



Systeme d'alerte



m:
<https://pandorafms.com/manual!/current/>
Permanent link:
https://pandorafms.com/manual!/current/fr/documentation/pandorafms/management_and_operation/01_alerts
2024/03/18 21:07



Système d'alerte

Nous travaillons sur la traduction de la documentation du FMS Pandora. Nous sommes désolés pour tout désagrément.

Introduction

Une alerte est la réaction de Pandora FMS à une valeur incorrecte d'un **module**. Cette réaction est configurable et peut consister en tout ce qui peut être déclenché par un script configuré dans le Système d'Exploitation où tourne le serveur Pandora FMS qui traite le module.

Il existe plusieurs types d'alertes :

- Les alertes simples.
- Les alertes événements.
- Les alertes pièges SNMP.

Dans ce chapitre, nous allons traiter le système d'alerte dans son ensemble et parler en détail des premiers.

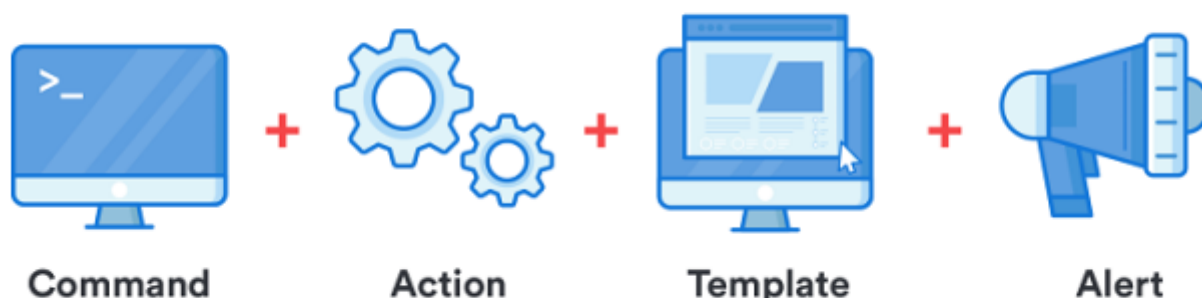
Introduction au système d'alerte

Dans Pandora FMS, les alertes fonctionnent par la définition de certaines conditions déclenchées, de certaines actions choisies pour cette alerte, et enfin l'exécution de certaines commandes dans le serveur Pandora FMS, qui seront chargées d'exécuter les actions configurées.

Le système d'alerte générale associe une seule alerte pour chaque module, cette alerte peut effectuer une ou plusieurs actions.

Structure d'une alerte

Alert Structure



Les alertes sont composées de :

- Commandes : Spécifiez *ce qui sera fait* ; ce sera l'exécution que le serveur Pandora FMS fera lors du déclenchement de l'alerte. Il peut s'agir d'écrire dans un log, d'envoyer un mail ou un SMS, d'exécuter un script, etc.
- Les actions : Spécifiez comment cela se fera, sont les personnalisations des arguments de la commande, permettent de personnaliser l'exécution en tant que telle, en passant à la commande des paramètres particuliers comme le nom du module, de l'agent, etc.
- Modèles : Spécifiez *quand*, définissez les conditions pour déclencher l'action ou les actions. Par exemple : lorsque le module passe à l'état critique.

Flux d'informations dans le système d'alerte

Lors de la configuration des modèles et des actions, les deux ont une série de champs génériques appelés Field1, Field2, Field3, ... Fieldn qui sont utilisés pour transférer les informations depuis le modèle à l'action et depuis l'action jusqu'à la commande pour finalement être utilisés comme des paramètres dans l'exécution de ladite commande.

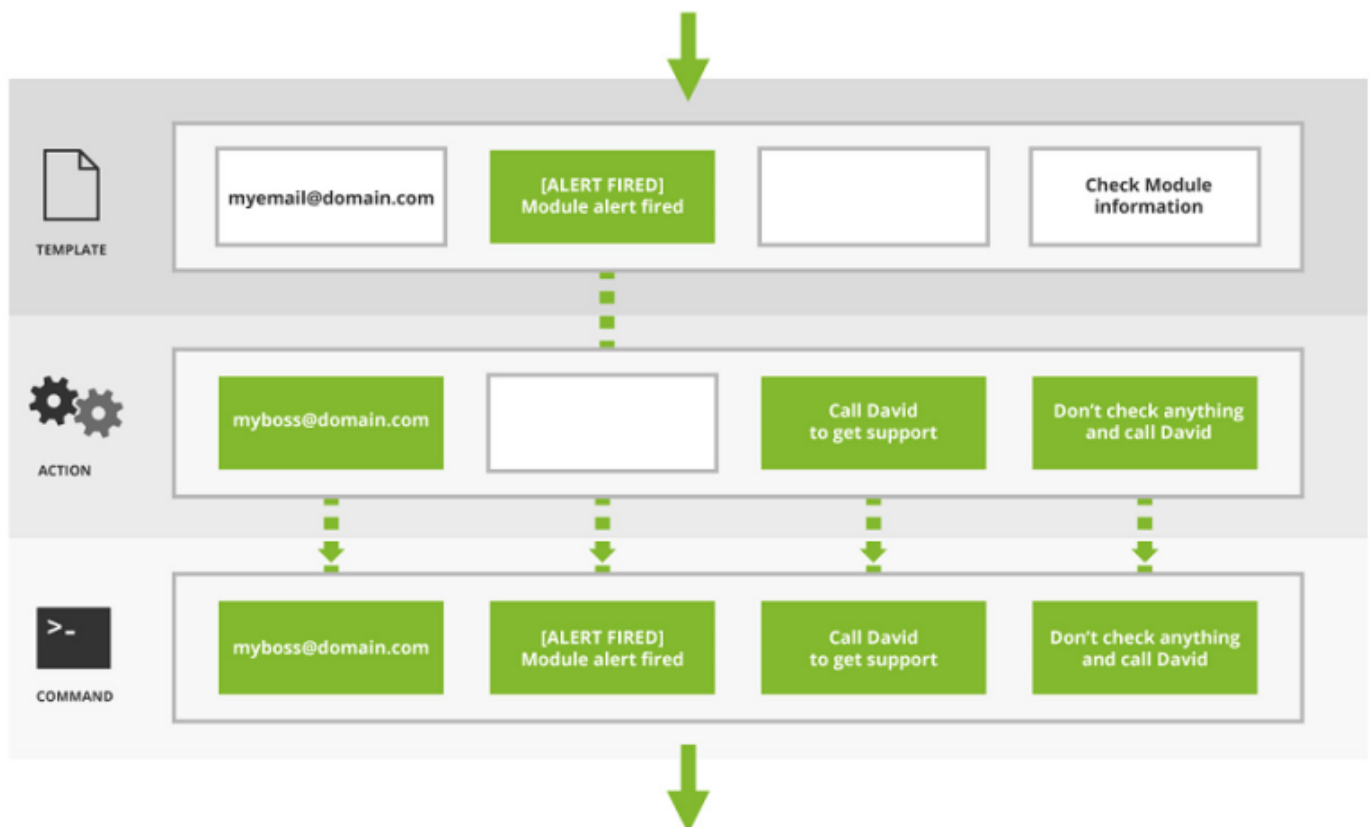
Ces informations sont transferts pendant que l'échelon suivante n'aie pas des informations définies dans ses champs Fieldn. C'est à dire, en cas de chevauchement de champs ou paramètres, il superpose l'action au modèle (par exemple, si le modèle a Field1 défini et l'action aussi, le Field1 de l'action prévaut).

Dans le schéma suivant vous pouvez voir ce transfert de paramètres depuis le modèle jusqu'à la commande :

PARAMETRES CARRYING



Exemple du chevauchement des valeurs du domèle en utilisant ceux de l'action :



Par exemple, un modèle qui déclenche l'alerte et envoie un e-mail avec les champs suivants :

- Modèle :
 - Field1: myemail@domain.com
 - Field2: [Alert] The alert was fired
 - Field3: The alert was fired!!! SOS!!!

- Action :
 - Field1: myboss @domain.com
 - Field2: <en blanc>
 - Field3: <en blanc>

Les valeurs qui atteindraient la commande seraient :

- Commande :
 - Field1: myboss@domain.com
 - Field2: [Alert] The alert was fired
 - Field3: The alert was fired!!! SOS!!!

Pour les champs Field2 et Field3, les valeurs définies dans le modèle sont conservées, mais pour le champ Field1, il utilise la valeur définie dans l'action.

Commande d'alerte

Introduction

Les actions que Pandora FMS effectuera en cas de situations d'alerte seront traduites à la fin en exécutions sur le serveur, sous la forme de commandes.

ALERTS » ALERT COMMANDS

Total items: 14

Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log /pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create >

Création d'une commande pour une alerte

Lorsque vous cliquez Create sur la section précédente :

Alerts » Configure alert command

Name	<input type="text"/>			
Command	<input type="text"/>			
Group	<div>All ▾</div>			
Description	<input type="text"/>			
1 field description	<input type="text"/>	1 field values	<input type="text"/>	Hide <input type="checkbox"/>
2 field description	<input type="text"/>	2 field values	<input type="text"/>	Hide <input type="checkbox"/>
3 field description	<input type="text"/>	3 field values	<input type="text"/>	Hide <input type="checkbox"/>
4 field description	<input type="text"/>	4 field values	<input type="text"/>	Hide <input type="checkbox"/>
5 field description	<input type="text"/>	5 field values	<input type="text"/>	Hide <input type="checkbox"/>
6 field description	<input type="text"/>	6 field values	<input type="text"/>	Hide <input type="checkbox"/>
7 field description	<input type="text"/>	7 field values	<input type="text"/>	Hide <input type="checkbox"/>
8 field description	<input type="text"/>	8 field values	<input type="text"/>	Hide <input type="checkbox"/>
9 field description	<input type="text"/>	9 field values	<input type="text"/>	Hide <input type="checkbox"/>
10 field description	<input type="text"/>	10 field values	<input type="text"/>	Hide <input type="checkbox"/>

Create

Name

Le nom du Commandement. Il doit être bref et descriptif.

Command

Commande qui sera exécutée lorsque l'alerte sera déclenchée. Il est possible d'utiliser des macros ([lire la section suivante](#)) pour remplacer les paramètres configurés dans la déclaration d'alerte.

Il est nécessaire de prendre en compte que ces commandes sont exécutées par le serveur Pandora FMS. Les alertes sont également exécutées avec les privilèges de l'utilisateur qui exécute le serveur Pandora FMS.

Il est recommandé de vérifier depuis la ligne de commande si l'exécution de la commande est réussie et qu'elle produit le résultat souhaité (envoyer un email, générer une entrée dans un fichier journal, etc.)

Group

Ceci déterminera à quel groupe d'alertes la commande peut être associée. Vous pouvez seulement attribuer un groupe auquel l'utilisateur qui crée la commande appartienne, à moins que ledit utilisateur appartienne particulièrement au groupe TOUS ([ALL](#)).

Description des champs et des valeurs possibles.

Pour chaque champ, il est possible de configurer :

- Description du champ : Ce sera l'étiquette à côté de la zone de texte dans le formulaire de configuration de l'action qui utilise cette commande.
- Valeurs du champ possibles : Un ensemble de valeurs possibles pour ce champ. Si ce champ est configuré (non vide), le champ sera une liste déroulante de sélection au lieu d'une zone de texte. Le combo a besoin pour chaque valeur possible d'une étiquette (l'option visible) et d'une valeur (l'option envoyée). La syntaxe est la suivante :

```
valeur1,étiquette1;valeur2,étiquette2;valeur3,étiquette3,étiquette3
```

- Hide : Cette case doit être cochée lorsque vous voulez masquer ou masquer la valeur du champ.

À partir de la version 6,0 il est possible de montrer un éditeur de code HTML dans un champ de commande pendant la création ou l'édition d'une action d'une alerte si ce champ de la commande a comme valeur le jeton spécial `_htm_editor_`

Une fois remplis correctement chaun des paramètres, cliquez Create pour sauvegarder.

Exemple

Un champ simple où il sera possible de choisir entre les quatre premiers numéros :

1, Numéro un;2, Numéro deux;3, Numéro trois;4, Numéro quatre

Le champ doit être configuré dans la commande:

Lorsque vous allez vers l'action vous le verrez de la manière suivante :

Macros de commandes

Les macros qui peuvent être utilisées dans la configuration d'une commande sont dans la liste des macros à la fina de ce chapitre.

Commandes prédéfinies

Il existe une série de commandes prédéfinies prêtes à être utilisées dans le système d'alerte Pandora FMS.

eMail

Envoyez un courriel à partir du [serveur Pandora FMS](#). Les emails sont envoyés au format HTML, ce qui vous permet de créer des modèles visuellement très attractifs. N'oubliez pas que le destinataire doit pouvoir accéder aux ressources utilisées dans le modèle, comme les images.

Lorsqu'une [URL publique](#) est définie pour une console Web, les courriels qui sont envoyés auront ce lien défini.

Internal audit

Génère une entrée dans le système d'audit interne de Pandora FMS. Ceci est stocké dans la base de données Pandora FMS et peut être consulté à l'aide du visualiseur d'événements de la console.

Monitoring Event

Créez un événement personnalisé dans la console d'événements Pandora FMS.

Pandora FMS Alertlog

C'est une alerte prédéfinie qui écrit les alertes en ASCII simple dans le fichier journal `/var/log/pandora/pandora_alert.log`.

SNMP Trap

Envoie un trap SNMP paramétré avec les arguments utilisés.

Syslog

Envoyez une alerte au journal système, utilisez la commande système `logger`.

Sound Alert

Il reproduit un bruit de la **console sonore d'événements** lorsqu'une alerte se produit.

Jabber Alert

Il envoie une alerte jabber à une salle de discussion sur un serveur prédéfini (configurez d'abord le fichier `sendxmpprc`). Dans le `field3` se trouve le message texte, dans le `field1` l'alias de l'utilisateur, et dans le `field2` le nom de la salle de chat.

SMS Text

Il envoie un SMS vers un certain téléphone mobile, bien sûr, vous devez définir une alerte avant de rendre cela possible et une passerelle pour envoyer des SMS configurée et accessible depuis le serveur Pandora FMS. Vous pouvez également en installer un en utilisant Gnokii pour envoyer des SMS, directement en utilisant un téléphone Nokia avec un câble USB. Le processus est décrit ci-dessous.

Validate Event

Il valide tous les événements liés à un module. Le nom de l'agent et le nom du module lui seront transmis.

Remote agent control

Il envoie des commandes aux agents avec le serveur UDP activé. Le serveur UDP est utilisé pour ordonner aux agents (Windows et Linux) de “rafraîchir” l'exécution de l'agent : c'est à dire, pour obliger à l'agent d'exécuter et d'envoyer des données.

Generate notification

Il permet d'envoyer une notification interne à n'importe quel utilisateur ou groupe.

Edition d'une commande pour une alerte

Allez vers Alerts > Command :

ALERTS » ALERT COMMANDS

Total items: 14

Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log /pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create >



Pour modifier la commande d'une alerte, il suffit de cliquer sur le nom de la commande.



