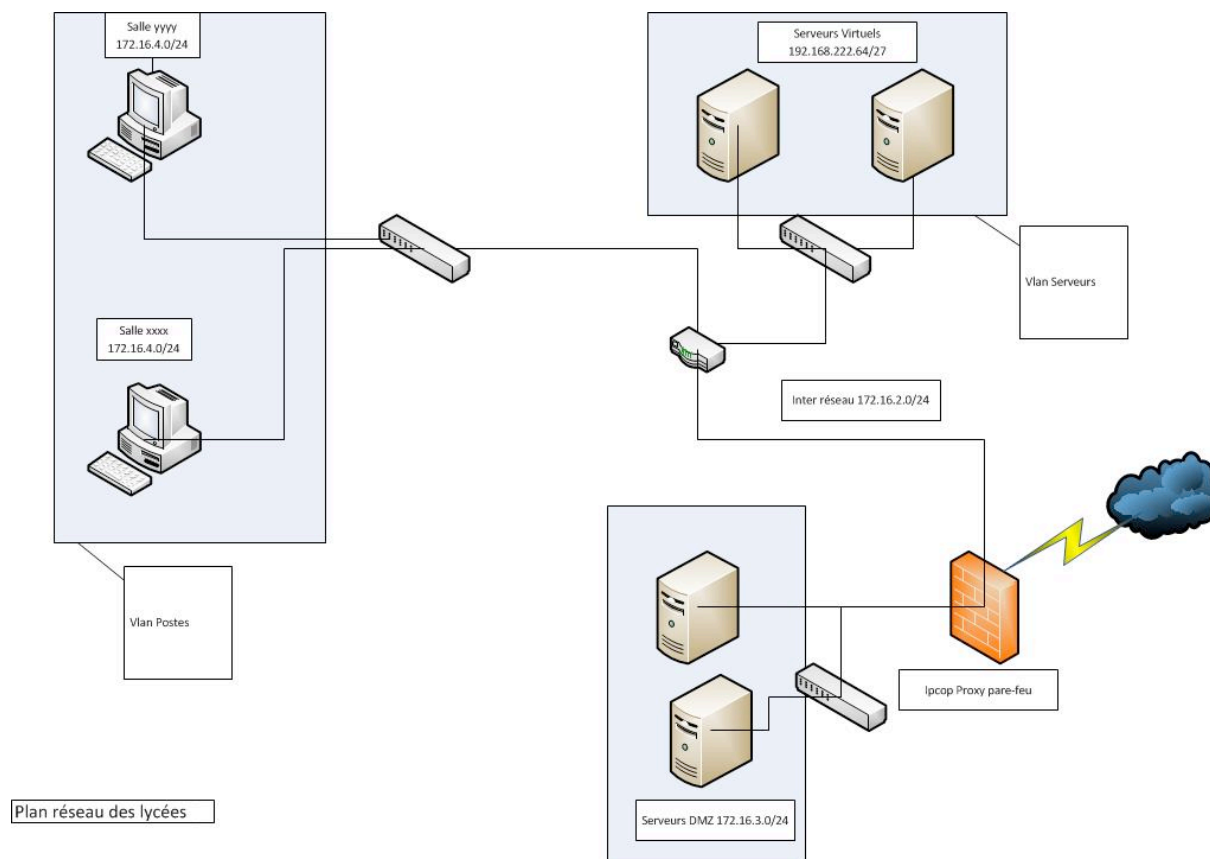


## Exonet sur le protocole Syslog

Propriétés	Description
<b>Intitulé long</b>	Exonet sur le protocole Syslog
<b>Formation concernée</b>	BTS SIO
<b>Matière</b>	SISR3 - Exploitation des services
<b>Présentation</b>	L'objectif consiste à : <ul style="list-style-type: none"><li>- Analyser des fichiers de trace et repérer les lacunes du protocole syslog</li><li>- Faciliter l'analyse de l'activité en proposant des améliorations</li></ul>
<b>Notions du programme</b>	<b>Activités supports de l'acquisition des compétences</b> <b>D2.1 - Exploitation des services</b> <ul style="list-style-type: none"><li>• A2.1.2 Évaluation et maintien de la qualité de service</li></ul> <b>D3.1 - Conception d'une solution d'infrastructure</b> <ul style="list-style-type: none"><li>• A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure</li></ul> <b>D3.3 - Administration et supervision d'une infrastructure</b> <ul style="list-style-type: none"><li>• A3.3.5 Gestion des indicateurs et des fichiers d'activité</li></ul> <b>Savoir-faire</b> <ul style="list-style-type: none"><li>• Analyser le contenu des fichiers d'activité</li></ul> <b>Savoirs associés</b> <ul style="list-style-type: none"><li>• Continuité et sécurité de service, méthodes, technologies, techniques normes et standards associés</li></ul>
<b>Pré-requis</b>	Savoir lire une capture de trames, connaître l'existence des serveurs de temps
<b>Mots-clés</b>	Syslog, protocole, log, trace, criticité.
<b>Durée</b>	2 h 00
<b>Auteur(es)</b>	Marie-pascale Delamare, relecture Roger Sanchez et Gaëlle Castel.
<b>Version</b>	v 1.0
<b>Date de publication</b>	Mars 2014

## Le Contexte :

Un bon nombre de lycées français a choisi le PGI OpenERP pour permettre l'enseignement des Sciences de gestion dans la nouvelle filière STMG. Le réseau type des lycées sur lequel est installé ce PGI est présenté ci-dessous :



Les matériels d'interconnexion des différents Vlan entre eux sont des commutateurs CISCO 2960 et un routeur CISCO 2901. Les serveurs sont des serveurs virtuels hébergés dans une ferme de serveurs ESX composée de deux serveurs en cluster avec déplacement automatique des machines virtuelles en cas de problème sur un des deux serveurs ESX.

La filière STMG ne va utiliser, pour le moment, qu'un seul contexte : le contexte Specibike qui nécessite l'installation de la version 6.0.3 du PGI OpenERP. Dans ce PGI, chaque contexte de gestion, est une base de données.

