

LoriotPro V4 Extended Edition

Module de corrélation d'événements de type down/up (BETA)

Lecoïnte Ludovic



Copyright © 2005-2006 LUTEUS SARL. All rights reserved. This documentation is copyrighted by LUTEUS SARL. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying or otherwise, without the prior express written permission of LUTEUS SARL

Sommaire

LoriotPro V4 Extended Edition.....	1
Module de corrélation d'événements de type down/up (BETA)	1
Introduction	2
Exemple d'utilisation	3
Paramètre de polling d'un host.....	4
Filtrage	5
Événement de type down	5
Événement de type UP	10
Exemple sur un groupe de machines.....	13
Problème posé par l'algorithme	15

Introduction

La corrélation d'événements permet de surveiller un ou des enchaînement(s) d'événements attendus et consécutifs sur une période de temps bornée. L'apparition ou l'absence de la séquence d'événements attendus permet d'alerter un administrateur d'une anomalie de fonctionnement.

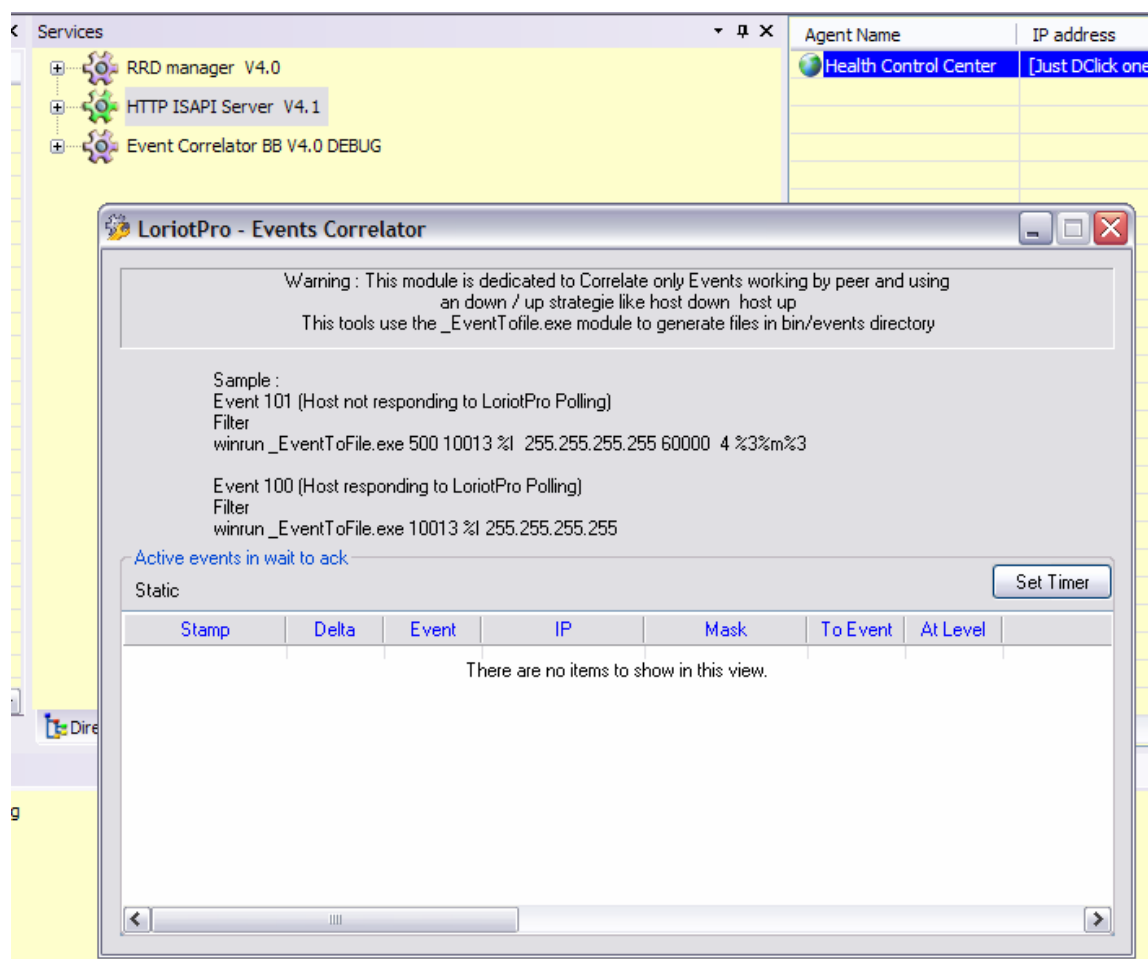
Il est fréquent que dans un contexte de supervision des événements ne doivent déclencher une action qu'après un certain laps de temps. Ce temps étant mis à profit pour recevoir un autre événement qui annulerait le premier.

La corrélation peut de cette façon s'appliquer à tous les événements qui fonctionnent par paires avec un événement d'alarme puis un événement d'acquiescement de cette alarme.

Dans le cas des Trap SNMP il sera nécessaire de créer un événement LoriotPro pour chaque Trap (Utilisation des filtres de TRAP) si l'on veut utiliser le module (Plugin) de corrélation.

L'exemple le plus fréquemment rencontré ou la corrélation de Trap se justifie est celui des interfaces réseaux qui peuvent momentanément être hors service (envoi d'un Trap Link down) suivi dans les secondes qui suivent d'un retour à la normal « link up ». La corrélation permet ici de surveiller l'intervalle de temps entre le Link Down et le Link Up et d'informer l'administrateur en cas de non retour à l'état UP dans un délai prédéfini.

Un nouveau Plugin de service LoriotPro associé à un programme indépendant (utilitaire DOS) permet de corréler des événements successifs.



