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 évenements.

PreludeManager (2)

Utilise Prélude

- Système de détection 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 systèmes de détections de type NIDS et HIDS.

ZephirLog (1)

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)

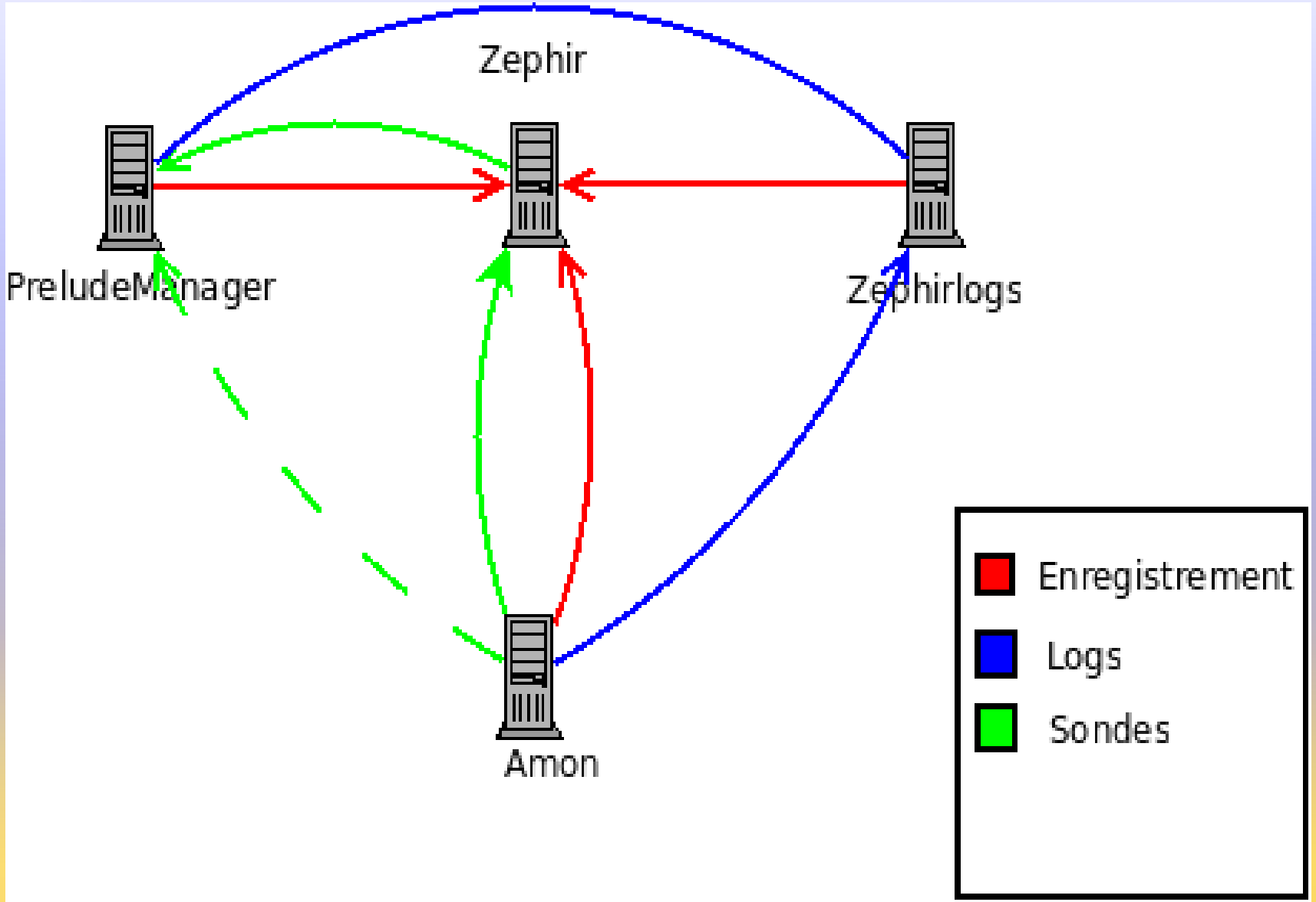
Nécessite l'inscription des modules au niveau de Zephir.