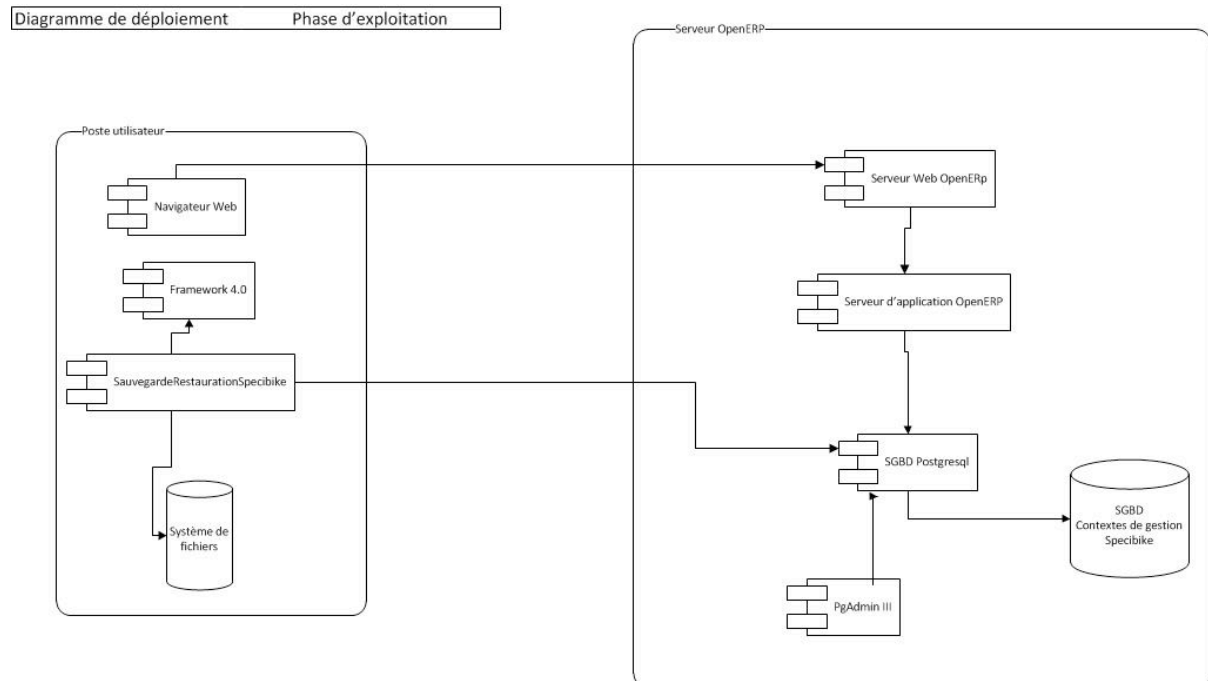
Chaque élève ou chaque groupe d'élèves, ou encore chaque classe, peut disposer de son contexte personnel (donc de sa base de données), disponible sur un serveur OpenERP commun à toutes les classes. Chaque élève dispose, sur son poste, d'un programme utilitaire nommé "SauvRestSpecibike" lui permettant de sauvegarder ou restaurer son contexte sans connaître les mots de passe d'administration du serveur Posgresql (serveur de base de données hébergeant