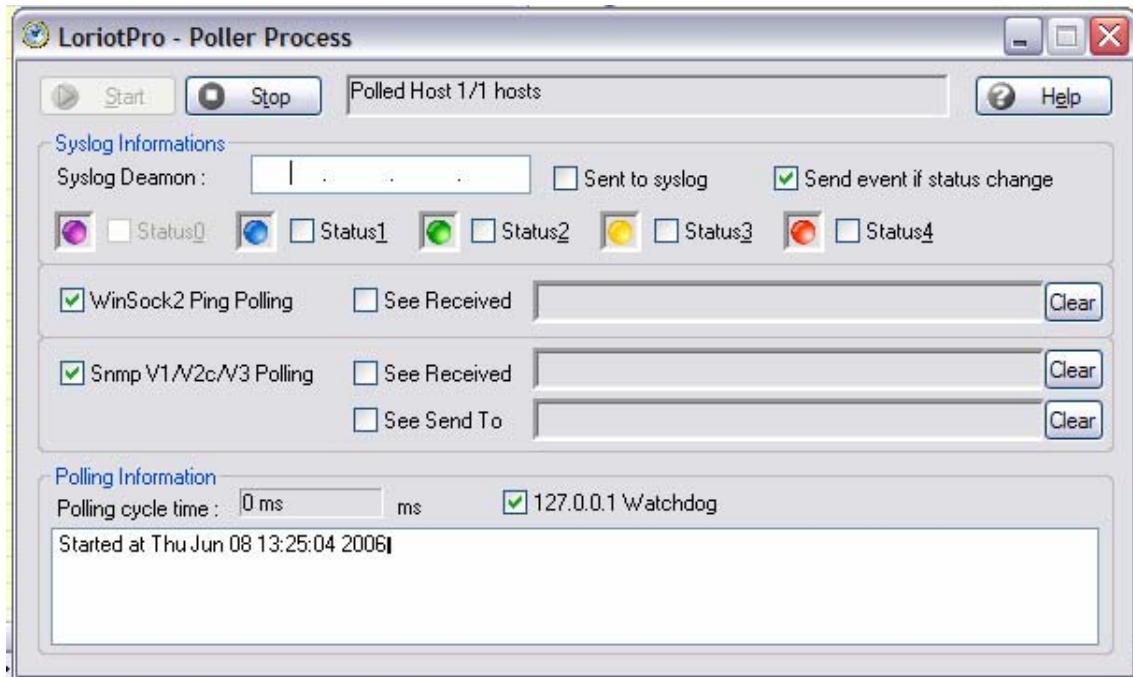
Le plugin « Event Correlator » doit être chargé dans les services pour activer le mécanisme de corrélation.

Exemple d'utilisation

Pour expliquer le principe d'utilisation de ce plugin il sera fait appel à un exemple simple et classique.

Un host passe en état « down » (il ne répond plus au polling de LorientPro) mais on désire lui donner le temps de repasser « up » (le host répond de nouveau au polling). Si il ne repasse pas « up » dans un temps donné alors on génère un événement pour prévenir l'administrateur du réseau.

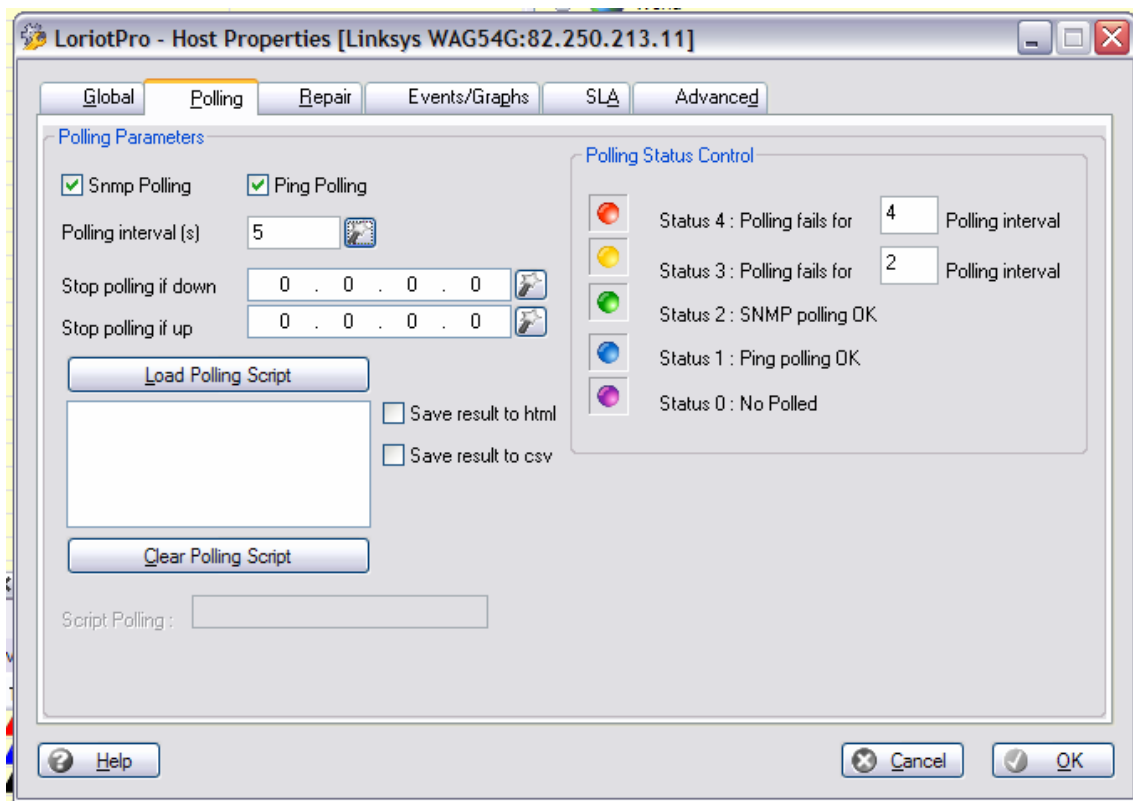
LorientPro émet un message référencé 101 lorsqu'un host passe down (level 4)
Et un message 100 lorsque le host passe up (level 1 ou 2)



Cette option se configure avec le module Poller Process.

Paramètre de polling d'un host

Les paramètres de polling d'un host sont définis dans le module de propriété du host.