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

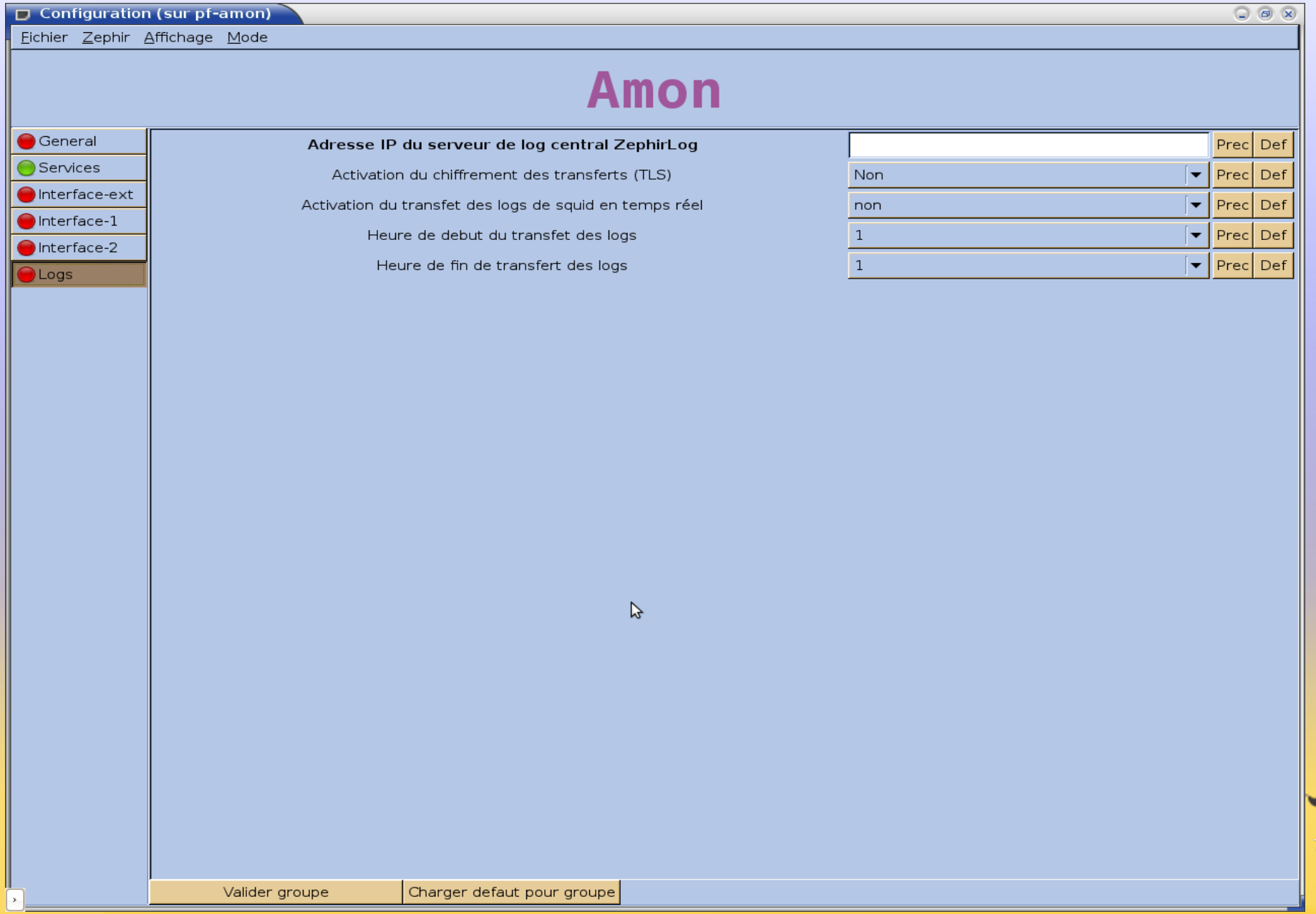
Utilise un système de communication XML-RPC sécurisé pour assurer les échanges.

