Supervision avec déroutements SNMP

Supervision avec déroutements SNMP

Opération avec des traps SNMP

Introduction

Les périphériques réseau qui prennent en charge le protocole SNMP, tels que les commutateurs, les routeurs, les serveurs, les imprimantes ou les points d'accès, peuvent envoyer des alarmes (ou des traps SNMP) lorsque certains événements se produisent, tels qu'un crash d'interface, un CPU ou une charge réseau trop élevée, un changement d'état de l'UPS ou une partition disque devenue pleine. Chaque appareil possède sa propre “collection” d'événements possibles, qui se reflète dans une collection, appelée MIB, dans ce cas, différente de la MIB utilisée pour interroger l'appareil.

Les traps ne sont envoyés que lorsque quelque chose se produit, de manière asynchrone (et non répétitive dans le temps) par l'appareil à un récepteur SNMP traps. Pandora FMS dispose d'une console de réception des traps qui permet de visualiser les traps envoyés par les objets surveillés et d'ajouter des alertes à ces traps. Les traps SNMP sont reçus par le démon du système d'exploitation que le serveur SNMP Pandora FMS démarre lorsque le serveur Pandora FMS démarre. Ce démon stocke les traps dans un journal situé par défaut dans:

```
/var/log/pandora/pandora_snmptrap.log
```

Les traps sont généralement reçus en format “brut”, c'est-à-dire avec des OID numériques, sauf si un MIB installé dans le système d'exploitation est capable de les résoudre. La console SNMP de Pandora FMS *Enterprise* permet de créer des règles pour renommer les OID numériques en OID alphanumériques ou en simples chaînes de caractères descriptif (ex. : L'interface a planté) afin de rendre plus intuitive l'utilisation de TRAPS. Pandora FMS permet également de charger les MIB Traps de n'importe quel fabricant pour définir automatiquement ces règles.

Afin de travailler avec des traps SNMP, modifiez tout d’abord le paramètre suivant dans `/etc/pandora/pandora_server.conf` pour activer la Console SNMP:

```
snmpconsole 1
```

Si vous voulez que les traps soient traduits (soit les liens variables, soit la chaîne Enterprise), vous devez activer les paramètres suivants (uniquement dans la version Enterprise) :

```
translate_variable_bindings 1
translate_enterprise_strings 1
```

Il faut aussi configurer l’archive `/etc/snmp/snmptrapd.conf` avec les paramètres nécessaires.

Par exemple :

```
authCommunity log public
disableAuthorization yes
```

Avec cette configuration, les traps seront créés pour la communauté public et ne nécessiteront pas d'autorisation.

SNMPv3

Les traps SNMPv3 sont rejetés à moins que l'utilisateur qui les envoie ne soit ajouté à `/etc/snmp/snmptrapd.conf` en utilisant la directive createUser. Par exemple :

```
disableAuthorization yes
createUser -e 0x0102030405 SNMPv3user SHA mypassword AES
```

Il faut préciser l'engineID avec l'option `-e`. Sinon, seuls
INFORMs SNMPv3 seront reçus.

Accès á la console de reception des traps

Operation → Monitoring → SNMP → SNMP Console. L'icône de la loupe peut être utilisée pour afficher toutes les informations du trap, de la même façon que pour les événements. Ici nous pouvons voir les informations détaillées d'un déroutement SNMP.

Pour chaque trap, les colonnes suivantes apparaissent :

- Status : Carré vert si le trap est validé, rouge dans le cas contraire.
- SNMP Agent : Agent qui a envoyé le trap.
- OID : OID du trap envoyé. Un trap ne peut envoyer qu'une seule donnée dans ce champs.
- Value : Champ de valeur du trap envoyé. Un trap ne peut envoyer qu'une seule donnée dans ce champ.

Couleur

- Bleu : Les traps de type entretien.
- Violet : Les traps de type information.
- Vert : Les traps de type `normal`.
- Jaune : Les traps de type `warning`.
- Rouge : Les traps de type `critical`.

L'option Toggle Filter apparaît en haut de la console de trap. Si vous cliquez sur cette option, les champs pour filtrer les déroutements apparaissent ou disparaissent.

Valider les traps

Afin de gérer efficacement les trappes, il est possible de valider les déroutements afin que l'administrateur puisse distinguer les déroutements qui ont été consultés de ceux qui ne le sont pas encore. Pour valider une trappe, cliquez sur le cercle à gauche ou en le marquant et en cliquant sur le bouton Validate.