ALERTS » CONFIGURE ALERT COMMAND

Name Jabber Alert

Command

echo_field3_| sendxmpp -r_field1_ --chatroom_field2_

Group

All

Description

Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file).
Uses field3 as text message, field1 as useralias
for source message, and field2 for chatroom name

1 field description

User alias

1 field
values

Hide

☐

2 field description

Chatroom name

2 field
values

Hide

☐

3 field description

Message

3 field
values

Hide

☐

4 field description

4 field
values

Hide

☐

5 field description

5 field
values

Hide

☐

6 field description

6 field
values

Hide

☐

7 field description

7 field
values

Hide

☐

8 field description

8 field
values

Hide

☐

9 field description

9 field
values

Hide

☐

10 field description

10 field
values

Hide

☐

Update

Une fois que l'alerte sélectionnée a été modifiée, cliquez sur le bouton Update.

Les commandes eMail, Internal Audit et Monitoring Event ne peuvent pas être modifiées ni supprimés.

Opération d'une commande d'alerte

ALERTS » ALERT COMMANDS

Total items: 14

Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log /pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create >

Supprimé : Pour supprimer une alerte, cliquez sur la corbeille grise à droite de l'alerte.

Copié : Les alertes peuvent être copiées. Il est particulièrement utile de générer des commandes similaires à d'autres commandes existantes en modifiant certains détails tels qu'un champ ou un groupe.

Exemples de commandes

Envoie d'alertes avec Jabber

Il est très utile de configurer Pandora FMS pour envoyer des alertes à un serveur Jabber qui peut être un système d'alerte en temps réel qui reste aussi historique et qui permet de les recevoir à un groupe de personnes simultanément.

Installation des services Jabber

Du côté du client :

1. Installez un client Jabber, par exemple *Gaim* (maintenant *Pidgin*).
2. Enregistrer un compte (en *Pidgin* : créez un compte en cliquant sur le bouton d'enregistrement du compte).
3. Connectez-vous avec le compte.

Dans la partie serveur de Pandora FMS :

1. Installer *sendxmpp*. Avec cet outil, vous pouvez envoyer des messages Jabber.
2. Créez un fichier dans le répertoire */home* avec le nom *.sendxmpprc* .
3. Modifiez le fichier et entrez ce qui suit :

```
useraccount@jabber.org password
```

1. Donnez les permissions au fichier :

```
chmod 0600 .sendxmpprc
```

Les messages privés peuvent maintenant être envoyés via la ligne de commande, par exemple :

```
$ echo "Hello" | sendxmpp -s pandora useraccount@jabber.org
```

Pour enregistrer l'alerte dans la console Pandora FMS, une nouvelle commande est ajoutée, et les variables de la commande sont configurées de la manière la plus pratique. C'est une bonne idée de procéder comme suit :

- **Field_1** : adresse jabber.
- **Field_2** : Envoyer du texte.

L'alerte serait donc définie comme suit :

```
echo _field2_ | sendxmpp -s pandora _field1__
```

D'autres exemples d'utilisation avec Jabber

Envoyer à un tchat :

```
$ echo "Dinner Time" | sendxmpp -r TheCook --chatroom  
test2@conference.jabber.org
```

Envoyez les lignes d'enregistrement telles qu'elles apparaissent à une destination Jabber :

```
$ tail -f /var/log/syslog | sendxmpp -i sysadmin@myjabberserver.com
```

REMARQUE : Veillez à ne pas surcharger les serveurs Jabber publics, sinon ils vous couperont l'accès.

Envoi d'email avec expect

Parfois, vous avez besoin d'utiliser un SMTP authentifié pour envoyer des e-mails. Pandora FMS a tout ce qui est nécessaire pour l'envoi normale des emails dans la [configuration générale de la Console](#) et là-bas vous pouvez même d'envoyer un email pour tester l'envoi. Mais afin d'utiliser un SMTP authentifié il se peut qu'il soit plus facile et polyvalent d'utiliser un script simple avec [Expect](#) au lieu de configurer sendmail.

Expect est un outil pour automatiser des applications interactives tels que telnet, ftp, passwd, fsck, rlogin, tip, etc. Expect fait ces tâches devenir triviales et il est aussi utile pour tester ceux applications. Expect peut faciliter n'importe quelle tâche qui est très difficile chez un autre outil. Expect est un outil inestimable, vous pourrez automatiser tout type des tâches et pourrez les automatiser rapide et facilement.

Cet exemple utilise Expect pour envoyer ser emails en utilisant un serveur MS Exchange®.

Un fichier appelé /etc/expect_snmp est créé avec le contenu suivant :

```
#!/usr/bin/expect -f  
set arg1 [lindex $argv 0]  
set arg2 [lindex $argv 1]  
set arg3 [lindex $argv 2]  
set timeout 1  
spawn telnet myserver.com 25  
expect "220"
```

```
send "ehlo mymachine.mydomain.com\r"
expect "250"
send "AUTH login\r"
expect "334"
send "2342348werhkwjersdf78sdf3w4rwe32wer=\r"
expect "334"
send "YRejewrhneruT==\r"
expect "235"
send "MAIL FROM: myuser@domain.com\r"
expect "Sender OK"
send "RCPT TO: $arg1\r"
expect "250"
send "data\r"
expect "354"
send "Subject: $arg2\r"
send "$arg3 \r\r"
send ".\r"
expect "delivery"
send "quit"
quit
```

Les permissions des fichiers sont modifiées pour permettre leur exécution :

```
chmod 700 /root/smtp
```

Avant d'essayer de l'utiliser, assurez-vous que `/usr/bin/expect` fonctionne correctement. Vous pouvez copier, sauvegarder, ou accorder le droit d'exécution au script suivant :

```
#!/usr/bin/expect -f

spawn date
sleep 20
expect
```

Pour l'utiliser avec Pandora FMS, vous devrez créer une nouvelle commande (ou modifier celle existante pour envoyer des alertes par e-mail) et spécifier les champs suivants dans la définition de la commande Alerte Pandora FMS. Dans le champ Command écrivez :

```
/etc/expect_smtp _field1_ _field2_ _field3_
```

Bien sûr, le script peut se trouver n'importe où dans le système. Il suffit de prendre en compte que le script d'alerte est lancé par le serveur qui traite les données : s'il s'agit d'une donnée réseau, ce sera le serveur réseau, s'il s'agit d'une donnée provenant d'un agent, via un fichier XML, alors ce sera le serveur de données qui le lance.

Si vous avez des serveurs physiques différents, vous devrez peut-être copier le même script au même endroit, avec les mêmes permissions et le même propriétaire d'utilisateur dans tous les systèmes où vous avez un serveur Pandora FMS qui veut exécuter cette alerte. Gardez également

à l'esprit que les serveurs réseau Pandora FMS doivent être exécutés en tant que root (pour pouvoir faire des tests de latence ICMP) et que les serveurs de données peuvent être exécutés avec un utilisateur sans privilèges.

L'alerte sera exécutée par l'utilisateur qui exécute le processus du serveur Pandora FMS.

Envoi de SMS avec Gnokii

Pour utiliser Gnokii, il est nécessaire d'utiliser un téléphone portable compatible Nokia ou Gnokii (vérifiez le matériel compatible sur la page du [projet Gnokii](#)). Vous aurez également besoin d'un câble de données USB auquel vous devrez connecter le téléphone portable et le serveur Pandora FMS sur lequel vous souhaitez envoyer des alertes SMS.

Gnokii supporte une grande variété de téléphones Nokia (et certains d'autres fabricants). Avec Gnokii, vous pouvez envoyer des SMS depuis la ligne de commande. De cette façon, il est très facile et rapide d'envoyer des SMS directement à partir d'un serveur Pandora FMS, évitant l'utilisation de passerelles pour envoyer des SMS sur Internet (peu utiles en cas de panne du réseau) ou de solutions matérielles GSM très coûteuses pour envoyer des messages.

Exemple d'envoi d'un SMS avec Gnokii depuis une ligne de commande :

```
echo "PANDORA: Server XXXX is down at XXXXX" | gnokii --sendsms 555123123
```

Gnokii ne peut pas envoyer de MMS avec des images jointes, mais il peut envoyer une URL HTTP/WAP à afficher lors de la réception d'un message, par exemple :

```
echo "Image capture sample" | gnokii --sendsms 555123123 -w  
http://artica.homelinux.com/capture.jpg
```

Vous pouvez envoyer une URL à partir d'une image, ou une URL qui mène à une version allégée de la console pour accéder à la console à partir de l'appareil mobile et analyser les données.

L'équipe de développement a testé l'envoi de SMS à partir d'un téléphone Nokia 6030, envoyant des alertes SMS lorsque la connexion Internet était inaccessible. Le Nokia 6030 utilise la définition du module 6510 dans le fichier gnokiirc, et prend environ quatre secondes pour envoyer un SMS.

Une autre alternative à l'utilisation de Gnokii est le projet Gammu. Une passerelle d'envoi plus puissante peut être implémentée en utilisant Gammu.

Exécution d'une commande distante dans un autre système (UNIX)

Parfois il est intéressant d'exécuter une commande dans un autre système, pour cela la

commande ssh est utilisée. Le système sur lequel la commande sera exécutée doit être UNIX et avoir le démon ssh installé, monté et accessible.

Afin d'éviter d'avoir le mot de passe d'accès à la machine qui a exécuté la commande dans Pandora Console, la première chose à faire est de copier la clé publique du serveur où vous voulez exécuter la commande à distance dans Pandora FMS serveur.

Une fois que cela a été fait, nous devons le définir comme une commande :

```
ssh user@hostname [_field1_]
```

En mettant `_field1_` comme variable, vous pouvez utiliser la commande que vous voulez.

Action

Introduction

Les actions sont les composants des alertes dans lesquelles une commande est liée aux variables génériques Field 1, Field2, ..., Field 10.

Les actions nous permettent de définir *comment* nous allons lancer la commande.

Création d'une action

Allez vers le menu Alerts > Alert actions > Create :

Alerts » Alert actions ?			
Name	Group	Copy	Delete
Mail to XXX			
Restart agent			
Pandora FMS Event			
Create a ticket in Integria IMS			

Create >

Le formulaire suivant apparaîtra :

Alerts » Configure alert action ?

Name

Group

All ▼

Command

None ▼

+ Create Command

Threshold

0

seconds ?

Firing

Recovery

Command preview

Create ✎

Name

Le nom de l'action.

Group

Le groupe de l'action. Vous pouvez seulement attribuer un groupe auquel l'utilisateur qui crée la commande d'alerte appartienne, à moins que cet utilisateur appartienne au groupe **ALL**. Si la commande associée a un groupe différent de All, seulement le groupe associé à la commande ou le groupe all peut être établi comme groupe de l'action. Si à cause de n'importe quelle raison ceux sont différents, vous verrez un message d'avertissement pour sa correction par un utilisateur avec les permissions nécessaires.



Command

Commande que sera utilisé si l'alerte est exécutée. Vous pouvez choisir entre les **différentes Commandes prédéfinis** sur Pandora FMS.

Threshold

Le seuil d'exécution de l'action.

Command Preview

Dans ce champ, pas editable, la commande qui va être exécutée dans le système sera montrée automatiquement.

Field 1 ~ Field 10

Ces champs définent la valeur des macros `_field1_` a `_field10_`, qui seront utilisées dans la commande si nécessaire. Ces champs peuvent être un champ de texte ou un combo de sélection si configuré.

Une fois les champs remplis correctement, sauvegardez avec le bouton Create.

Alerts » Configure alert action ?

Name

Problem in CPD

Group

All ▼

Command

SNMP Trap ▼ + Create Command

Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.

Threshold

0 seconds ?

Firing

Recovery

Command preview

/usr/bin/snmptrap -v 1 -c _field1_ _field2_ _field3_ _field4_

/usr/bin/snmptrap -v 1 -c _field1_ _field2_ _field3_ _field4_

Community

Field 1 ?

Destination address

Field 2

OID

Field 3

Source address

Field 4

Create

















Après, depuis le menu Actions > Alerts vous pouvez éditer les actions créés.

Lorsque vous attribuez une valeur aux champs (Field) dans la section de déclenchement (Firing), de manière prédéfinie ils seront les mêmes valeurs pour la récupération, à moins que vous attribuez une valeur différente.

Macros d'actions

Vous pouvez trouver les macros qui peuvent être utilisées dans la configuration d'une action à la fin du chapitre.

Modifier une action

ALERTS » ALERT ACTIONS 			
Name	Group	Copy	Delete
Mail to Admin			
Restart agent			
Pandora FMS Event			
Create a ticket in Integria IMS			
Acción Test			

Create >

Pour modifier l'action, cliquez simplement sur le nom de l'action.

ALERTS » CONFIGURE ALERT ACTION ?

Name	<input type="text" value="Acción Test"/>	
Group	<input type="text" value="All"/>	
Command	<input type="text" value="test"/>	+ Create Command
Threshold	<input type="text" value="0"/> seconds	?
	Firing	Recovery
Command preview	<pre>/path/a/script "_field1_" "definición en acción" "definición en acción" "definición en comando"</pre>	<pre>/path/a/script "_field1_" "_field2_" "_field3_" "definición en comando"</pre>
campo 1 Field 1 ?	<input type="text"/>	<input type="text"/>
campo 2 Field 2	<input type="text" value="definición en acción"/>	<input type="text"/>

Lorsque vous avez terminé, vous pouvez enregistrer vos modifications en cliquant sur le bouton "Mettre à jour".

Effacer une action

Vous pouvez supprimer une action en cliquant sur l'icône de la corbeille (colonne Delete).

Alerts » Alert actions ?

Name	Group	Copy	Delete
Mail to XXX			
Restart agent			
Pandora FMS Event			
Create a ticket in Integria IMS			
Problem in CPD			

Create >

Modèle d'alerte

Introduction

Les modèles définissent les conditions de déclenchement de l'alerte (*quand* pour exécuter l'action).

Les modèles d'alerte sont associés aux modules, de sorte que dès que les conditions du modèle sont remplies, la ou les actions associées sont exécutées.

Sa conception permet de générer un groupe réduit de modèles génériques qui sont utiles pour la plupart des cas possibles dans Pandora FMS.

Création d'un modèle

Accédez au menu Alerts → Templates et cliquez Create.

The screenshot shows the Pandora FMS web interface. On the left is a dark sidebar menu with the following items: Events, Workspace, Tools, Discovery, Resources, Profiles, Configuration, Alerts (highlighted with a green bar), Events, Servers, Setup, Admin tools, Links, Update manager, and Module library. A sub-menu is open for 'Alerts', listing: List of Alerts, Templates (highlighted with a white box), Actions, Commands, List of special days, Alert correlation, SNMP alerts, and Inventory alerts. The main content area displays a table of alert templates. At the top, it says 'Total items: 5'. The table has columns: Name, Group, Type, and Op. (with icons for copy and delete). The table contains five rows of templates. At the bottom right of the table is a 'Create >' button.

Name	Group	Type	Op.
Critical condition			
Critical status		Critical status	
Max and min		Max and min	
Warning status		Warning status	
Critical status		Critical status	
Regular expression		Regular expression	

Create >

Pandora FMS v7.0NG.758 - OUM 758 - MR.50
Page generated on 2021-11-10 15:53:12

Après suivez les trois étapes indiqués.

Étape 1 : Général

ALERTS » CONFIGURE ALERT TEMPLATE

Step 1 »

General

Step 2 »

Conditions

Step 3 »

Advanced fields

Name

Group

All



Description

Priority

Informative



Next



Pandora FMS v7.0NG.758 - OUM 758 - MR.50

Page generated on 2021-11-10 16:06:17

Dans cet assistant de modèle, vous pouvez spécifier :

Name

Le nom du modèle, obligatoire.