les contextes). Le PGI étant gratuit, les élèves peuvent donc l'installer chez eux et travailler à domicile sur leur contexte récupéré via cet utilitaire au sein de leur établissement.

Pour différencier les bases de données entre elles, la codification suivante a été retenue :

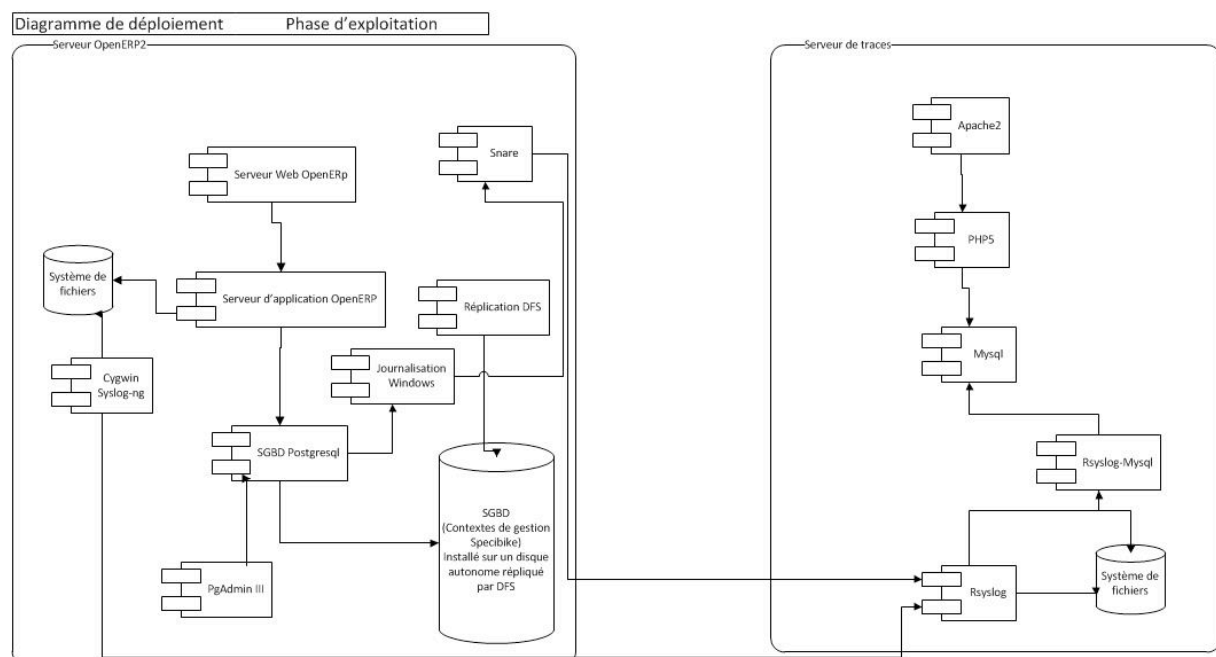
- SpecibikeNomEtudiant pour les contextes personnels ;
- SpecibikeNomClasseNomGroupe pour les contextes de groupes ;
- SpecibikeNomClasse pour les contextes de classes.

