Surveillance avec des agents logiciels

Surveillance avec des agents logiciels

Supervision avec des agents logiciels

Les agents logiciels s'exécutent sur les systèmes d'exploitation à partir desquels ils collectent des informations, en effectuant une vérification pour chaque module.

Les directives de l'agent logiciel sont utilisées pour collecter certaines données directement à partir du système d'exploitation (par exemple, utilisation du processeur, mémoire, événements, etc.), en exécutant des commandes spécifiques au système d'exploitation en suivant les instructions de scripts prédéfinis.

Le serveur de données Pandora FMS traite et stocke dans la base de données toutes les informations générées et envoyées dans un fichier XML par les agents logiciels.

Configuration des agents logiciels

Toute la configuration et tous les paramètres sont stockés dans le fichier pandora_agent.conf, qui est également installé localement avec votre agent logiciel. La configuration de base est couverte dans « Configuration des agents Pandora FMS », la configuration avancée est expliquée ci-dessous.

Configuration local

Dans le fichier de configuration de l'agent logiciel, les modules sont définis avec la structure de texte de base suivante :

```
module_begin
module_name <your module name>
module_type generic_data
module_exec <your command>
module_description <your description>
module_end
```

- Pour l'agent logiciel sur MS Windows® et l'instruction `module_name`, si vous souhaitez ou devez utiliser des caractères ASCII étendus (áéíóú, par exemple), vous devez utiliser un plugin ou un script externe. Voir la section plugin pour les agents logiciels.
- Pour l'agent logiciel sous MS Windows®, `module_exec_powershell` est également disponible pour l'exécution native des contrôles avec PowerShell®.

Configuration à distance

Pour activer la configuration à distance, activez le paramètre : `remote_config 1` et redémarrez l'agent logiciel.

Il est possible de gérer à distance les fichiers de l'agent logiciel depuis la console Web Pandora FMS. La configuration de chaque agent est stockée sur le serveur Pandora FMS dans deux fichiers : <md5>.conf et <md5>.md5, où <md5> est le hachage du nom de l'agent logiciel. Ces fichiers sont stockés respectivement dans :

```
/var/spool/pandora/data_in/conf
```

et

```
/var/spool/pandora/data_in/md5
```

Une fois la configuration de l'agent distant activée, toutes les modifications apportées localement au fichier de configuration seront écrasées par la configuration stockée dans la console. Pour revenir à l'administration locale de l'agent logiciel, arrêtez son service, réinitialisez « remote_config » à zéro et redémarrez le service.

Custom fields

Les champs personnalisés vous permettent d'ajouter des informations supplémentaires à l'agent. Les champs personnalisés peuvent être créés avec l'API PFMS 1.0 et la commande set create_custom_field ou via la console Web dans le menu Gestion → Ressources → Champs personnalisés → Créer un champ.

- Les options Combo activé, Type de mot de passe et Type de lien s'excluent mutuellement, c'est-à-dire qu'une seule d'entre elles peut être utilisée (ou aucune, valeur par défaut).
- En activant le champ Afficher à l'avant, les informations du champ personnalisé seront affichées, s'il a une valeur définie, dans l'aperçu de l'agent. De plus, il sera nécessaire d'activer ce jeton pour envoyer les informations des champs personnalisés au Command Center (Métaconsole).
- Enabled combo : Ce paramètre permet d'activer la configuration des paramètres sélectionnables à partir d'un menu déroulant. Une fois activé, un nouveau champ apparaîtra dans la fenêtre de configuration du champ personnalisé correspondant pour saisir les valeurs du combo séparées par des virgules.
- Password type : La valeur du champ (mot de passe) sera affichée à l'aide d'astérisques dans la console Web.
- Link type : Permet d'ajouter un champ personnalisé qui hébergera un lien web à renseigner par la Web Console ou dans un XML reçu par un agent . Il est possible d'inclure des liens dans les champs

personnalisés d'un XML au format JSON embarqué avec les instructions CDATA <![CDATA[…]]>. Par exemple, si le format JSON du lien est :

```
["Web name","https://example.com"]
```

Le XML aurait cette syntaxe :

```
<custom_fields>
  <name>![CDATA[web]]</name>
  <value>![CDATA[["Web name","https://example.com"|]]]</value>
</custom_fields>
```

Voir « XML Validation », la Security Architecture for the Tentacle protocol (mécanisme chargé de délivrer les données dans format XML vers le serveur de données PFMS) et là Architecture de sécurité pour le serveur de données PFMS (limiter la création automatique d'agents et établir un mot de passe pour le groupe d'agents auquel appartient chaque agent).

Les custom fields peuvent aussi être passés du fichier de configuration de l'agent, en utilisant les token custom_fieldx_name et custom_fieldx_value, par exemple:

```
custom_field1_name Serial Number
custom_field1_value 56446456KS7000
```

Le champ personnalisé appelé `Serial Number` est créé par défaut lors de l'installation de PFMS et vous pouvez créer autant de champs personnalisés que nécessaire et de chaque type différent (valeur simple, lien web, type de mot de passe et type de liste d'options). L'ordre de l'identifiant numérique de chaque champ personnalisé n'a pas d'importance, il vous suffit de vous assurer que le nom est exactement le même :

```
custom_field11_name Simple custom field name
custom_field11_value Simple custom field value

custom_field12_name Custom field Link type
custom_field12_value ["Pandora FMS web site","https://pandorafms.com"]

custom_field13_name Custom field Password type
custom_field13_value My;Password;

custom_field14_name Custom field Combo type
custom_field14_value Two
```

Dans les champs personnalisés `Combo type` la valeur envoyée par l'agent logiciel doit correspondre exactement à l'un de ses éléments, sinon la valeur ne sera pas modifiée.

