Architecture

Architecture

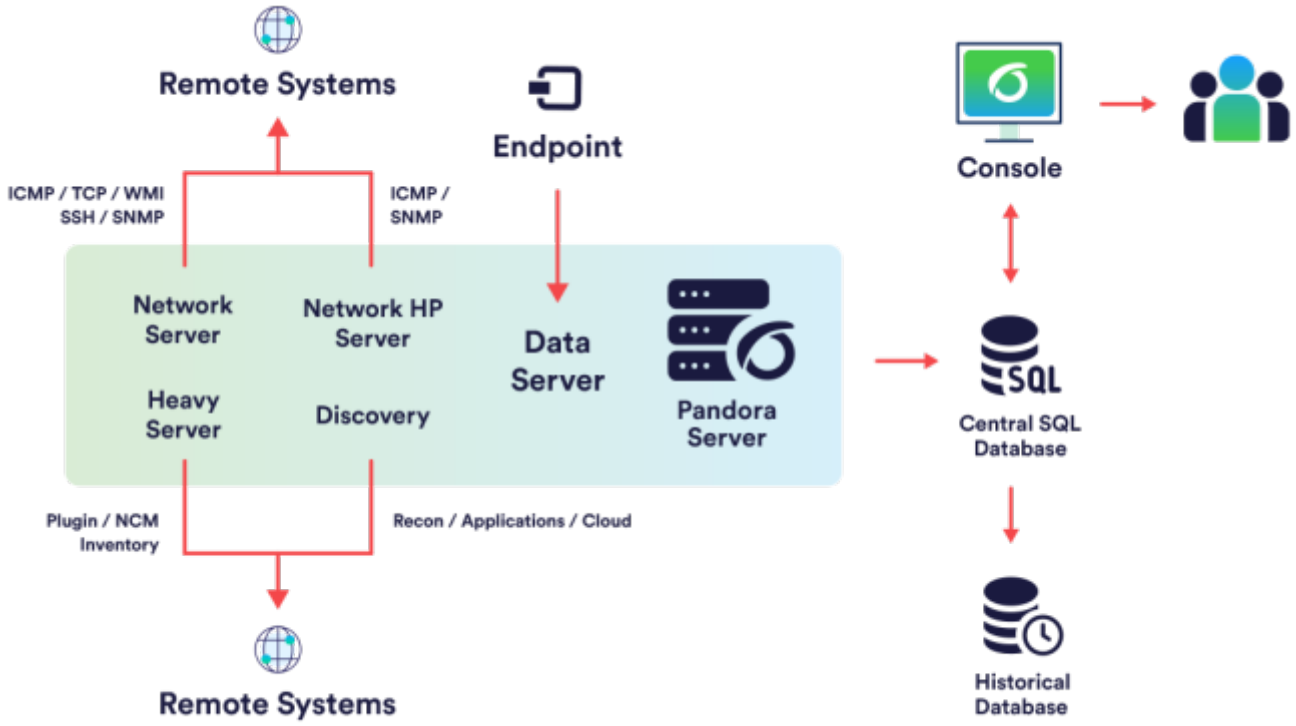
Introduction

Le composant vital et où presque toutes les informations sont stockées est la base de données MySQL. Tous les composants Pandora FMS peuvent être répliqués et fonctionner dans un environnement purement HA (Actif/Passif) ou dans un environnement en cluster (Actif/Actif avec load balancing).

Les Serveurs PFMS sont responsables de la collecte et du traitement des données. Les serveurs, avec les informations générées par eux ou par les agents, introduisent les données dans la base de données. La Console est la partie chargée d'afficher les données présentes dans la base de données et d'interagir avec l'utilisateur final. Les EndPoints sont des applications qui s'exécutent dans les systèmes surveillés et collectent les informations pour les envoyer aux Pandora FMS serveurs.