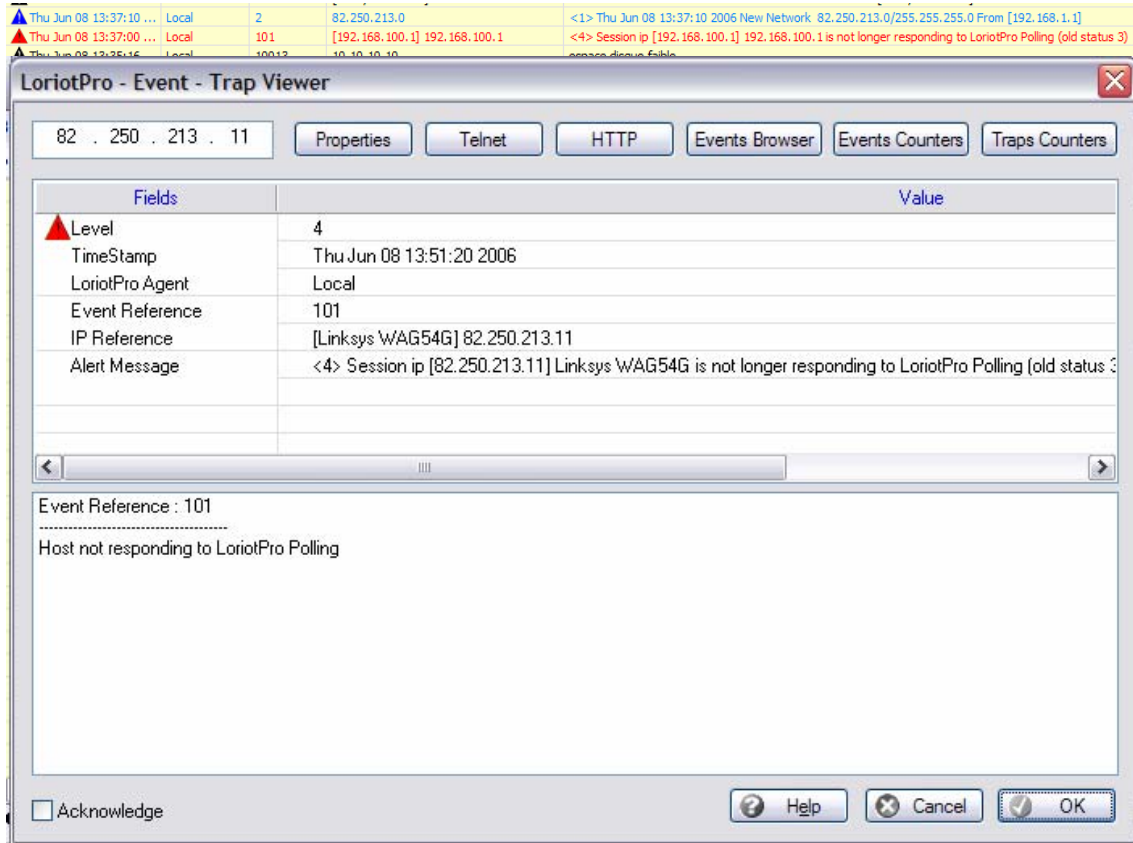
Not For Public Diffusion

Ce host sera down après 4 non réponse (4*5) = 20 s « environ » et un événement 101 sera émit avec les paramètres du host concerné.

Filtrage

Événement de type down

Il est possible de définir un filtre sur la réception de l'événement 101 qui va réaliser une action de mémorisation de l'événement.



Le message 101 suivant :

```
<4> Session ip [82.250.213.11] Linksys WAG54G is not longer responding to LorientPro Polling (old status 3)
```

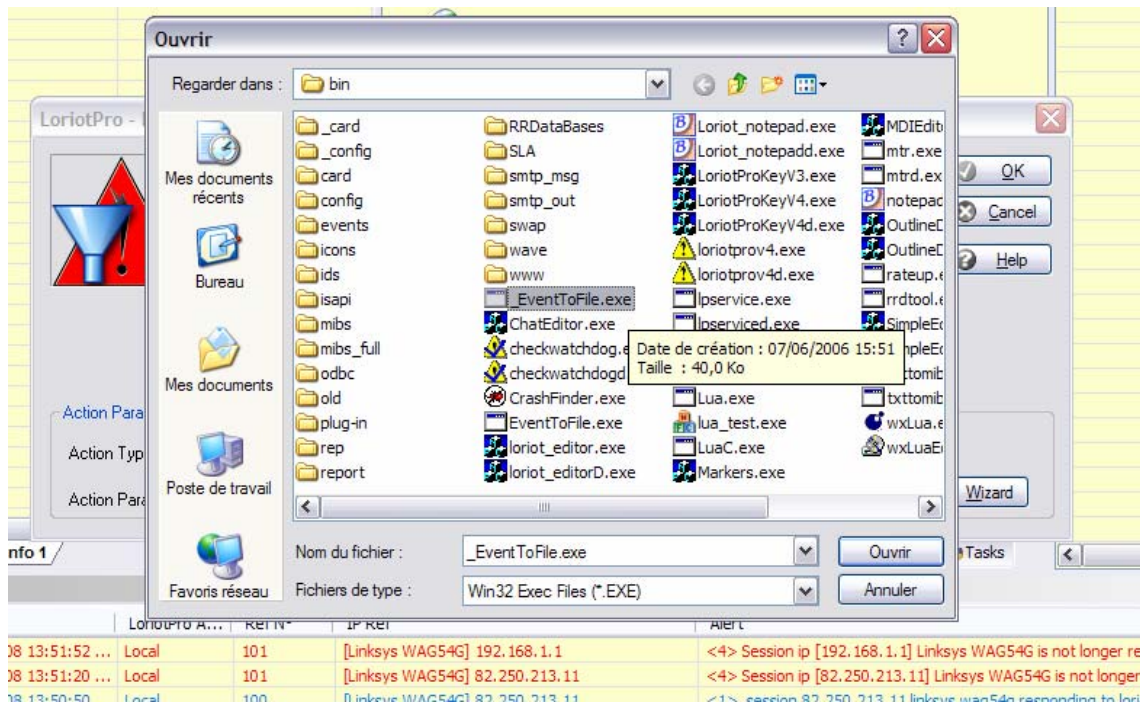
Nous indique que le host 192.168.100.1 ne répond plus (down) et que son ancien statut était 3.

IP Ref	Alert
[Linksys WAG54G] 192.168.1.1	<4> Session ip [192.168.1.1] Linksys WAG54G is not longer res
[Linksys WAG54G] 82.250.213.11	<4> Session ip [82.250.213.11] Linksys WAG54G is not longer r
[Linksys WAG54G] 82.250.213.11	<1> session 8
[Linksys WAG54G] 82.250.213.11	<1> session 8
192.168.1.0	<1> Thu Jun 0
[Linksys WAG54G] 82.250.213.11	<0> Thu Jun 0
82.250.213.0	<1> Thu Jun 0
[192.168.100.1] 192.168.100.1	<4> Session ip
10.10.10.10	espace disque
10.10.10.10	espace disque
10.10.10.10	espace disque
10.10.10.10	espace disque
10.10.10.10	espace disque
10.10.10.10	espace disque
10.10.10.10	service smtpv
10.10.10.10	service smtpscheduler v1.0