Possibilité de définir certains paramètres de configuration en utilisant gen_config.

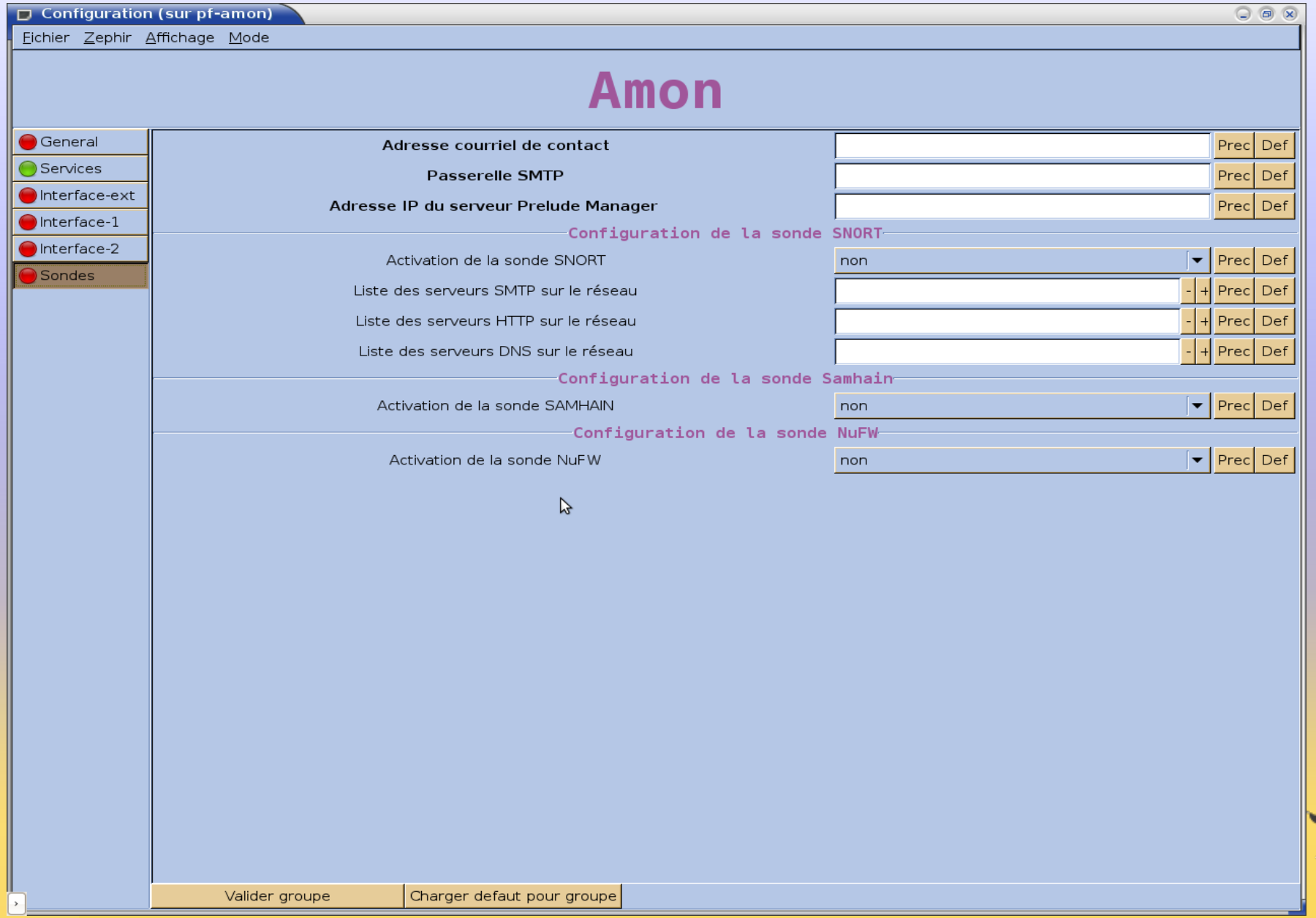
Intégration Eole (2)