Les bases de données respectant cette codification sont sauvegardées tous les soirs vers un serveur de sauvegardes.

Le diagramme de déploiement de ce service est présenté ci-dessous :



Un serveur de traces centralisé est installé sur le réseau. Tous les serveurs (au sens SE et au sens applicatif) redirigent leurs messages de traces vers ce serveur centralisé de la manière suivante :



Pour un serveur Windows, on utilise donc le logiciel Snare pour rediriger les messages du journal du système d'exploitation vers le serveur de traces centralisé, et pour les applicatifs ne sachant pas travailler avec le système de journalisation Windows on utilise un serveur syslog-ng installé dans un environnement Cygwin (émulation d'un environnement Linux).

En stage dans un lycée, votre mission est d'aider l'administrateur réseau à mettre au point cette architecture.

## Action 1 : Comprendre le protocole Syslog

### Documents à utiliser : Partie 1

En vous appuyant sur le cours concernant le protocole syslog (<http://ram-0000.developpez.com/tutoriels/reseau/Syslog/>) et les documents fournis :

- 1) Donner l'adresse du serveur syslog récepteur, l'adresse du serveur émetteur, le port d'écoute utilisé par le serveur syslog et les protocoles utilisés pour le transfert.
- 2) Dire quelle est la priorité du message (en base 10).
- 3) Vérifier que la priorité est bien fonction de la fonctionnalité et de la sévérité.
- 4) Préciser à quelle date et à quelle heure ce message a été transmis.
- 5) Donner le nom du serveur ayant émis ce message.
- 6) Citer l'application qui a émis ce message.
- 7) En regardant le corps du message, donner la source (au sens syslog) qui envoie le message et préciser combien il y a de destinataires (au sens syslog) à ce message.
- 8) Expliquer pourquoi il peut être nécessaire de conserver un fichier log en local sur chaque machine.

## Action 2 : Améliorer le paramétrage des applicatifs émetteurs de traces

### Documents à utiliser : Partie 2

- 1) Donner l'adresse du serveur syslog récepteur, l'adresse du serveur émetteur, le port d'écoute utilisé par le serveur de syslog et le protocole utilisé pour le transfert.
- 2) Dire quelle est la priorité du message (en base 10).
- 3) Préciser à quelle date et à quelle heure ce message a été transmis.
- 4) Donner le nom du serveur ayant émis ce message.
- 5) Conclure sur la difficulté d'analyse des messages syslog en cas d'émetteurs différents situés à la même adresse.
- 6) Proposer, devant l'abondance des messages émis, des modifications dans le paramétrage de Snare afin de faciliter l'analyse.
- 7) En faisant une synthèse des parties 1 et 2, retrouver sur le diagramme de déploiement les parcours possibles des messages syslog.

## Action 3 : Vérifier la cohérence de l'architecture mise en place

### Documents à utiliser : Partie 3

- 1) Citer les incohérences présentes dans ce fichier.
- 2) Préciser l'origine de ces incohérences.
- 3) Proposer une solution pour régler définitivement ce problème.