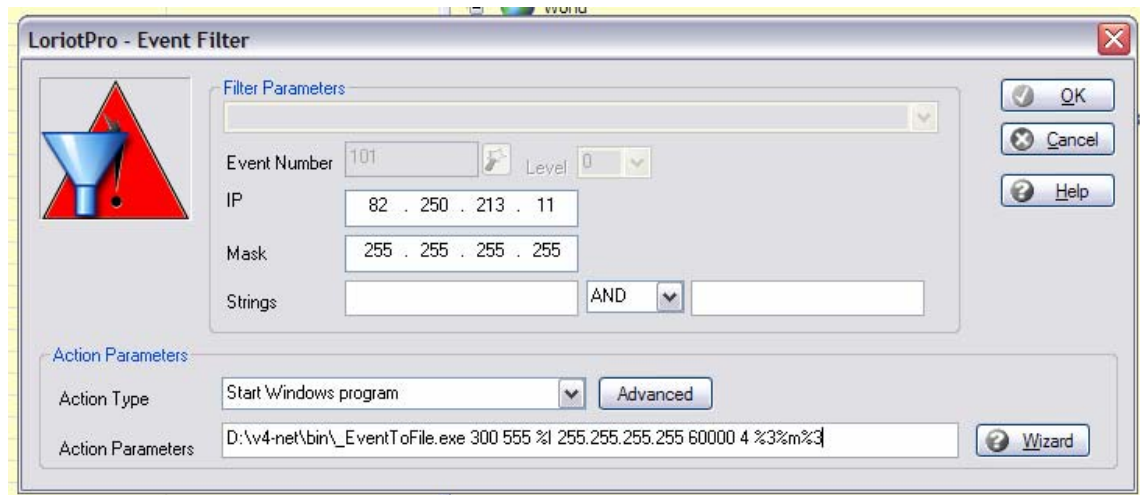
TimeStamp	LorientPro A...	RefN°	IP Ref	Alert
Thu Jun 08 13:51:52 ...	Local	101	[Linksys WAG54G] 192.168.1.1	<4> Session ip [192.168.1.1] Linksys WAG54G is not longer responding to LorientPro Polling (old status 3)
Thu Jun 08 13:51:20 ...	Local	101	[Linksys WAG54G] 82.250.213.11	<4> Session ip [82.250.213.11] Linksys WAG54G is not longer responding to LorientPro Polling (old status 3)

Le wizard nous propose de créer un nouveau filtre d'événement.

On choisit « Start Windows program »



On sélectionne le programme `_EventToFile.exe` présent dans le répertoire `bin` de LorientPro.

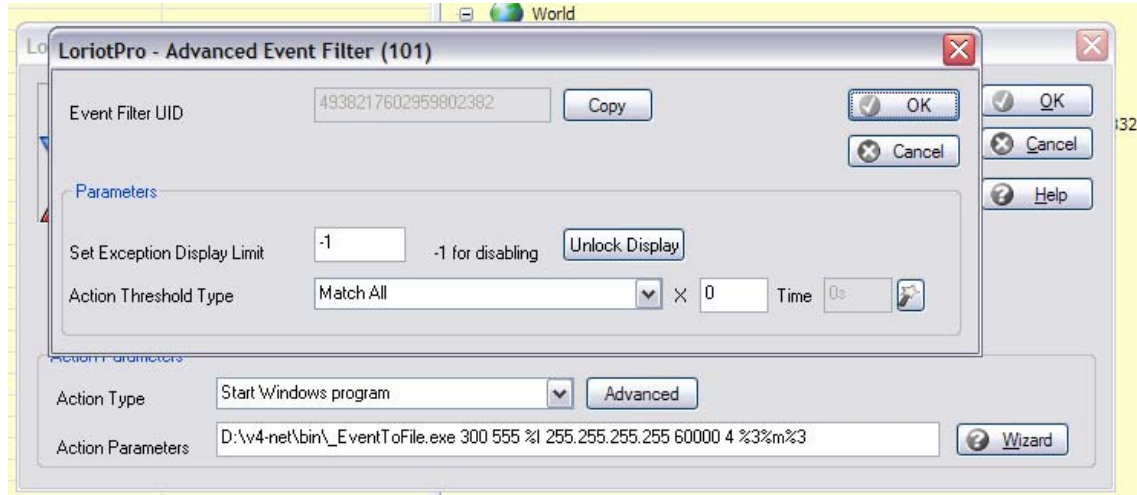


On utilise la syntaxe suivante :

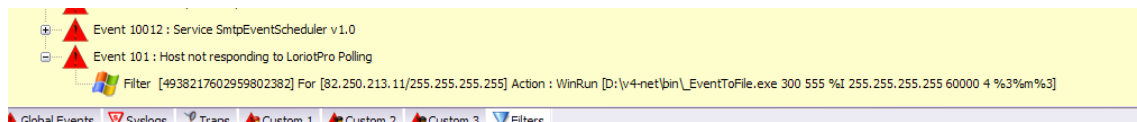
`_EventToFile temps numero ip mask numero_event level %3message%3`

temps	le temps d'attente en secondes avant d'envoyer un nouveau message avec le numero_event et le level contenant le message.
numero	une référence pour identifier l'événement sauvegardé
ip	l'adresse IP concerné par cet événement, ici la variable %l est utilisée
mask	le mask de l'adresse IP
numero_event	le numéro d'événement utilisé pour envoyer un événement si cette événement n'est pas acquitté dans (temps) secondes
level	le level du message renvoyer (0-9)
message	le message accompagnant l'émission de l'événement ici on réutilise le message

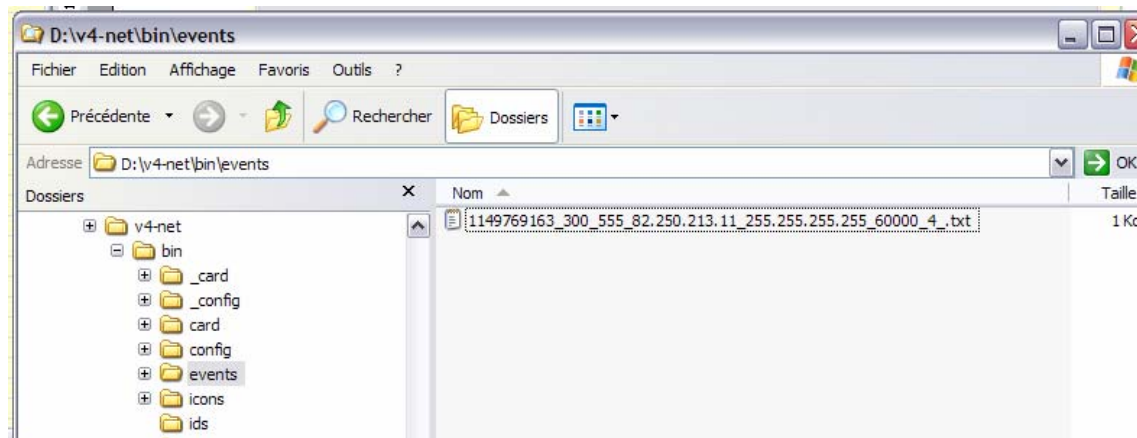
d'origine %3%m%3 le message doit être encadré par %3message%3 si il contient des blancs. Il ne doit pas contenir de caractères « .