Groupe

Groupe auquel le modèle sera appliqué. Vous pouvez seulement attribuer un groupe auquel appartient l'utilisateur qui crée le modèle, à moins que cet utilisateur appartienne spécifiquement au groupe **ALL**.

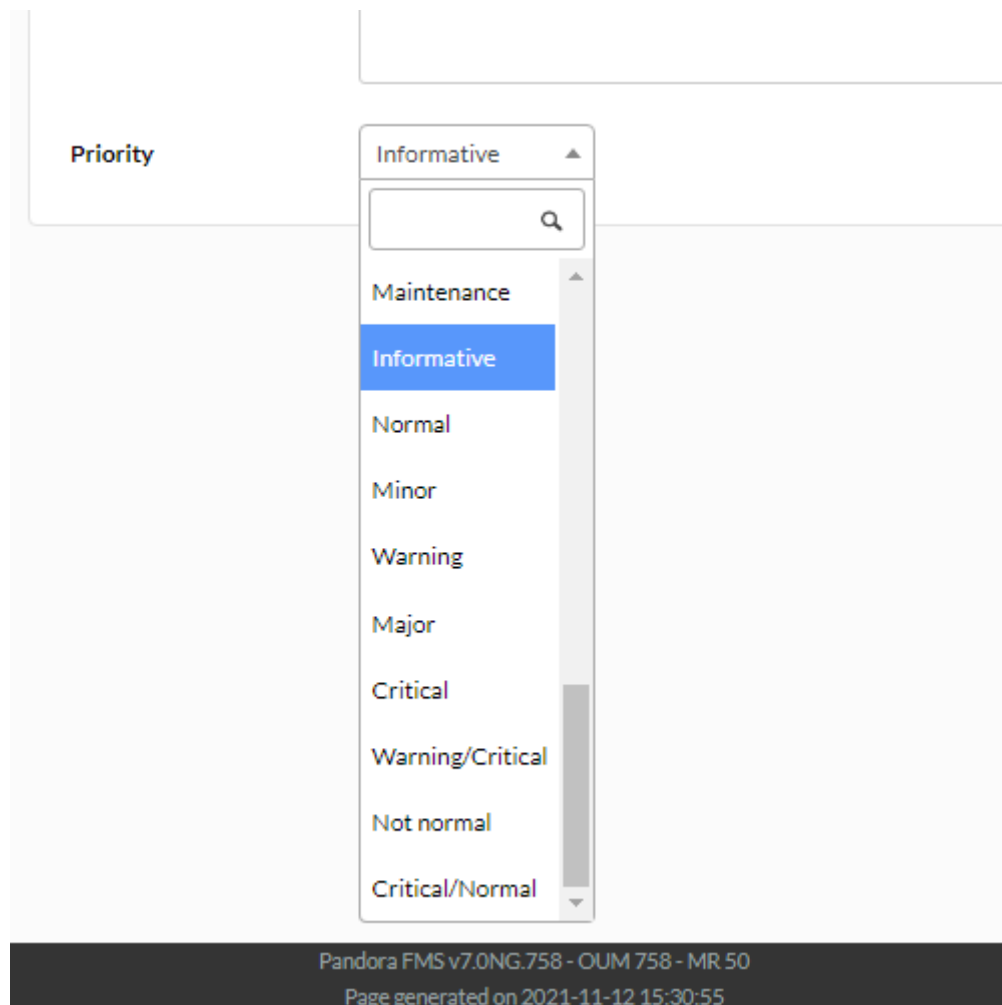
Description

il décrit la fonction du modèle, et est utile pour identifier le modèle parmi d'autres dans l'aperçu des alertes.

Priority

Champ d'information sur l'alerte. L'événement généré lors du déclenchement de l'alerte héritera de cette priorité. Il est également très utile pour filtrer lors de la recherche d'alertes. Vous pouvez choisir parmi les priorités suivantes :

- Maintenance
- Informational
- Normal
- Minor
- Warning
- Major
- Critical
- Warning/critical
- Not normal
- Critical/normal



Etape 2: Conditions

ALERTS » CONFIGURE ALERT TEMPLATE ?

Step 1 »
General

Step 2 »
Conditions

Step 3 »
Advanced fields

Use special days list

None

Detailed

Simple

Schedule

Mon	Tue	Wed	Thu	Fri	Sat	Sun
● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day

Time threshold

5 minutes

Min. number of alerts

0

Reset counter for non-sustained alerts i

☐

Max. number of alerts

1

Disable event

☐

Default action

None

i

Condition type

Critical status

i The alert is triggered when the module is in critical status.

Next >

Use special days list

Il établit le calendrier des jours spéciaux utilisé pour le modèle.

Schedule

Il définit les jours pendant lesquels l'alerte peut être déclenchée.

Versión NG 760 ou ultérieure.

Il est possible de visualiser et de configurer quand l'alerte sera active chaque jour de la semaine grâce à l'éditeur intégré qui s'affiche par défaut en mode simple.

Detailed

Simple

Schedule

Mon	Tue	Wed	Thu	Fri	Sat	Sun
● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day	● 0:00 All day

Dans ce mode simple, elles peuvent être configurées en cliquant sur la période d'alarme de chaque jour et en définissant l'heure de début ou de fin dans le formulaire contextuel. Saisissez l'heure de début dans le

champ From et l'heure de fin dans le champ To. Vous pouvez utiliser le bouton Remove pour supprimer la période d'alarme sélectionnée, le bouton Cancel pour ignorer les modifications ou le bouton OK pour mettre à jour le calendrier.

Alert

From: 07:00:00

To: 19:00:00

Remove

Cancel

Ok

En outre, en accédant au mode détaillé, vous pouvez configurer les horaires de manière plus précise. Dans ce mode, vous pouvez également utiliser le formulaire contextuel pour régler l'heure :

- Cliquez sur la période d'alarme de chaque jour et faites glisser le bord supérieur ou inférieur pour étendre la période d'alarme.
- Pour le déplacer, cliquez au milieu de la période d'alarme de chaque jour et faites-le glisser à l'endroit voulu. Vous verrez que les temps changent au fur et à mesure que vous vous déplacez.
- Pour ajouter une nouvelle période d'alarme, cliquez dans une cellule vide et celle-ci marquera une durée. Vous pouvez déplacer ou modifier comme décrit dans les deux étapes précédentes.
- Pour supprimer draguez une période d'alarme hors le calendrier et lâchez.

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
all-day							
00						0:00 All day	
02							
04							
06							
08	7:00 - 19:00	7:00 - 19:00	7:00 - 19:00	7:00 - 19:00	7:00 - 0:00		
10							
12							
14							
16							
18							
20							
22							

Vous pouvez ajouter autant de périodes que vous le souhaitez. Lorsque vous retournez en mode simple, vous obtenez quelque chose comme ce qui suit :

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Schedule	<ul style="list-style-type: none"> 0:00 - 3:00 5:00 - 6:00 7:00 - 14:00 +2 more 	<ul style="list-style-type: none"> 0:00 - 10:00 14:00 - 0:00 	<ul style="list-style-type: none"> 0:00 - 1:00 2:00 - 7:00 9:00 - 14:00 +2 more 	<ul style="list-style-type: none"> 0:00 - 7:00 9:00 - 13:00 	<ul style="list-style-type: none"> 3:00 - 19:00 	<ul style="list-style-type: none"> 0:00 All day 	<ul style="list-style-type: none"> 0:00 All day

Time Threshold

Temps qui doit s'écouler avant de redémarrer le compteur d'alerte. Il définit l'intervalle de temps pendant lequel il est garanti qu'une alerte ne sera pas déclenchée plus de fois que le nombre établi dans « Nombre maximal d'alertes » (Max. number of alerts). Après l'intervalle défini, le compteur sera remis à zéro. La remise à zéro du compteur de déclenchement ne doit pas être relancée si l'alerte est levée à la réception d'une valeur correcte, à moins que la valeur « Remise à zéro du compteur pour les alertes non maintenues » (« Reset counter for non-sustained alerts ») ne soit activée, auquel cas le compteur doit être relancé immédiatement après la réception d'une valeur correcte.

Min number of alerts

Nombre minimum de fois que la situation définie dans le modèle doit se produire (en comptant toujours à partir du nombre défini dans le paramètre FlipFlop du module) pour lancer une alerte. La valeur par défaut est 0, ce qui signifie que l'alerte sera déclenchée lorsque la première valeur qui remplit la condition arrive. Il fonctionne comme un filtre, utile pour ignorer les faux positifs.

Max number of alerts

Nombre maximum d'alertes qui peuvent être envoyées consécutivement dans le même intervalle de temps (Time Threshold). C'est la valeur maximale du compteur d'alertes. Il n'y aura pas plus d'alertes par intervalle de temps que celles indiquées dans ce champ.

Reset counter for non-sustained alerts

Son activation dépend du fait que le nombre indiqué dans « Nombre minimum d'alertes » (Min. number of alerts) soit supérieur à 0. L'activation de ce *token* relance le compteur d'alertes lorsque la condition indiquée n'est pas répétée consécutivement. Par exemple, si le champ « Nombre minimum d'alertes » (Min. number of alerts) a une valeur de 2, cela signifie que le module doit passer par l'état attribué dans « Type de condition » Condition type 3 fois pour déclencher l'alerte. Il y a deux scénarios avec ce dernier *token* :

- Si le *token* de réinitialisation est coché, il faudra que le nombre de critiques soit consécutif, sinon le compteur sera remis à zéro.

```
normal -> critical -> critical -> critical
```

- Si le jeton de redémarrage n'est pas coché, l'alerte sera déclenchée après une séquence alternative ou continue de critiques :

```
normal -> critical -> normal -> critical -> normal -> critical
```

Disable event

En cochant ce *token*, l'événement généré dans la vue des événements du déclencheur d'alerte ne sera pas créé.

Default Action

Dans cette liste déroulante, vous définissez l'action par défaut du modèle. Il s'agit de l'action qui sera créée automatiquement lorsque vous affecterez le modèle au module. Vous pouvez n'en mettre aucune ou une, mais vous ne pouvez pas mettre plusieurs actions par défaut.

Condition Type

Champ dans lequel est défini le type de condition qui sera appliqué à l'alerte.

Min. number of alerts: 0

Condition type: Critical status

i The alert is triggered when the status is critical status.

- None
- Regular expression
- Max and min
- Max.
- Min.
- Equal to
- Not equal to
- Warning status
- Critical status**
- Unknown status
- On change
- Always
- Not normal status


Pandora FMS v7.0NG.758 - OUM 758 - MR 50
Page generated on 2021-11-12 15:39:42


Les listes nécessaires seront ajoutées selon le type choisi précédemment ; il existe les types suivants :

- Regular Expression : Une expression régulière est utilisée. L'alerte est déclenchée lorsque la valeur du module remplit une condition établie. Lorsque vous choisissez la condition régulière, il apparaît la possibilité de cocher la case Triggered when the value matches. Si vous le cochez, l'alerte sera lancée lorsque la valeur se correspond.

Condition type Regular expression ▼

☐ Triggered when the value matches

Value 

 The alert is triggered when the value does not match *Empty*

Pandora FMS v7.0NG.758 - OUM 758 - MR 50

Page generated on 2021-11-12 15:59:44


- Max et Min : Intervalle numérique dimensionné. Lorsque vous cochez Trigger when matches the value, l'alerte sera lancée lorsque la valeur est dans le rang indiqué entre le maximum et le minimum et, si vous ne le cochez pas, l'alerte sera lancée lorsque la valeur est hors le rang indiqué.

Condition type Max and min ▼

☐ Triggered when the value matches

Min.

Max.

 The alert would fire when the value is not between 0 and 0

Pandora FMS v7.0NG.758 - OUM 758 - MR 50

Page generated on 2021-11-12 15:59:44

- Max : Une valeur maximale est utilisée. L'alerte saute lorsque la valeur du module est supérieure à la valeur maximale marquée.

Condition type ▼

Max.

i The alert is triggered when the value is over 0

Pandora FMS v7.0NG.758 - OUM 758 - MR 50

Page generated on 2021-11-12 15:59:44

- Min : Une valeur minimale est utilisée. L'alerte est déclenchée lorsque la valeur du module est inférieure à la valeur minimale marquée.

Condition type ▼

Min.

i The alert is triggered when the value is below 0

Pandora FMS v7.0NG.758 - OUM 758 - MR 50

Page generated on 2021-11-12 15:59:44

- Equal to : Utilisé pour déclencher l'alerte lorsqu'une valeur est fournie, elle doit être égale aux données reçues.

Condition type

Value

i The alert is triggered when the value is equal to *Empty*

Pandora FMS v7.0NG.758 - OUM 758 - MR 50
Page generated on 2021-11-12 15:59:44

- Not equal to : Identique à ce qui précède, mais annulant la condition (opérateur logique NON).

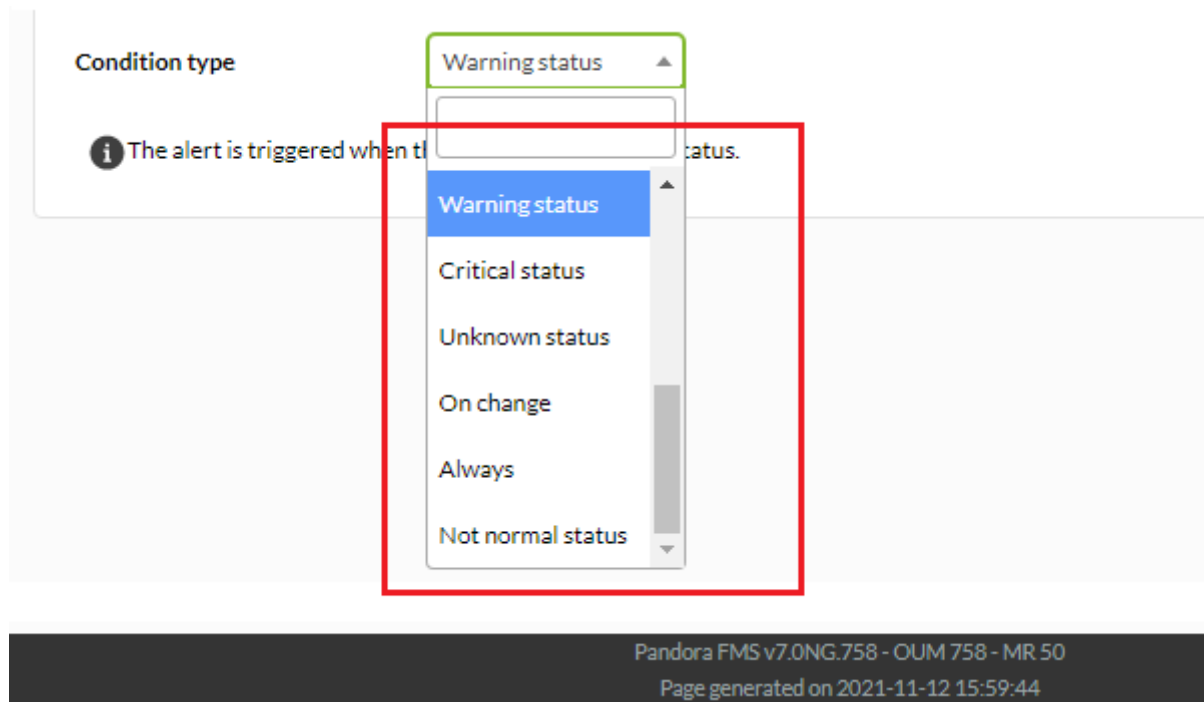
Condition type

Value

i The alert is triggered when the value is different to *Empty*

Pandora FMS v7.0NG.758 - OUM 758 - MR 50
Page generated on 2021-11-12 15:59:44


- Module status : Le module est utilisé n'importe son état (Critical status, Warning status, Unknown status, Not normal status) ou son changement de valeur (On change, mais lorsque vous cochez la case de vérification Triggered when the value matches permet de déclencher si la valeur est égale) ou simplement toujours (Always) si nécessaire.