Serveurs de Pandora FMS

Les serveurs sont intégrés dans une seule application, génériquement appelée Pandora Server, qui est une application *multi thread* qui exécute simultanément différentes instances ou serveurs spécialisés de Pandora FMS. Ensuite, chacun des serveurs spécialisés de Pandora FMS est décrit. Ceux sont les éléments chargés d'effectuer les contrôles existants. Ils les vérifient et modifient leur statut en fonction des résultats obtenus. Ils sont également chargés de déclencher les alertes qui sont établies pour contrôler l'état des données.



Il peut y avoir des serveurs simultanés; l'un d'eux est le serveur principal et le reste des serveurs sont des serveurs esclaves. Bien qu'il y ait un serveur esclave et un serveur maître, ils fonctionnent tous simultanément. La différence entre les deux est que lorsqu'un serveur du même type tombe en panne (par exemple, un serveur réseau), le serveur maître est chargé de traiter toutes les données associées au serveur qui est tombé en panne.

Pandora FMS gère automatiquement l'état de chaque serveur, son niveau de charge et d'autres paramètres. L'utilisateur peut surveiller l'état de chaque serveur via la section état du serveur de la Console Web.

Voir aussi:

- Architecture des serveurs (version 784).
- Sync Server.
- SIEM Server.
- Supervision du réseau avec NetFlow et sFlow.
- Policy Manager.
- MADE Server.

Data Server

Il traite les informations envoyées par les EndPoints via Tentacle et API 2.0. Les EndPoints collectent les informations localement à partir des systèmes dans lesquels ils sont installés et construisent un paquet d'informations au format XML. Ces paquets au format XML sont envoyés au

serveur. Dans le serveur, ils sont reçus dans un répertoire spécifique, le serveur traite tous les fichiers qui arrivent dans ce répertoire d'entrée et stocke les informations dans la base de données.

Différents serveurs de données peuvent être installés sur différents systèmes ou sur le même hôte en utilisant des serveurs virtuels ou avec de différents CPU.

Malgré sa simplicité, le serveur de données est l'un des éléments critiques du système, car il traite toutes les informations des agents et génère des alertes et des événements système basés sur ces données.

Network Server

Il exécute des tâches de supervision à distance via le réseau: contrôles ICMP (ping, temps de latence), requêtes TCP et requêtes SNMP. Il est très important que les machines exécutant les serveurs réseau aient une «visibilité réseau» aux appareils à superviser à distance.

Ce serveur est également chargé d'autres tâches:

- WMI est une norme Microsoft® permettant d'obtenir des informations et des applications du système d'exploitation à partir d'environnements MS Windows®. Pandora FMS dispose d'un serveur dédié pour surveiller les systèmes MS Windows® à distance via le protocole WMI.
- Une composante d'Intelligence Artificielle qui implémente statistiquement une prévision de données basée sur des données passées avec une profondeur allant jusqu'à 30 jours en quatre références temporelles, permettant de prédire les valeurs d'une donnée avec un intervalle de 10-15 minutes, et de savoir si une donnée à l'heure actuelle est anormale par rapport à son historique. Fondamentalement, nous devrons construire une ligne de base dynamique avec un profil hebdomadaire.
- Il effectue des contrôles Web complets, tels que le processus d'identification d'un utilisateur, l'envoi de paramètres dans un formulaire, le contrôle du contenu, la navigation dans les menus, etc. Il est utilisé pour les contrôles de disponibilité vrai/faux et pour obtenir des temps de latence (en secondes) d'expérience de navigation complète.

SNMP trap Server

Ce serveur utilise le démon standard du système de collecte de trap, snmptrapd: Ce démon reçoit les traps SNMP et la console SNMP de Pandora FMS les traite et les stocke dans la base de données. Il se charge également de lancer les alertes associées aux trappes SNMP que vous avez définies.

Discovery Server

Anciennement appelé Recon Server, le serveur Discovery est utilisé pour analyser régulièrement le réseau, détecter de nouveaux systèmes en fonctionnement, appliquer un modèle de supervision et commencer immédiatement à superviser le nouveau système. En utilisant les applications GNU système nmap, xprobe et traceroute, il est également capable de détecter les systèmes d'exploitation et d'établir la topologie du réseau.