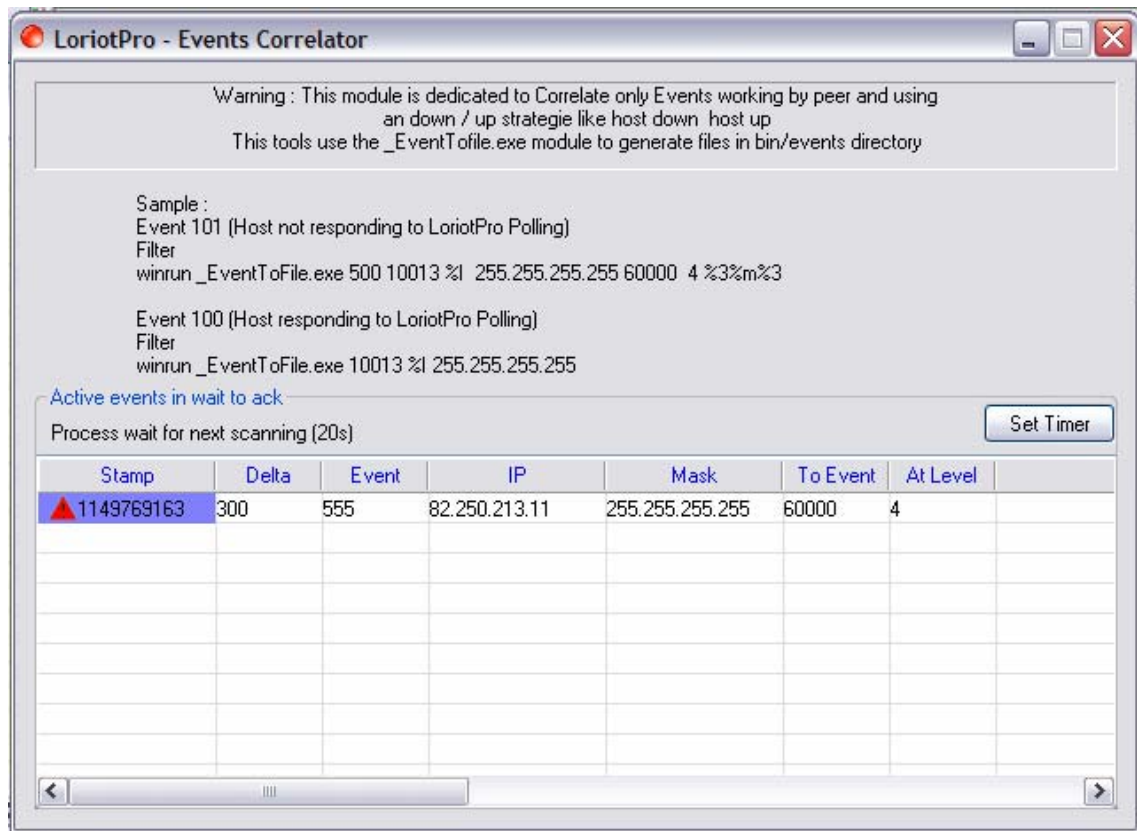
Ont choisie l'option **Match All**.



Maintenant lorsque un message 101 arrive pour ce host il y a un fichier stocké dans le répertoire bin/events



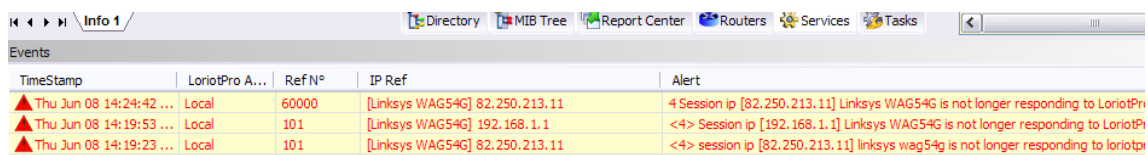
Le plugin de corrélation scanne a intervalle régulier ce répertoire et reroute les messages n'étant pas arrêtés dans les temps.



5 minutes après la mémorisation de ce message un événement 60000 au level 4 sera envoyé à LorientPro. Si un autre message d'annulation n'est pas envoyé à temps. Par défaut le plugin balaye le répertoire toutes les 20secondes mais il est possible de changer ce paramètre (minimum 5s)



Le message 60000 pourra être filtré à son tour par LorientPro et réaliser une action différente.



Événement de type UP

Il est possible de définir un filtre sur la réception de l'événement 100 qui va réaliser une action d'acquiescement de l'événement. L'événement 100 est utilisé pour différent type de passe du host dans un état up il faudra donc analyser les variable de l'événement.

IP Ref	Alert
[Linksys WAG54G] 192.168.1.1	<1> session 192.168.1.1 linksys wag54g responding to loriopro snmp polling (old status 1)
[Linksys WAG54G] 192.168.1.1	<1> session 192.168.1.1 linksys wag54g responding to loriopro ping polling (old status 4)
[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to loriopro snmp polling (old status 1)
[Linksys WAG54G] 192.168.1.1	<4> Session ip [192.168.1.1] Linksys WAG54G is not longer responding to LorientPro Polling (old status 4)
[Linksys WAG54G] 82.250.213.11	<4> Session ip [82.250.213.11] Linksys WAG54G is not longer responding to LorientPro Polling (old status 4)
[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to loriopro snmp polling (old status 1)

LorientPro - Event - Trap Viewer

82 . 250 . 213 . 11

Properties Telnet HTTP Events Browser Events Counters Traps Counters

Fields	Value
Level	1
TimeStamp	Thu Jun 08 13:41:21 2006
LorientPro Agent	Local
Event Reference	100
IP Reference	[Linksys WAG54G] 82.250.213.11
Alert Message	<1> session 82.250.213.11 linksys wag54g responding to loriopro snmp polling (old status 1)