Pour vérifier périodiquement les modules d'état inconnus (Unknown status), vous pouvez soit activer le `token unknown_updates` dans la [configuration du serveur PFMS](#).


- Vous pouvez également définir des alertes complexes (Complex alert), par exemple si la somme est exactement égale à deux au cours des trente derniers jours :

Configure alert template


Alerts 


Time threshold 	Default action 
<div>5 minutes </div> 	<div>None</div>
Min. number of alerts	Reset counter for non-sustained a
<div>0</div>	<input checked="" type="checkbox"/>
Max. number of alerts	Disable event
<div>1</div>	<input type="checkbox"/>


Condition type

Complex alert 


Math function

Sum. 

Time window 


Last 30 days 

Alert condition

= 

Value

2

 Alert would fire when the sum within the last 30 days is equal to 2

ALERTS » CONFIGURE ALERT TEMPLATE ?

Step 1 »
General

Step 2 »
Conditions

Step 3 »
Advanced fields

Alert recovery

Enabled

Triggering fields

Basic ☒ Advanced ☐

Field 1

Recovery fields

Basic ☒ Advanced ☐

Basic ☒ Advanced ☐

Field 2

Basic ☒ Advanced ☐

Basic ☒ Advanced ☐

Field 3

Basic ☒ Advanced ☐

Alert recovery

Combo où vous pouvez définir si vous voulez activer ou non la récupération des alertes. Si la récupération des alertes est activée, lorsque le module ne remplit plus les conditions indiquées par le modèle, l'action associée aux arguments spécifiés par les champs *field* définis dans cette colonne sera exécutée.

Field 1 - Field 10

Vous pouvez utiliser ici une série de macros décrites ci-dessous.

Une fois complétée la configuration, finissez en cliquant sur le bouton Finish.

Macros remplaçables dans les champs Field1, Field2, Field3... Field10

Dans tous les cas des champs field1, field2... field10 (dans le modèle d'alerte, ainsi que dans la commande et dans l'action) on peut utiliser les macros dans la liste de macros à la fin du chapitre, qui sont des mots clé qui sont remplacés au moment de l'exécution par une valeur qui varie selon le moment, la valeur, l'agent qui déclenche l'alerte, etc.

Exemple d'alerte avec remplacement de macros

En supposant que vous voulez créer une entrée dans un LOG où le format suivant apparaît sur chaque ligne :

```
2009-12-24 00:12:00 pandora [CRITICAL] Agent <agent_name> Data <module_data>
Module <module_name> in CRITICAL status
```

Command Configuration

```
echo _timestamp_ pandora _field2_>> _field1_
```

Action Configuration

```
Field1 = /var/log/pandora/pandora_alert.log
Field2 = <En blanc>
Field3 = <En blanc>
```

Template Configuration

```
Field1 = <En blanc>
Field2 = [CRITICAL] Agent _agent_ Data _data_ Module _module_ in CRITICAL status
Field3 = <En blanc>
```

Dans la section récupération :

```
Field2 = [RECOVERED] [CRITICAL] Agent _agent_ Data _data_ Module _module_ in
CRITICAL status
Field3 = <En blanc>
```

Ainsi, lors de l'exécution d'une alerte, la ligne suivante sera placée dans le LOG :

```
2009-10-13 13:37:00 pandora [CRITICAL] Agent raz0r Data 0.00 Module Host Alive
in CRITICAL status
```

Et la ligne suivante pour récupérer l'alerte :

```
2009-10-13 13:41:55 pandora [RECOVERED] [CRITICAL] Agent raz0r Data 1.00 Module
Host Alive in CRITICAL status
```

Modifier un modèle

Allez vers le menu Alerts > Templates et cliquez sur le nom du modèle à éditer.

Alerts » Alert templates

Type
All
Search
Search

Total items : 4

Name	Group	Type	Op.
Critical condition		Critical status	
Manual alert		Max and min	
Warning condition		Warning status	
Test		Max.	

Create >

Supprimer un modèle

Pour supprimer un modèle, cliquez sur l'icône de la corbeille grise à droite de l'alerte.

Alerts » Alert templates

Type
All
Search
Search

Total items : 4

Name	Group	Type	Op.
Critical condition		Critical status	
Manual alert		Max and min	
Warning condition		Warning status	
Prueba		Max.	

Create >

Assigner des modèles d'alerte aux modules

Connaissant les informations de base sur le système d'alerte, nous allons vous montrer les possibilités d'affecter les alertes aux modules.

Gestion des alertes à partir du sous-menu Alertes

Affectation d'alerte dans le sous-menu Alertes

A partir de la section Alerts > List of Alerts, vous pourrez créer de nouvelles alertes en cliquant sur l'icône du crayon (Builder alert) et configurez les champs :

Ce sont les champs qui doivent être remplis :

Agent

Auto-complétion intelligente pour choisir l'agent.

Module

Liste des modules de l'agent précédemment sélectionné.

Actions

Action qui sera exécutée lorsque l'alerte sera déclenchée. Si le modèle a déjà une action par défaut, il peut être laissé en *Default*.

Template

Gabarit qui contiendra les conditions d'alerte de tir.

Threshold

Une action d'alerte ne sera pas exécutée plus d'une `action_threshold` toutes les secondes, malgré le nombre de fois que l'alerte est déclenchée.

Modifier les alertes dans le sous-menu Alertes

Une fois qu'une alerte a été créée, il n'est possible de modifier que les actions qui ont été ajoutées à l'action du modèle.

Il est également possible de supprimer l'action sélectionnée lors de la création de l'alerte en cliquant sur l'icône de la corbeille grise à droite de l'action, ou d'ajouter de nouvelles actions en cliquant sur le bouton "Ajouter".

Alerts » Manage alerts » list ?

Alert control filter

Total items : 1

Agent	Module Template	Actions	Status	Op.
localhost.[...]domain	CPU Load Critical condition	Mail to XXX (Default) ★ Create a ticke...ntegria IMS (Always)		

Create >

Désactiver les alertes à partir du sous-menu Alertes

Une fois l'alerte créée, il est possible de la désactiver en cliquant sur l'icône de l'ampoule à droite du nom de l'alerte.

Alerts » Manage alerts » list ?

Alert control filter

Total items : 1

Agent	Module Template	Actions	Status	Op.
localhost.[...]domain	CPU Load Critical condition	Mail to XXX (Default) ★ Create a ticke...ntegria IMS (Always)		

Disable

Create >

Supprimer les alertes du sous-menu Alertes

Il est possible de supprimer toute alerte en cliquant sur la corbeille à droite de l'alerte.

Alerts » Manage alerts » list

> Alert control filter

Total items : 1

Agent	Module Template	Actions	Status	Op.
localhost.l[...].domain	CPU Load Critical condition	Mail to XXX (Default) ★ Create a ticke...ntegria IMS (Always)		

Create >

Gérer les alertes depuis l'agent

Affectation des alertes de l'agent

Depuis la section d'administration de l'agent, nous pouvons ajouter de nouvelles alertes en naviguant vers l'onglet correspondant :

> Alert control filter

Total items : 3

Module ▲▼	Template ▲▼	Actions	Status	Op.
Free_RAM	Critical condition 🔍	◦ Mail to Admin (Default) ★	<div></div>	💡 🔔 + 🗑️ 🔍
Free_RAM	test 🔍	◦ Acción Test (Default) ★ Create a ticket in Integria IMS (From 1 to 3) 🗑️ 🔧	<div></div>	💡 🔔 + 🗑️ 🔍
System_Load_AVC	Critical condition 🔍	◦ Mail to Admin (Default) ★	<div></div>	💡 🔔 + 🗑️ 🔍

Module

Select ▼

Actions

Default action ▼

+ Create Action

Template

Select ▼

+ Create Template

Threshold

0

seconds ?

Add alert 🌟

Nous allons maintenant détailler les champs disponibles dans le formulaire :

Module

Liste des modules agents.

Actions

Action qui sera exécutée lorsque l'alerte sera déclenchée. Si le modèle a déjà une action par défaut, il peut être laissé dans Default.

Template

Modèle qui contiendra les conditions de déclenchement de l'alerte.

Threshold

Une action d'alerte ne sera pas exécutée plus d'une fois toutes action_threshold secondes, malgré le nombre de fois que l'alerte est déclenchée.

Modifier les alertes de l'agent

Une fois l'alerte créée, il n'est possible de modifier que les actions qui ont été ajoutées à l'action du modèle.

Il est possible de supprimer l'action qui a été sélectionnée pour créer l'alerte en cliquant sur l'icône de la corbeille à droite de l'action, ou en ajoutant de nouvelles actions en cliquant sur le bouton "Ajouter".



Désactiver les alertes de l'agent

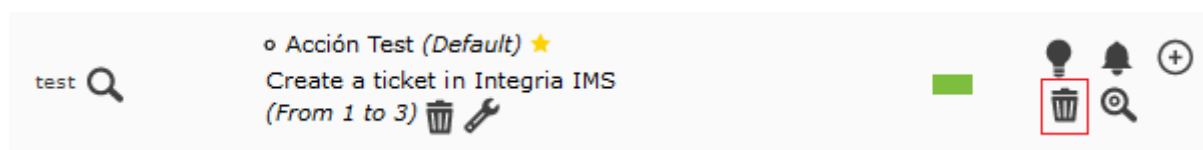
Une fois qu'une alerte a été créée, il est possible de la désactiver en cliquant sur l'icône de l'ampoule située à droite du nom de l'alerte.



Dans l'image d'exemple, la deuxième alerte est désactivée (notez que la couleur de la police et l'icône d'alerte désactivée sont gris clair).

Supprimer des alertes depuis l'Agent

Vous pouvez supprimer une alerte en cliquant sur l'icône de la corbeille à droite de l'alerte.



Détail des alertes

En cliquant sur l'icône loupe dans le bouton des options d'alerte, on accède à une page

récapitulative de la configuration effective de l'alerte.

C'est l'écran où nous pourrions confirmer chacune des configurations que nous avons sélectionnées pour notre alerte :

ALERT DETAILS

Alert details
Firing conditions

List alerts List alerts

Agent nova

Module Free_RAM

Template test ★

Last fired Unknown

Status ■ Alert not fired

Priority Informative

Stand by No

The alert is triggered when the module is in critical status

Mon	Tue	Wed	Thu	Fri	Sat	Sun
✓	✓	✓	✓	✓	✓	✓

00:00:00
-
23:59:59
✓

Use special days list No

Time threshold 1 days

Number of alerts (Min./Max.) 0/1

Actions
#1 #2 #3 >#3 Threshold ?

Acción Test (Default) ★	×	×	×	✓	No
Create a ticket in Integria IMS	×	✓	✓	×	No
Acción Test	✓	×	×	×	No

Select the desired action and mode to view the Firing/Recovery fields for this action

Action

Choose an action
▼

Sélectionnez une action spécifique dans la liste déroulante des actions pour voir un exemple de la commande finale :



Accédez au formulaire d'édition du module pour établir les seuils suivants :

Base options form for the CPU Load module. The form includes fields for Name (CPU Load), ID (1), Type (Generic numeric (generic_data)), Warning status (Min: 70.00, Max: 90.00, Inverse interval: ☐), Critical status (Min: 91.00, Max: 100.00, Inverse interval: ☐), and Historical data (checked). A legend on the right shows the status colors: Normal Status (green), Warning Status (yellow), and Critical Status (red).

Acceptez et sauvegardez la modification. Maintenant lorsque la valeur du module *CPU Load* est entre 70 et 90, son état deviendra WARNING, et entre 91 et 100 il deviendra CRITICAL, en affichant son état en rouge :



Configurer l'action

Nous devons maintenant créer une action qui est "Envoyer un email à l'opérateur". Allez dans le menu : Alertes > Actions et cliquez sur le bouton Create pour créer une nouvelle action :

Alerts » Configure alert action ?

Name	<input type="text" value="Mail_to_XXX"/>		
Group	<input type="text" value="All"/>		
	<input type="text" value="eMail"/>	+ Create Command	
Command	This alert send an email using internal Pandora FMS Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message.		
Threshold	<input type="text" value="0"/>	seconds	?
	Firing	Recovery	
Command preview	<div>Internal type</div>	<div>Internal type</div>	
Destination address Field 1 ?	<div></div>	<div></div>	
Subject Field 2	<div></div>	<div></div>	

Cette action utilisera la commande eMail, et ses champs Field1, Field2 et Field3 correspondront à l'adresse de destination, l'objet de l'e-mail et le corps du message.

Configurer le modèle

Un modèle d'alerte générique sera créé pour tout module en état critique, son action par défaut sera de notifier le groupe d'opérateurs par email. Accédez à la section *Templates*.

Étape 1 :

Alerts » Configure alert template

Step 1 »

General

Step 2 »

Conditions

Step 3 »

Advanced fields

Name

Critical Condition

Group

All



Description

Priority

Informative



Maintenance

Informative

Normal

Minor

Warning

Major

Critical

Warning/Critical

Not normal

Critical/Normal

Next



La priorité définie ici Informative sera utilisée pour afficher l'événement dans une certaine couleur lorsque l'alerte est déclenchée.

Dans l'étape 2, vous spécifiez les paramètres qui déterminent les conditions de déclenchement spécifiques, telles que l'état que le module doit avoir ou les intervalles de temps dans lesquels le module doit fonctionner.

Étape 2 :

Alerts » Configure alert template ?

Step 1 »
General

Step 2 »
Conditions

Step 3 »
Advanced fields

Days of week

Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun ☒

Use special days list

☐

Set initial time

12:00:00

Set end time

12:00:00

Time threshold

1 day

Min. number of alerts

0

Reset counter for non-sustained alerts

☐

Max. number of alerts

1

Disable event

☐

Default action

None

Condition type

Critical status
None
Regular expression
Max and min
Max.
Min.
Equal to
Not equal to
Warning status
Critical status
Unknown status
On change
Always
Not normal status

The alert is triggered when the status of the module is **Critical status**.

Next >

Condition type

Il détermine si l'alerte sera déclenchée par un changement d'état, une variation d'une valeur, etc. C'est le paramètre le plus important pour que l'alerte fonctionne comme souhaité. Nous utiliserons la condition *Etat critique* pour que l'alerte soit déclenchée lorsqu'un module est dans un état critique.

Default action

Action par défaut à exécuter lorsque l'alerte est déclenchée. Elle est facultative.

Time threshold

Temps pendant lequel l'alerte ne sera pas répétée si l'état incorrect est maintenu en permanence. Si nous le laissons dans un jour (24 heures), il ne nous enverra l'alerte qu'une fois toutes les 24h même si le module reste plus longtemps dans le mauvais état.

