# Introduction

# Introduction

## Introduction

### Qu’est-ce-que Pandora FMS ?

Pandora FMS est un logiciel de supervision orienté à tout environnement. Pandora FMS est conçu pour être utilisé pour tout type de rôles et organisations. Son objectif est d’être suffisamment flexible, notamment pour gestionner et contrôler toute votre infrastructure, sans investir du temps ni de l’argent dans d’autres outils.

FMS est l’acronyme de “ Système de Supervision Flexible “
(en anglais : Flexible Monitoring System).

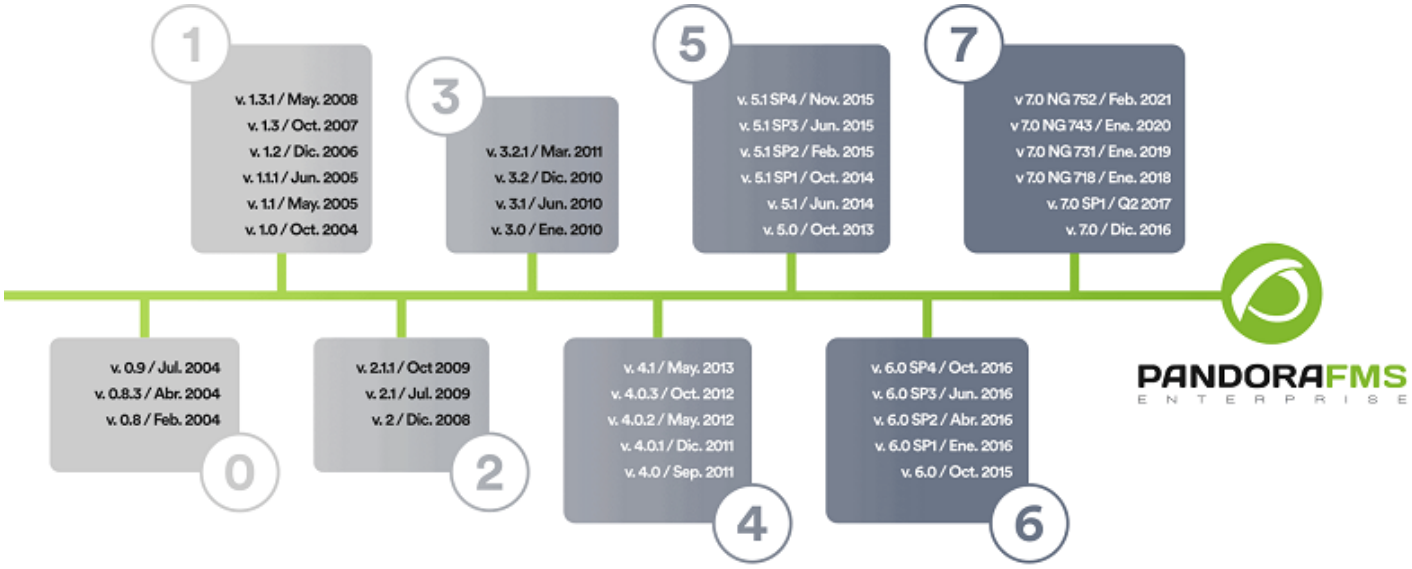
Pandora FMS dispose actuellement d’agents pour tous les systèmes d’exploitation du marché. Pandora FMS peut tout aussi bien s’utiliser pour superviser des systèmes que pour superviser tout type de dispositifs réseau, soit utilisant SNMP ou par des sondes de protocole TCP, ICMP, UDP ou des agents logiciels.

### Approche de la documentation

- En plus de la documentation officielle, il existe un forum des utilisateurs où vous pouvez poser vos questions
- Il existe un programme de formation officielle avec sa correspondante certification dispensé par les dévellopeurs de Pandora FMS.
- Par ailleurs, il existe des guides rapides pour aider à configurer Pandora FMS et implémenter des surveillances simples, telles que pour l’installation d’agents logiciel, aussi bien pour GNU/Linux® que pour MS Windows®.
- Pour plus d’information, veuillez consulter notre site web : https://pandorafms.com/fr

### L’évolution du projet Pandora FMS

Pandora FMS vient d’un développement personnel de son auteur original, Sancho Lerena, en 2003. Même si, initialement, c’était un code ouvert à 100%, au fil des années, la nécessité d’offrir une version pensée pour les grandes entreprises s’en ait fait sentir : Pandora FMS Enterprise capable de traiter de grands volumes d’informations grâce à la Métaconsole.