Le Discovery Server permet également de lancer des tâches planifiées et de lancer une supervision spécifique contre les environnements virtuels, le Cloud, les bases de données ou toutes les applications ou environnements qui nécessitent d'explorer ce qui existe avant de commencer à le superviser.

Event Server

Ce serveur spécial sert à corréler les événements et générer des alertes mais il n'exécute pas des tâches de supervision. Ce serveur, contrairement au reste ne dispose pas de threads ni d'haute disponibilité.

Satellite Server

Ce composant est installé séparément sur le serveur principal de Pandora FMS. Il permet le transfert des fichiers de données des EndPoints au serveur principal, agissant comme *proxy* des agents dans des topologies distribuées. Il envoie les données de supervision sous forme de fichiers XML via une connexion Tentacle, de sorte qu'il n'a pas besoin d'une connexion à la base de données.

WUX Server

Combiné à la grille de Selenium, il permet d'effectuer des transactions WEB complexes de manière distribuée. Ces transactions sont exécutées dans un navigateur réel, et que leur sortie est capturée et traitée pour être affichée étape par étape, y compris la capture des erreurs, ainsi que les statistiques détaillées.

Syslog Server

Il permet Pandora FMS d'analyser le syslog de la machine où il se trouve, en analysant son

contenu et en stockant les références dans le OpenSearch serveur correspondant.

Log Server

Il vous permet de corréler log et d'exécuter vos alertes.

Alert Server

S'il est actif il sera chargé de l'exécution de toutes les alertes de supervision, puisque par défaut chaque serveur sera chargée de ses propres alertes et dans quelques situations ils peuvent se produire des délais de supervision si une alerte doit s'exécuter et prend plus de temps de se faire.

Heavy Server

Heavy Server exécute des contrôles complexes à distance à l'aide de scripts personnalisés. Ils peuvent être développés dans n'importe quel langage et intégrés dans l'interface Pandora FMS, en étant gérés de manière centralisée. Ceci permet à un utilisateur avancé de définir ses propres tests complexes, développés par lui-même, et de les intégrer dans l'application afin qu'ils puissent être utilisés de manière confortable et centralisée depuis Pandora FMS.

Il exécute également des fonctions supplémentaires:

- Prend en charge tout ce qui est nécessaire pour Network Config Management (NCM).
- Obtient et affiche les informations d'inventaire des systèmes: Logiciel installé, modèle des éléments matériels, disques durs, services fonctionnant dans le système, etc. Ce serveur peut obtenir ces informations à distance et localement.
- Il permet d'exporter les données d'un appareil supervisé d'une installation Pandora FMS à une autre, et donc de répliquer les données. Ceci est particulièrement utile lorsque vous avez un déploiement important, avec plusieurs installations Pandora FMS, et que vous souhaitez centraliser.

Network High Performance Server

Network HP Server utilise des stratégies avancées pour effectuer des vérifications ICMP (ping) et SNMP en masse, ce qui se traduit par des performances élevées.