Event Reference : 100

Host responding to LorientPro Polling

Acknowledge

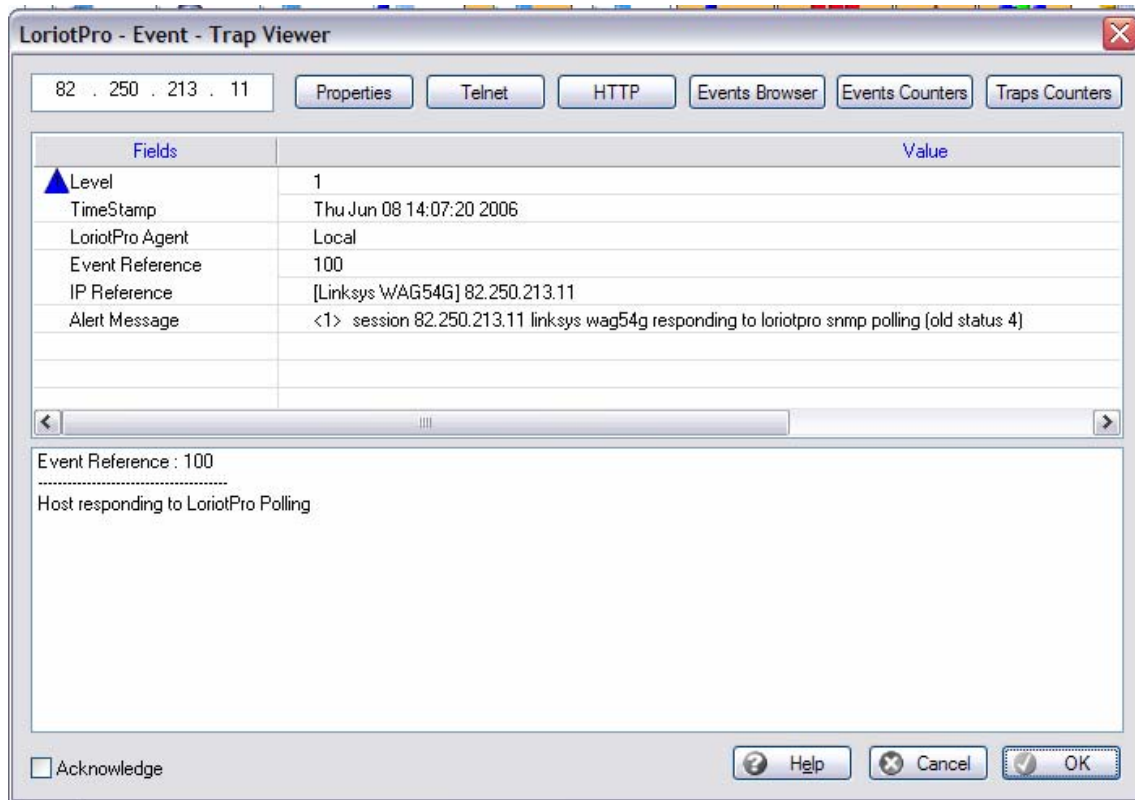
Help Cancel OK

le message 100 suivant :

`<1> session 82.250.213.11 linksys wag54g responding to loriopro snmp polling (old status 1)`

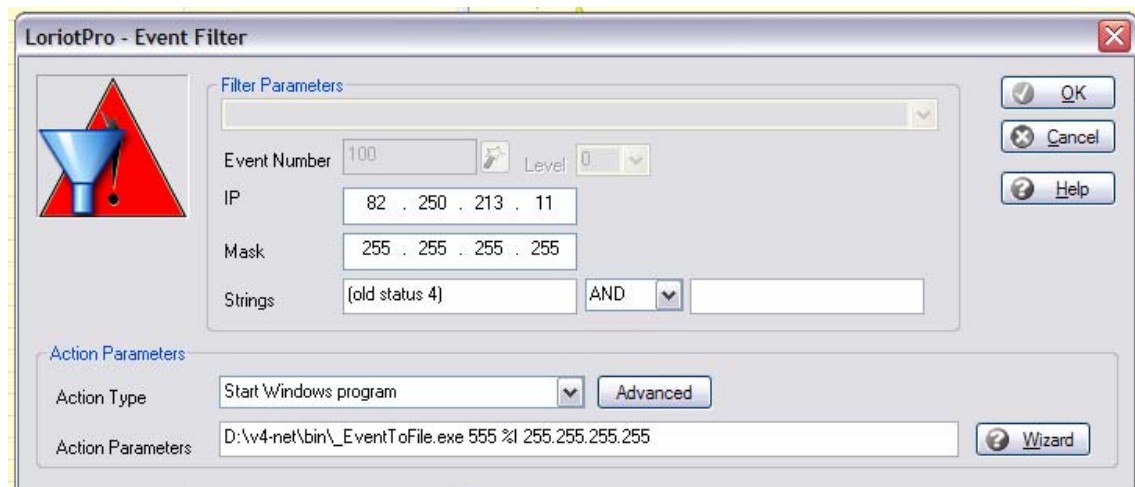
Indique que le host 82.250.213.11 était déjà UP mais a un niveau ICMP (1) uniquement. Ce message ne nous intéresse pas.

Nous sommes uniquement intéressé par un message 100 avec l'information suivante :



<1> session 82.250.213.11 linksys wag54g responding to lorientpro snmp polling (old status 4)

Notre filtre sera plus complexe :



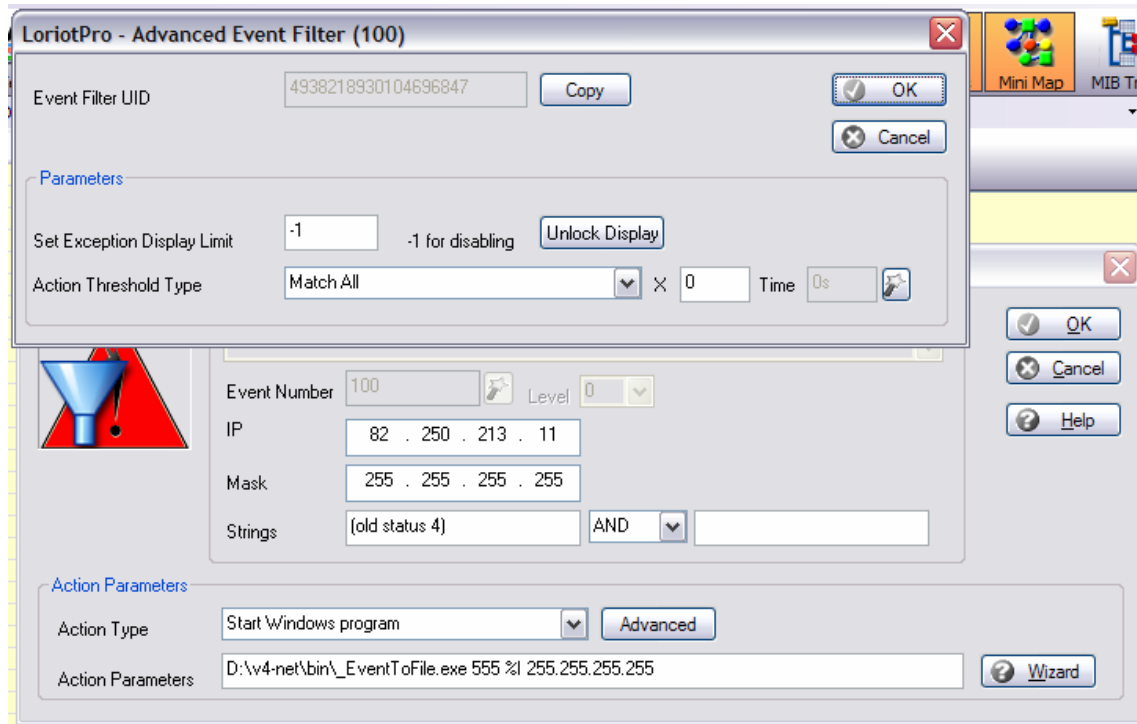
Il intègre une recherche sur la chaîne de caractères (strings) (old status 4) pour être sûr qu'il s'agit bien d'un passage du mode down à un mode up.