Nombre minimum/maximum d'alertes

Nombre d'alertes, le nombre minimum/maximum de fois que la condition devra être donnée (dans ce cas, que le module est à l'état **critical**) avant que Pandora FMS exécute les actions associées au modèle d'alerte. Avec la valeur 0, la première fois que le module est incorrect, il déclenchera l'alerte.

Étape 3 :

ALERTS » CONFIGURE ALERT TEMPLATE

Step 1 » General Step 2 » Conditions **Step 3 » Advanced fields**

Alert recovery: Enabled ▼

Triggering fields	Recovery fields
<p>Field 1 ?</p> <p>Basic ● Advanced ○</p>	<p>Basic ● Advanced ○</p>
<p>Field 2 ?</p> <p>Basic ● Advanced ○</p>	<p>Basic ● Advanced ○</p> <p>[PANDORA] Alert RECOVERED for CRITICAL status on _agent_ / _module_</p>
<p>Field 3 ?</p> <p>Basic ● Advanced ○</p> <pre></style> <table style="width: 100%; border-collapse: collapse;" align="center"> <tbody> <tr> <td align="center" valign="top" bgcolor="#ffffff" width="100%"> <table style="width: 100%; border-collapse: collapse;"> <tbody> <tr> <td style="background-color: #1f1f1f; height: 70px; width: 100%"><center> <table class="w320" style="width: 600px; border-collapse: collapse;"> <tbody> <tr> <td class="mobile-block mobile-no-padding-bottom mobile-center" style="background-color: #1f1f1f; padding: 10px 10px 20px 20px; align="top" width="270"></td> <td class="mobile-block mobile-center" style="background-color: #1f1f1f; padding: 17px 15px 10px 10px; align="top" width="270">&nbsp;</td> </tr> </tbody> </table> </td> </tr> </tbody> </table> </center></td></pre>	<p>Basic ● Advanced ○</p> <pre><style type="text/css"><!-- /* Take care of image borders and formatting */ img { max-width: 600px; outline: none; text-decoration: none; -ms-interpolation-mode: bicubic; } a { border: 0; outline: none; } a img { border: none; } /* General styling */</pre>

Dans la section 3 nous avons les champs Field1, Field2, Field3, etc. qui, comme nous l'avons expliqué, nous serviront à transférer les paramètres du modèle vers l'action, et de l'action vers la commande.

Aussi dans cette troisième section nous pouvons activer ou désactiver la récupération d'alerte, qui est d'exécuter une autre action lorsque la situation problématique revient à la normale.

Associer l'alerte au module

Nous avons déjà tout ce dont nous avons besoin, il ne nous reste plus qu'à associer le modèle d'alerte au module. Pour ce faire, nous allons dans l'onglet alerte à l'intérieur de l'agent où se trouve le module :

The screenshot shows the top configuration bar of the Pandora FMS interface. It includes a 'Module' dropdown menu with 'Select' as the current value, a 'Template' dropdown menu with 'Select' as the current value, and a '+ Create Template' button. Below these, there is an 'Actions' dropdown menu with 'Default action' as the current value, a 'Create Action' button, a 'Threshold' input field with the value '0', a unit dropdown menu with 'seconds' as the current value, a calendar icon, and a help icon. At the bottom right of this bar is a dark green 'Add alert' button with a green arrow icon.

Nous avons créé une association entre le module `cpu_user` et le modèle d'alerte Critical condition. Par défaut, il affichera l'action que nous avons définie dans ce modèle "Envoyer un email à XXX".

Escalade d'alerte

L'escalade des alertes est des actions supplémentaires qui seront exécutées si l'alerte est répétée un certain nombre de fois de suite (il faut au début d'associer une alerte complète à un module comme expliqué dans les sections précédentes).

Vous avez seulement à ajouter les actions supplémentaires et déterminer entre quels répétitions consecutives de l'alerte vous allez exécuter cette action. Exemple :

The screenshot shows the 'Add action' dialog box. It has a green header bar with the text 'Add action' and a close button (X). The dialog contains the following fields: 'Agent' (empty), 'Module' (set to 'Host Alive'), 'Action' (set to 'Mail 24x7'), 'Number of alerts match from' (set to '3') with a help icon, 'to' (set to '5'), and 'Threshold' (empty) with a help icon. At the bottom right is a dark green 'Add' button with a green arrow icon.

Lorsqu'une alerte est récupérée, toutes les actions exécutées jusqu'à présent seront réexécutées, et pas seulement celles correspondant à la configuration de Number of alerts match from actuelle.

De plus, nous pouvons mettre un seuil (Threshold) en tant que seconde paramètre à partir duquel une alerte ne peut pas être lancée plus d'une fois pendant cet intervalle.

Envoi de messages d'alerte à travers de messages instantanés

1. **Telegram** est une plate-forme instantanée par laquelle vous pouvez recevoir des messages d'alertes depuis Pandora FMS.

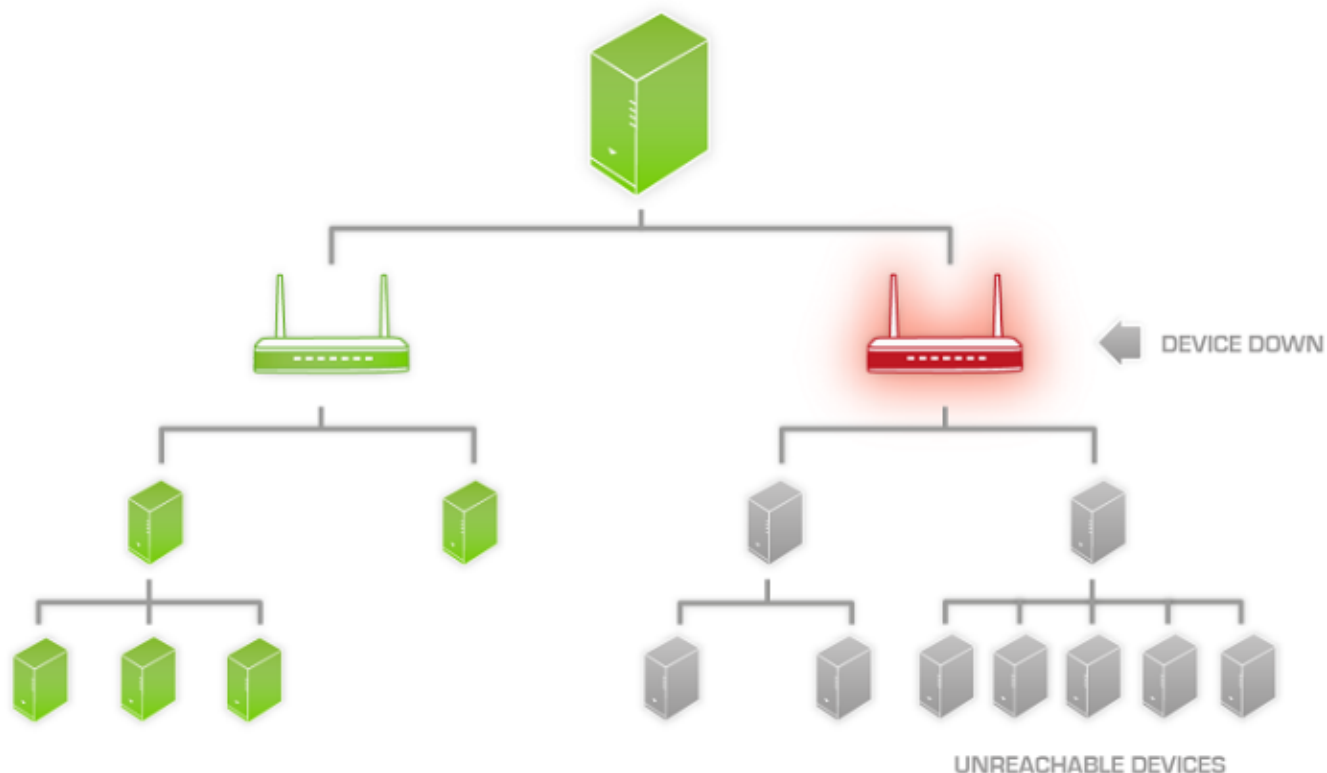
Alertes en Standby

Les alertes peuvent être activées, désactivées ou en veille. La différence entre les alertes désactivées et les alertes de veille est que les alertes désactivées ne fonctionneront tout simplement pas et ne seront donc pas affichées dans la vue d'alerte. Les alertes de veille, par contre, seront affichées dans la vue Alertes et ne fonctionneront qu'au niveau de la vue. En d'autres termes, il sera montré s'ils sont déclenchés ou non, mais ils n'exécuteront pas les actions qu'ils ont programmées ni ne généreront d'événements.

Les alertes de veille sont utiles pour pouvoir les visualiser sans les perturber sur d'autres aspects.

Protection en cascade

La protection en cascade est une fonction de Pandora FMS qui permet d'éviter un bombardement massif d'alertes lorsqu'un groupe d'agents n'est pas accessible, en raison d'une connexion principale qui échoue. Ce genre de choses se produit lorsqu'un élément de réseau intermédiaire comme un routeur ou un commutateur tombe en panne, et qu'il est laissé inaccessible à une grande partie du réseau géré avec Pandora FMS. Parce que les contrôles réseau échoueraient dans ce scénario, les alertes pour les appareils hors service commenceraient à se déclencher sans être vraies.



La protection en cascade est activée à partir de la configuration de l'agent. Cliquez sur l'option

Cascade protection.

localhost.localdomain - Setup

Setup

Home

Key

Network

Folder

Group

Check

Star

Alert

Monitor

Settings

Tools

Eye

Agent name

localhost.localdomain

ID 1

Search

Calendar

Star

Trash

IP Address

192.168.70.150

192.168.70.150

Delete selected

QR Code Agent view

Parent

Cascade protection

Group

Unknown

Interval

5 minutes

OS

Linux

Server

localhost.localdomain

Description

Created by localhost.localdomain

Pour que l'agent fonctionne avec la protection en cascade activée, vous devez avoir l'Agent père configuré correctement, dont il dépend. Si l'agent père a à ce moment là quelque alerte de module en état critique déclenchée, l'agent inférieur avec protection en cascade n'exécutera ses alertes. Cela n'est pas appliqué aux alertes de modules en état warning ou unknown.

Exemples

Vous avez les agents suivants :

- Router : module de contrôle ICMP et module de contrôle SNMP, utilisant un OID standard pour vérifier l'état d'un port ATM. Nous pouvons également vérifier la latence jusqu'au routeur de notre fournisseur.
- Web server : possède plusieurs modules exécutés par l'agent : Vérification du CPU, de la mémoire, du processus Apache. Il dispose également d'un contrôle de latence WEB en quatre étapes.
- Database server : possède plusieurs modules exécutés par l'agent : Vérification du CPU, de la mémoire, du processus MySQL. En outre, il dispose de quelques contrôles supplémentaires de l'intégrité de la BD. Il dispose également d'une vérification de la connectivité à distance à une autre base de données, à l'aide d'un plugin spécifique qui se connecte, interroge et quitte, en mesurant le

temps total.

Dans WEB SERVER et DATABASE SERVER, nous définissons ROUTER comme parent. Activez la case à cocher Protection en cascade dans WEBSERVER et DATABASE SERVER.

Nous définissons maintenant plusieurs alertes simples :

- ROUTER

SNMP Check / CRITICAL → Action, send MAIL. Latency > 200ms / WARNING → Action, send MAIL.

- WEB SERVER

CPU / WARNING MEM / WARNING PROCESS / CRITICAL → Action, send MAIL. HTTP LATENCY / CRITICAL → Action, send MAIL.

- DATABASE SERVER

CPU / WARNING MEM / WARNING PROCESS / CRITICAL → Action, send MAIL. SQL LATENCY / CRITICAL > Action, send MAIL.

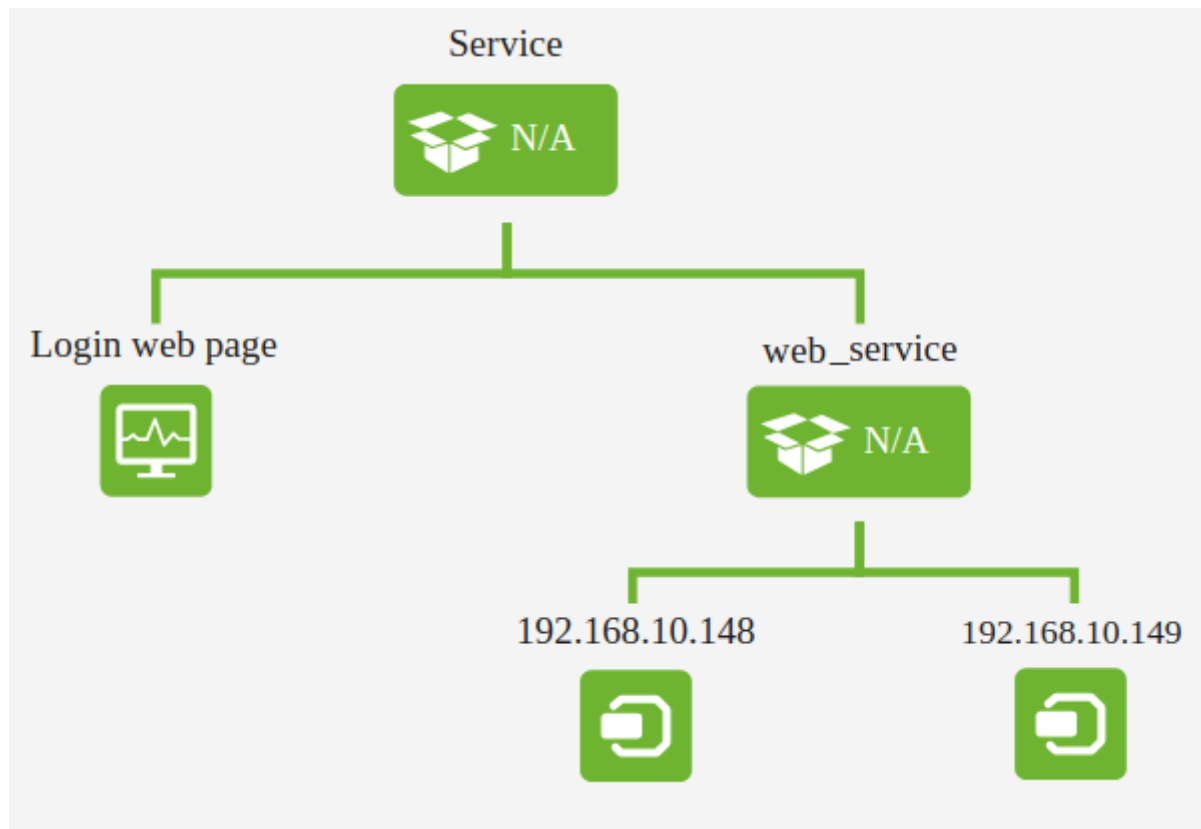
- Si la connexion ROUTER tombe en panne, c'est-à-dire là où Pandora FMS se connecte à WEB SERVER et DATABASE ; sans activer la protection en cascade, il recevrait six alertes, essayez d'imaginer l'effet que cela aurait si au lieu de deux serveurs, il avait deux cents. Cet effet est connu sous le nom de "tempête d'événements", dans le pire des cas, peut faire tomber votre serveur de messagerie, serveur de surveillance et votre propre mobile, l'inonder de SMS.
- Si vous disposez d'une protection en cascade, vous ne recevrez qu'une alerte indiquant que l'interface ATM du routeur est hors service. Cependant, je verrais les éléments WEBSERVER et DATABASE SERVER en rouge, mais je n'aurais pas les alertes.