Effacer des déroutements

Il est possible d'effacer les déroutements une fois traités, soit individuellement, soit par sélection multiple en cliquant sur Delete.

Pour éviter que les déroutements ne s'accumulent, il existe une option de configuration qui supprime automatiquement les déroutements de plus de 10 jours par défaut.

Alertes des déroutements SNMP

Introduction

Pandora FMS dispose également d'un système d'alerte pour les déroutements SNMP qu'il reçoit. Ils sont principalement basées sur des règles de filtrage, recherchant les coïncidences dans tous les champs possibles selon les règles que vous configurez pour déclencher l'alerte.

Ajouter une alerte

Les alertes de déroutement SNMP ont plusieurs champs qui seront utilisés pour rechercher des correspondances dans le déroutement SNMP reçu dans la console. Vous pouvez éventuellement utiliser les champs que vous souhaitez pour créer des règles plus générales ou plus spécifiques en fonction des besoins. Accès par le menu Management → Alerts → SNMP alerts → Create.
Paramètres importants:

- Enterprise String : OID principal du déroutement. La présence de la chaîne sera recherchée, pouvant être un morceau de l'OID, de sorte que si vous voulez rechercher, par exemple : `1.21.34.2.3` dans un OID plus long, vous pouvez l'utiliser de la même manière dans le champ, et effectuer la recherche comme si elle était : `*1.21.34.2.3*` Donc vous ne devez PAS utiliser d'astérisque. Pour les coïncidences exactes, finissez la chaîne avec le craactère `$` .
- Custom Value/OID : Il recherche dans les champs Value du trap, ainsi que dans les champs Custom OID et Custom Value, c'est-à-dire dans le reste des champs TRAP. C'est là que la recherche d'expressions régulières fonctionne. Par exemple, si vous avez un trap qui envoie la chaîne `Testing`

TRAP 225, je peux rechercher n'importe quel trap avec la sous-chaîne `Testing TRAP` avec l'expression régulière `Testing.*TRAP.*`.
- SNMP Agent : IP de l'agent qui envoie le déroutement. De la même manière, vous pouvez utiliser une expression régulière ou une chaîne de caractères.
- Trap type : Filtre selon le type de trap, pouvant être : Cold start, Warm start, Link down, Link up, Authentication failure ou Other. La plupart des traps générés sont généralement du type Other ; si vous ne spécifiez rien, il recherchera n'importe quel type de déroutement.
- Single value : Filtre par la valeur du trap. Dans l'exemple égal à .666, il s'agit uniquement de la valeur simple de l'OID primaire et non d'un OID secondaire.
- Variable bindings/Data #1-20 : Ce sont des expressions régulières qui tentent de faire correspondre les variables 1 à 20, si un résultat est trouvé, l'alerte se déclenche. La valeur de la variable est stockée dans la macro `_snmp_fx_` correspondante (`_snmp_f1_`, `_snmp_f2_`, ...). Bien qu'une seule expression régulière puisse être spécifiée pour vingt variables, les macros `_snmp_fx_` sont disponibles pour toutes (`_snmp_f11_`, `_snmp_f12_`,...).
- Alert Action : Combo où l'action qui exécutera l'alerte est déterminée. Si un événement est choisi, l'événement normal de génération d'alerte ne sera pas généré.
- Priority : Liste dans laquelle la priorité de l'alarme est définie.

Les priorités des alertes sont différentes et n'ont rien à voir avec la priorité des déroutements SNMP, ni avec la priorité des événements de Pandora FMS.

Macros de fields sur les alertes

Les macros suivantes peuvent être utilisées dans n'importe quel champ « field » des alertes :

- `_data_` : Trap entier.
- `_agent_` : Nom de l'agent.
- `_address_` : Adresse IP.
- `_timestamp_` : Date trap.
- `_snmp_oid_` : OID du trap.
- `_snmp_value_` : Valeur de l'OID du trap.

Travailler dans des environnements avec beaucoup de traps

Protection face à une avalanche de traps

Il y a quelques paramètres sur le serveur qui sont utilisés pour protéger le système contre l'arrivée d'une avalanche de traps provenant de la même source. Pour ce faire, les paramètres de configuration suivants sont utilisés dans le fichier `pandora_server.conf` :

- `snmp_storm_protection` : Nombre maximal de traps traités dans l'intervalle de protection.
- `snmp_storm_timeout` : Intervalle en secondes de la protection contre les orages des traps. Pendant cet intervalle, seuls X traps provenant de la même source (même IP) peuvent être traités.
- `snmp_storm_silence_period` : S'il est supérieur à 0 chaque fois que la *storm protection* est déclenchée pour une source particulière, l'heure actuelle plus le temps de coupure sont ajoutés. Tant

que ce délai n'est pas écoulé, aucun nouveau piège ne sera enregistré pour la source en question.