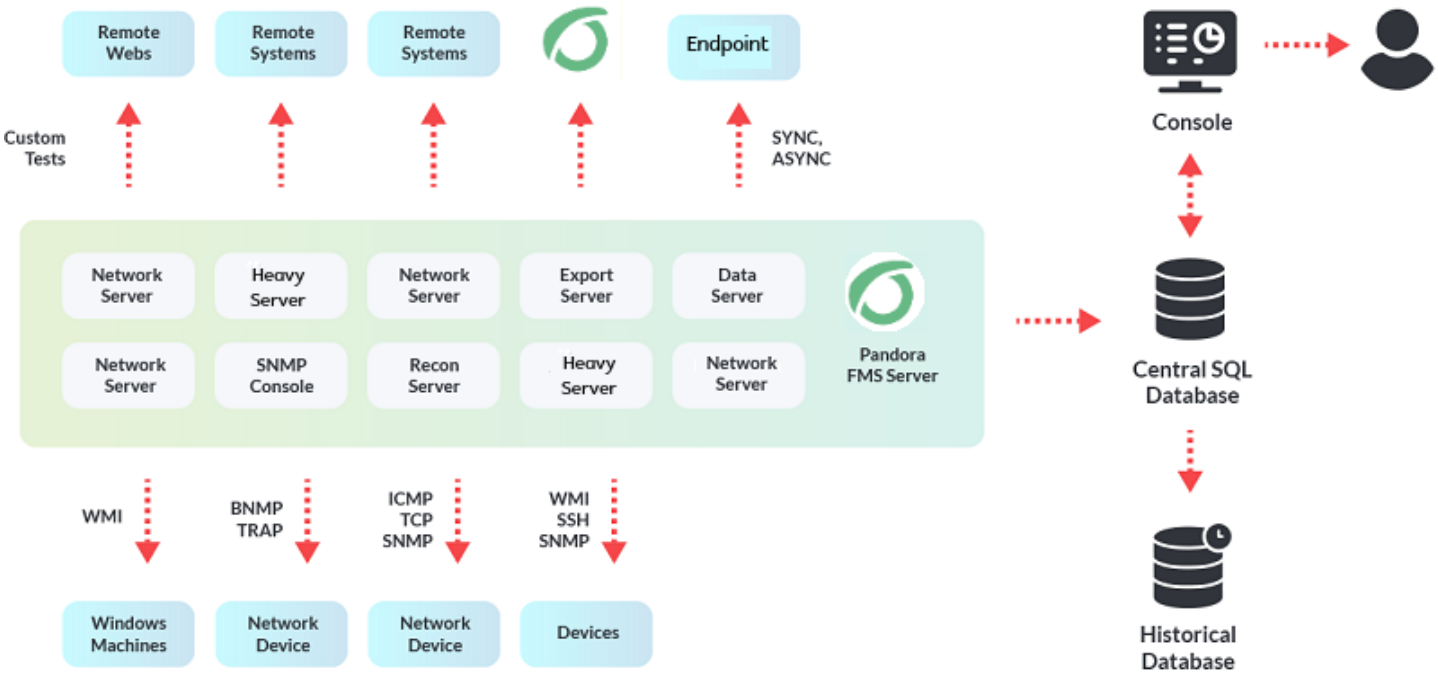
Console web de Pandora FMS

C'est l'interface utilisateur de Pandora FMS. Cette console d'administration et d'exploitation permet à différents utilisateurs, avec différents privilèges, de contrôler l'état des agents, de voir les informations statistiques, de générer des graphiques et des tableaux de données, ainsi que de gérer les incidents avec son système intégré. Il est également capable de générer des rapports et de définir de manière centralisée de nouveaux modules, agents, alertes et de créer d'autres utilisateurs et profils.

La console web peut fonctionner sur plusieurs serveurs pour répartir la charge et pour faciliter l'accès par des problèmes logistiques (grands réseaux, nombreux groupes d'utilisateurs différents, différences géographiques, différences administratives, etc.).

Base de données de Pandora FMS

Pandora FMS utilise une base de données MySQL dans laquelle il stocke toutes les informations reçues en temps réel, en normalisant toutes les données provenant des différentes sources. Actuellement, Pandora FMS ne supporte que MySQL, MariaDB et Percona.



EndPoints Pandora FMS

Il est important de distinguer deux concepts: Agent, ou agent en console, comme

conteneur, EndPoint, en tant que logiciel est installé et fonctionne sur un ordinateur.

Agent (Conteneur)

