



**Séminaire EOLE**  
**Dijon**  
**20-21 Octobre 2008**

**Prelude Manager /**  
**Zephirlogs**





# Introduction

Le module Preludemanager

Le module ZephirLog

Intégration Eole de Prelude

Les différentes sondes disponibles sur les modules

Prospectives.





# PreludeManager (1)

Nouveau module Eole

Permet de détecter des intrusions :

- En corrélant les logs des différents modules et serveurs.

- En utilisant des sondes installés sur les modules

Interface visuelle d'analyse de ces événements.





# PreludeManager (2)

## Utilise Prélude

Systeme de detection d'intrusion hybride.

Se base sur le standard IDMEF

Dispose d'une interface standardisée permettant de communiquer avec différents types de sondes.

Interagit avec des systemes de detections de type NIDS et HIDS.





# ZephirLog <sup>(1)</sup>

Module permettant la centralisation et l'archivage des logs des différents modules Eole installés en établissements (principalement Amon pour le moment).

Utilise rsyslog

Communication chiffrée entre les modules et le serveur ZephirLog

Utilisation de certificats X509 pour authentifier les machines sur ZephirLog





# ZephirLog (2)

Journaux stockés sous forme de fichiers plats avec possibilité de stockage en base de données.

Interagit avec PreludeManager grâce à une sonde d'analyse de logs installée sur le module (PreludeLML)





# Intégration Eole (1)

Nécessite l'inscription des modules au niveau de Zephir.

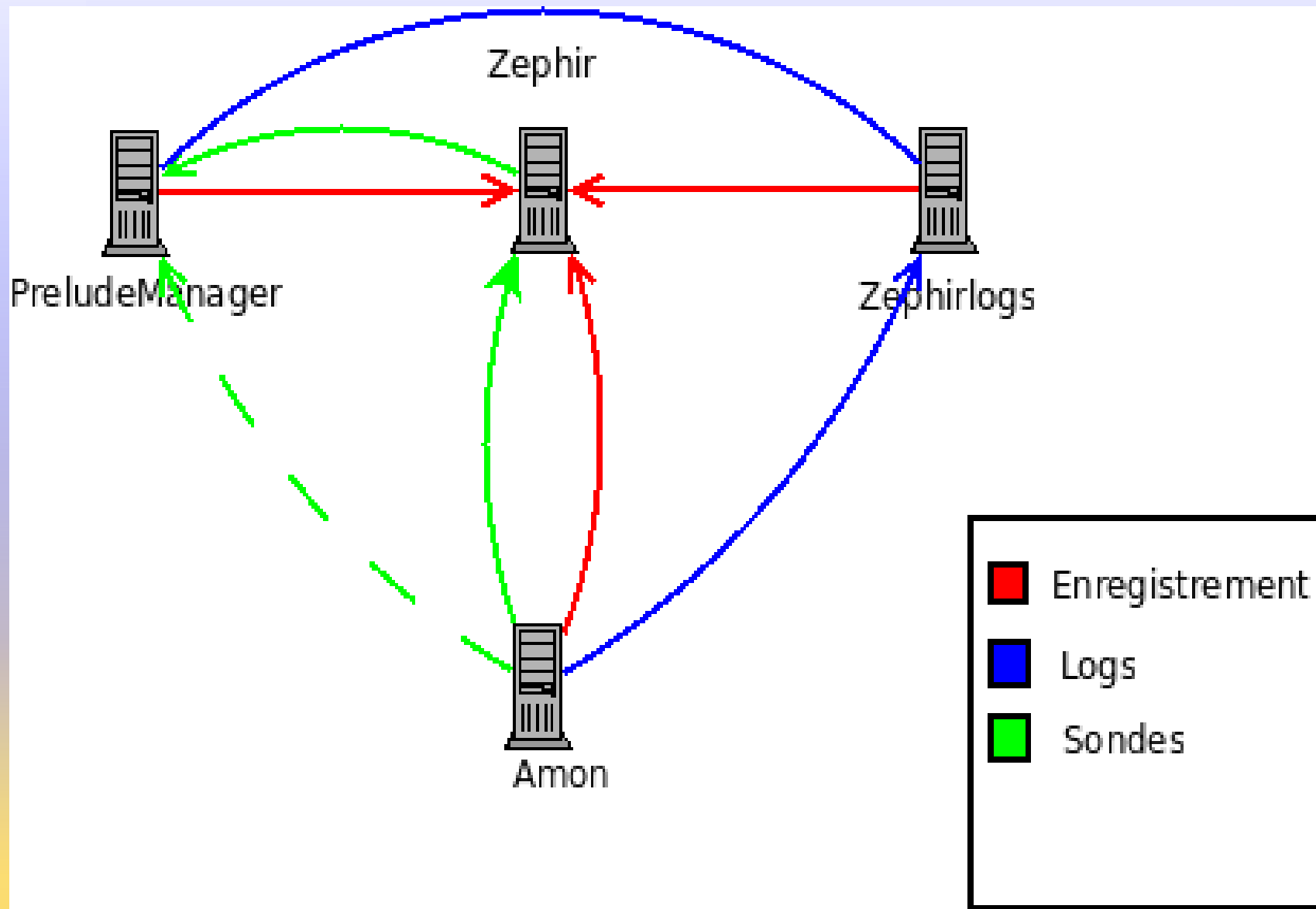
Automatisation des enregistrements des différentes composantes de Prelude sur le module PreludeManager.