Paramètres de configuration communs

Paramètres les plus importants pour la configuration de base de Agentes Software :

- server_ip : Adresse IP du serveur Pandora FMS.
- server_path : Chemin du dossier d'entrée entrant du serveur Pandora FMS, par défaut `/var/spool/pandora/data_in`.
- temporaire : Dossier, par défaut `/tmp`.
- fichier journal : Fichier journal de l'agent logiciel, par défaut `/var/log/pandora/pandora_agent.log`.
- intervalle : Intervalle d'exécution de l'agent, `300` secondes par défaut.

Groupes protégés par mot de passe

Par défaut, lorsqu'un agent envoie des données pour la première fois au serveur Pandora FMS, il est automatiquement ajouté au groupe défini dans le fichier de configuration de l'agent.

Il est possible de configurer un mot de passe pour un groupe, de cette façon un agent ne sera pas ajouté à un groupe à moins que le mot de passe correct n'ait été spécifié dans le fichier de configuration de l'agent.

Pour modifier et ajouter un mot de passe de groupe, allez dans le menu Management → Profiles → Manage agent groups → cliquez sur le nom du groupe.

Pour ajouter un nouvel agent à ce groupe, modifiez son fichier de configuration et ajoutez l'option de configuration suivante `group_password` et redémarrez l'agent logiciel.

Modules dans les agents et agents logiciels

Types de modules

Selon les données renvoyées :

- generic_data : Numeric.
- generic_data_inc : Incremental.
- generic_data_inc_abs : Incrémentiel absolu.
- generic_proc : Boolean.
- generic_data_string : Alphanumeric.
- async_data : Asynchronous numeric.
- async_string : Alphanumérique asynchrone.
- async_proc : Boolean asynchronous.
- Module image : Ils utilisent un module de type chaîne de texte (`generic_data_string` ou `async_string`) comme base. Si la donnée contenue dans le module est une image encodée en base64, (en-tête `data:image`) sera identifiée comme une image et permettra un lien vers une fenêtre pour récupérer l'image dans les vues. De plus, le contenu des différentes images qui

composent les chaînes stockées sera affiché dans leur historique respectif.

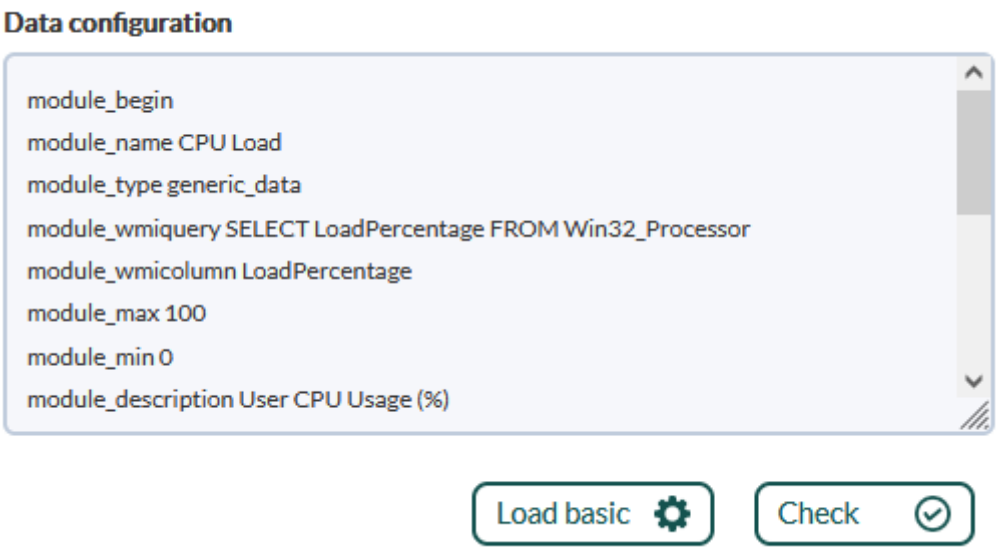
Intervalles dans les modules locaux

Les modules locaux (ou agents logiciels) ont tous leur intervalle d'agent comme « base ». Cependant, ils peuvent prendre des valeurs multiples de cette base si vous modifiez le paramètre `module_interval` avec un multiplicateur entier supérieur à zéro.

Interface de création de modules

La configuration à distance de l'agent logiciel correspondant doit être activée.

La création de modules locaux dans la console se fait à l'aide d'un formulaire où, en plus de la configuration commune de chaque module (seuils, type, groupe, etc.), se trouve une zone de texte où vous pouvez spécifier les données de configuration à établir dans le fichier de configuration de l'agent logiciel.