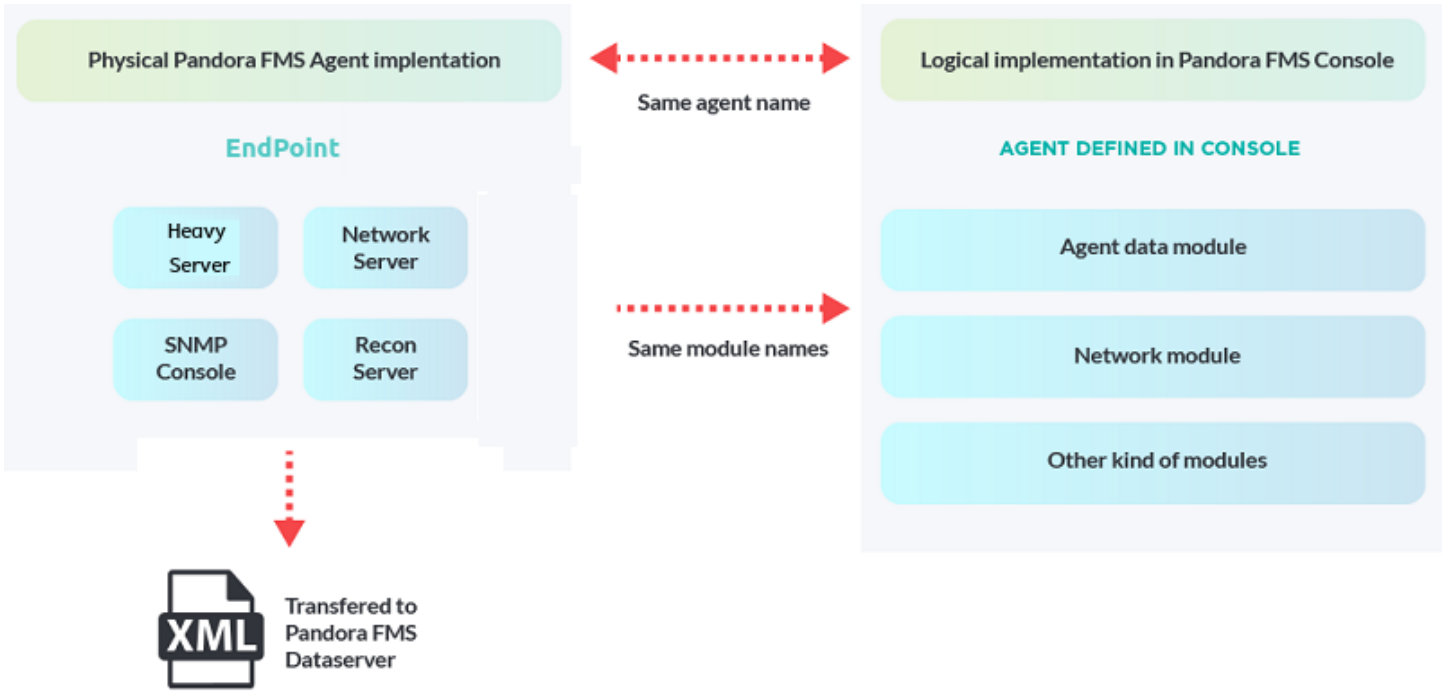
L'agent Pandora FMS est simplement un élément d'organisation créé dans la console web de Pandora FMS et qui est associé à un groupe de modules (ou éléments de surveillance individuels). De plus, cet agent peut avoir (en option) une ou plusieurs adresses IP associées.

Un Agent peut contenir des modules de type distant ou local. Les modules de type distant sont exécutés par les serveurs qui obtiennent les informations à distance (tels que le Network Server), et les modules de type local sont exécutés par les EndPoints et collectés et traités par le serveur de données (Data Server).

EndPoint

Les EndPoints sont installés sur les ordinateurs qui veulent être surveillés localement, en extrayant l'information de l'ordinateur lui-même. Ils sont principalement utilisés dans les serveurs pour surveiller les ressources machines (CPU, RAM, disques...) et les applications installées (MySQL, Apache, JBoss...). Généralement, le supervision des serveurs et de l'équipement sera effectuée à l'aide d'EndPoints, tandis que la surveillance de l'équipement réseau sera effectuée à distance sans l'installation d'aucun logiciel.

Toutes les informations des contrôles effectués sont saisies dans un seul fichier de données au format XML, qui est envoyé par le biais du protocole au serveur Pandora FMS dans une intervalle prédéfini de 300 secondes. Il est également possible de transférer les packets en utilisant SSH ou FTP.