# Dossier documentaire

## Partie 1 :

### a) Extrait d'une capture de trames effectuée sur un serveur du réseau

syslog.pcapng [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

Filter: **syslog**

No.	Time	Source	Destination	Protocol	Length	Info
37632	190.054263	172.31.0.150	172.31.0.50	syslog	1514	USER.NOTICE: Oct 31 20:01:03 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t302\tjeu. oct. 31 20:01:01 2
37635	190.056076	172.31.0.150	172.31.0.50	syslog	561	USER.NOTICE: Oct 31 20:01:03 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t303\tjeu. oct. 31 20:01:01 2
38017	192.084016	172.31.0.150	172.31.0.50	syslog	1514	USER.NOTICE: Oct 31 20:01:05 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t304\tjeu. oct. 31 20:01:04 2
39093	200.193116	172.31.0.150	172.31.0.50	syslog	1514	USER.NOTICE: Oct 31 20:01:13 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t305\tjeu. oct. 31 20:01:11 2
40320	203.235191	172.31.0.150	172.31.0.50	syslog	605	USER.NOTICE: Oct 31 20:01:16 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t306\tjeu. oct. 31 20:01:14 2
41643	209.969544	172.31.0.150	172.31.0.50	syslog	306	USER.NOTICE: Oct 31 20:01:23 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t307\tjeu. oct. 31 20:01:23 201
52063	263.170246	172.31.0.150	172.31.0.50	syslog	617	SYSLOG.INFO: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, process
53646	272.192945	172.31.0.150	172.31.0.50	syslog	566	USER.NOTICE: Oct 31 20:02:25 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t308\tjeu. oct. 31 20:02:24 2
95392	490.195188	172.31.0.150	172.31.0.50	syslog	1514	USER.NOTICE: Oct 31 20:06:03 WIN2008.de.lamare.local MSWineventLog\0\tsecurity\t309\tjeu. oct. 31 20:06:01 2

Frame 52063: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits) on interface 0  
Ethernet II, Src: Vmware\_8c:42:2d (00:0c:29:8c:42:2d), Dst: Vmware\_d8:3e:82 (00:0c:29:d8:3e:82)  
Internet Protocol Version 4, Src: 172.31.0.150 (172.31.0.150), Dst: 172.31.0.50 (172.31.0.50)  
User Datagram Protocol, Src Port: 51738 (51738), Dst Port: syslog (514)  
Source port: 51738 (51738)  
Destination port: syslog (514)  
Length: 583  
Checksum: 0x5b5f [validation disabled]  
[Good Checksum: False]  
[Bad Checksum: False]

[truncated] Syslog message: SYSLOG.INFO: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, processed=src.internal(s\_local#1)=2, stamp=src.internal(s\_local#1)=138...  
Facility: SYSLOG - messages generated internally by syslog (5)  
Level: INFO - informational (6)  
Message [truncated]: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, processed=src.internal(s\_local#1)=2, stamp=src.internal(s\_local#1)=138...

### b) Détail de la trame sélectionnée

52063 263.170246000 172.31.0.150 172.31.0.50 Syslog 617 SYSLOG.INFO: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, processed=src.internal(s\_local#1)=2, stamp=src.internal(s\_local#1)=138...

Frame 52063: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits) on interface 0  
Ethernet II, Src: Vmware\_8c:42:2d (00:0c:29:8c:42:2d), Dst: Vmware\_d8:3e:82 (00:0c:29:d8:3e:82)  
Internet Protocol Version 4, Src: 172.31.0.150 (172.31.0.150), Dst: 172.31.0.50 (172.31.0.50)  
User Datagram Protocol, Src Port: 51738 (51738), Dst Port: syslog (514)  
[truncated] Syslog message: SYSLOG.INFO: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, processed=src.internal(s\_local#1)=2, stamp=src.internal(s\_local#1)=138...  
Facility: SYSLOG - messages generated internally by syslog (5)  
Level: INFO - informational (6)  
Message [truncated]: Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed=center(received)=0, processed=src.internal(s\_local#1)=2, stamp=src.internal(s\_local#1)=138...