La syntaxe utilisée avec le programme `_EventToFile.exe` est différente :

`_EventToFile` numero ip mask

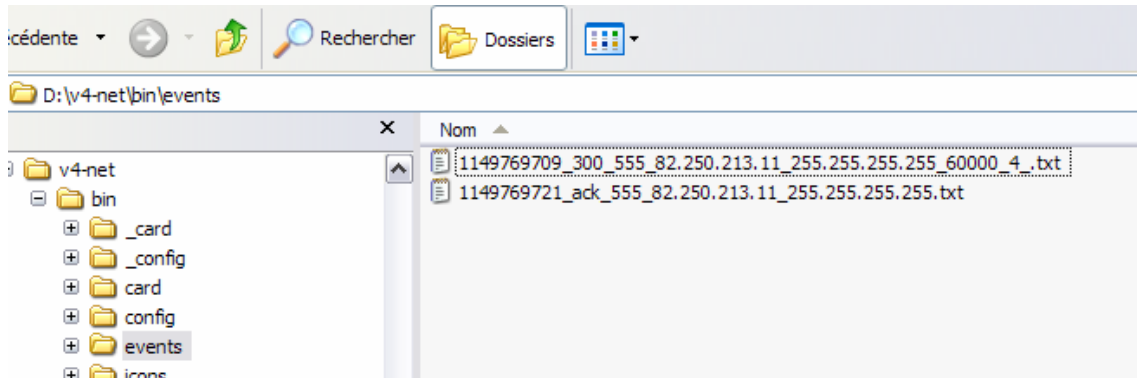
Numéro	une référence pour identifier l'événement sauvegardé
--------	--

IP	l'adresse IP concernée par cet événement, ici la variable %I est utilisée
Mask	le mask de l'adresse IP



On sélectionne l'option « Match all » pour tous les événements de ce type.

A la réception de cet événement un fichier de type **ack** est créé dans le répertoire bin/events



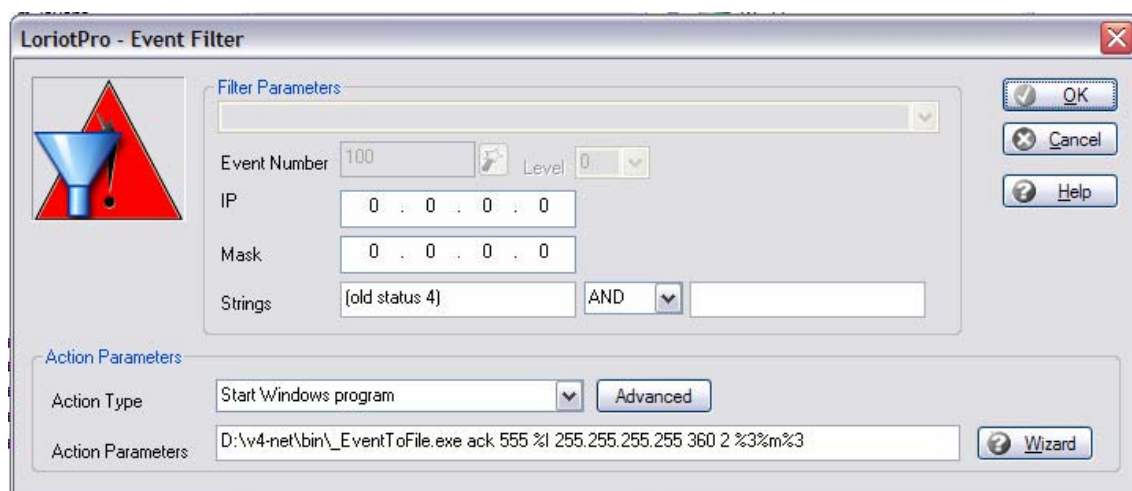
Le plugin de corrélation n'envoie pas le message 60000 et supprime les fichiers.

RefN°	IP Ref	Alert
100	[Linksys WAG54G] 192.168.1.1	<1> session 192.168.1.1 linksys wag54g responding to lorientpro snmp polling (old status 1)
100	[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to lorientpro snmp polling (old status 1)
100	[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to lorientpro ping polling (old status 4)
101	[Linksys WAG54G] 82.250.213.11	<4> session ip [82.250.213.11] linksys wag54g is not longer responding to lorientpro polling (old status 4)
100	[Linksys WAG54G] 192.168.1.1	<1> session 192.168.1.1 linksys wag54g responding to lorientpro snmp polling (old status 1)
100	[Linksys WAG54G] 192.168.1.1	<1> session 192.168.1.1 linksys wag54g responding to lorientpro ping polling (old status 4)
100	[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to lorientpro snmp polling (old status 1)
100	[Linksys WAG54G] 82.250.213.11	<1> session 82.250.213.11 linksys wag54g responding to lorientpro ping polling (old status 4)

Si on désire envoyer un événement sur un acquittement « **ack** » qui arrive trop tard la syntaxe est la suivante :

`_EventToFile ack numero ip mask numero_event level %3message%3`

ack	le mot ack (pour différencier la syntaxe associée a un événement de type down)
Numéro	une référence pour identifier l'événement sauvegardé
IP	l'adresse IP concerné par cet événement, ici la variable %I est utilisée
Mask	le mask de l'adresse IP
Numero_event	le numéro d'événement utilisé pour envoyer un événement si cette événement n'est pas acquitté dans (temps) secondes
Level	le level du message renvoyer (0-9)
Message	le message accompagnant l'émission de l'événement ici ont réutilise le message d'origine %3%m%3 le message doit être encadré par %3message%3 si il contient des blanc. Il ne doit pas contenir de caractère « . »