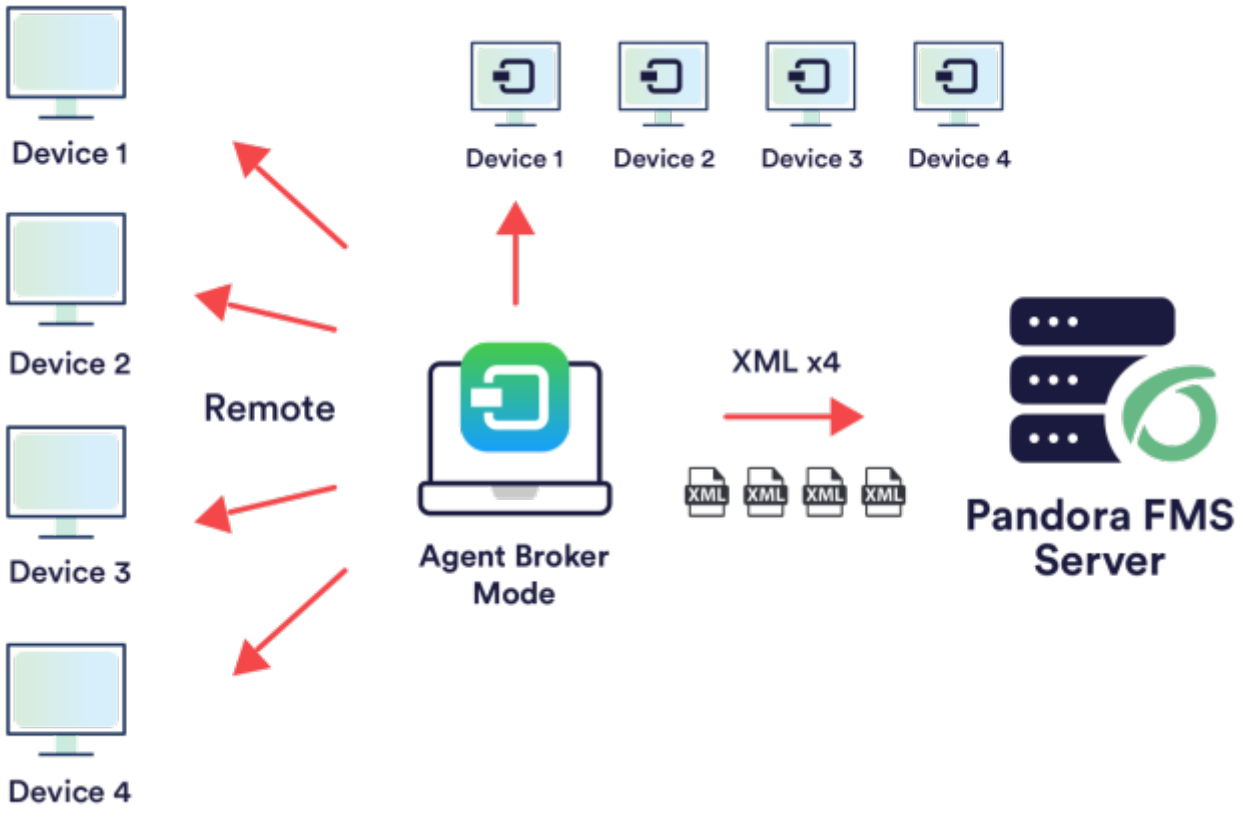
Topologies, schémas et modèles de supervision