- En cliquant sur le bouton Load basic (template), le contenu de la configuration des données sera supprimé avec un modèle de base que vous devrez modifier selon le besoin de supervision.
- Une fois modifiée, cliquez sur Check (syntaxe) vérifiera que la syntaxe du modèle est toujours correcte, mais le reste des commandes ne sera pas vérifié.

Lorsqu'un module est chargé depuis un composant local, il peut avoir des macros. Si vous avez des macros, la boîte de configuration sera masquée et un champ apparaîtra pour chaque macro, voir plus d'informations dans Modèles et composants

Supervision conditionnelle

Postconditions

L'agent logiciel prend en charge l'exécution de commandes et de scripts en mode postconditions. Cela signifie que des actions peuvent être effectuées en fonction de la valeur obtenue lors de l'exécution du module. Le paramètre module_condition est utilisé pour cela, par exemple : `module_condition < 20 add_processes.sh`.

Conditions préalables

Le paramètre `module_precondition` permet d'évaluer une condition avant l'exécution du module et avec le résultat de décider si le module doit être exécuté ou non, par exemple : `module_precondition> 10 number_active_processes.sh` .

Supervision intensive

Certains modules ont une importance particulière, comme les processus ou services critiques en cours d'exécution. Afin d'avoir une supervision plus contrôlé de ces cas, une supervision intensif existe.

Il s'agit de signaler dans un intervalle plus court qu'un problème grave est apparu sans qu'il soit nécessaire de réduire l'intervalle général de l'agent.

Configuration dans l'agent logiciel :

- intervalle : Le temps d'échantillonnage de l'agent obligatoire en secondes est l'intervalle général pour tous les modules locaux.
- intensive_interval : Temps pendant lequel il notifiera s'il y a un problème, et il sera toujours exécuté dans cette période et s'il correspond à la condition, il sera notifié dans cette période de temps (sinon les données seront envoyées sur intervalle).

Configuration des modules :

- module_intensive_condition = <value> : Si le module obtient comme résultat la <value> indiquée dans ce paramètre, il notifiera à l'intervalle intensif défini ci-dessus. D'autres opérateurs pouvant être utilisés sont : <, >, `!=`, une plage de valeurs `(m,n)` et =~.

Exemple

Le service sshd est très important car il permet de se connecter à distance via shell, il faut surveiller son fonctionnement :

```
intensive_interval 10
interval 300
```

```
module_begin
module_name SSH Daemon
module_type generic_data
module exec ps aux | grep sshd | grep -v grep | wc -l
module_intensive_condition = 0
module_end
```

Si le service est absent, il vous avertira dans les 10 secondes suivantes, s'il fonctionne, il vous avertira toutes les 5 minutes (intervalle normal, 300 secondes).

Supervision programmée

L'agent logiciel prend en charge la définition de modules planifiés qui sont exécutés à des heures définies. La syntaxe utilisée est la même que celle du fichier crontab.

Contrôles à distance avec l'agent logiciel

Un agent logiciel est capable d'effectuer des contrôles à distance, de remplacer le serveur PFMS principal et même de les distribuer aux agents courtiers.

Vérifications ICMP

Les vérifications ICMP ou pingsont très utiles pour savoir si une machine est connectée à un réseau ou non.

Unix

```
module_exec ping -c 1 dir_IP> /dev/null 2>&1; if [ $? -eq 0 ]; then echo 1; else
echo 0; fi
```

MS Windows®.

```
module_ping dir_IP
```

Remarque : module_advanced_optionspermet des options avancées pour `ping.exe`.

Vérifications TCP

Les vérifications TCP sont utiles pour vérifier que les ports d'une machine restent ouverts et permettent de savoir si une application se connecte ou non au réseau.

Unix

Avec la commande nmap et ses paramètres de configuration en ligne de commande, on vérifie une adresse IP si le port 80 est ouvert (timeout de réponse de 5 secondes) :

```
module_begin
module_name PortOpen
module_type generic_proc
module_exec nmap 192.168.100.54 -p 80 | grep open> /dev/null 2>&1; echo $?; if [
$? == 0 ]; then echo 1; else echo 0; fi
module_timeout 5
module_end
```

MS Windows®.

Les paramètres doivent être spécifiésr dans :

- module_tcpcheck : adresse IP de l'appareil.
- module_port : numéro de port.
- module_timeout : délai d'attente pour la réponse.

Exemple :

```
module_begin
module_name TcpCheck
module_type generic_proc
module_tcpcheck 192.168.100.54
module_port 80
module_timeout 5
module_end
```

Vérifications SNMP

Les contrôles SNMP sont courants dans la supervision des périphériques réseau pour vérifier l'état des interfaces, des octets d'entrée/sortie, etc.

