Supervision à distance

Supervision à distance

Supervision à distance

Introduction

Le serveur de réseau exécute les tâches qui lui sont assignées par le biais d'un système de file d'attente multiprocessus, il peut travailler avec d'autres serveurs de réseau (mode HA).

Il doit avoir une visibilité totale (adresses IP et ports) sur lesquels les tests doivent être effectués. Ce chapitre couvre également le serveur Plugin et le serveur WMI.

Supervision de base du réseau

1. Tests ICMP: Ce sont des tests de base du réseau qui permettent de savoir si un host est accessible et opérationnel et le temps qu'il faut pour arriver à ce dispositif par le réseau.
2. Tests TCP: À distance, il est possible de vérifier qu'un système a bien son port TCP d'ouvert, qui est précisé dans la définition du module.
3. Tests SNMP: À distance, il est possible de lancer des requêtes SNMP (*SNMP Polling*) vers des systèmes qui ont leur service SNMP d'activé et accessible pour obtenir des données comme l'état des interfaces, la consommation de réseau par interface, etc.

Le serveur réseau est celui qui exécute les différents tests attribués à chaque agent. Chacun est assigné à un serveur réseau et c'est ce dernier qui se charge de son exécution, en insérant les résultats dans la base de données du système de Pandora FMS.

Configuration générique d'un module pour la surveillance réseau

Pour surveiller un équipement ou un service d'équipement (FTP, SSH, etc.) à distance, il faudra tout d'abord créer l'agent correspondant pour surveiller le service, menu Management → Resources → Manage agents → Create agent. Remplissez les détails de votre nouvel agent et cliquez sur le bouton Create.

Une fois l'agent créé, appuyez sur le volet au-dessus des modules (Modules). Sélectionnez créer un nouveau module réseau et appuyez sur le bouton Create. Sur le formulaire suivant, sélectionnez un module de composant réseau. Lorsque le menu déployable à droite sera chargé, cherchez la vérification test qui vous intéresse.

Supervision ICMP

L'exemple précédent est un exemple de supervision ICMP. Ce sont les vérifications les plus basiques et simples qui nous fournissent des informations importantes et exactes.

- icmp_proc: Ou vérification d'host (ping), qui permet de savoir si une adresse IP répond ou non.
- icmp_data: Ou vérification de latence. Il nous informe du temps en millisecondes qu'il faut pour l'adresse IP afin de répondre à une consultation de base de ICMP.

Supervision TCP

TCP est conçu vers la connexion, donc en envoi TCP Send se corresponde à une réponse TCP Receive qui indique l'état d'un port ou d'un service à superviser. De façon facultative, vous pouvez lui envoyer une chaîne de caractères et attendre de recevoir une réponse traité par Pandora FMS comme donnée.

- TCP send: Un champ pour configurer les paramètres à envoyer au port TCP. Il admet la chaîne `^M` pour la remplacer par l'envoi d'un retour de charriot.
- TCP receive: Champ pour configurer les chaînes de texte qui attendent de recevoir la connexion TCP. S'ils s'envoient/reçoivent en différentes étapes, chacune se séparent par ce caractère `|`.

Exemple:

TCP Send

```
HELO myhostname.com^M|MAIL FROM: ^M| RCPT TO: ^M
```

TCP Receive

```
250|250|250
```

Modules d'exécution à distance

Pour pouvoir exécuter correctement ces modules, vous avez besoin des identifiants de connexion de l'agent à superviser. Pourtant tout ça doit être enregistré dans l' entrepôt sécurisé d'identifiants.Les instructions relatives à la configuration générique d'un module sont répétées, mais l'un des éléments suivants est sélectionné:

- `remote_execution_data`: Numérique.
- `remote_execution proc`: *Booléen* (0 FAUX, autre que zero VRAI).
- `remote_execution_data_string`: Alphanumérique (chaîne).
- `remote_execution_data_inc`: Incremental (ratio).

Les paramètres suivants doivent être définis:

1. Target IP : L'IP cible (si vous n'entrez rien, il utilisera celle de l'agent).

2. Port : Le port auquel vous connecter (22 sur GNU/Linux, n'importe quel sur MS Windows®).
3. Command : La commande à exécuter pour la supervision.
4. Credential identifier : Le set d'identifiants à utiliser pour vous connecter.

À partir de la version 743 dans le fichier `pandora_server.conf` vous devez disposer de *tokens* pour la configuration des paramètres suivants liés à l'exécution à distance de modules: `ssh_launcher`, `rcmd_timeout` et `rcmd_timeout_bin`.