Utilise un système de communication XML-RPC sécurisé pour assurer les échanges.

Possibilité de définir certains paramètres de configuration en utilisant `gen_config`.



# Intégration Eole (2)





# Intégration Eole (3)

Configuration (sur pf-amon)

Eichier Zephir Affichage Mode

## Amon

● General	<b>Adresse IP du serveur de log central ZephirLog</b>	<input type="text"/>	Prec	Def
● Services	Activation du chiffrement des transferts (TLS)	Non	Prec	Def
● Interface-ext	Activation du transfert des logs de squid en temps réel	non	Prec	Def
● Interface-1	Heure de debut du transfert des logs	1	Prec	Def
● Interface-2	Heure de fin de transfert des logs	1	Prec	Def
● Logs				





# Intégration Eole (4)

Configuration (sur pf-amon)

Fichier Zephir Affichage Mode

## Amon

- General
- Services
- Interface-ext
- Interface-1
- Interface-2
- Sondes

**Adresse courriel de contact**

**Passerelle SMTP**

**Adresse IP du serveur Prelude Manager**

**Configuration de la sonde SNORT**

Activation de la sonde SNORT

Liste des serveurs SMTP sur le réseau

Liste des serveurs HTTP sur le réseau

Liste des serveurs DNS sur le réseau

**Configuration de la sonde Samhain**

Activation de la sonde SAMHAIN

**Configuration de la sonde NuFW**

Activation de la sonde NuFW





# Intégration Eole (5)

Prewikka ac-dijon. Prelude console

admin on friday 16 october 2009 [logout](#)

Alerts CorrelationAlerts ToolAlerts

Classification	Source	Target	Sensor	Time	
32 x <b>Server recognition</b> (failed)	localhost	192.168.10.172	sshd (zephirlogs.eole.lan)	11:38:44 - 10:39:19	<input type="checkbox"/>
31 x <b>Server recognition</b> (failed)	localhost	n/a	sshd (pf-amon)	11:36:54 - 10:39:24	<input type="checkbox"/>
40 x <b>Proxy ACL violation attempt</b> (failed)	10.21.11.10	n/a	Squid (pf-amon)	11:36:31 - 10:39:32	<input type="checkbox"/>
190 x <b>File Modified</b> (succeeded)	n/a	192.168.10.178	samhain (pf-amon.eole.lan)	10:55:22 - 10:53:27	<input type="checkbox"/>