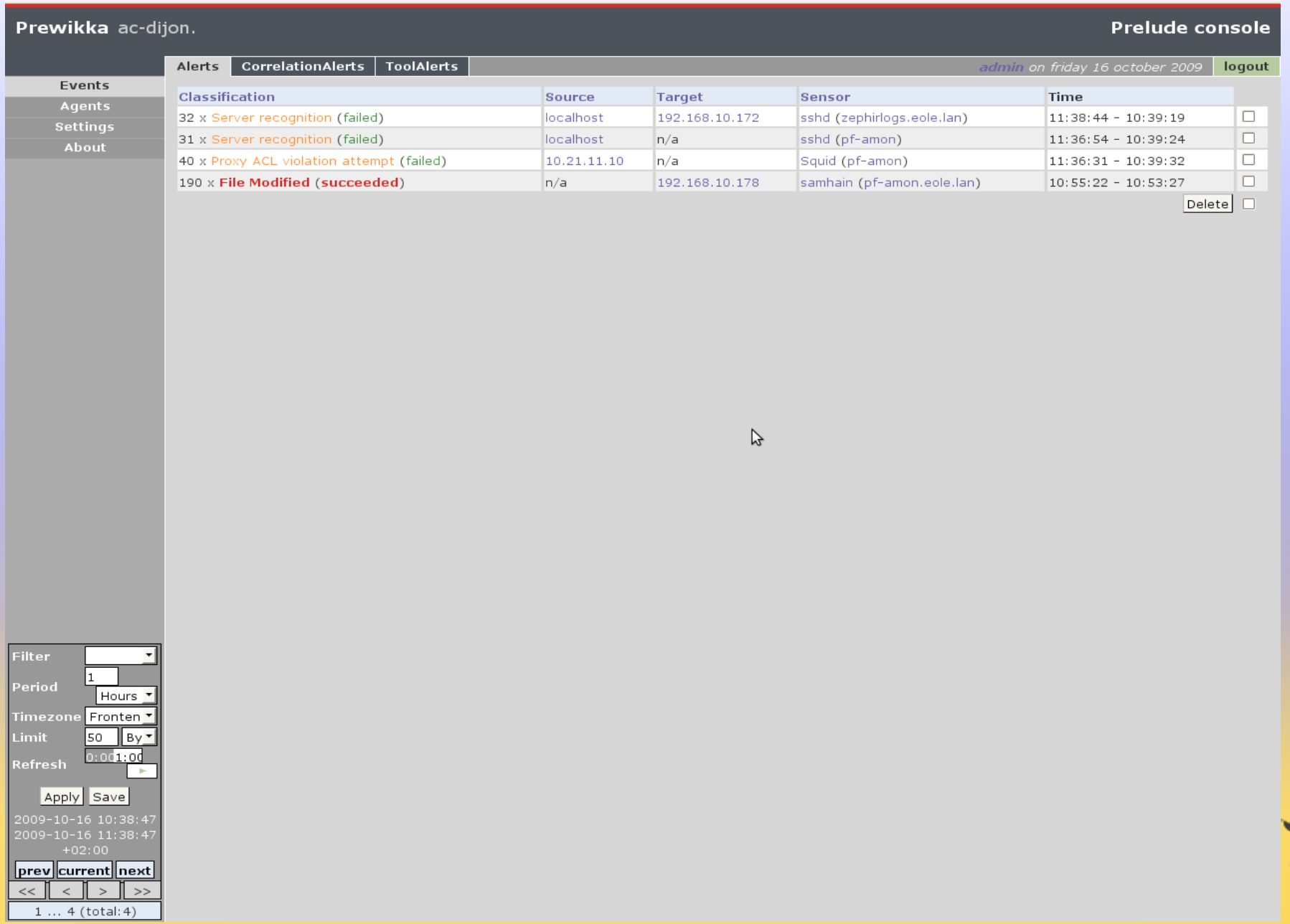
Intégration Eole (3)