Propriétés avancées communes des modules réseau

- Custom ID : Il permet de stocker un ID d'une application externe pour faciliter l'intégration de Pandroa FMS avec des applications tiers. Par exemple, une *Configuration management database* (CMDB).
- Interval : Intervalle ou exécution du module, qui peut être personnalisé par un utilisateur administrateur de manière prédéfinie et ensuite être utilisé par des utilisateurs standard.
- Post process : Post processus du modèle (multiplier ou diviser la valeur renvoyée), comme par exemple lorsqu'ils obtiennent des bytes et qu'il faut montrer la valeur en Megabytes.
- Min. Value et Max. Value : Toute valeur inférieure regardant le minimum et supérieure au maximum sera considérée comme invalide et sera ignorée.
- Export target : Cela n'est disponible qu'en version Enterprise de Pandora FMS et si un serveur d'exportation a été configurée.
- Category: Cette catégorisation n'a pas d'effet depuis l'interface de l'utilisateur normal. Elle est pensée pour être utilisée avec la Métaconsole.
- Si *Cron from* est activé, le module sera exécuté une fois lorsque la date et l'heure coincident avec la dete et l'heure configurées dans *Cron from*, en ignorant l'intervale propre du module.

Supervision SNMP

Introduction à la surveillance SNMP

- Polling SNMP: Se fait de temps en temps de manière active et implique d'ordonner à Pandora FMS d'exécuter une commande `get` vers un dispositif SNMP.
- Trap SNMP: Est fait avec des changements ou d'événements dans un appareil, qui peuvent se produire à tout moment ou pa. Il est nécessaire d'activer la console de *traps* ou déroutements SNMP Pandora FMS, où ceux qui sont reçues depuis n'importe quel appareil seront affichés. Définissez alertes par le biais de règles de filtrage de *traps* a travers n'importe quel champ.

Pandora FMS travaille avec SNMP en gérant des OIDs individuels. Pour Pandora FMS, chaque OID est un module réseau.

Pour travailler avec des dispositifs SNMP, il faut

- Activer la gestion SNMP de l'appareil pour que le serveur réseau puisse faire que requêtes SNMP.
- Connaître l'IP et la communauté SNMP du dispositif distant.

- Connaître l'OID du dispositif distant (ou utiliser l'un des divers *wizards* dont Pandora FMS dispose ou son explorateur de OIDs SNMP).
- Savoir comment gérer les données que renvoie le dispositif. Les SNMP renvoient des données dans différents formats. Pandora FMS peut presque tous les traités. Celles de type compteur sont celles que Pandora FMS gère comme `remote_snmp_inc` et sont d'une importance capitale puisqu'en étant compteurs, elles ne peuvent être traitées comme données numériques mais comment taux d'éléments par seconde. La majorité des données statistiques SNMP sont de type compteur et doivent être configurées comme `remote_snmp_inc` si vous souhaitez les superviser correctement.

Supervision avec modules réseau type SNMP

Pandora FMS inclut quelques OID dans sa base de données que vous pouvez utiliser directement. Les MIB sont un ensemble de définitions qui définissent les propriétés de l'objet géré au sein de l'appareil à gérer.

Il existent plus de MIBs inclues dans Pandora FMS, et avec la version Enterprise des packages de MIBs pour différents appareils sont inclus.

Pour pouvoir superviser d'autres éléments par SNMP vous devez connaître leur communauté SNMP. En créant le module, sélectionnez Manual setup. Dans le champ Type il y a trois options pour SNMP, lorsque vous sélectionnez l'un d'entre elles le formulaires deviendra plus grand en affichant les champs additionnels pour SNMP.

- SNMP community: C'est comme une identification d'utilisateur ou mot de passe qui permet l'accès aux statistiques d'un routeur ou d'autre appareil (versions SNMPv1 et SNMPv2 puisque SNMPv3 utilise l'authentification par identifiants). Par défaut les appareils incluent la communauté publique (public) de lecture seulement et en général chaque administrateur réseau change toutes les chaînes de la communauté à des valeurs personnalisées dans la configuration de l'appareil.
- SNMP OID: Identificateur OID à surveiller. Il consiste en une chaîne de numéros et de points. Ces chaînes sont automatiquement traduites par des chaînes alphanumériques plus descriptives si les MIB correspondants se trouvent installés dans le système.

Surveiller SNMP à partir des agents logiciels

Un agent logiciel est généralement utilisé pour obtenir des données locales, mais il peut également effectuer une surveillance SNMP.