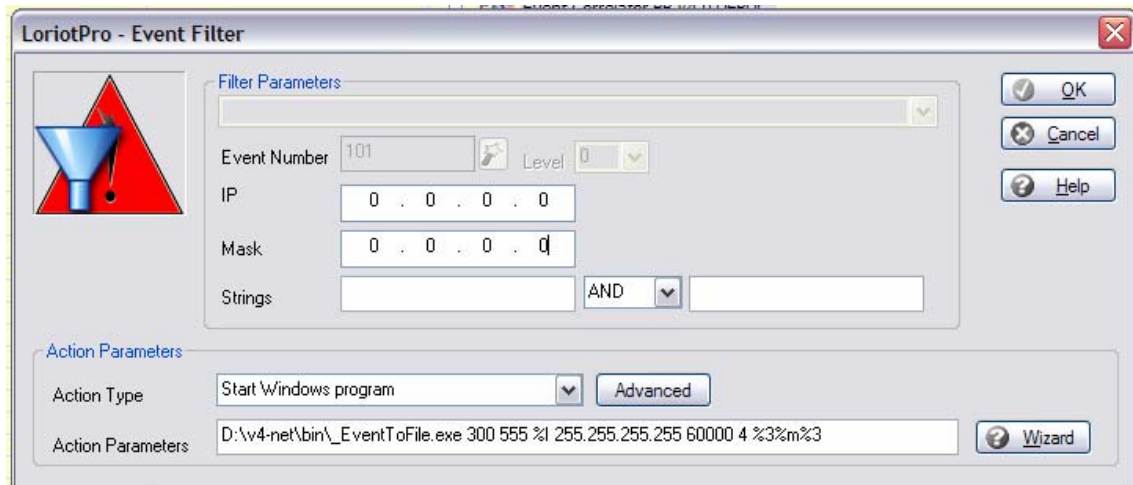


TimeStamp	LorientPro A...	Ref N°	IP Ref	Alert
Sat Jun 10 15:59:28 2006	Local	360	[Linksys ...	1 session 192.168.1.1 linksys wag54g responding to lorientpro snmp polling (old status 4)
Sat Jun 10 15:59:26 2006	Local	100	[Linksys ...	<1> session 192.168.1.1 linksys wag54g responding to lorientpro snmp polling (old status 4)
Sat Jun 10 15:59:03 2006	Local	361	[Linksys ...	4 Session ip [192.168.1.1] Linksys WAG54G is not longer responding to LorientPro Polling (old status 4)
Sat Jun 10 15:58:32 2006	Local	101	[Linksys ...	<4> session ip [192.168.1.1] linksys wag54g is not longer responding to lorientpro polling (old status 4)

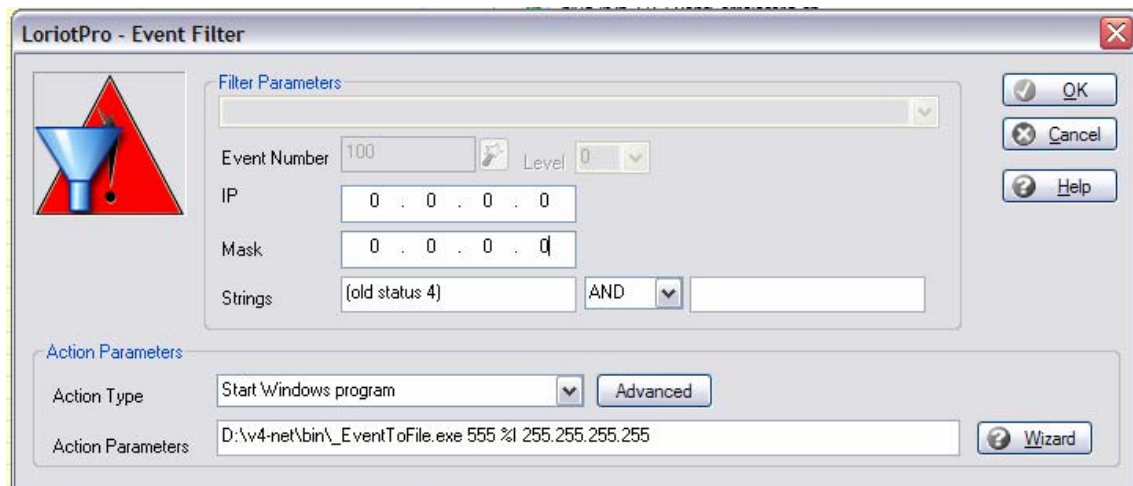
Exemple sur un groupe de machines

On peut vouloir temporiser une action sur l'événement « host down » de façon globale pour éviter les flux de messages « host goes down » en cas de coupure de ligne avec un rétablissement rapide.

Exemple de filtre down sur 101 pour un ensemble de machines (dans notre cas toutes)



Exemple de filtre down sur 100 pour un ensemble de machines



Les fichiers générés seront personnalisés par adresse IP. Dans ce cas car nous utilisons comme variable l'adresse IP du host en défaut.

The screenshot shows the LorientPro - Events Correlator application window. It displays a warning message and sample event filters. Below, a table lists active events in wait to ack. A file explorer window is open, showing a file named '1149770483_30_555_82.250.213.11_255.255.255.255_60000_4_.txt' in the 'D:\v4-net\bin\events' directory.

Warning : This module is dedicated to Correlate only Events working by peer and using an down / up strategie like host down host up
This tools use the _EventToFile.exe module to generate files in bin/events directory

Sample :
Event 101 (Host not responding to LorientPro Polling)
Filter
winrun_EventToFile.exe 500 10013 %I 255.255.255.255 60000 4 %3%m%3

Event 100 (Host responding to LorientPro Polling)
Filter
winrun_EventToFile.exe 10013 %I 255.255.255.255

Active events in wait to ack
Process wait for next scanning (10s) Set Timer

Stamp	Delta	Event	IP	Mask	To Event	At Level
▲ 1149770483	30	555	82.250.213.11	255.255.255.255	60000	4

Info 1

Stamp	LorientPro A...	Ref N°	IP Ref	Alert
Thu Jun 08 14:41:23 ...	Local	101	[Linksys WAG54G] 82.250.213.11	<4> session ip [82.250.213.11] linksys wag54g is not longer responding to

D:\v4-net\bin\events

1149770483_30_555_82.250.213.11_255.255.255.255_60000_4_.txt 1 Ko

▲ Thu Jun 08 14:41:58 ...	Local	60000	[Linksys WAG54G] 82.250.213.11	4 Session ip [82.250.213.11] Linksys WAG54G is not longer responding to LorientPro Polling (old status 3)
▲ Thu Jun 08 14:41:23 ...	Local	101	[Linksys WAG54G] 82.250.213.11	<4> session ip [82.250.213.11] linksys wag54g is not longer responding to lorientpro polling (old status 3)

Problème posé par l'algorithme

Il n'y a pas de lien réel entre le fichier généré au « down » et le fichier généré au « up » (autre que des références temporelles – time stamp) si plusieurs fichiers de type down arrive durant la période down+temps alors un fichier de up peut annulé un fichier down qui n'est pas le sien. C'est pour cela que le système ne marche bien que sur des mécanismes down/up et des paramètres de temps cohérent. Les filtres doivent être le plus précis possible.