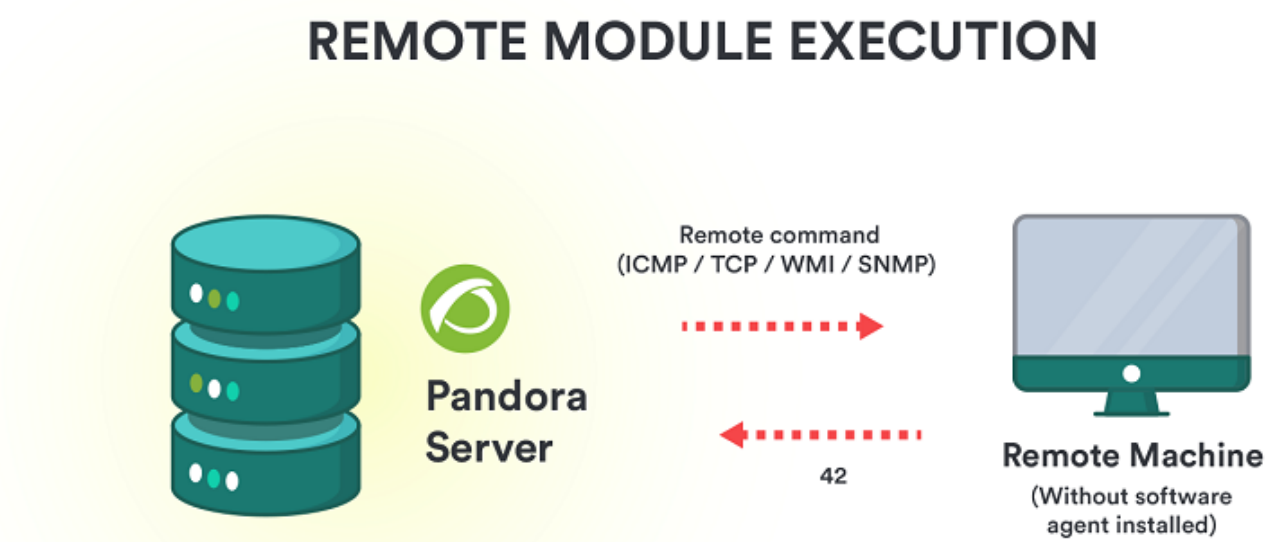



## Un coup d'oeil aux fonctionnalités de Pandora FMS

- Auto supervision : La supervision par défaut des agents de Pandora FMS permet de détecter les disques durs, les partitions ou les bases de données, entres autres.
- Auto découverte : À distance et en utilisant le réseau, il est possible de détecter tous les éléments du réseau, les classer selon leur système d'exploitation et, avec un profil, de commencer à les surveiller.
- Agents : Ils peuvent obtenir des informations, de l'exécution d'une commande à l'appel, à un niveau inférieur de la API de Windows® : événements, journaux, utilisation de mémoire ou de CPU. Pandora FMS dispose d'une bibliothèque de vérifications par défaut pour plus de vitesse.
- Contrôler : Les propres agents peuvent activer des services, effacer des fichiers temporaires ou exécuter des processus. Dans la version Enterprise il est possible de le fire depuis la Console Web, en exécutant à distance des tâches telles que arrêter ou démarrer des services, y compris des exécutions périodiques. De plus, Pandora FMS peut être utilisé pour accéder, à distance, aux systèmes éloignés, grâce à eHorus (Telnet, VNC ou SSH).
- Alerter et notifier : Prévenir d'une erreur est aussi important que de la détecter. Avec Pandora FMS, vous disposez d'une variété de formes et formats de notifications.
- Visualiser et analyser : Surveiller, ce n'est pas seulement recevoir un trap ou visualiser un service défaillant, c'est aussi présenter des rapports de tendances, des graphiques résumés de données reliées pendant des mois, générer des portails d'utilisateurs, déléguer des rapports à des tiers ou définir ses propres graphiques et tables.
- Inventorier : Contrairement à d'autres solutions pour lesquelles le concept de CMDB est la base, pour Pandora FMS, c'est optionnel. L'inventaire est flexible et dynamique et peut se contrôler à distance, effectuer une auto-découverte etc. Il peut notifier des changements (par exemple, un logiciel désinstallé dans un appareil) ou simplement être utilisé pour dresser des listes.

## Supervision à distance

Quand nous évoquons la surveillance à distance, nous faisons référence au serveur de Pandora FMS qui contrôle, de manière régulière ou synchrone, les dispositifs que vous souhaitez surveiller. Ce processus de de contrôle synchrone est connu sous le nom de *polling* ou supervision à distance.




En général la supervision à distance s'utilise pour :

- Vérifier qu'ils sont actifs et en exécution.
- Obtenir une valeur numérique (par exemple, mesurer le trafic réseau ou le nombre de connexions actives).

Cette supervision, quand elle est synchrone, se fait toujours dans le même sens : du serveur de supervision à l'élément supervisé et peut se faire avec les protocôles les plus eténdus comme SNMP et WMI (MS Microsoft®).