Sur GNU/Linux®

snmpget est installée par défaut normalement, donc il peut être appelé depuis la ligne *module_exec*.

```
module_exec snmpget -v <version> -c <communauté> <adresse IP> <OID numérique>
```

Il faut souligner que seulement les OID “de base” peuvent être traduits par son equivalent numérique et il est recommandable d'utiliser toujours des OID numériques, puisque vous ne savez pas s'il va savoir la traduire ou pas. Dans tous les cas, il est possible de charger les mibs dans le répertoire:

```
/usr/share/snmp/mibs
```

Sur MS Windows®

snmpget.exe (qui conforme le projet net-snmp, avec licence BSD) est ajouté à l'agent logiciel ensemble avec les MIBs de base, outre un empaqueteur (*wrapper*) ou *script* pour encapsuler l'appel. Tout comme Linux, les MIBs peuvent être chargées dans le répertoire:

```
/util/mibs
```

Gestionnaire de MIBS

Pandora FMS utilise les MIBs stockées par le système d'exploitation dans:

```
/usr/share/snmp/mibs
```

Utilisez la fonctionnalité MIB uploader pour en ajouter de nouvelles, menu Operation → Monitoring → SNMP.

Ces MIBs ne seront utilisées que par Pandora FMS stockées dans le chemin:

```
{PANDORA_CONSOLE}/attachment/mibs
```

Cette fonctionnalité gère seulement les MIB pour *Polling SNMP*, pour les *Trap SNMP* lisez la séction Supervision avec traps SNMP.

Navigateur SNMP de Pandora FMS

Version Enterprise NG 744 ou ultérieure.

Le navigateur SNMP fait une collecte entière de l’arbre de l'appareil et ladite opération peut prendre quelques minutes. Il est aussi possible d'explorer seulement quelques sous-branche, ce qui vous fera gagner du temps. Pour y accéder, allez vers Monitoring > SNMP > SNMP Browser.

Le système demandera cette information au système et montrera, par ailleurs, les informations de l’OID sollicité. S’il n’en existe aucune sur le OID du dispositif, elle ne s’affichera qu’en format

numérique. L'information descriptive des OID se conservent via les MIB. Si vous ne disposez pas de MIB pour le dispositif que vous souhaitez explorer, vous devrez sûrement aller chercher "des morceaux d'informations" dans les informations visualisées par Pandora FMS, ce qui est complexe et long.

L'explorateur SNMP permet également de rechercher une chaîne de texte à la fois dans les valeurs d'OID obtenues et dans les valeurs traduites des OID eux-mêmes (si elles sont disponibles). Cette fonction est particulièrement utile pour rechercher des chaînes de caractères connues et localiser leur OID. S'il trouve plusieurs entrées, il nous permettra de passer d'une occurrence à l'autre et les affichera en jaune.

Il est possible de sélectionner plusieurs OID et de les ajouter à un agent en cliquant sur le bouton Créer des modules d'agents. Pour ce faire, sélectionnez les agents qui seront surveillés avec ces OID et ajoutez-les dans la case de droite. Il est également possible de sélectionner plusieurs OID pour les ajouter à une politique de surveillance.

Wizard SNMP de Pandora FMS

La vue d'administration d'un agent.

Vous devrez définir l'IP de destination, la communauté et d'autres paramètres (SNMP v3 est supporté) pour faire un *Walk* à la machine. Une fois l'information reçue, un formulaire apparaîtra pour la création de modules tels que Devices, Processes, Free space on disk, Temperature sensors et Other SNMP data.

Le type de module est sélectionné et ajouté à la liste de création. Lorsque ce processus est terminé, le bouton Create des modules peut être cliqué.

Ce *wizard* créera deux types de modules:

- Modules SNMP pour les consultations avec OID statique (Capteurs, Mémoire, CPU, etc.)
- Modules Plugin pour les consultations avec OID dynamique ou les données calculées (Processus, Espace sur le disque, Mémoire utilisée exprimée en pourcentage, etc).

Pour les modules de type plugin, nous utiliserons le plugin de SNMP. C'est pourquoi, si le plugin n'est pas installé dans le système, ces caractéristiques resteront désactivées. Le plugin devra avoir le nom snmp_remote.pl. La localisation où il de sa conservation importera peu.

