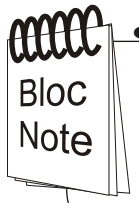
En réalité, grâce au Help-Desk, nous pouvons mesurer le nombre d’appel par jour + le temps de résolution moyen - divisés par le temps de travail (hors congés) - ça nous donne le nombre de personnes nécessaires au minimum dans l’équipe informatique.

Lorsque l’équipe est de taille normale, et que les alertes (appels) sont en nombre normal, la surveillance est optimale puisqu’on prend le temps de voir si tout va bien.

Une supervision tient la route quand on gère les incidents !

IMPORTANT

Si l’équipe est trop petite, nous sommes les “pompiers” / à ce moment là, prenons du temps lorsque les utilisateurs ne sont pas là pour mesurer les motifs des appels afin de réorganiser le travail ou d’augmenter l’équipe.



CE QU’IL FAUT RETENIR

La supervision me permet d’anticiper seulement si c’est humainement possible / Dans tous les cas, il faut préciser les soucis trouvés, pour les inscrire dans le Help-Desk.

Une organisation en Crise

conditions de crise

4.9.6

Un état de CRISE peut venir de plusieurs origines :
Une panne blocante
Trop d'appels
Une priorité qui met tous les appels en attente
Des appels nombreux pour le même motif

Afin d'éviter les escalades automatiques qui viendraient s'ajouter à la crise, prévoyons un "état de crise" qui bloquera toutes les alertes.

A ce jour, seul SoftsChecker (CGS) l'envisage !

Si nous faisons nos propres agents de surveillance, pensons à intégrer cette option.

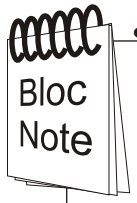
Exemple Sous UNIX :
Le chemin : /BACKUP/Agents/ contient tous les shells appelés avec CRON pour la gestion des escalades et alertes.

Le chemin : /BACKUP/AgentsEnCrise/ contient tous les shells vides.

Dès que la crise arrive, les 2 chemins sont alors inversés …

IMPORTANT

N'ajoutons pas un autre stress à celui d'une période de crise - pensons à nous préparer.
Par exemple, préparons des messages (WALL) pour les usagers + mails explicatifs...



CE QU'IL FAUT RETENIR

Un jour ou l'autre, nous vivrons une crise - préparons-nous le mieux possible pour l'affronter avec professionnalisme / par ailleurs, "prévenir" nous donne encore du temps car les usagers seront patients.

Se préparer au reporting

4.9.7

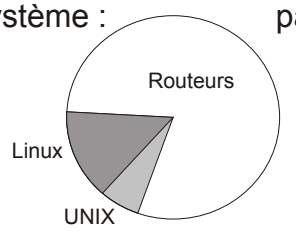
Nous abordons maintenant la partie appelée “Qualité” de la supervision.

Que ça aille bien ou pas - il nous faut préparer des reportings afin de mettre en exergue les choses que l’on ne voit pas.

Reporting = Requêtes visuelles

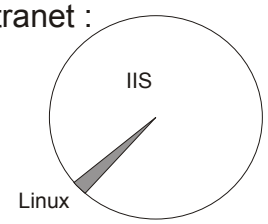
En préparant des requêtes dans tous les sens, certaines vont paraître intéressantes...

Interventions du mois
par Système :



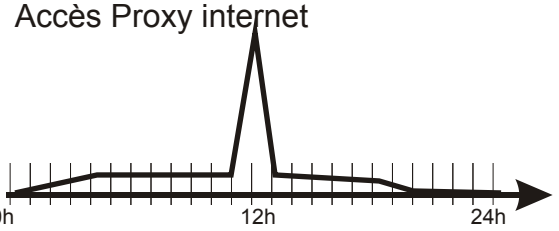
ce graph montre que les routeurs ont l’air d’avoir un soucis

par intranet :



ce graph montre que l’intranet sur IIS fonctionne avec de gros besoin de maintenance humaine.

Accès Proxy internet



Ici, nous voyons clairement que les usagers se servent d’internet pour jouer le midi : RISQUE VIRAL et SPYWARE très important !

IMPORTANT

Les reportings ne sont QUE des requêtes SQL sur les informations stockées dans le Help-Desk et WorkFlow.

CE QU’IL FAUT RETENIR

Bloc Note

Faire du reporting (même inutile) montre aussi notre transparence + crédibilité + professionnalisme.