Exemple Unix

```
module_exec snmpget dir_IP -v 1 -c public .1.3.6.1.2.1.2.2.1.1.148 | awk '{print
$4}'
```

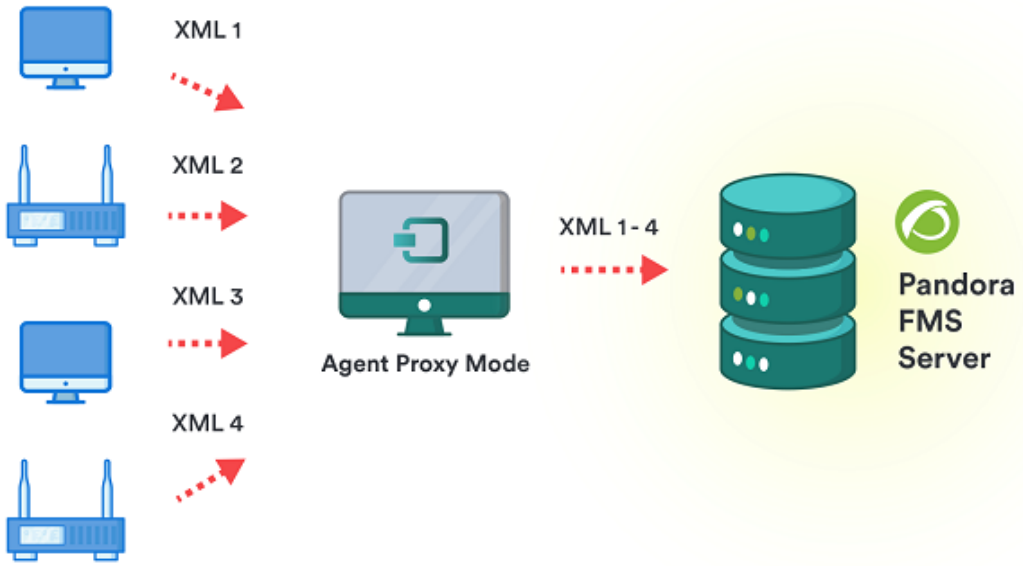
Exemple dans MS Windows®

```
module_snmpget
module_snmpversion 1
module_snmp_community public
module_snmp_agent 192.168.100.54
module_snmp_oid .1.3.6.1.2.1.2.2.1.1.148
module_end
```

Mode proxy

Pour utiliser le mode proxy de l'agent Pandora FMS sous Linux/Unix® il ne peut pas être exécuté par l'utilisateur root, donc une installation spéciale de l'agent Pandora FMS est nécessaire. Pour cela, consultez Installation d'agent personnalisé.

Ce mode vous permet de rediriger les fichiers de données générés par d'autres agents logiciels vers le serveur Pandora FMS. L'agent logiciel qui agit en mode proxy peut également effectuer des tâches de supervision.

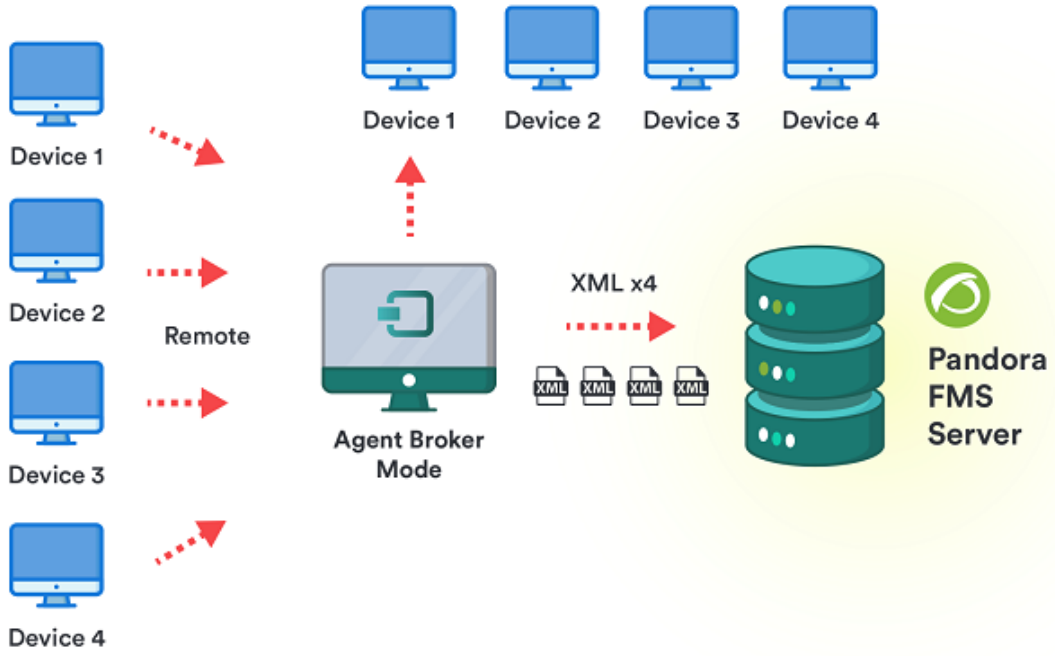


Configuration des paramètres :

- server_ip : L'adresse IP du serveur Pandora FMS.
- proxy_mode : Activé (1) ou désactivé (0).
- proxy_max_connection : Nombre de connexions proxy simultanées, par défaut 10.
- proxy_timeout : Délai d'attente de réponse pour le proxy, par défaut 1 seconde.
- proxy_address : Adresse sur laquelle le proxy écoute.
- proxy_port : Port sur lequel le proxy écoute.

Mode courtier

Le mode Broker des agents logiciels permet à un seul agent d'effectuer des vérifications et de gérer la configuration comme s'il s'agissait de plusieurs agents différents.