Pour que le *wizard* SNMP puisse obtenir les données d'un appareil SNMP grâce aux composants distants, il est nécessaire de remplir 2 conditions:

- Avoir enregistré dans Pandora FMS le Private Enterprise Number (PEN) du fabricant de l'appareil.
- Avoir enregistrés et habilités les composants du wizard SNMP dans Pandora FMS pour le fabricant de l'appareil.

Si l'appareil exploré remplit ces conditions, tous les modules dont il y a des données obtenues seront affichés pour vous donner l'opportunité de sélectionner lequel créer ou pas.

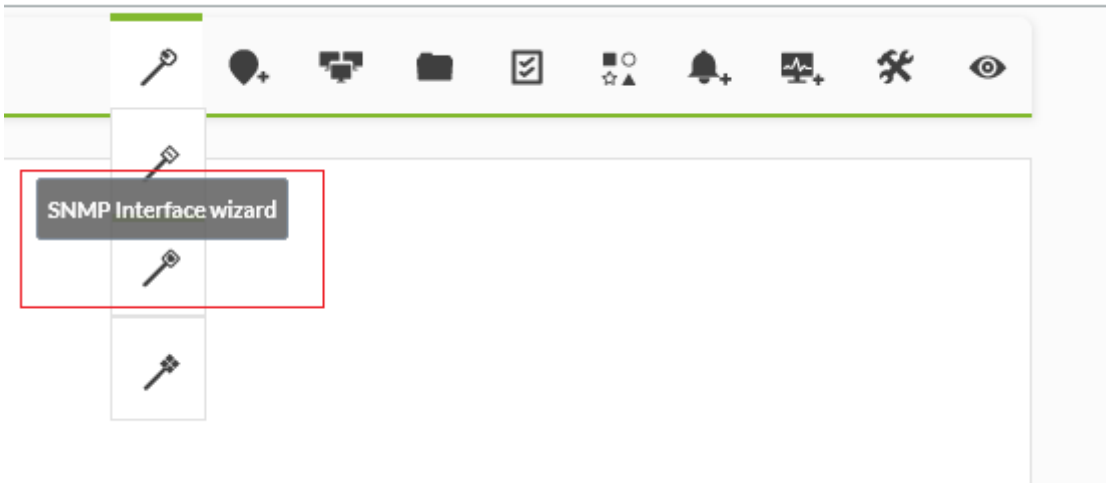
Une fois *Create modules* cliqué, vous verrez une liste que résume les modules choisis avec leur configuration correspondante. Cette liste montrera les modules qui ne sont pas crées qu'il soit parce qu'ils existent déjà sur l'agent ou parce que vous avez configuré 2 ou plus modules avec le même nom dans le *wizard* il même.

Regardez à l'esprit que si la valeur du module recueilli par le *wizard* est incrémentale ou incrémentale absolue, ladite valeur n'est pas l'incrément mais une valeur référentielle. Pour obtenir une valeur incrémentale il a besoin de deux lectures, donc la valeur du module indiquera "zero" jusqu'à la prochaine lecture.

Avant d'être ajoutés à l'agent, il y aura une dernière opportunité de confirmer la création de ces modules o de la canceler et de continuer à modifier le résultat du *wizard*.

Wizard WMI

Utilisé pour naviguer et créer des modules avec des requêtes WMI pour un agent en particulier. Dans le *Wizard* d'agent (onglet dans la vue d'administration d'un agent), cliquez sur l'icône:



Cet assistant navigue dans la branche SNMP IF-MIB::interfaces, offrant la possibilité de créer plusieurs modules à partir de diverses interfaces avec une sélection multiple. Après avoir sélectionné l'adresse IP cible, la communauté, etc., le système effectue une requête SNMP vers la machine cible et remplit le formulaire de création de module.

Vous devez avoir les composants du wizard WMI registrés et habilités dans Pandora FMS: de cette manière, tous les modules dont des données ont été obtenues seront montrés pour vous offrir l'opportunité de les créer ou pas.

Une fois que la création des modules a été confirmée, ceux-ci seront réévalués un par un pour déterminer s'ils peuvent être créés ou non, afin d'éviter les modules en double au cas où les mêmes modules auraient été créés par d'autres moyens pendant la période de confirmation.

Nous serons informés si le processus a pu être mené à bien ou, au contraire, si des modules n'ont pas pu être créés.

Surveillance à distance de MS Windows avec WMI

WMI est une technologie utilisée dans le système d'exploitation Microsoft® (O.S.) pour obtenir des informations à distance à partir d'ordinateurs fonctionnant sous Windows® ; elle est disponible à partir de la version Windows XP jusqu'aux versions les plus récentes. WMI permet d'obtenir toutes sortes d'informations à partir du système d'exploitation, des applications et même du matériel. Les requêtes WMI peuvent être effectuées localement avec l'agent logiciel (en appelant l'API de l'O.S.) ou à distance.

