J-EOLE 4-5 Juin 2014

Le module ZéphirLog

Joël Cuissinat

Table des matières

Qu’est-ce que le module ZéphirLog ?

- Concentrateur de fichiers journaux
- Stockage et archivage des journaux d'événements

Historique du projet

- 2009 : EOLE 2.2
  - Module ZéphirLog
  - Mise en place de l'IDS Prélude
- 2011 : EOLE 2.3
  - Refonte de l'arborescence Rsyslog
  - Chaque Module est configurable pour envoyer ou recevoir les logs

À qui s’adresse le module ZéphirLog ?

Centralisé → services académiques

Les services du module ZéphirLog

- Rsyslog
- Protocoles de communication : UDP, RELP, TCP, TLS over TCP
- Envoi différé possible pour certains logs

Mise en place de ZéphirLog

- Configuration du module EoleBase 2.4 en réception des logs

Démonstration

L’avenir du module ZéphirLog

- Publication d'un module EOLE 2.4 dédié
- Revoir le déploiement des filtres pour rsyslog
- Étude et intégration des recommandations techniques de l'ANSSI

Licence

Cette présentation est mise à disposition sous licence

Creative Commons by-nc-sa 2.0-fr

Attribution	Partage dans les mêmes conditions
Pas d'utilisation commerciale	France

Vous pouvez obtenir une copie de la licence :

- Par internet : https://creativecommons.org/licenses/by-nc-sa/2.0/fr/
- Par courrier postal : Creative Commons, 444 Castro Street, Suite 900 Mountain View, California, 94041, USA