Le cas contraire s'appele supervision asynchrone et on parle généralement des traps SNMP.

Pour superviser des environnements réseau le protocole à choisir c'est celui de SNMP avec un moteur de recherche des appareils SNMP, accès aux collections MIB des fabriquants des appareils réseau (bibliothèques d'OID) et l'écoute des traps. Après les collectuons d'OID personnalisées de chaque appareil seront ajoutées. Pour les systèmes Unix® et GNU/Linux® vous devez garder sur compte d'activer les focntions SNMP.

Pour les serveurs MS Windows® la supervision à distance WMI est très appropri´ée et puissante lorsqu'ell se ait avec les idéntifiants d'accès.

À la fin vous pouvez superviser des éléments réseau par le biais de l'utilisation des tests TCP (par

exemple le protocole HTTP o SNMP) ou ICMP (par exemple ping ou temps de latence).

### Supervision locale (avec des agents logiciels)

Lorsqu'on parle de systèmes et d'applications, nul doute que la meilleure façon d'obtenir l'information est directement sur le système, en exécutant des commandes ou en consultant des sources de données du système depuis la machine même que vous souhaitez surveiller. Ceci suppose qu'il faille exécuter n'importe quel type de commande, script ou faire n'importe quelle forme de consultation sur le système ou l'application. Nous utiliserons pour cela l'agent logiciel de Pandora FMS.

Les agents, en plus de leur fonction essentielle qui est de récolter les informations grâce aux commandes, comprennent une autre série de fonctions avancées, comme obtenir l'information d'inventaire. Il est également possible de configurer pour qu'ils agissent efficacement en cas de problèmes ou de failles, interagissant automatiquement avec le système, effaçant quelque fichier temporaire ou exécutant quelque commande. Lorsqu'un agent logiciel ne peut pas connecter au serveur Pandora FMS indiqué vous pouvez utiliser le Serveur Satellite PFMS ou bien un agent broker.

### Procédés de supervision

Avant de débuter une étape de déploiement, il est important d'identifier quels sont les points critiques et de hautes importances de la plate-forme technologique à surveiller. De cette façon, avant d'avoir des informations de données concrètes sur les systèmes, nous pouvons savoir quoi faire avec eux et comment les exploiter sans perdre du temps en recherches de détails banaux.

- Disponibilité : Le plus intéressant est surtout la supervision basée sur des événements et il se peut que ça suffit avec la supervision à distance. Elle est plus rapide de déployer et d'avoir de brefs résultats. Les rapports de SLA seront les plus importants dans ce cas.
- Productivité : Elle concerne les graphiques et les nombres. Vous pouvez obtenir cette information aussi bien avec des agents qu'avec des vérifications à distance. Mais il faut probablement des agents pour obtenir une information détaillée de systèmes. Son intérêt est les rapports regroupés et les graphiques combinés possibles.
- Planification de capacité : Beaucoup plus spécialisée, elle a besoin d'obtenir des données, comme dans le deuxième cas, mais il doit jouer avec des moniteurs de types prédictifs et des rapports de protection très spécifiques. Établir des alertes dès le début sera de grande aide. Il faudra bien connaître les concepts des états WARNNG et CRITICAL, en plus d'élaborer une série de politiques de gestion d'événements qui permettent de prévoir le problème avant que n'arrive, certainement, le cas le plus complexe et intéressant.

### Procédés d'intervention

Pour pouvoir élaborer des procédés d'intervention, il faudra prendre en compte divers facteurs :

- *Niveau de gravité de l'événement*: être capable de différencier quelque chose d'habituel de quelque chose de peu fréquent ou grave.
- Notifications: email, sms, Telegram, alerte sonore...
- Échelonnement: différentes façons d'alerter après la réitération d'un problème. Habituellement, une notification est adressée à un responsable après un certain temps sans résolution du problème.

Avant de commencer les configurations, il est conseillé de bien avoir en tête ces concepts, d'élaborer des schémas avec les éléments critiques, penser à la manière de les surveiller, quoi faire avec toute l'information obtenue et comment notifier les problèmes qui surviennent.

## Modèles de supervision

- Le modèle de supervision directe implique qu'il y a une ou plusieurs personnes observant sans cesse le système. Vous pouvez probablement voir de petits changements, sans gravité, et avoir beaucoup plus de flexibilité. Il n'est pas nécessaire de définir des alertes afin de comprendre qu'est-ce qui se produit dans le système à ce moment. C'est le modèle utilisé pour de grands environnements.
- Le modèle de supervision indirecte implique l'utilisation de notifications automatiques. Ce système est adéquate pour des environnements qui disposent de peu de dispositifs, ou qui ont très bien identifiés les éléments critiques et la manière d'aborder le problème avec sa notification et solution.