Des fois, ils servent aussi à noyer le poisson … ;-)

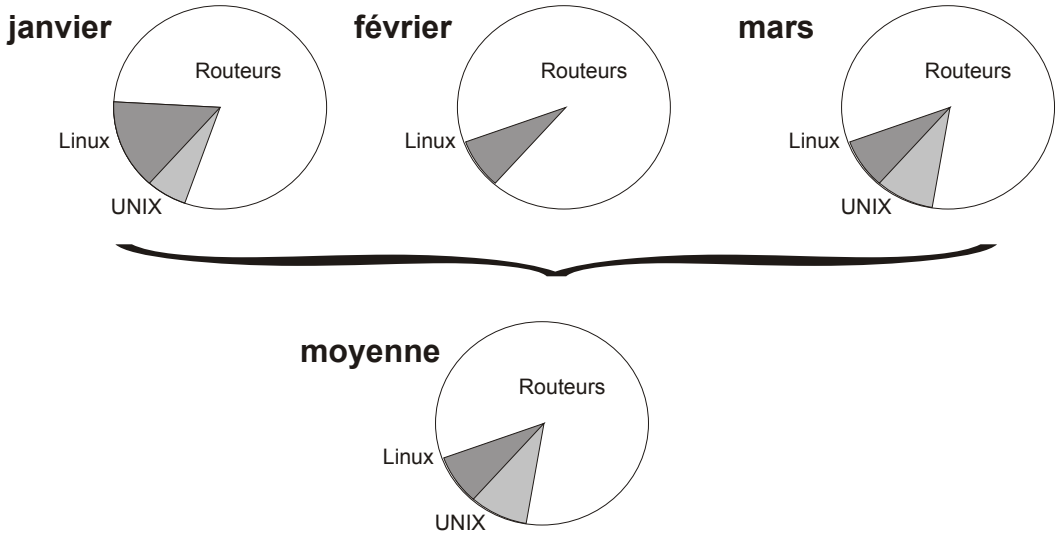
Tableaux de Bord

Les reportings ne sont QUE des requêtes avec des schémas (excel / OpenOffice / ou directement en PHP) - sans commentaire.

Nous pouvons être amenés à faire une étude sur le remplacement des routeurs BayNetworks pour migrer vers NetGear .
Les reportings vont nous montrer des interventions nombreuses sur les routeurs.
Ce type d'information demande non plus de faire n'importe quelle requête mais de s'interroger sur les résultats récurrents.

C'est l'une des missions principales des RI.

Interventions par mois par Système :



IMPORTANT

Un tableau de bord n'est pas technique - il répond à un besoin lors d'un réunion de travail avec un comité directoire pluri-compétence.

CE QU'IL FAUT RETENIR

Bloc Note

Des tableaux de bord me permettent une sérénité. Car les éléments étranges des reportings sont étudiés & commentés afin de savoir si c'est un Bug réparé ou un défaut matériel.