Dans certains systèmes, l'accès à distance à WMI n'est pas activé et doit l'être pour pouvoir être consulté de l'extérieur.

Il est nécessaire d'activer le composant wmiserver dans le fichier de configuration du serveur Pandora FMS.

```
# wmiserver: 1 or 0. Set to 1 to activate WMI server with this setup
# DISABLED BY DEFAULT
wmiserver 1
```

Les requêtes sont effectuées en WQL, une sorte de langage SQL spécifique à Microsoft®, pour tout objet apparaissant dans la base de données du système WMI.

Para comenzar a monitorizar por WMI, primero se deberá crear el agente correspondiente, luego se pulsará sobre la solapa superior de los módulos (Modules). Una vez en ella, se selecciona Create a new WMI server module y se pulsa el botón Create.

Pour commencer la surveillance via WMI, il faut d'abord créer l'agent correspondant, puis cliquer sur l'onglet supérieur des modules (Modules). Une fois là, sélectionnez Create a new WMI server module et cliquez sur le bouton Create.

Champs spécifiques à WMI:

- Namespace: Espace de noms WMI ; dans certaines requêtes, ce champ est différent de la chaîne vide (par défaut), en fonction du fournisseur d'informations sur l'application surveillée.
- Key string: Facultatif, champ à comparer avec la chaîne renvoyée par la requête, et si disponible, le module renvoie 1 ou 0, au lieu de la chaîne elle-même.
- Field number: Le numéro du champ renvoyé à partir de 0 (les requêtes WMI peuvent renvoyer plus d'un champ). Dans la plupart des cas, il s'agit de 0 ou 1.
- WMI Query: Requête WMI, similaire à une instruction SQL.

Wizard WMI

Utilisé pour parcourir et créer des modules avec des requêtes WMI vers un agent spécifique. Dans l'assistant de l'agent (onglet de la vue de gestion d'un agent), cliquez sur l'icône:

Vous devez spécifier le nom d'utilisateur et le mot de passe qui ont les permissions de faire des

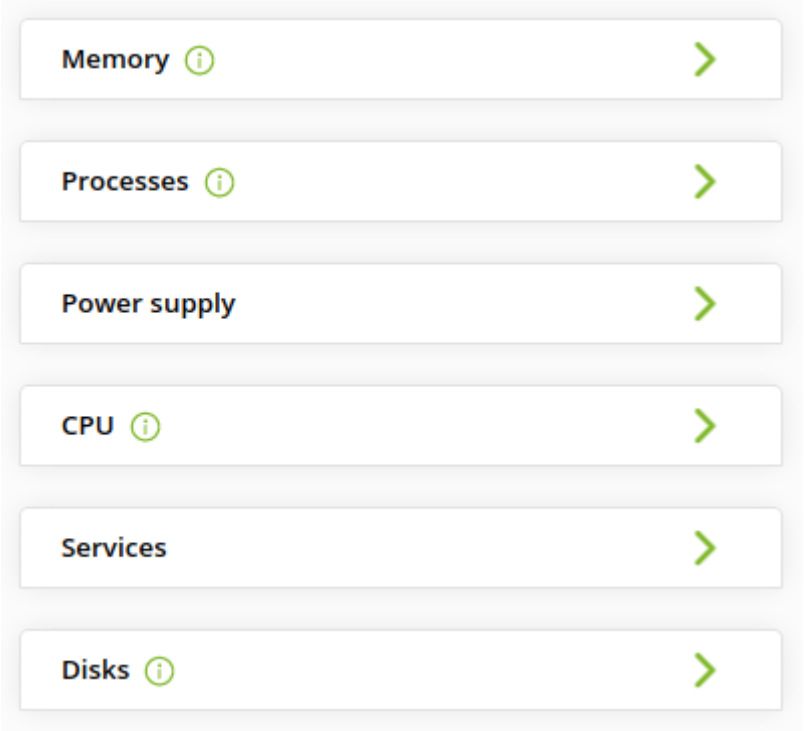
requêtes WMI (ou à défaut l'Administrateur) sur le serveur cible pour faire les premières requêtes WMI. Ces informations seront utilisées pour la création des modules.