**c) Configuration du serveur syslog émetteur :**

```
#####  
# Default syslog-ng.conf file which collects all local logs into a  
# single file called /var/log/syslog.  
  
@version: 3.2  
@include "scl.conf"  
  
source s_local {  
    system();  
    internal();  
    file("/var/log/openerp-server.log");  
};  
  
destination d_local {  
    file("/var/log/messages");  
};  
  
destination d_logger {  
    udp("172.31.0.50");  
};  
  
log {  
    source(s_local);  
    # uncomment this line to open port 514 to receive messages  
    #source(s_network);  
    destination(d_local);  
};  
  
log {  
    source(s_local);  
    # uncomment this line to open port 514 to receive messages  
    #source(s_network);  
    destination(d_logger);  
};
```

source s\_local : indique d'où viennent les messages (ici on récupère les messages du serveur d'application OpenERP, ce fichier est conservé car il est en fait géré par OpenERP).

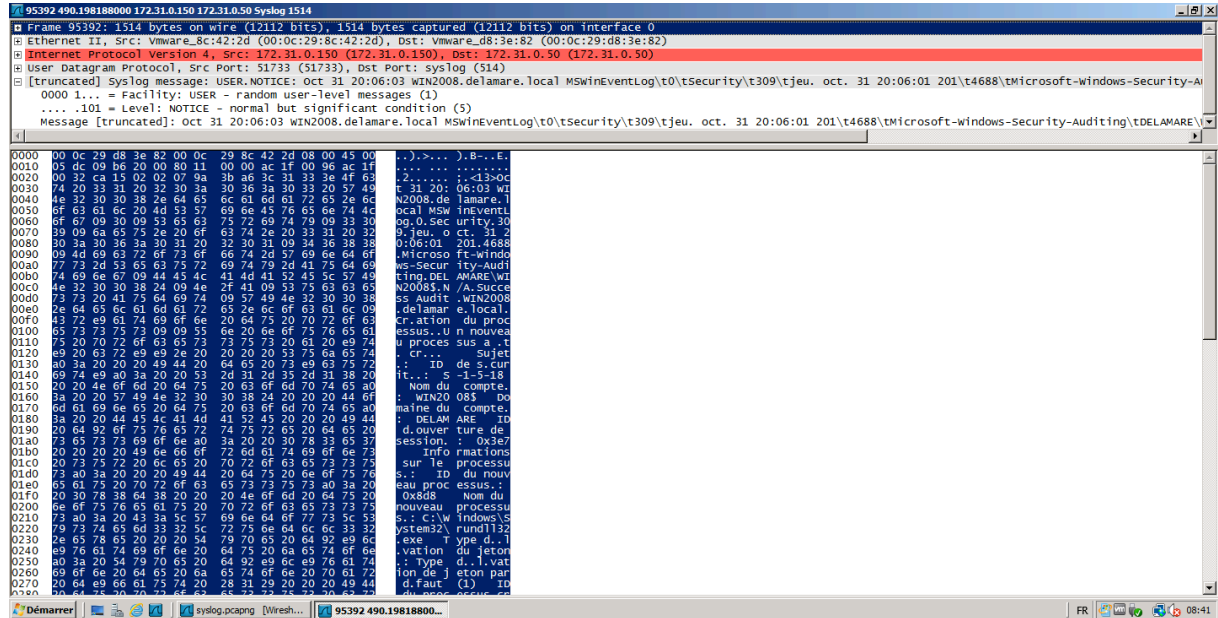
destination : indique où envoyer les messages  
destination d\_local : on en garde en local dans le fichier /var/log/messages.  
destination d\_logger : on les transfère aussi vers le serveur de traces centralisé en UDP..