La protection contre les tempêtes de traps, combinée au filtrage des traps (voir ci-dessous), permet si vous recevez des centaines de milliers de traps par jour, de travailler avec seulement quelques milliers, afin d'éliminer ceux qui sont redondants ou ceux qui ne sont pas utiles.

Filtrage de traps dans le serveur

Certains systèmes reçoivent un nombre élevé de traps, dont un faible pourcentage est utile pour la supervision. Depuis Monitoring → SNMP → SNMP Filters vous pouvez définir plusieurs filtres. Cliquez sur le bouton Create, ajoutez une description et autant de filtres que nécessaire à l'aide du bouton +.

Personnaliser Traps SNMP

E Les caractéristiques suivantes ne sont que pour la version Enterprise.

Renommage et personnalisation des traps

Veuillez noter que tous les pièges précédents ne changeront pas d'apparence, mais que cette modification s'appliquera aux nouveaux pièges entrant dans le système à partir de ce moment.

Nous appelons « éditer un trap » le processus où il est possible de « personnaliser » l'apparence d'un trap dans la console. Pour éditer un trap, allez dans Operation → Monitoring → SNMP → SNMP trap editor.

Custom OID est une expression régulière compatible avec Perl qui sera comparée avec la partie de la chaîne de trappes qui contient les variables de liaison. Il n'est généralement pas nécessaire de traduire un piège.

« Custom OID » n'est pas destiné à contenir toute la chaîne de variables bindings, qui peut être plus longue que la longueur maximale qu'elle supporte, mais une expression régulière qui correspond à une ou plusieurs variables.

Télécharger les MIB du fabricant

Cette option est utilisée pour télécharger des MIB et étendre la base de données de traduction interne de Pandora FMS, de sorte que lorsqu'un piège SNMP arrive, il est automatiquement traduit par sa description. Allez vers Operation → Monitoring → SNMP → MIB uploader.

Associer un trap au reste des alertes Pandora FMS

Il s'agit d'une fonction Enterprise qui est configurée dans Management → Setup → Setup → Enterprise → Forward SNMP traps to an agent (if it exists).

Si vous modifiez cette option, redémarrez le serveur
Pandora FMS pour commencer à fonctionner.

Cette option (générale pour le serveur) transmet le déroutement SNMP à un module d'agent spécial appelé SNMPTrap sous la forme d'une chaîne de texte, si et seulement si l'adresse IP source du piège SNMP est définie comme une adresse IP d'agent. Dans ce cas, le déroutement SNMP arrive sous la forme d'une chaîne de texte à l'agent de ce module, qui est un module défini uniquement lorsque le premier déroutement SNMP arrive.

Des alertes textuelles peuvent être spécifiées sur ce module, et ces alertes sont tout à fait standard, comme celles de n'importe quel autre module. Cela vous permet de personnaliser la supervision SNMP de sorte que certaines traps, provenant de certaines sources, puissent être traités comme un autre module, et donc intégrés dans le reste de la supervision, y compris la corrélation des alertes.

Une autre solution consiste à monter une alerte sur le trap qui active un module d'agent. Par exemple, le trap c'est d'écrire dans un fichier de logs, et vous avez un agent qui lit ce fichier et saute quand il y a un 1 d'écrit. De cette façon, le module sautera lorsque le trap désiré sera reçu et la corrélation pourra être établie en fonction du trap reçu.

Gestionnaire TRAPS externe

La console SNMP est limitée à la réception de traps, car elle ne traite TRAP que comme une entité individuelle, mais un trap peut contenir beaucoup d'informations.

Parfois, il arrive que la seule supervision que vous puissiez faire soit basée sur des traps SNMP.

Pour ce faire, vous pouvez choisir de « post-traiter » les informations collectées dans un trap par un script externe, qui agit comme un plugin.

Pour ce faire, une commande d'alerte doit être créée pour exécuter ce script afin de post-traiter le piège SNMP reçu.

L'application de cette technologie est infinie, mais que si chaque script est particularisé puisqu'il peut avoir une structure très dynamique. Dans de nombreux systèmes, l'information qui est reçue n'est pas seulement du texte, mais aussi numérique, avec laquelle il peut alimenter des modules d'information numérique et donc représenter des graphiques etc. Cependant, nous devons tenir compte du fait que les données générées en XML doivent toujours être asynchrones.