Protection en cascade basée sur les services

Version NG 727 ou supérieur

Il est possible d'utiliser les **Services** pour éviter que les alertes de différents sources arrivent informant sur la même incidence.

Si vous activez la protection en cascade basée sur les services, les éléments de service (agents, modules ou autres services) ne signaleront pas les problèmes, mais le service lui-même avertira au nom de l'élément affecté.

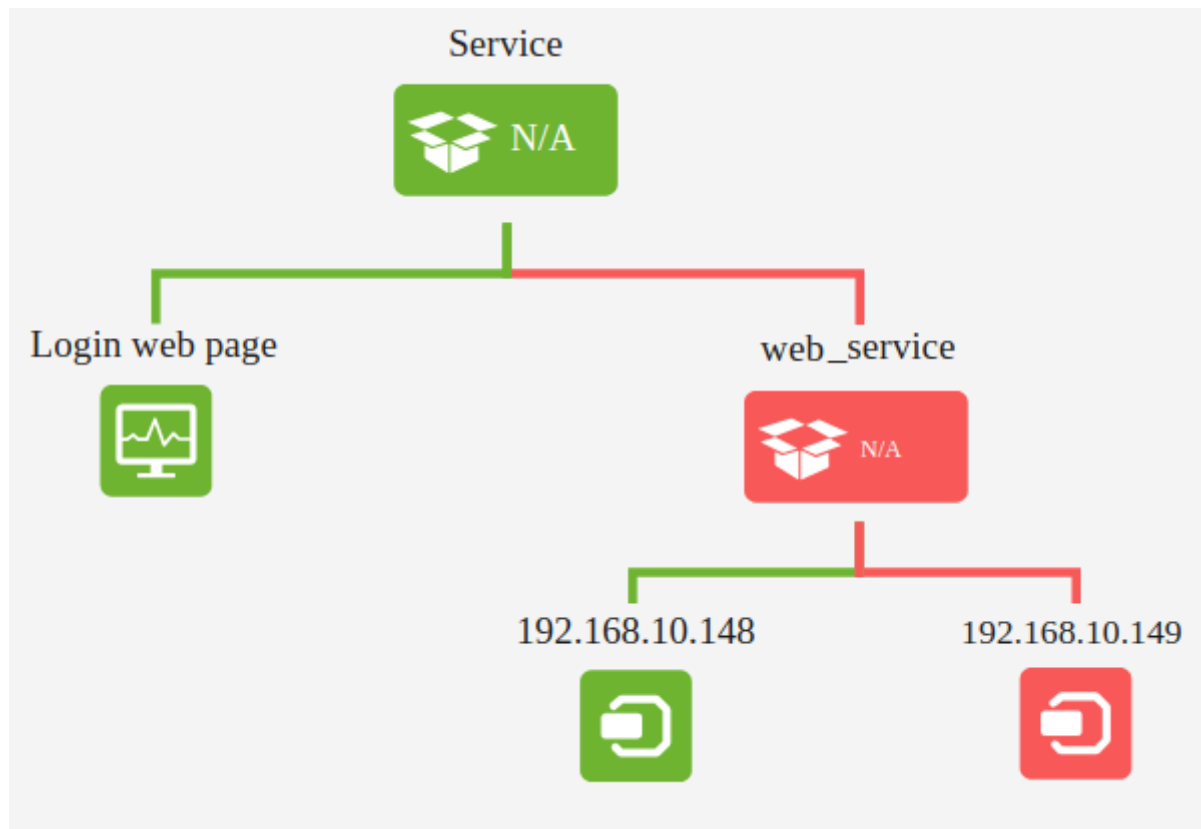


Si l'élément *192.168.10.149* entre dans un état critique sans affecter le reste du service, l'opérateur reçoit une alerte indiquant que *192.168.10.149* est en panne, mais que le service *Service* fonctionne normalement.

Pour recevoir ces informations, vous devez éditer ou créer un nouveau modèle d'alerte, en utilisant la macro `_rca_` pour un *root cause analysis* (root cause analysis).

`_rca_`

Cette macro fournira à l'opérateur des informations sur le 'chemin' affecté dans le service.



Par exemple, la valeur de la macro `_rca_` correspondant à l'état de service dans l'image serait :

```
[Service -> web_service -> 192.168.10.149]
```

Bien que l'état du service soit correct car il ne dépasse pas le 50 % des composants en état critique (vous pouvez obtenir plus d'information sur ça dans la section [Services](#))

Observation : La chaîne d'événements représentée dans l'analyse de la cause fondamentale représente les éléments critiques d'un service, nous permettant de voir quels éléments affectent mon service.

Protection en cascade basée sur des modules

L'état d'un module d'un agent parent peut être utilisé pour éviter les alertes d'agent au cas où le module de l'agent parent passe en état critique.

^

Advanced options

Secondary groups

Please select...

Parent

Cascade protection modules

Any

Mode de fonctionnement sûr

Quiet

Disabled mode

Remote configuration

Not available

Safe operation mode ☒

Module

CPU Load

Any

CPU Load

DiskUsed_C:

echo_1

freedisk_C

Memory Used

✓ Custom fields

Click to display

Serial Number

Department

Additional ID

eHorusID

Le mode de fonctionnement sécurisé peut être activé dans les options de configuration avancées d'un agent.

Si l'état du module sélectionné devient `critical`, les autres modules de l'agent sont désactivés jusqu'à ce qu'il revienne à `normal` ou `warning`. Cela permet, par exemple, de désactiver les modules distants en cas de perte de connectivité.

Exemples d'alertes

Envoi d'alertes par SMS

Vous devez avoir installé un outil qui permet l'envoi de SMS sous forme de `smstools`.

Supposons que vous ayez configuré votre compte SMS. Exécutez la commande :

```
> sendsms
```

Vous devez indiquer deux paramètres, destination et message :

```
<destination> 'Full message'
```

Placez le numéro de destination de manière complète (exemple 346276226223 pour des téléphones en Espagne) et le texte du message entre des guillemets simples (' et ').

Nous allons maintenant pouvoir utiliser la commande d'alerte dans l'interface d'administration de Pandora FMS.

Alerts » Configure alert command ?

Name	<input type="text" value="SMS"/>		
Command ?	<div>sendsms _field1_ _field2_</div>		
Description	<div>Send SMS using the Pandora FMS standard SMS device</div>		
Field 1 description ?	<input type="text" value="Destination number"/>	Field 1 values ?	<input type="text" value="123456789"/>
Field 2 description	<input type="text"/>	Field 2 values	<input type="text"/>
Field 3 description	<input type="text"/>	Field 3 values	<input type="text"/>
Field 4 description	<input type="text"/>	Field 4 values	<input type="text"/>

Dans cette commande Field 1 sera le numéro de téléphone de destination et le Field 2 le message lui-même. Rappelez-vous que ces champs seront “ passés ” à l'alerte et que ses valeurs pourront être pris ou remplacés, donc dans l'image précédente le numéro de destination pour l'exemple est “123456789 ”.

Maintenant configurez l'action pour cette commande :

Alerts » Configure alert action ?

Name	<input type="text" value="SMS"/>	
Group	<input type="text" value="All"/>	
Command	<input type="text" value="SMS"/> + Create Command	
	Send SMS using the Pandora FMS standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Threshold	<input type="text" value="0"/> seconds ?	
	Firing	Recovery
Command preview	<pre>sendsms 346666666666 Hola</pre>	<pre>sendsms _field1_ _field2_</pre>
Destination number <small>Field 1</small> ?	<input type="text" value="346666666666"/>	<input type="text"/>
Message <small>Field 2</small>	<input type="text" value="Hola"/>	<input type="text"/>

Create

Cette action exécute la commande définie précédemment, en remplaçant Field 1 et Field 2 avec des valeurs personnalisées. Dans Field 1 il sera le téléphone de destination ("346666666666 " dans l'exemple de la figure précédente) et le Field 2 le texte défini dans cet action (" Salut " dans l'exemple de la figure précédente).

Dans Pandora FMS, vous pouvez utiliser un mot (alphanumérique) pour le numéro de téléphone de destination, mais gardez à l'esprit que quelques opérateurs mobiles ne gèrent pas correctement les identifications alphanumériques.

Dans l'étape suivante, vous pouvez utiliser un modèle d'alerte existante ou en créer une nouvelle :

Alerts » Configure alert template ?

Step 1 »
General

Step 2 »
Conditions

Step 3 »
Advanced fields

Name

Critical condition

Group

All ▼

Description

This is a generic alert template to fire on condition CRITICAL

Priority

Critical ▼

Next >

Dans ce cas, le modèle d'alerte sera seulement “ déclenchée ” lorsque un module est en état critical.

Une fois il est défini, configurez l'alerte pour qu'elle soit déclenchée une fois par jour maximum, mais si elle est récupérée, elle sera lancée chaque fois qu'elle est récupérée et déclenchée à nouveau ; regardez l'image suivante.

Alerts » Configure alert template ?Step 1 »
General**Step 2 »**
ConditionsStep 3 »
Advanced fields

Days of week	Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/>	Use special days list	<input type="checkbox"/>
Time from ★	<input type="text" value="12:00:00"/>	Time to ★	<input type="text" value="12:00:00"/>
Time threshold	<input type="text" value="1 day"/>		
Min. number of alerts	<input type="text" value="0"/>	Max. number of alerts	<input type="text" value="1"/>
Default action	<input type="text" value="Mail to XXX"/> ★		
Condition type	<input type="text" value="Critical status"/>		

The alert would fire when the module is in critical status

Next >

Maintenant, tout ce que vous avez à faire est d'assigner un module avec un modèle d'alerte et une action d'alerte :

Module	<input type="text" value="CPU Load"/>	<i>Latest value: 0.00</i>	Template	<input type="text" value="Critical condition"/>	
Create Template					
Actions	<input type="text" value="SMS"/>	Create Action	Threshold	<input type="text" value="0"/>	<input type="text" value="seconds"/>

Add alert

Sur un module de charge de travail d'UCT, réglez une valeur bas de 20 pour pouvoir tester l'envoi du message, regardez la capture d'écran suivante :

localhost.localdomain - Modules

Name ★

CPU Load

ID 1

Disabled

Type ? ★

Generic numeric (generic_data)

Module group

Not assigned ▼

Warning status ?

Min. 0.00

Max. 0.00

Inverse interval ☐

Critical status ?

Min. 20.00

Max. 0.00

Inverse interval ☐

FF threshold ?

☒ All states changing : 0
 ☐ Each state changing : To 'normal' 0 To 'warning' 0 To 'critical' 0

Historical data

☒

Data configuration

```

module_begin
module_name CPU Load
module_type generic_data
module_interval 1
module_exec vmstat 1 2 | tail -1 | awk '{ print $13 }'
module_max 100
module_min 0
module_description User CPU Usage (%)
          
```

Load basic ★

Check ★

Advanced options

Custom macros ?

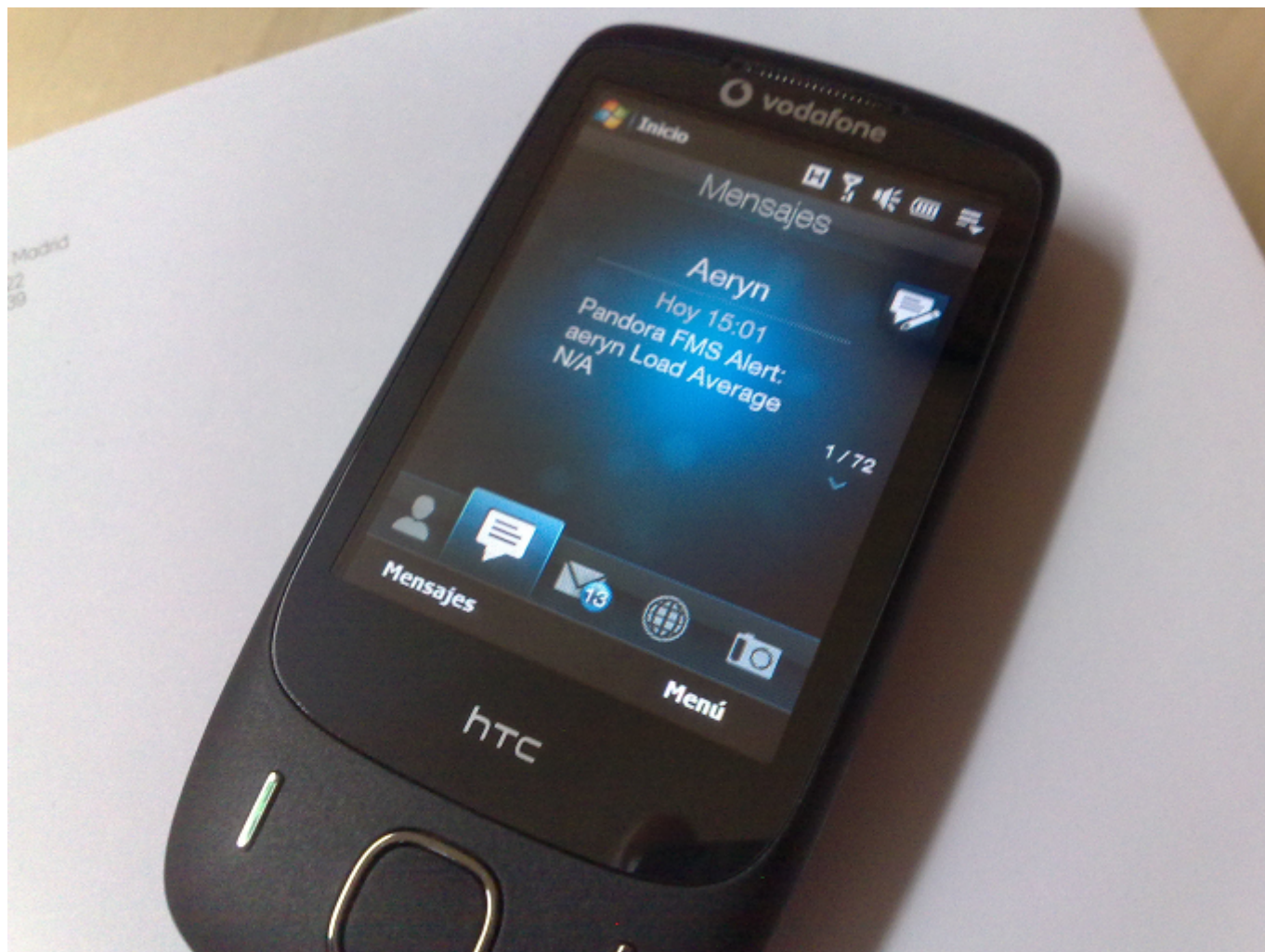
Module relations

Update

Tout est prêt. Vous pouvez maintenant “ forcer ” l'alerte à l'exécuter et à la tester. Pour forcer l'alerte, allez à la vue d'alerte de l'agent et cliquez sur l'icône circulaire verte.

		Galaga login		N/A - N/A	4.9		101	1 minutes 23 seconds
--	--	--------------	--	-----------	-----	--	-----	----------------------

Un SMS peut apparaître sur votre téléphone portable, comme le montre la photo ci-dessous. Notez que le message de teste a été changée par le texte “ aeryn ” ; en plus la valeur de la charge de CPU montre “ N/A ” parce que lors de forcer une alerte aucun donnée réelle est recue par la module, donc il n'a pas eu du temps pour collecter des valeurs.