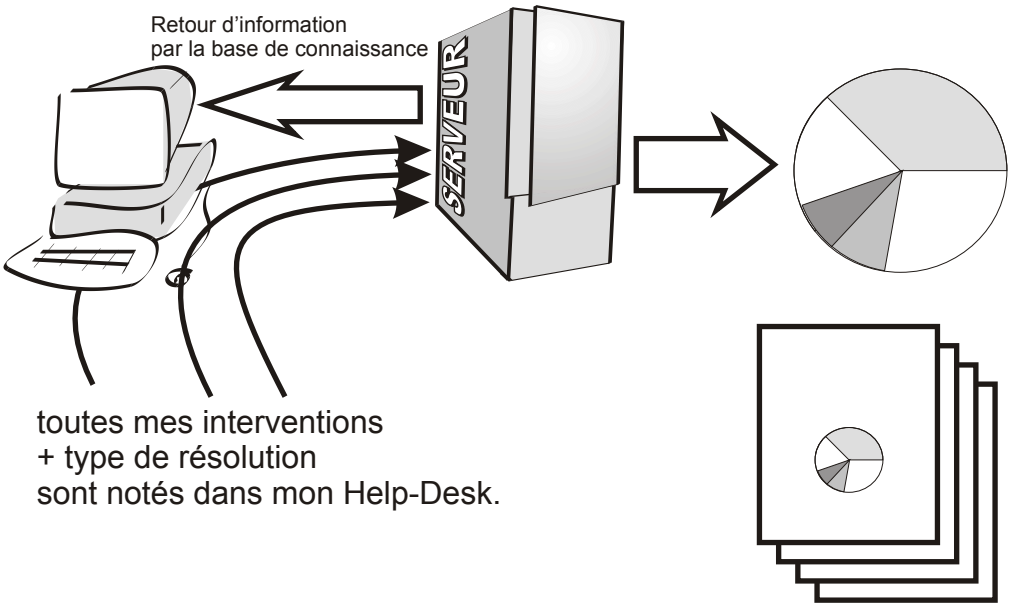
Conclusion

TOME IV chapitre 10

Ma responsabilité

4.10.1

Elle dépend du rôle que je joue dans l'Entreprise / mais dans tous les cas la supervision sera, pour moi, l'outil de ma sérénité et la démonstration de mon professionnalisme.



toutes mes interventions
+ type de résolution
sont notés dans mon Help-Desk.

Rapport mensuel

Les enjeux professionnels

4.10.2

Mon professionnalisme reconnu me permet d'être reconnu.

Jadis, les informaticiens étaient :
soit très pros / balaise
soit très nuls, mais écrivant beaucoup (rapports)

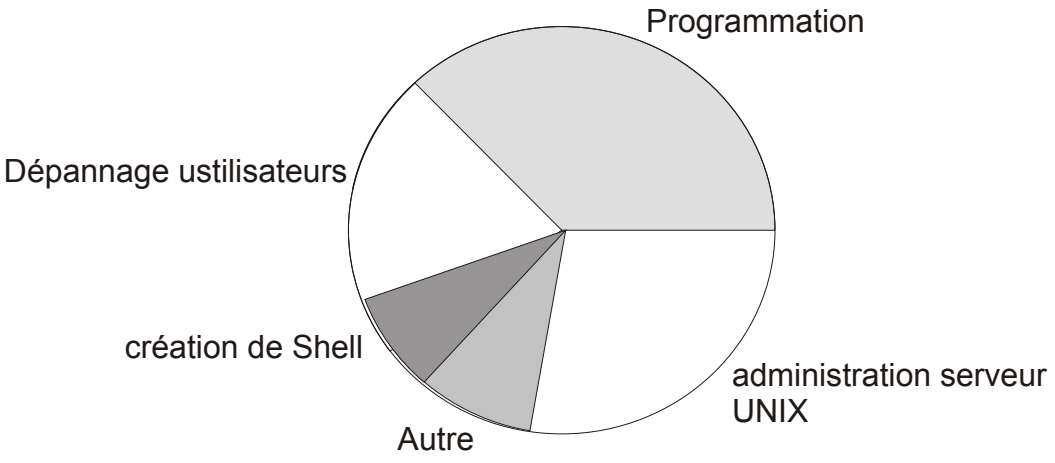
Encore aujourd'hui, celui qui écrit est le mieux reconnu !

A l'EPITAn, le professionnalisme est reconnu / mais s'attarder sur le papier, sur le renseignement des bases de données va faire la vraie différence sur le terrain.

Vous partez en stage - notez que le reporting commence le premier jour ! (Ce que vous faites au jour le jour + temps d'exécution)

Bien des stagiaires gardent le travail pour la fin … c'est une erreur, car vous passez à coté de l'historique et de ce vous a apporté personnellement le stage (bien plus que technique)...

D'une part, vous ferez la différence, d'autre part, lorsque vous montrerez le temps passé lors de votre soutien et aussi chez l'Entreprise, vous aurez quelque chose de concret à définir :



Se reposer sur une méthode

4.10.3

Aujourd'hui, vous avez eu une méthode !

A vous de fabriquer la vôtre.

Un conseil tout de même : n'empruntez pas une méthode inadaptée (ex: MERISE pour l'administration réseau) :-(

La méthodologie, ce n'est pas écrire pour écrire / c'est écrire ce que l'on fait en triant ses écrits d'une manière logique.

A force, vous construirez votre plan qui sera valable dans telle entreprise et pas dans telle autre …

Vous souhaitez en savoir plus, ou prendre contact :

Jean-François Casquet
jfcasquet@yahoo.fr

AZERTY MicroSystem
http://gp.azerty.fr
jfcasquet@azerty.fr

SOMMAIRE

SOMMAIRE