Lorsque le mode Broker est activé dans un agent logiciel, un nouveau fichier de configuration est créé. À partir de ce moment, l'agent logiciel d'origine et le nouveau courtier seront gérés séparément avec leurs fichiers de configuration indépendants, comme s'il s'agissait de deux agents logiciels complètement distincts sur la même machine.

Pour créer un Broker, ajoutez une ou plusieurs lignes avec le paramètre broker_agent <broker_name> (une ligne pour chaque Broker).

Dans la console Web Pandora FMS, les courtiers sont vus et gérés comme des agents indépendants.

- Les modules qui enregistrent les données en mémoire entre les exécutions (`module_logevent` et `module_regexp` sur MS Windows®) ne fonctionnent pas lorsque les agents courtiers sont configurés.
- Les instances en mode Broker ne peuvent pas utiliser les collections.

Inventaire avec agent logiciel

Pour plus d'informations visitez la section Inventaire local avec agents logiciels.

Collecte de journaux avec un agent logiciel

Pour plus d'informations visitez la rubrique Collecte et surveillance des journaux.

Actions à distance via UDP

Un agent logiciel est capable de recevoir des demandes à distance et d'exécuter des commandes.

Gardez à l'esprit qu'UDP est intrinsèquement non sécurisé
(mais efficace pour envoyer des messages sans
compromettre une certaine réponse).

Pour permettre au serveur PFMS d'envoyer des commandes aux Agents Logiciels dont il a la charge, les éléments suivants doivent être configurés :

- udp_server : zéro par défaut, valeur un (1) pour activer cette fonctionnalité.
- udp_server_port : port d'écoute sur Software Agent.
- udp_server_auth_address : adresse IP du serveur Pandora FMS

Redémarrez l'agent logiciel pour que les modifications prennent effet.

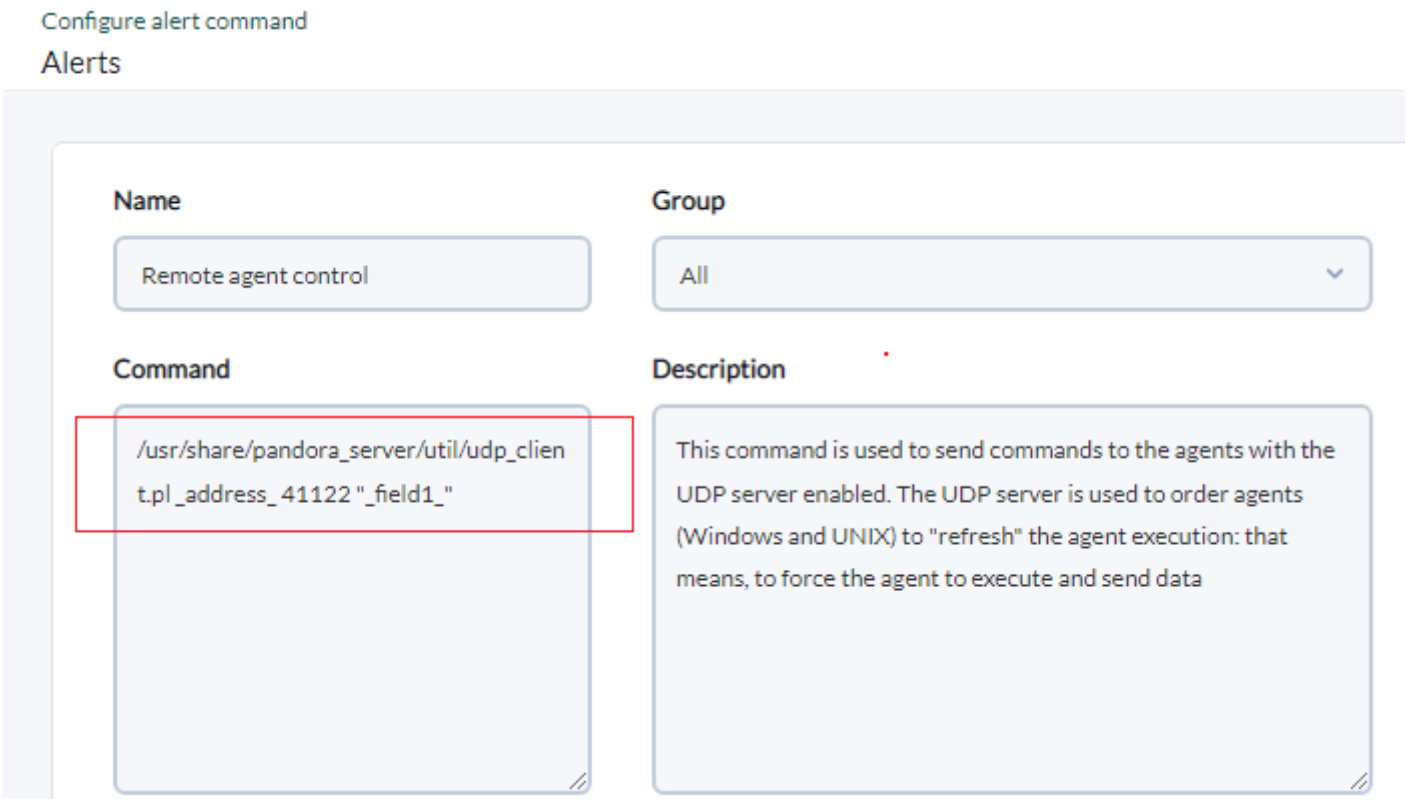
Bien qu'il puisse être défini sur 0.0.0.0 pour accepter toutes les sources, cette pratique n'est pas recommandée. Si vous disposez de plusieurs serveurs PFMS et/ou utilisez IPv6, vous pouvez placer différentes adresses IP séparées par des virgules. Par exemple, si vous disposez d'IPv6 : `2001:0db8:0000:130F:0000:0000:087C:140B` et que son abréviation est `2001:0db8:0:130F::87C:140B`, utilisez les deux séparés par des virgules.