Utilisation de commandes d'alerte autres que l'email

Pandora FMS est caractérisé par sa flexibilité, pour que de cette manière il puisse toujours être utile, à tout moment. La pratique suivante est avancée et doit toujours être considérée comme une exception aux règles.

L'email, car la commande est interne à Pandora FMS et ne peut pas être configuré, c'est-à-dire que le Field1, le Field2 et le Field3 sont des champs définis qui sont utilisés comme destinataire, objet et texte du message. Mais, que se passe-t-il si je veux exécuter une action différente, définie de manière personnalisée ?

Imaginez que nous vouliez générer un fichier journal avec chaque alerte que Pandora FMS trouve. Le format de ce fichier journal doit être quelque chose comme :

```
DATE_HEURE - NOM_AGENT - NOM_MODULE - VALEUR - DESCRIPTION DU PROBLÈME
```

Où VALEUR est la valeur du module à ce moment. Il y aura plusieurs fichiers journaux, selon l'action qui appelle la commande. L'action définira la description et le fichier vers lequel se dirigeront les événements.

Pour ce faire, nous allons d'abord créer une commande comme suit :

Alerts » Configure alert command ?

Name

Sample Alert

Command ?

Echo _timestamp_

Description

Sample alert

Field 1 description ?

Field 1 values ?

Field 2 description

Field 2 values

Field 3 description

Field 3 values

Et vous allez définir une action :

Alerts » Configure alert action ?

Name

Custom Log Alert #1

Group

All ▼

Command

Sample Alert ▼

+ Create Command

Sample alert

Threshold

0

seconds ?

Firing

echo_timestamp_

Recovery

echo_timestamp_

Command preview

Create

Lorsque les alarmes sont exécutées, le fichier du journal que vous avez créé doit être quelque chose de pareille à ceci :

```
2010-05-25 18:17:10 - farscape - cpu_user - 23.00 - Custom log alert #1
```

L'alerte a été déclenchée à 18:17:10 dans l'agent "farscape", dans le module "cpu_sys" avec une donnée de "23.00" et avec la description que nous avons mise lors de la définition de l'action.

Depuis l'exécution de la commande, l'ordre des champs et d'autres choses peuvent nous faire ne pas bien comprendre comment la commande est exécutée à la fin, le plus simple est d'activer les traces de débogage du serveur pandora (verbose 10) dans le fichier de configuration de Pandora Server dans /etc/pandora/pandora_server.conf, redémarrons le serveur (/etc/init.d/pandora_server restart) et regardons le fichier /var/log/pandora/pandora_server.log cherchant la ligne exacte avec l'exécution de la commande d'alerte que nous avons définie, pour voir comment le serveur Pandora FMS lance cette commande.

À partir de la version NG 754 dispose d'[options additionnelles du démarrage et arrête manuel](#) d'Environnements de Haute Disponibilité (HA).

Exemple d'alerte avec macros de substitution

Supposons que vous vouliez générer une entrée dans un LOG où le format suivant apparaît sur chaque ligne :

```
2009-12-24 00:12:00 pandora [CRITICAL] Agent <agent_name> Data <module_data>
Module <module_name> in CRITICAL status
```

Configuration de la commande

```
echo _timestamp_ pandora _field2_ » _field1_
```

Configuration de l'action

```
Field1 = /var/log/pandora/pandora_alert.log
Field2 = <En blanc>
Field3 = <En blanc>
```

Configuration du modèle

```
Field1 = <En blanco>
Field2 = [CRITICAL] Agent _agent_ Data _data_ Module _module_ in CRITICAL status
Field3 = <En blanc>
```

Dans la section récupération :

```
Field2 = [RECOVERED] [CRITICAL] Agent _agent_ Data _data_ Module _module_ in
CRITICAL status
Field3 = <En blanc>
```

Ainsi, lors de l'exécution d'un signalement, la ligne suivante serait insérée dans le LOG :

```
2009-10-13 13:37:00 pandora [CRITICAL] Agent raz0r Data 0.00 Module Host Alive
in CRITICAL status
```

Et la ligne suivante quand l'alerte est récupérée :

```
2009-10-13 13:41:55 pandora [RECOVERED] [CRITICAL] Agent raz0r Data 1.00 Module
Host Alive in CRITICAL status
```

Macros personnalisées d'alertes module

N'importe quel nombre de macros (Custom macros) peut être ajouté à un module d'agent.

localhost.localdomain - Modules

Using module component ? --Manual setup--

Name

Type ?

Warning status ?

FF threshold ?

Historical data

Target IP

Remote ICMP network agent (l

Min. 0
Max. 0
Inverse interval

All states changing : 0

Each state changing : To 'normal' To 'warning' To 'critical'

☒

192.168.70.150

Disabled

Module group

Min. 0
Max. 0
Inverse interval

Critical status ?

Port

General

0

0

Advanced options

Custom macros ?

Custom macros +

Name

Value

Module relations

Create

Ces macros ont les caractéristiques suivantes :

- Définis dans le module.
- Stocker les données dans la DDBBB .
- Peut avoir n'importe quel nom, par ex : `_pepito`
- Ils ne sont pas reflétés dans la configuration locale (`.conf`).
- Utilisé exclusivement pour les alertes.
- Ne peut pas être défini au niveau composant.
- Peut être défini dans policies..

Ces macros spécifiques peuvent être ajoutées en développant la section macro de n'importe quel module.

> **Advanced options**

^ **Custom macros**

Name Value

Custom macros

Name Value

Les valeurs définies peuvent être utilisées comme partie des champs dans la définition des alertes.

Exemple : Pour inclure une macro à l'action d'envoi d'e-mail, il est nécessaire de configurer le champ corps du message comme suit :

```

Hello, this is an automated email coming from Pandora FMS

This alert has been fired because a CRITICAL condition in one of
your monitored items:

Agent : _agent_
Module: _module_
Module description: _moduledescription_
Timestamp _timestamp_
Current value: _data_
Component: _tecnology_

Thanks for your time.

Best regards
Pandora FMS

```

Si un module est ajouté à cette alerte sans avoir configuré la macro, la section où la valeur de la macro doit apparaître dans l'action sera vide.

Configuration des emails pour les alertes dans Pandora FMS

Pandora FMS lui même a la capacité d'envoyer des emails comme expliqué dans la [configuration générale de la Console](#).


Cependant sa flexibilité permet l'envoi des emails avec des différents plate-formes d'email.






Configuration d'email avec une compte Gmail


Pour que le serveur Pandora FMS puisse envoyer les alertes via le compte mail Gmail, [configurez la console générale de Pandora FMS](#) ou la configuration du [serveur Pandora FMS](#) et ajoutez vos identifiants, domaine web Office365, noms d'utilisateur, mot de passe etc.).

Configuration d'action

Ajoutez une action, par exemple avec le nom Mail to Admin et pour configurer un destinataire d'email utilisez la commande eMail :

ALERTS » CONFIGURE ALERT ACTION 

Name	<input type="text" value="Mail to Admin"/>		
Group	<input type="text" value="All"/> <input type="text" value="eMail"/> <input type="button" value="Create Command"/> 		
Command	This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).		
Threshold	<input type="text" value="0 seconds"/> 		
	Triggering	Recovery	
Command preview	<div>Internal type</div> <div>Internal type</div>		
Destination address	<input type="text" value="example1@example.com,example2@example.com,example3@"/>		
Field 1			
Subject	<input type="text" value="[PANDORA] Alert from agent _agent_ on module _module_"/>		
Field 2			
	Basic  <input checked="" type="radio"/> Advanced <input type="radio"/>	Basic <input checked="" type="radio"/> Advanced <input type="radio"/>	
Text	<div> <pre><style type="text/css"> /* Take care of image borders and formatting */ img { max-width: 600px;</pre> </div> <div> <pre><style type="text/css"><!-- /* Take care of image borders and formatting */ img { max-width: 600px;</pre> </div>		
Field 3			
Content Type	Text/plain  <input type="radio"/> Text/html <input checked="" type="radio"/> Text/plain  <input type="radio"/> Text/html <input checked="" type="radio"/>		
Field 4			

Update 

Configuration de l'Alerte

Dans ce cas a été généré dans la configuration de *Module > Alertes*, une nouvelle alerte avec le module que vous pouvez voir dans la capture d'écran.

216.58.208.0 - Alert ?

Alert control filter

Module: Host Alive Latest value: 1.00 Template: Critical condition Create Template

Actions: Mail to Admin Create Action Threshold: 0 seconds ?

Add alert

Une fois l'alerte déclenchée, nous observons comment elle atteindra le mail choisi dans l'action :

[PANDORA] Alert from agent 2003 on module Host Alive • Pandora FMS • 10/13

De Pandora FMS <pandora@mydomain.com>
 Asunto [PANDORA] Alert from agent 2003 on module Host Alive
 Para mi

Hello, this is an automated email coming from Pandora FMS

This alert has been fired because a CRITICAL condition in one of your monitored items:

Agent : 2003
 Module: Host Alive
 Module description: Check if host is alive using ICMP ping check.
 Timestamp 2013-05-10 12:52:13
 Current value: 0.00

Thanks for your time.

Best regards
 Pandora FMS

Configuration d'email avec une compte Office365

Pandora FMS peut utiliser Office365® par le biais de la configuration suivante :

- Vous devez avoir une compte sur Office365.

- Allez vers la [configuration générale de la Console](#) ou vers la configuration du [serveur Pandora FMS](#) et entrez vos identifiants (domaine web Office365, noms d'utilisateur, mot de passe, etc.).

Corrélation des alertes : alertes dans les événements et les journaux

Avec Pandora vous pouvez créer des alertes basées sur les événements reçus ou sur les logs collectés avec le [système de collecte de journaux](#). Vous pouvez créer des alertes simples ou plus complexes, basées sur un ensemble de règles avec des relations logiques. Cette fonctionnalité remplace la précédente des alertes d'événements.

Les alertes de *log* ne s'exécutent pas dans le Command Center (Metaconsole).

Ce type d'alertes permet de travailler dans une perspective beaucoup plus flexible, car les alertes ne sont pas générées en fonction de l'état d'un module spécifique, mais d'un événement qui peut avoir été généré par plusieurs modules différents, depuis différents agents.

Les alertes d'événements/journaux sont basées sur des règles de filtrage qui utilisent des opérateurs logiques:

- and
- or
- xor
- nand
- nor
- nxor

Ils recherchent les événements/expressions dans les journaux qui correspondent aux règles de filtrage configurées, et si des correspondances sont trouvées, l'alerte sera déclenchée.

Ils utilisent également des modèles pour définir certains paramètres, tels que les jours pendant lesquels l'alerte fonctionnera ; cependant, dans ce cas, les modèles ne déterminent pas quand l'alerte d'événement est déclenchée, mais c'est à travers les règles de filtrage qu'ils rechercheront et déclencheront les alertes des événements correspondants.

Il est recommandé d'utiliser un nouvel éditeur de règles, ce qui permet de construire les règles de manière visuelle. Pendant un certain temps, vous pourrez continuer à utiliser l'ancien éditeur d'alertes d'événements.

En raison du nombre élevé d'événements que la base de données Pandora FMS peut héberger, le serveur travaille

sur une fenêtre d'événements maximum, qui est définie dans le fichier de configuration `pandora_server.conf` via le paramètre `event_window`. Les événements générés en dehors de cette fenêtre temporelle ne seront pas traités par le serveur, il n'est donc pas utile de spécifier dans une règle une fenêtre temporelle supérieure à celle configurée dans le serveur.

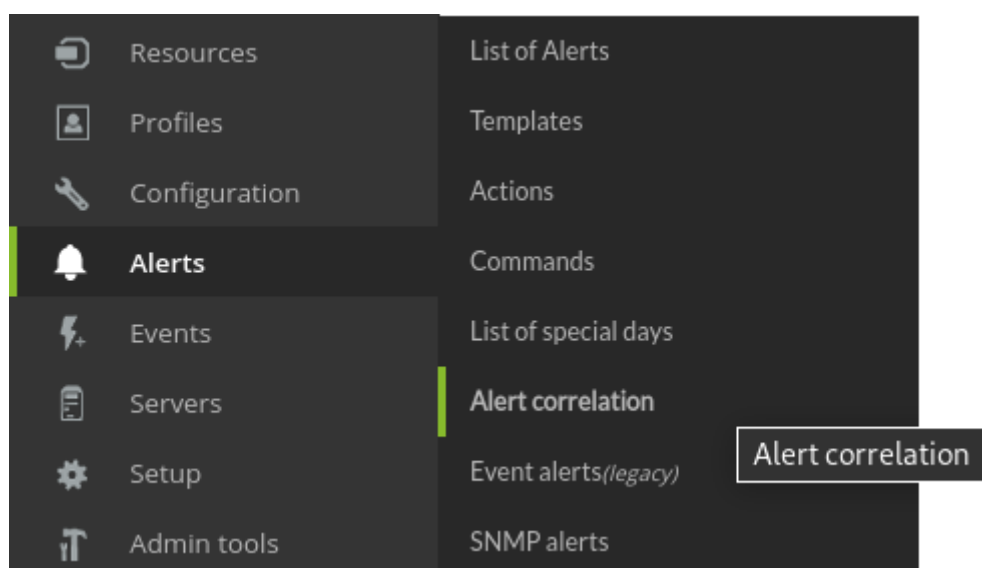
Lors de la définition des alertes sur des événements, il sera nécessaire d'indiquer les paramètres agent, module et événement.

Création d'alertes de corrélation

Afin que les alertes de corrélation d'événements fonctionnent, il faut activer le serveur de corrélation d'événements avec le paramètre `eventserver 1` dans le fichier de configuration du serveur Pandora FMS.

Alertes de corrélation / modèles






























Pour configurer une alerte corrélée, accédez à la section Alert correlation du menu.





Dans cette vue globale, on peut regarder les champs suivants :

Correlated alerts

> Filters

Sort	Name	Group	Matched	Triggered	Action	Options	
	test custom fields				Monitoring Event (Until 10 Threshold 1 days)	     	<input type="checkbox"/>
	Sample secondary groups rule				No associated actions	    	<input type="checkbox"/>
	testpat				Mail to Admin (On 3 Threshold 1 days)	     	<input type="checkbox"/>

Validate 

Create 

Sort

Il marque l'ordre d'évaluation d'alertes corrélées en évaluant s'il est configuré en tant que pass ou drop. Si elle est en haut de la liste, l'alerte sera évaluée plus tôt.

Name

Nom de l'alerte.

Group

Groupe dans lequel elle est organisée. L'utilisateur pourra regarder seulement les groupes auxquels il appartient, à moins que cet utilisateur appartienne spécifiquement au groupe TOUS (ALL).

Matched

Combien de fois un événement qui correspond à la règle de déclenchement dans le seuil actuel a été détecté.

Triggered

Combien de fois l'alerte a été lancée dans le seuil qui a été configuré.

Action

Il montre les actions configurées dans l'alerte.

Options

Il permet d'opérer avec l'action désactivée, sous mode standby, ajouter plus d'actions, éditer ou

supprimer l'alerte corrélée.

Créez une règle et définissez sa performance (le processus est similaire à la création d'Alert Templates) :

Global alerts / [Configure](#) / Conditions / Rules / Fields / Triggering

Configure ?