[Delete](#)

Filter  1  
Period  Hours  
Timezone  Fronten  
Limit  50  By  
Refresh  0:00 1:00   
   
2009-10-16 10:38:47  
2009-10-16 11:38:47  
+02:00  
    
<< < > >>  
1 ... 4 (total:4)





# Intégration Eole (6)

Prewikka ac-dijon. Prelude console

admin on friday 16 october 2009 [logout](#)

Alerts CorrelationAlerts ToolAlerts

Events Agents Settings About

Classification	Source	Target	Sensor	Time	
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:39:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:39:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:36:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:36:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:33:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:33:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:30:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:30:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:27:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:27:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:24:41	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:24:41	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:21:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:21:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:18:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:18:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:15:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:15:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:12:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:12:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:09:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:09:32	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:06:31	<input type="checkbox"/>
Proxy ACL violation attempt (failed) (vendor-specific: TCP_DENIED, vendor-specific: 407)	10.21.11.10	pf-amon Process name: squid (5814)	Squid (pf-amon)	11:06:31	<input type="checkbox"/>

Filter [ ]

Period 1 Hours

Timezone Fronten

Limit 50 By

Refresh 0:00:1:00


Apply Save

2009-10-16 10:39:39  
2009-10-16 11:39:39  
+02:00

prev current next

<< < > >>

1 ... 40 (total: 40)





# Intégration Eole (7)

Prewikka ac-dijon. Prelude console

admin on friday 16 october 2009 [logout](#)

Alerts **CorrelationAlerts** TotalAlerts

Events  
Agents  
Settings  
About

### Alert

Create time	Detect time	Analyzer time
2009-10-16 11:39:31.296275 +02:00	<b>2009-10-16 11:39:31 +02:00</b>	2009-10-16 11:39:31.296406 +02:00

MessageID  
ce30c172-ba37-11de-9835

Text	Severity	Completion	Type	Description
<b>Proxy ACL violation attempt</b>	medium	failed	other	Host 10.21.11.10 tried to violate Squid ACL

Origin	Name	Meaning
vendor-specific	TCP_DENIED	squid_id
vendor-specific	407	squid_status

### Analyzer #2

Name	Class	Manufacturer
<b>Squid</b>	Proxy	www.squid-cache.org

Node name  
pf-amon

Process	Process PID
squid	5814

Analyzer Path (2 not shown)


### Source(0)

Node name (resolved)	Node address
10.21.11.10	10.21.11.10

### Target(0)

Node name  
pf-amon

Process	Process PID
squid	5814





# Intégration Eole (8)

Prewikka ac-dijon. Prelude console

*admin on friday 16 october 2009* [logout](#)

**Agents** | **Heartbeats**

- Events
- Agents**
- Settings
- About


**ac-dijon**

pf-amon.eole.lan	192.168.10.178 bruno.boiget@ac-dijon.fr	Linux	2.6.24-24-eole	Total: 2	2
prelude-manager.eole.lan	192.168.10.160 jsoyer@edenwall.com	Linux	2.6.24-24-eole	Total: 1	1

**ac-dijon.fr**

zephirlogs.eole.lan	192.168.10.172 jsoyer@edenwall.com	Linux	2.6.24-24-eole	Total: 1	1
---------------------	---------------------------------------	-------	----------------	----------	---

Alerts    Heartbeats  





# Les sondes utilisées

Sur Amon :

sonde NIDS (snort)

sonde HIDS (samhain)

sonde NuFW

Sur ZephirLog :

sonde PreludeLML





**Merci de votre attention**





# Prospective

Possibilité d'enregistrer et d'utiliser d'autres sondes sur Amon

Ajout de sondes sur les autres modules (nepentes, Ossec, Sancp)

Ajout facilité par la simple insertion de dictionnaires sur les modules.