Réseaux accessibles

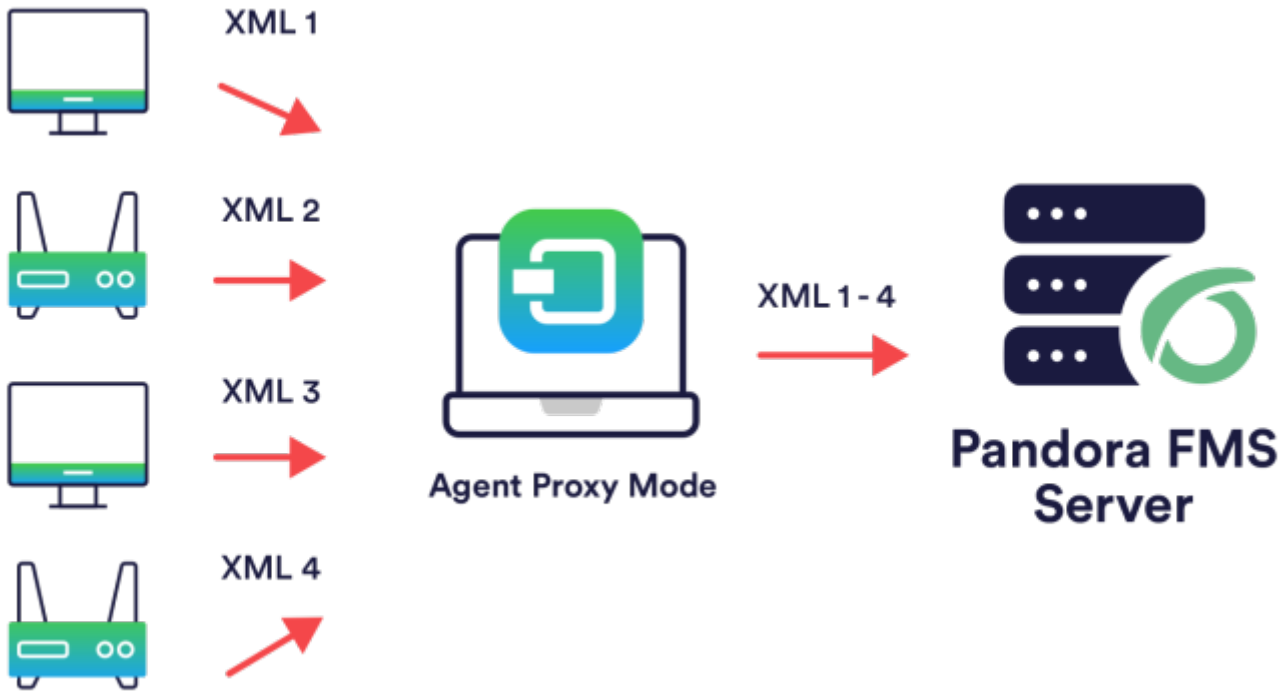
- Réseau accessible pour supervision à distance centralisée. Où, à partir du serveur Pandora FMS, nous pouvons accéder à toutes les machines à sonder à distance.
- Réseau accessible pour la surveillance basée sur les agents. D'où, à partir des EndPoints installés dans les machines surveillées, ils peuvent accéder sans problème au serveur Pandora FMS.

Réseau difficile d’accès

- Le réseau distant n'est pas accessible par les contrôles à distance Pandora FMS: Il utilises le mode *broker agent*.



- EndPoints qui n'ont pas accès au serveur Pandora FMS: Dans ce cas il utilise la fonction *proxy* des EndPoints, qui permet, à un agent qui n'a pas d'accès, d'utiliser un agent qui a accès au serveur, pour se connecter via celui-ci, en transférant les fichiers XML de tous les agents en plus du sien. Le Satellite Server peut aussi agir comme un agent *proxy*.



- Besoin de superviser des différents réseaux pour la surveillance à distance avec le serveur: Dans ce

cas, nous pouvons aussi utiliser le Satellite Server, ou monter plusieurs serveurs Pandora FMS différents, connectés à la même base de données.

Caractéristiques organisationnelles spéciales

- Double reporting: De plus, vous pouvez configurer les agents pour qu'ils rapportent à deux serveurs Pandora FMS différents, bien qu'ils ne puissent être gérés que par l'un d'eux.
- Gestion fragmentée: Il est nécessaire de déléguer la gestion d'une partie des équipes à différents personnels, avec différents accès. Ceci, plus qu'un problème d'architecture, c'est un problème de gestion. Il est résolu avec les permissions assignées sur les politiques.

Grands environnements

- Nombreux réseaux: Lorsque elles ne peuvent pas être centralisées dans un seul serveur des serveurs en mode broker qui distribuent la charge de vérifications à distance.
- Serveurs redondants: En raisons de sécurité, si le matériel principale tombe en panne, un serveur en HA peut automatiquement réinstaller et déléguer la charge de travail de supervision.

← Retour à l'index de la documentation de Pandora FMS