L'assistant WMI permet de créer des modules de différents types d'informations WMI:

- Services: Les moniteurs booléens sont créés dans un état normal si le service est en cours d'exécution et dans un état critique lorsque le service est arrêté.
- Processus: Les moniteurs de processus ne reçoivent des informations que lorsque le processus est actif. Dans le cas contraire, ils tomberont dans un état inconnu.
- Espace disque libre.
- Composants WMI: dans ce cas, vous pouvez choisir parmi les composants WMI enregistrés dans le système.

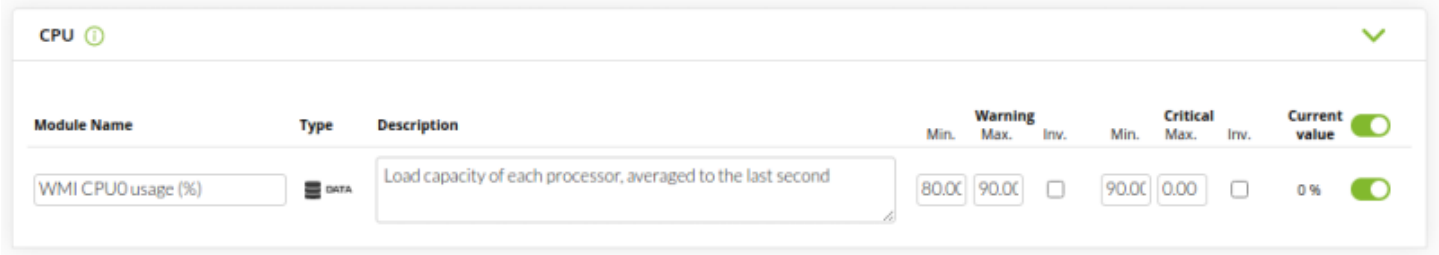
Les composants de l'assistant WMI doivent être enregistrés et activés dans Pandora: de cette manière, tous les modules à partir desquels vous avez pu obtenir des données seront affichés afin d'avoir la possibilité de les créer ou non.

Ces modules sont affichés sous forme de blocs en fonction du groupe auquel appartient le composant de l'assistant qui les a générés.



Tous les blocs sont d'abord affichés sous forme comprimée pour faciliter la visualisation et peuvent être développés pour modifier les blocs sélectionnés ou les données. En outre, dans chaque bloc où des modules ont été marqués pour la création, une icône d'information sera affichée pour indiquer.

Si nous déployons un bloc, il sera possible de choisir les modules qui seront ajoutés et ceux qui ne le seront pas, ainsi que de modifier le nom, la description ou les seuils de chaque module individuellement.



Après avoir appuyé sur le bouton *Créer des modules*, une liste s'affiche avec un résumé des modules choisis et de leur configuration. Dans cette liste, vous verrez les modules qui ne peuvent pas être créés, soit parce qu'ils existent déjà dans l'agent, soit parce que deux ou plusieurs modules portant le même nom ont été configurés dans le même *wizard*.

Malgré toutes les modifications effectuées, il y aura une dernière possibilité de confirmer la création de ces modules ou de l'annuler et de continuer à modifier le résultat du *wizard*.

Une fois la création des modules confirmée, ceux-ci seront réévalués un par un pour déterminer s'ils peuvent être créés ou non, afin d'éviter les modules en double au cas où les mêmes modules auraient été créés par d'autres moyens pendant la période de confirmation.

L'assistant indiquera si le processus s'est achevé avec succès ou si certains modules n'ont pas pu être créés.

Supervision avec plugins de serveur à distance

Un *plugin à distance* est un *script* ou exécutable qui admet des paramètres et renvoie une seule valeur. Le résultat pourrait être un numéro, une valeur booléenne (0 = error, OK <> 0) ou une chaîne de texte. Un plugin distant permet d'habitude des paramètres d'entrée. Par défaut quelques plugins de serveur sont installées et prêts à l'usage et l'utilisateur peut ajouter ceux dont il a besoin.

Il y a deux genres de plugin distant: standard et Nagios. La différence est que les plugins Nagios répondent avec un niveau d'erreurs (*error level*) et aussi facultativement, avec une chaîne descriptive.

Gestion des plugins distants

Accessible via Management → Servers → Plugins, une nouvelle fenêtre s'ouvrira avec une liste des plugins enregistrés. Chaque élément a ses boutons d'édition et de suppression correspondants,

sauf si vous avez des modules en cours d'utilisation qui peuvent être listés à l'aide du bouton Lock.