SNMP trap forwarding

Avec Pandora FMS, il est possible d'activer le transfert des traps SNMP vers un hôte externe en activant le jeton snmp_forward_trap dans le fichier de configuration Pandora.

Gestion indépendante du démon snmptrapd

Il est possible que pour une raison quelconque vous préfériez gérer le démon snmptrapd indépendamment de Pandora FMS (pour l'arrêter ou l'élever indépendamment du Démon principal de Pandora FMS). Pour ce faire, vous devez tenir compte de plusieurs facteurs :

1.Vous devez également activer le paramètre `snmpconsole` dans le serveur Pandora FMS.

2. Les logs configurés dans le serveur Pandora FMS doivent être les mêmes que ceux générés dans l'appel indépendant à snmptrapd.

3. L'appel à snmptrapd doit avoir un format spécifique l'appel au démon système standard n'est pas valide. L'appel doit être ainsi (le paramètre `-A` est particulièrement important !) :

```
/usr/sbin/snmptrapd -A -t -On -n -a -Lf /var/log/pandora/pandora_snmptrap.log -p
/var/run/pandora_snmptrapd.pid --format1=SNMPv1[**]%4y-%02.2m-
%l[**]%02.2h:%02.2j:%02.2k[**]%a[**]%N[**]%w[**]%W[**]%q[**]%v\n --
format2=SNMPv2[**]%4y-%02.2m-%l[**]%02.2h:%02.2j:%02.2k[**]%b[**]%v\n
```

4. Vous devez configurer le jeton dans le fichier de configuration du serveur :

```
snmp_trapd manual
```

5. Lorsque vous définissez cette fonction. Vous devez effectuer l'opération suivante :

- Changez la configuration dans `/etc/pandora/pandora_server.conf`
- Arrêter le serveur Pandora FMS.
- Vérifiez que le processus snmptrapd n'est plus exécuté (et si c'est le cas, attendez qu'il meure ou le tue).
- Lancez snmptrapd manuellement (dans le format indiqué ci-dessus).
- Démarrez le serveur Pandora FMS.

Gestion du fichier journal des traps

Le processus *snmptrapd* peut être arrêté et démarré sans arrêter et démarrer le processus du serveur Pandora FMS, tant que les fichiers `pandora_snmptrap.log.index` et `pandora_snmptrap.log` ne sont pas modifiés. Si ces fichiers sont modifiés, il est nécessaire de redémarrer le serveur Pandora FMS. Si vous devez effectuer une rotation externe des traps *log*, vous devez redémarrer le serveur Pandora FMS après avoir supprimé les fichiers mentionnés précédemment.

Buffering des traps SNMP

Il est plus efficace pour la console SNMP de traiter les traps directement à partir du fichier journal snmptrapd. Cette configuration n'est recommandée que si la fiabilité ou la connectivité directe est un problème.

Si les traps SNMP sont envoyés à un gestionnaire externe par le biais d'une connexion peu fiable, une partie des informations sera perdue. Pandora FMS vous permet, au contraire, de transmettre les traps d'un snmptrapd local à votre serveur Pandora FMS d'une manière fiable.

Pré requis :

- Un snmptrapd local qui a des traps.
- Un agent local de Pandora FMS.
- Une installation Pandora FMS.

snmp_extlog peut être n'importe quel fichier dans lequel le serveur Pandora FMS peut écrire, mais il doit être différent de snmp_logfile (également défini dans `/etc/pandora/pandora_agent.conf`).

Générateur de Traps

Avec cet outil, vous pouvez générer des traps personnalisés que vous pourrez voir plus tard dans

la console SNMP. Accèdez à travers le menyu Operation → SNMP → SNMP trap generator.

Choisissez un type SNMP parmi les options suivantes :

- Cold Start : Il indique que l'agent a été lancé ou redémarré.
- Warm Start : Il indique que la configuration de l’agent a été modifiée.
- Link down : Il indique que l'interface de communication est hors service (inactive).
- Link up: Il indique qu’une interface de communication a été activée.
- Authentication failure : Il indique que l'agent a reçu une demande d'un SGEN non autorisé (contrôlé par la collectivité).
- EGP neighbor loss : Il indique que sur les systèmes où les routeurs qui utilisent le protocole EGP, un hôte proche est hors service.
- Enterprise : Dans cette catégorie vous trouverez tous les nouveaux traps. Y compris les traps des fournisseurs.

Retour à l'index de documentation du Pandora FMS