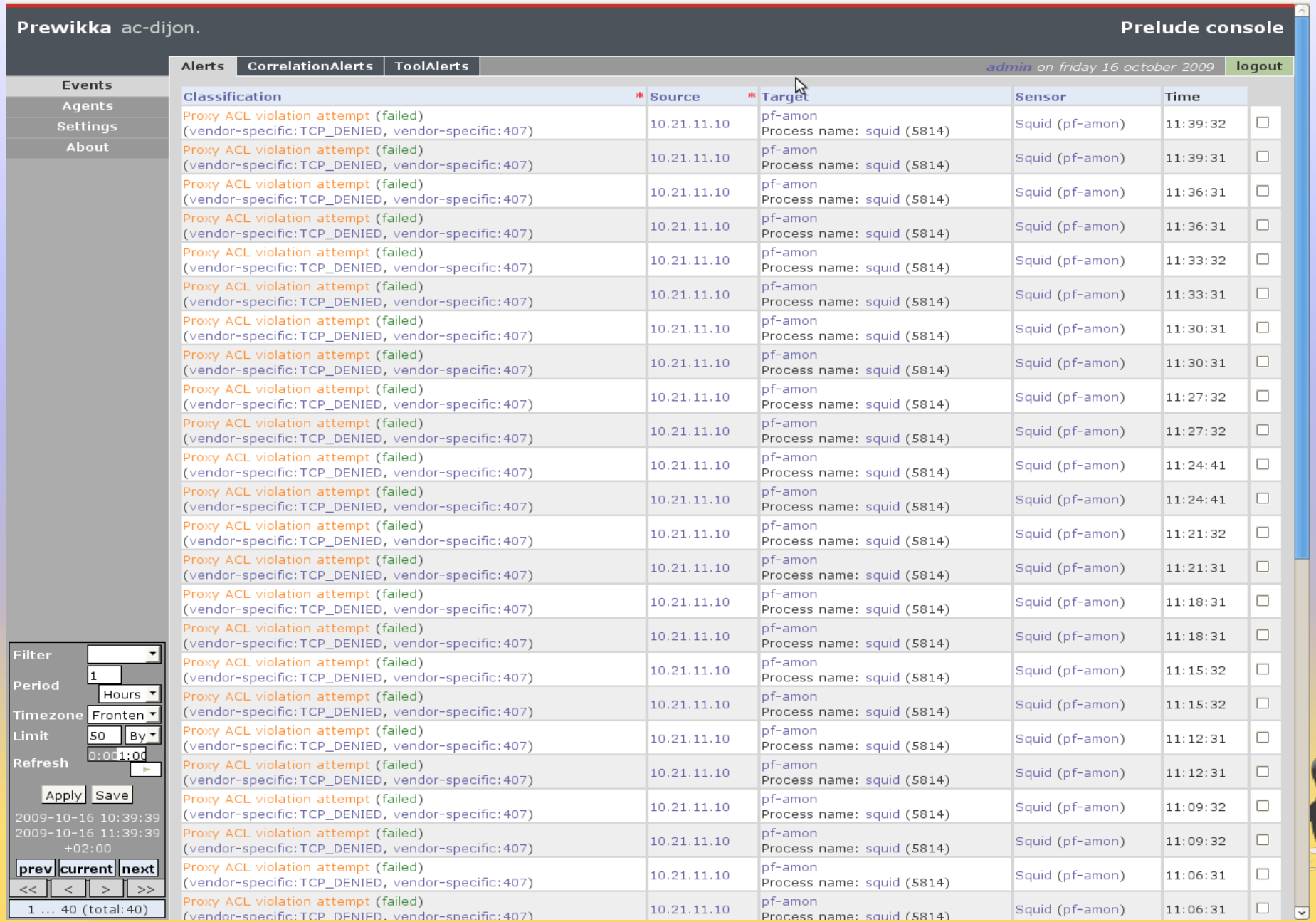
Intégration Eole (4)