Name

SSL Certificate Expiration

Group

All

Description

Priority

Critical

Next >

Global alerts / [Configure](#) / [Conditions](#) / Rules / Fields / Triggering

Conditions ?

Days a week

Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun ☒

Use special days list

☐

Time

from 12:00:00 to 12:00:00

Execute alert

from 0 to 1 times in 1 day threshold.

Rule evaluation mode

Pass

Grouped by

None

Next >

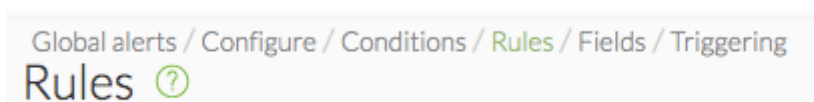
Les paramètres de configuration des modèles pour les alertes de corrélation sont similaires à ceux d'une alerte de module. Il n'y a que deux paramètres spécifiques aux alertes d'événements :

- Mode d'évaluation des règles (Rule evaluation mode) : Peut être Pass ou Drop. Pass signifie que si un événement coïncide avec une alerte, le reste des alertes continuera à être évalué. Drop signifie que si un événement coïncide avec une alerte, le reste des alertes ne sera pas évalué.
- Groupe (Group by) : Permet de regrouper les règles par agent, module, alerte ou groupe. Par exemple, si une règle est configurée pour sauter lorsque deux événements critiques sont reçus et qu'elle est groupée par agent, deux événements critiques doivent arriver du même agent. Il peut être désactivé.

Dans le cas d'alertes contenant des règles de journalisation, cela n'affectera que le regroupement par agent. Si vous choisissez un groupe différent, les alertes basées sur les entrées du journal ne seront jamais remplies.

Chaque règle est configurée pour sauter à un certain type d'événement ou de correspondance de journal ; lorsque l'équation logique définie par les règles et leurs opérateurs est satisfaite, l'alerte se déclenche.

Règles dans une alerte de corrélation



Pour définir les règles de l'alerte, vous devrez faire glisser les éléments du côté gauche vers la zone de dépôt du côté droit pour construire votre règle.

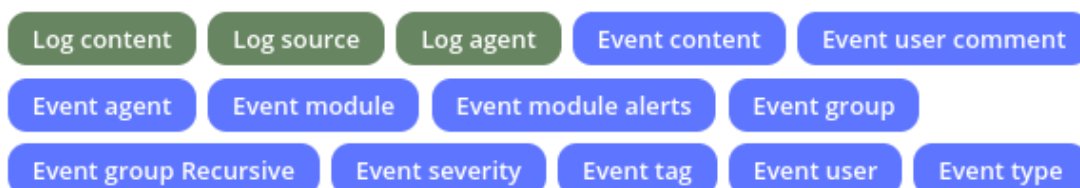
Éléments de configuration disponibles :

Available items

Block:



Fields:



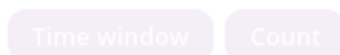
Operators:



Variables



Modifiers:



Nexos:



Ces éléments seront activés pour guider l'utilisateur dans le respect de la grammaire de la règle.
Vous trouverez ci-dessous une explication simplifiée de la grammaire à utiliser :

```
S -> R | R NEX0 R
R -> CAMPO OPERADOR C | CAMPO OPERADOR C MODIFICADOR
C -> VARIABLE
```

Où S est l'ensemble des règles définies pour l'alerte corrélée.

Il sera nécessaire de faire glisser l'élément sur la zone de définition des règles :

Rule definition

Drop here

Cleanup

Reset

De manière que l'image ressemble a celle-ci par exemple :

Available items

Block:

()

Fields:

Log content

Log source

Log agent

Event content

Event user comment

Event agent

Event module

Event module alerts

Event group

Event group Recursive

Event severity

Event tag

Event user

Event type

Operators:

>

<

>=

<=

==

!=

REGEX

NOT REGEX

Modifiers:

Time window

Count

Nexos:

AND

NAND

OR

NOR

XOR

NXOR

Rule definition

(

Log content

==

ERROR

AND

Log agent

==

192.168.70.3

Count

1

Time window

any

)

Remove rule

Remove item

Cleanup

Reset

Next

Dans les opérateurs de comparaison == et != les chaînes de texte sont comparées littéralement. Pour plus de flexibilité, considérez utiliser l'opérateur REGEX qui utilise des **Expressions régulières**.

Pour nettoyer et annuler tous les changements, deux boutons sont disponibles: 'Cleanup' et 'Reset'.

Aucun changement ne sera sauvegardé jusqu'à ce que le bouton Next soit pressé.

REMARQUE : Les blocs ont une simultanéité au moment où la condition est remplie.

(A and B)

Elle force l'élément analysé (événement ou journal) à se conformer simultanément à A et B.

A and B

Force les deux règles (A) et (B) à être remplies dans la fenêtre d'évaluation. Cela signifie qu'il doit y avoir dans les dernières secondes (définies par les paramètres log_window et event_window) des

entrées satisfaisant aux deux règles.

Fields dans une alerte de corrélation

Version NG 764 ou ultérieure:

Les macros relatives aux modules et aux agents ne sont pas disponibles dans les champs de la section de récupération puisque la récupération de ces alertes est exécutée lorsque le seuil se termine et qu'il manque un événement de récupération pour obtenir ces informations.

Dans la section précédente [Système d'alertes](#) on explique avec plus de détail le fonctionnement des champs des alertes.

Triggering dans une alerte de corrélation

Dans cette section, vous devez configurer les actions que vous allez faire lorsque l'alerte est déclenchée et indiquer dans quels intervalles et avec quelle fréquence cette action sera exécutée.

Triggering Condition

	Mon	Tue	Wed	Thu	Fri	Sat	Sun	00:00:00 - 23:59:59
	✓	✓	✓	✓	✓	✓	✓	✓
Use special days list	No							
Time threshold	1 days							
Number of alerts (Min./Max.)	0/1							

Dans cette section, on voit un aperçu de la configuration dans la section Conditions pour le garder sur compte lors de la configuration de l'exécution d'une action.

Actions

None

Number of alerts match

to

Treshold

1 day

Add >

Actions	Triggering	Treshold	Options
custom_id	Always	1 d	
Mail to Admin	(From 1 to 3) ✓	1 d	
Restart agent	(1) ✕ (From 2 to 3) ✓	1 d	

Configurez les actions par le biais des champs :

Actions

Action que vous avez besoin d'exécuter.

Number of alerts match

Nombre d'intervalles qui doivent se passer depuis que l'alerte a été déclenchée pour que l'action soit exécutée. Si vous voulez qu'il soit toujours, laissez ces champs vides.

Treshold

Intervalle qui doit se passer pour que l'action soit exécutée à nouveau une fois l'alarme soit déclenchée.

Après, regardez la liste d'actions configurées. Dans cette liste, le champ triggering montre dans quels intervalles de l'alerte l'action sera exécutée, tout comme vous avez configuré dans number of alerts match. En outre, dans la colonne Options vous pouvez supprimer ou modifier les actions configurées.

Alertes multiples corrélées

Lorsque nous avons plusieurs alertes, elles ont un ordre d'évaluation spécifique. Ils seront toujours évalués dans l'ordre en commençant par le premier de la liste.

Si nous configurons le mode d'évaluation des règles PASS, si une alerte corrélée est exécutée, les éléments suivants seront également évalués. C'est le mode 'normal'.

Si l'on configure le mode d'évaluation des règles DROP, si une alerte corrélée configurée avec ce mode est exécutée, l'évaluation des règles ci-dessous sera arrêtée. Cette fonction nous donne la possibilité d'une protection d'alerte en cascade.

Par exemple :

- Alerte générique.
- Alerte spécifique.

Si l'alerte générique échoue, il n'est pas nécessaire d'évaluer l'alerte spécifique. Configurez les deux avec DROP.

















Cliquez sur l'icône de tri et faites-la glisser pour modifier l'ordre dans lequel les règles sont évaluées.


Pandora FMS
the Flexible Monitoring System


Enter keywords to search

Correlated alerts ?

> Filters

Sort elements	Group	Matched	Triggered	Action	Options
	sample2			Monitoring Event (Always)	    
	sample			Mail to Admin (From 1 to 3 Threshold 1 days)	    

Validate 

Create 

Les autres règles de corrélation (champs d'action et application des actions) fonctionnent de la même manière que les autres alertes Pandora FMS et ne nécessitent aucune explication supplémentaire.

Macros d'alertes d'événements

Liste de macros

Les macros de commandes, macros d'actions et macros d'alerte d'événement sont communes entre eux mais avec les exceptions suivantes: `_modulelaststatuschange_`, `_rca_` et `_secondarygroups_`

`_address_`

Adresse de l'agent qui a déclenché l'alerte.

`_address_n_`

L'adresse de l'agent qui correspond à la position indiquée dans "n". Exemple : `adress_1_`, `adress_2_`.

`_agent_`

Alias de l'agent qui a déclenché l'alerte. Si aucun alias n'est attribué, le nom de l'agent est utilisé.

`_agentalias_`

Alias de l'agent qui a lancé l'alerte.

`_agentcustomfield_n_`

Numéro de champ personnalisé n de l'agent (ex. `_agentcustomfield_9_`).

`_agentcustomid_`

ID d'agent personnalisé.

`_agentdescription_`

Description de l'agent qui a déclenché l'alerte.

`_agentgroup_`

Nom du groupe d'agents.

`_agentname_`

Nom de l'agent qui a déclenché l'alerte.

`_agentos_`

Système d'exploitation de l'agent.

agentstatus État actuel de l'agent.

_alert_critical_instructions_

Instructions contenues dans le module pour un état CRITIQUE.

_alert_description_

Description de l'alerte.

_alert_name_

Nom de l'alerte.

_alert_priority_

Priorité numérique de l'alerte.

_alert_text_severity_

Priorité dans le texte d'alerte (Maintenance, Informatif, Normal Minor, Avertissement, Major, Critique).

_alert_threshold_

Seuil d'alerte.

_alert_times_fired_

Nombre de fois où l'alerte a été déclenchée.

_alert_unknown_instructions_

Instructions contenues dans le module pour un état UNKNOWN.

_alert_warning_instructions_

Instructions contenues dans le module pour un état WARNING.

_all_address_

Toutes les adresses de l'agent qui a déclenché l'alerte.

_critical_threshold_max_

Seuil critique maximal.

`_critical_threshold_min_`

Seuil critique minimal.

`_data_`

Données qui ont déclenché l'alerte.

`_email_tag_`

Emails associés aux tags du module.

`_event_cfX_`

(Uniquement les alertes d'événements). Clé du champ personnalisé de l'événement qui a déclenché l'alerte. Par exemple, s'il existe un champ personnalisé dont la clé est IPAM, sa valeur peut être obtenue en utilisant la macro `_event_cfIPAM_`.

`_event_description_`

(Alertes d'événements uniquement). Description textuelle de l'événement Pandora FMS.

`_event_extra_id_`

(Uniquement les alertes d'événements). Extra Id.

`_event_id_`

(Uniquement les alertes d'événements). Id de l'événement qui a déclenché l'alerte.

`_event_text_severity_`

(Alertes événements uniquement). Priorité dans le texte de l'événement qui déclenche l'alerte (Maintenance, Informational, Normal Minor, Warning, Major, Critical).

`_eventTimestamp_`

Horodatage dans lequel l'événement a été créé.

`_fieldX_`

Champ C défini par l'utilisateur.

`_group_contact_`

Coordonnées du groupe. Il est configuré lors de la création du groupe.

`_groupcustomid_`

ID de groupe personnalisé.

`_groupother_`

Autres informations sur le groupe. Il est configuré lors de la création du groupe.

`_homeurl_`

C'est un lien de l'URL publique qui doit être configuré dans les options générales de la configuration.

`_id_agent_`

Agent ID, utile pour construire l'URL d'accès à la console Pandora FMS.

`_id_alert_`

Alert ID, utile pour exécuter l'alerte dans des outils tiers.

`_id_group_`

ID du groupe d'agents.

`_id_module_`

ID module.

`_interval_`

Intervalle d'exécution du module.

`_module_`

Nom du module.

`_modulecustomid_`

ID personnalisé du module.

`_moduledata_X_`

En utilisant cette macro ("X" est le nom du module en question) on collecte les dernières données de ce module et s'il est numérique, on le retourne formaté avec les décimales spécifiées dans la configuration de la console et avec son unité (si elle le possède). Il serait utile, par exemple, lors de l'envoi d'un e-mail lors du saut d'une alerte de module, envoyer également des informations supplémentaires (et peut-être très pertinentes) à partir d'autres modules du même agent.

Si le nom du module contient des espaces, ceux doivent être entrés en tant qu'entité HTML :

Vous pouvez trouver la [liste d'entités HTML sur Wikipédia](#).

`_moduledescription_`

Description du module.

`_modulegraph_nh_`

(Uniquement pour les alertes qui utilisent la commande eMail). Retourne une image codée en base64 d'un graphique de module avec une période de n heures (ex. `_modulegraph_24h_`). Il nécessite une configuration correcte de la connexion du serveur à la console via api, ce qui se fait dans le fichier de configuration du serveur.

`_modulegraphth_nh_`

(Uniquement pour les alertes qui utilisent la commande `_email_tag_`). Même opération que la macro précédente mais seulement avec les seuils critiques et d'alerte du module, au cas où ils seraient définis.

`_modulegroup_`

Nom du groupe de modules.

`_modulestatus_` État du module.

`_moduletags_`

URLs associées aux balises de module.

`_name_tag_`

Nom des balises associées au module.

`_phone_tag_`

Téléphones associés aux tags de module.

`_plugin_parameters_`

Paramètres du module plugin.

`_policy_`

Nom de la politique à laquelle le module appartient (si applicable).

`_prevdata_`

Données antérieures avant le déclenchement de l'alerte. Il est nécessaire de décommenter la section suivante dans le fichier de configuration du serveur Pandora FMS :

```
# Default texts for some events. The macros _module_ and _data_ are supported.
text_going_down_normal Module '_module_' is going to NORMAL (_data_) with
previous data (_prevdata_)
#text_going_up_critical Module '_module_' is going to CRITICAL (_data_)
#text_going_up_warning Module '_module_' is going to WARNING (_data_)
#text_going_down_warning Module '_module_' is going to WARNING (_data_)
#text_going_unknown Module '_module_' is going to UNKNOWN
```

Le processus du serveur doit être redémarré pour que les nouvelles modifications soient appliquées.

`_rca_`

Chaîne d'analyse des causes profondes (uniquement pour les services).

`_server_ip_`

IP du serveur auquel l'agent est affecté.

`_server_name_`

Nom du serveur auquel l'agent est affecté.

`_target_ip_`

Adresse IP de la cible du module.

`_target_port_`

Port cible du module.

`_time_down_human_`

Heure au format long, par exemple "1day 10h 35m 40s" (cette macro ne fonctionne que pour les alertes de récupération).

`_time_down_seconds_`

Temps en secondes (cette macro ne fonctionne que pour les alertes de récupération).

`_timestamp_`

Heure et date du déclenchement de l'alerte.

timezone

Fuseau horaire représenté dans _timestamp_.

_warning_threshold_max_

Seuil d'alerte maximum.

_warning_threshold_min_

Seuil d'alerte minimum.

[Retour à l'index de documentation du Pandora FMS](#)