Lors de l'édition d'un plugin:

- Plug-in type: Il permet d'établir si c'est standard ou Nagios.
- Max. timeout: Pour fixer le temps d'attente pour son exécution, *vous devez faire attention à cette valeur puisqu'elle doit durer le temps suffisant pour son exécution autrement vous n'obtiendrez aucune donnée*.

- Lors de l'exécution d'un *plugin*, il existe trois timeouts: celui du serveur, celui du *plugin*, et celui du module. Tenez compte que celui du serveur prévaut sur les autres, puis en deuxième place, celui du *plugin*. C'est-à-dire que si vous avez un serveur avec un timeout de 10 secondes et un *plugin* avec un timeout de 20 et un module qui utilise ce *plugin* avec un timeout de 30, le temps maximum pour l'exécution de ce module sera de 10 secondes.
- Lorsque vous modifiez un *plugin* et qu'il est utilisé par au moins un agent, vous ne pourrez pas *ajouter ou supprimer* de macros.

Macros internes

De même que les alertes, vous pouvez utiliser aussi des macros internes pour la configuration des plugins. Les macros supportées sont les suivantes:

- `_agent_` ou `_agentalias_`: Alias de l'agent auquel le module appartient.
- `_agentname_`: Nom de l'agent auquel le module appartient.
- `_agentdescription_`: Description de l'agent auquel le module appartient.
- `_agentstatus_`: État actuel de l'agent.
- `_address_`: Adresse de l'agent auquel le module appartient.
- `_module_`: Nom du module.
- `_modulegroup_`: Nom du groupe du module.
- `_moduledescription_`: Description du module.
- `_modulestatus_`: État du module.
- `_moduletags_`: Etiquettes (*tags*) associées au module.
- `_id_agent_`: ID de de l'agent, utile pour construire directement l'URL ou rediriger à la Console de Pandora FMS.
- `_id_module_`: ID du module.
- `_policy_`: Nom de la politique auquelle le module appartienne s'il y a quelque-une établi.
- `_interval_`: Intervalle d'exécution du module.
- `_target_ip_>` Adresse IP du destin du module.
- `_target_port_`: Port de destin du module.
- `_plugin_parameters_`: Paramètres de *plugin* du module.
- `_email_tag_`: Courriers électroniques associés aux *tags* de modules.

Macros des champs personnalisés pour la supervision à distance

Lorsque des modules à distants sont configurés, devoir mettre des informations relatives à un même agent plusieurs fois peut rapidement s'avérer monotone (par exemple, une chaîne de communauté SNMP). Les macros de champs personnalisés permettent d'utiliser les champs personnalisés des agents comme macros pour certaines options de configuration des modules.

Les macros de champs personnalisés fonctionnent avec des modules de type SNMP, WMI, plugin et inventaire. Ils peuvent être utilisés dans des modules indépendants, des composants réseau et des modules de politique.

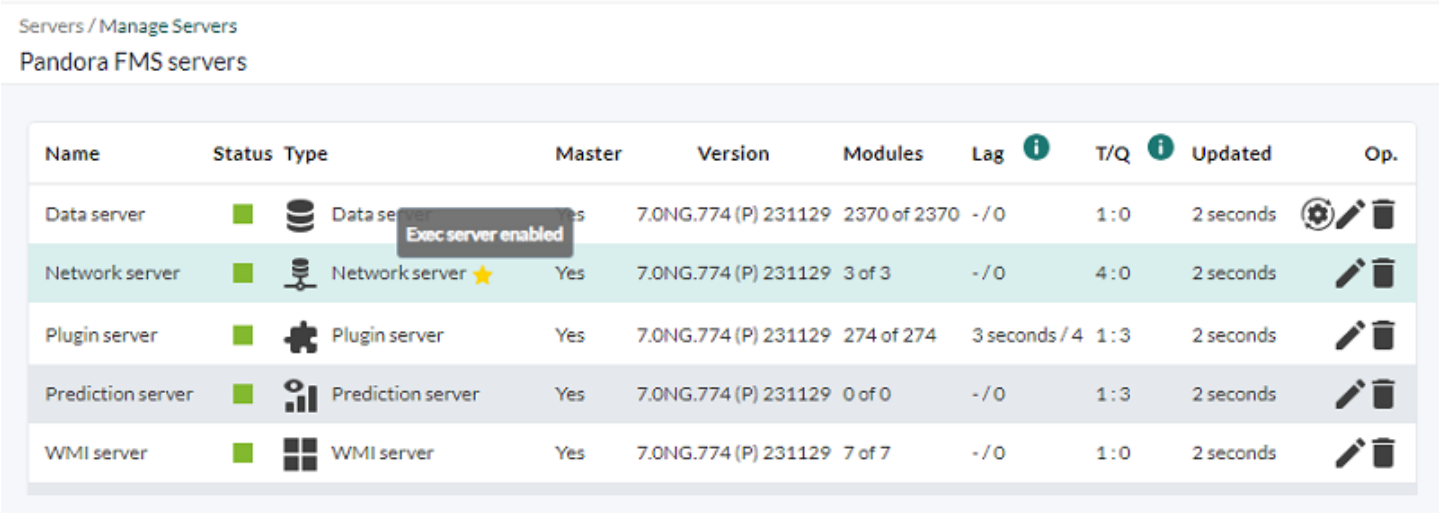
On y accède via Management → Resources → Custom fields → Create field dans ce nouveau champ personnalisé, la chaîne de communauté SNMP sera stockée. Notez son ID, car il fera plus tard partie de la macro, et remplissez la chaîne de communauté avec la valeur appropriée dans vos agents SNMP.