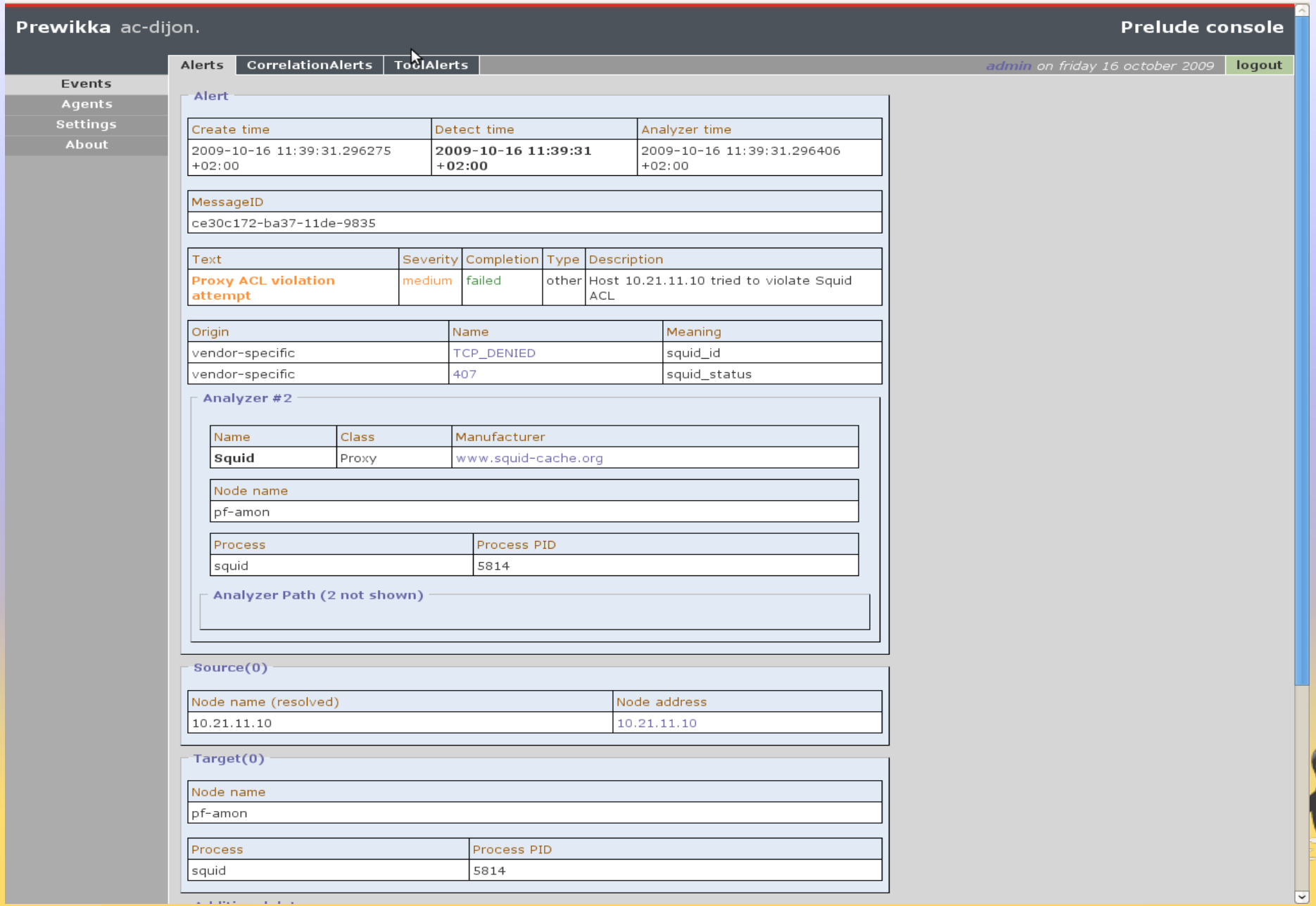
Intégration Eole (5)