Comment demander un redémarrage du service Agents logiciels

Vous devez utiliser le script situé à l'adresse :

```
/usr/share/pandora_server/util/udp_client.pl
```

Il peut être exécuté depuis la ligne de commande ou utilisé dans une alerte, à l'aide de la commande fournie preconfigured dans la console Remote agent control.



Actions à distance personnalisées

En plus de l'action de service de redémarrage de l'agent logiciel, des actions personnalisées peuvent être spécifiées.

```
process_<order_name>_start command
```

Vous pouvez également créer des commandes qui appellent des scripts pour effectuer plusieurs actions à distance en appuyant simplement sur un bouton.

Plugins dans les agents logiciels

Contrairement aux plugins serveur, exécutés par le serveur Pandora FMS, les plugins Software Agent signalent un ou plusieurs modules à la fois.

Exécution sur les systèmes Windows

Sous MS Windows®, tous les plugins enregistrés par défaut sont programmés en VBScript, pour les exécuter l'interpréteur `cscript.exe` est utilisé.

Vérifications utilisation PowerShell

À partir de la version 776, le module `module_exec_powershell` permet d'entrer des commandes plus complexes dans PowerShell avec des caractères spéciaux et des instructions complexes (une instruction délivre des résultats à la suivante), ce qui n'est pas possible avec le module `module_exec`.

```
# Example of Powershell execution module
module_begin
module_name Powershell
module_type generic_data_string
module_exec_powershell < command_1 > | < command_2 > | … | < command_N >
module_end
```

Les commandes sont saisies telles quelles, sans guillemets, afin d'être traitées par l'agent logiciel PFMS (les commandes PowerShell, en revanche, peuvent nécessiter des guillemets). Si la commande n'est pas valide, une erreur est ajoutée au journal de l'agent (fichier `pandora_agent.log`).

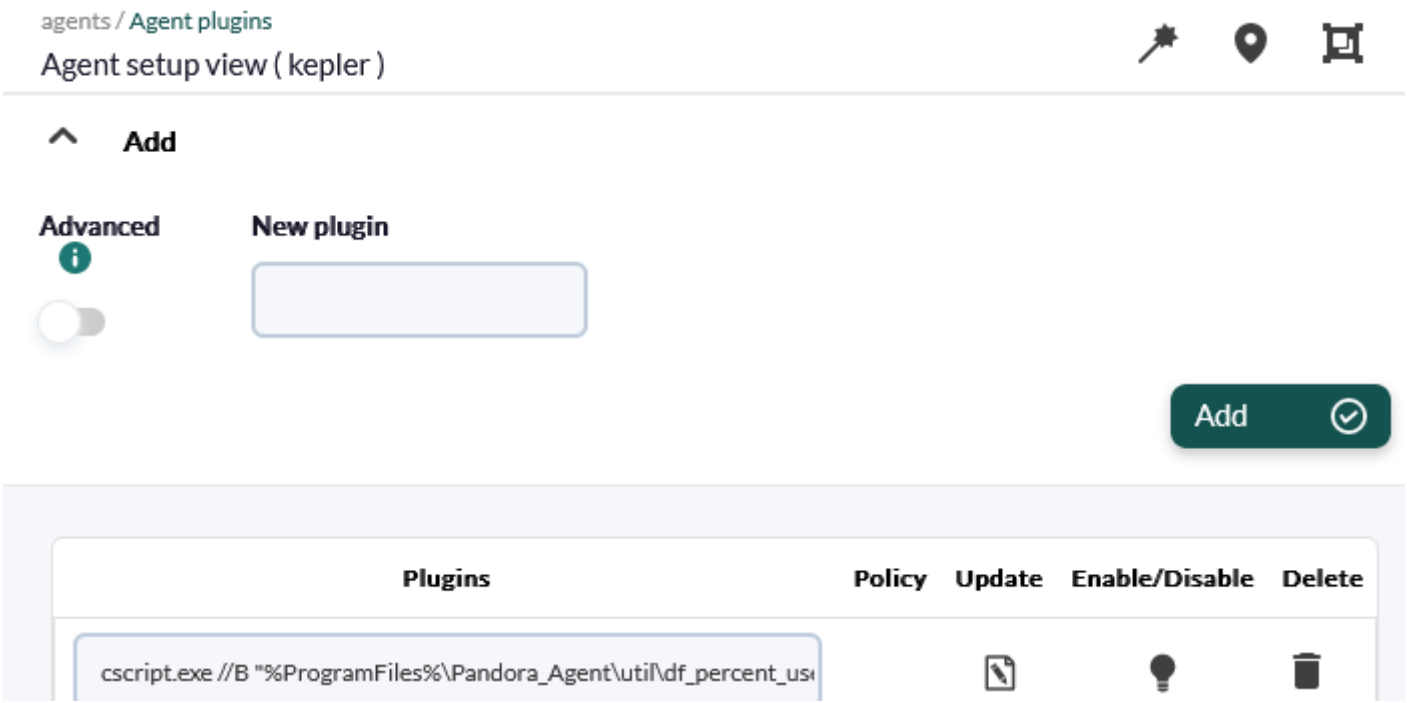
Exécution sur les systèmes Unix

Les plugins Unix se trouvent par défaut dans le répertoire de l'agent :

```
/etc/pandora/plugins
```