Ensuite, un composant réseau SNMP doit être créé et `_agentcustomfield_<n>_` *doit être saisi comme chaîne dans la* SNMP community, *où n est l'ID du champ personnalisé créé*.

Exécution à distance de wizards et tests réseau (Exec Server)

Seulement pour des serveurs Pandora FMS installés chez GNU/Linux.

Cette fonctionnalité permet, à partir de la console Pandora FMS, d'exécuter certaines actions sur des serveurs Pandora FMS distants.



Lorsqu'un serveur Exec est configuré, vous pouvez choisir l'une des options suivantes :

- Le navigateur SNMP dans la section SNMP.
- Les réponses aux événements dans la section des événements.
- Les assistants SNMP de l'agent.

- Les assistants WMI de l'agent.
- Les assistants de l'interface SNMP de l'agent (sauf pour les serveurs satellites).

En fonction du serveur sélectionné lors du lancement de chaque *wizard*, les modules adaptés au serveur ou au serveur satellite seront créés. Dans ce dernier cas, les modules seront écrits dans le fichier de configuration à distance afin qu'ils puissent être exécutés par le serveur.

Les serveurs Exec fonctionnent en interne par l'exécution de commandes SSH à distance depuis la console de Pandora FMS vers les serveurs activés, appelés Exec server. Ces commandes peuvent être Network servers ou Satellite servers de Pandora FMS.

Le processus de configuration nécessitera l'assistance de la personne chargée de l'administration du réseau pour configurer à la fois les serveurs PFMS et les ordinateurs cibles, la connexion et le trafic de données, ainsi que d'autres aspects tels que les pare-feu et les réseaux locaux virtuels (VLAN) pour une sécurité accrue.

- Un agent logique doit être configuré avec la configuration à distance activée.

Si la configuration à distance n'est pas activée vous n'aurez pas la possibilité de créer des modules Satellite à partir des assistants (*wizards*).

- Vous devez avoir créé des clés numériques (clé publique et clé privée) pour la connexion SSH.
- La clé publique doit être copiée sur les serveurs cibles et doit être configurée pour se connecter uniquement de cette manière, par clé numérique.
- Sur le serveur qui exécute la console Web de PFMS, vous devez disposer d'un utilisateur créé au niveau du système d'exploitation, disposant d'un accès approprié à son propre répertoire et permettant d'exécuter un *shell* valide pour les tâches à confier.
- Dans la console Web de PFMS, vous devez vous connecter en tant qu'utilisateur *superadmin* ou *Pandora Administrator*.

Voir l'annexe technique pour plus d'informations.

Supervision des chemins

Pandora FMS permet par défaut, de surveiller les chemins d’accès entre deux points du réseaux, en indiquant le chemin à suivre à tout moment pour communiquer entre ces deux points. L'analyseur d'itinéraire Pandora FMS utilise un plugin d'agent pour cartographier l'itinéraire.

Pour utiliser ce systèmes, il faut:

- Un agent software dans le point d’origine du chemin à analyser.
- Pouvoir analyser via ICMP le point de destination à partir du point d’origine.

En option, si vous souhaitez effectuer des analyses d'itinéraires via Internet, il est recommandé de

déployer l'application MTR sur l'ordinateur source de l'itinéraire.

Accédez à l'onglet de configuration des plugins dans l'agent et ajoutez la ligne suivante:

```
route_parser -t <target_address>
```

Enfin, activez l'exécution du plugin.

Retour à l'index de documentation du Pandora FMS