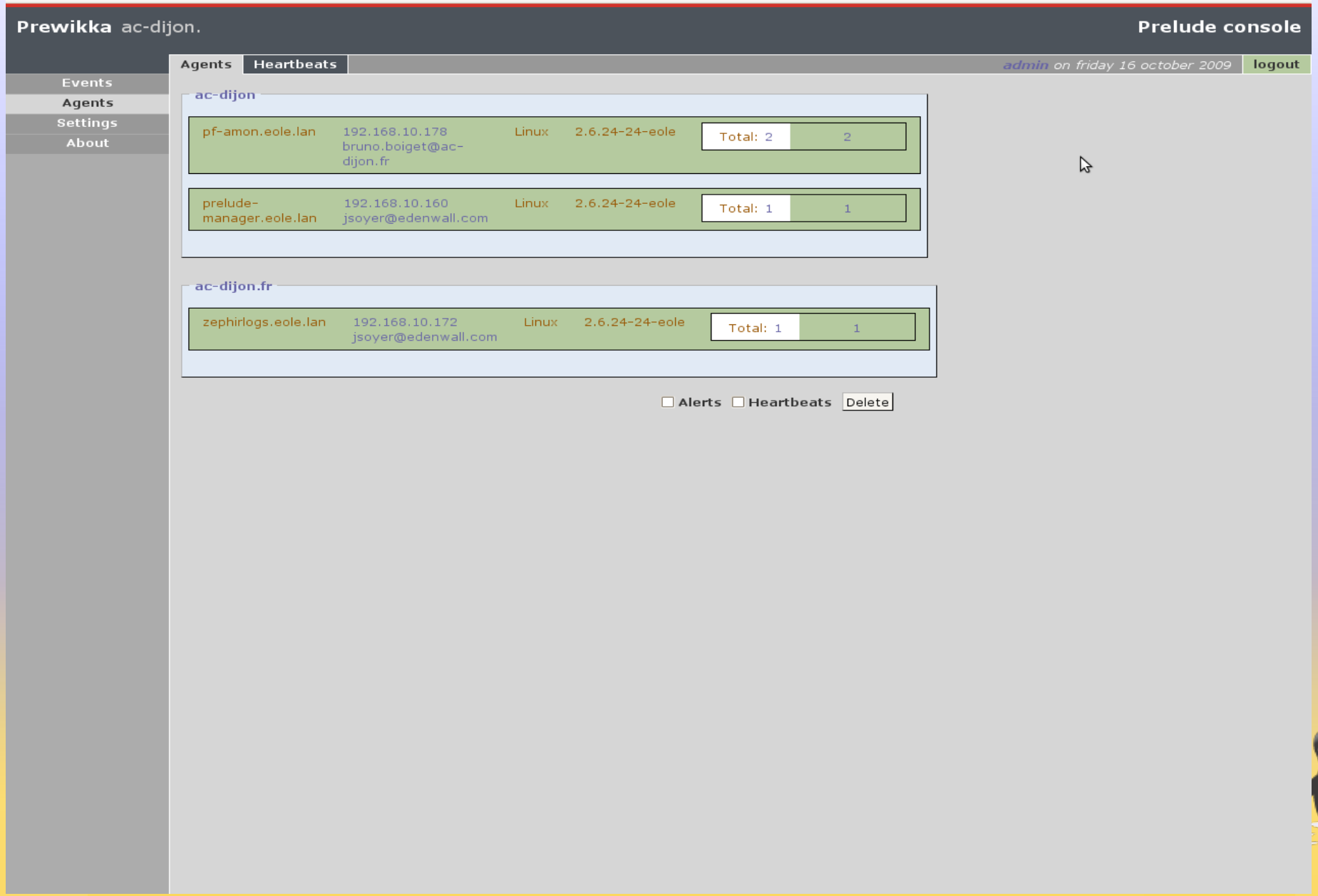
Intégration Eole (6)



Intégration Eole (7)



Intégration Eole (8)



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 (nephentes, Ossec, Sancp)

Nepenthes

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