Gestion des plugins Agent Logiciel depuis la Console

Il est possible de gérer sans éditer directement le fichier de configuration. En activant la configuration à distance, un agent logiciel dans sa vue d'administration aura l'onglet éditeur de plugin.



Gestion des plugins avancés de l'Agent Logiciel depuis la Console

Version NG 750 ou ultérieure.

Il est possible d'ajouter un jeton dans la configuration du plug-in de l'agent qui, lorsqu'il est activé, permet d'« encapsuler » les définitions du plug-in dans les balises `module_begin` et `module_end`.

Ce jeton activé permet d'insérer des blocs de configuration tels que `module_interval` ou `module_crontab`, entre autres.

Comment créer des plugins personnalisés pour l'agent logiciel

Les plugins peuvent être créés dans n'importe quel langage de programmation. Seules les règles générales et les règles spécifiques doivent être prises en compte pour son développement.

Assurez-vous de terminer la sortie du nouveau plugin (s'il s'agit d'un script) avec un `errorlevel 0` sinon l'agent interprétera que le plugin a eu une erreur et n'a pas pu exécuter le travail.

Utilisation des plugins Nagios depuis Software Agent

Nagios dispose d'un grand nombre de plugins que vous pouvez utiliser avec Pandora FMS. Une façon de procéder consiste à utiliser des plugins distants avec le Plugin Server, en utilisant la

Compatibilité Nagios.

Surveillance avec KeepAlive

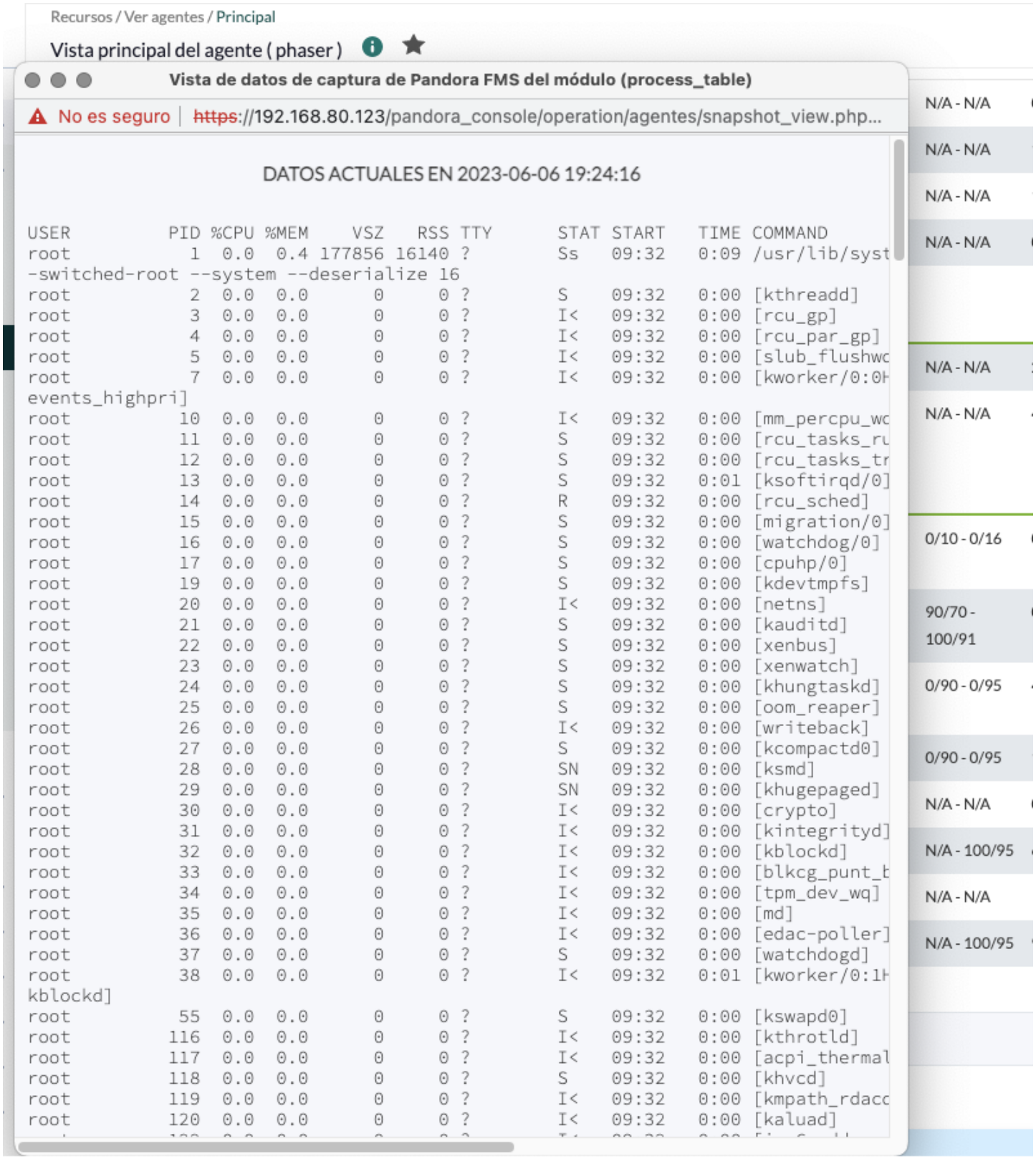
Le module KeepAlive ne peut être créé que depuis la Console, même si la configuration à distance n'est pas activée et ne laisse aucune trace dans le fichier `pandora_agent.conf`.

Un module unique dans Pandora FMS est du type appelé `keep_alive`, utilisé pour alerter si un agent logiciel a cessé d'envoyer des informations.

Vous devez vous rendre dans l'onglet modules (Gestion → Gérer les agents → cliquer sur le nom de l'agent → Modules).

Vous devez appuyer sur Create a module et sélectionner Create a new data server module → Create → saisir le nom du nouveau module → Create.

Supervision des instantanés de commandes (Command snapshots)



Les commandes qui ont de longues sorties, telles que `top` ou `netstat -n` peuvent être entièrement capturées par un module et lues telles quelles. Le module doit être configuré en type texte, exemple :

```
module_begin
module_name process_table
module_type generic_data_string
module_exec ps aux
module_description Command snapshot of running processes
module_group System
module_end
```

- Pour que cela fonctionne ainsi, configurez correctement à la fois la console Pandora (installation) et l'agent qui collecte ces informations, en vous assurant qu'il s'agit de texte brut.
- Dans la Console, l'option Command line snapshot doit être activée.

Supervision et affichage des images

Cette méthode permet de définir des modules de type chaîne (`generic_data_string` ou `async_string`) qui contiennent des images au format texte avec un encodage base64, pouvant afficher ladite image au lieu d'un résultat spécifique.

Par exemple :

```
#!/bin/bash
echo "<module>"
echo "<name>Actual leader</name>"
echo "<type>async_string</type>"
echo "<data><![CDATA[....]]></data>"
echo "</module>"
```

Écrivez ce contenu dans un fichier sur l'agent (ou distribuez-le à collections) et exécutez-le comme ceci :

```
module_plugin <complete path to the file>
```

Supervision spécifique à Windows

- Si le nom du processus contient des espaces no use “ ” .
- Le nom du processus doit être le même que le Gestionnaire des tâches de Windows (`taskmngr`), y compris l'extension `.exe`.
- Il est important de respecter les majuscules et les minuscules.

Supervision des processus et watchdog de processus

Supervision de processus

Le paramètre module_proc vérifie si un nom de processus donné fonctionne sur cette machine. Exemple :

```
module_begin
```

```
module_name CMDProcess
module_type generic_proc
module_proc cmd.exe
module_description Process Command line
module_end
```

Le paramètre module_async yes doit être ajouté :

```
module_begin
module_name CMDProcess
module_type generic_proc
module_proc cmd.exe
module_async yes
module_description Process Command line
module_end
```

Watchdog des processus

La fonctionnalité Watchdog pour MS Windows® permet de redémarrer un processus interrompu, par exemple :

```
module_begin
module_name Notepad
module_type generic_data
module_proc notepad.exe
module_description Notepad
module_async yes
module_watchdog yes
module_user_session yes
module_start_command "%SystemRoot%\notepad.exe"
module_startdelay 3000
module_retrydelay 2000
module_retries 5
module_end
```

Supervision des services et watchdog des services

Supervision des services

Le paramètre module_service vérifie si un certain service est en cours d'exécution sur la machine. La définition d'un module utilisant ce paramètre serait :

```
module_begin
module_name Service_Dhcp
module_type generic_proc
module_service Dhcp
```

```
module_description Service DHCP Client
module_end
```

Pour avertir immédiatement lorsqu'un processus cesse de fonctionner, le paramètre module_async yes doit être ajouté (voir règles communes au début de la section Windows) :

```
module_begin
module_name Service_Dhcp
module_type generic_proc
module_service Dhcp
module_description Service DHCP Client
module_async yes
module_end
```

Watchdog de services

Il fonctionne de la même manière que Process Watchdog. Exemple :

```
module_begin
module_name ServiceSched
module_type generic_proc
module_service Schedule
module_description Service Task scheduler
module_async yes
module_watchdog yes
module_end
```

La définition du watchdog pour les services ne nécessite aucun paramètre supplémentaire tel que des processus, car ces informations figurent déjà dans la définition du service.

Supervision des ressources de base

Lors de l'installation de l'agent logiciel PFMS pour MS Windows®, les modules de base nécessaires sont inclus, certains sont actifs et d'autres doivent être activés par Remote configuration (ou en éditant localement le fichier `.conf` de l'agent).

Revenir à l'index de la documentation Pandora FMS