**d) Message retrouvé dans le fichier syslog du serveur de traces centralisé :**

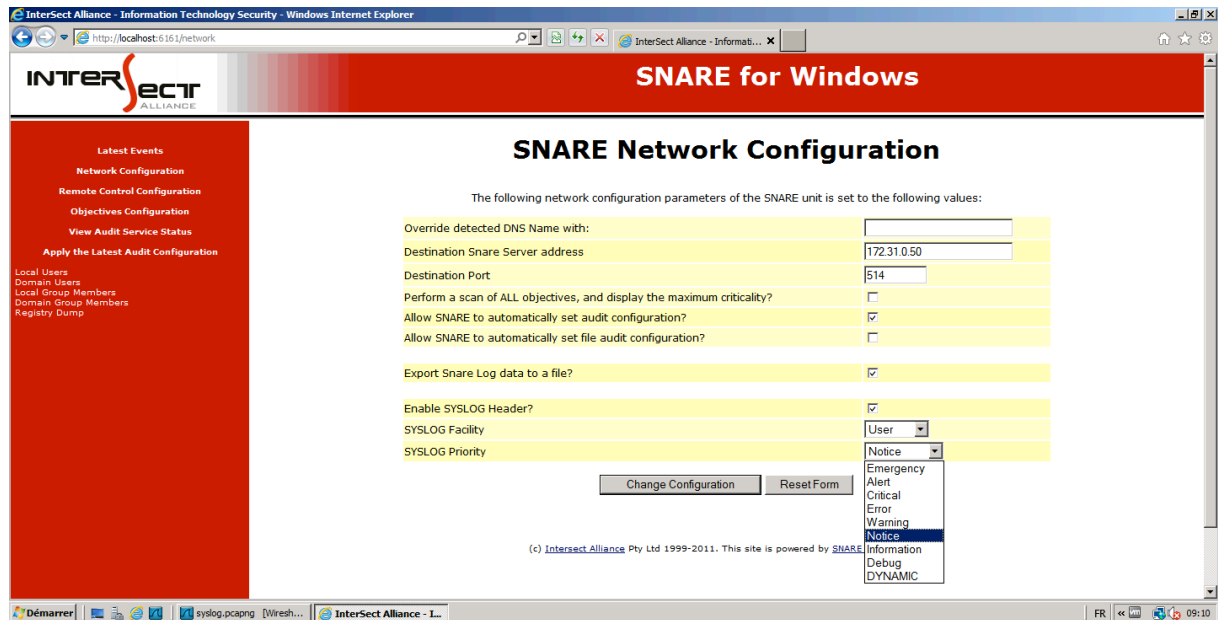
```
Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed='center(received)=0',  
processed='src.internal(s_local#1)=2', stamp='src.internal(s_local#1)=1383245518',  
processed='center(queued)=0', processed='global(payload_reallocs)=0',  
dropped='dst.udp(d_logger#0,172.31.0.50:514)=0',  
processed='dst.udp(d_logger#0,172.31.0.50:514)=364',  
stored='dst.udp(d_logger#0,172.31.0.50:514)=0', processed='global(sdata_updates)=0',  
processed='destination(d_local)=364', processed='global(msg_clones)=0',  
processed='source(s_local)=364', processed='destination(d_logger)=364'
```

## Partie 2

a) Un autre message syslog transmis depuis le même serveur et présent dans la même capture de trame :



b) Paramétrage du logiciel Snare



## c) La visualisation des messages via l'interface web du serveur de traces centralisé

The screenshot shows the web interface of Php-Syslog-NG 2.9.1. The search query is: `SELECT SQL_CALC_FOUND_ROWS * FROM logs WHERE host not in ('WIN2008') and msg like '%Win2008'`. The table displays log entries with columns for SEQ, HOST, FACILITY, DATE TIME, and MESSAGE. The messages are Windows Security Audit logs related to user privilege elevation.

SEQ	HOST	FACILITY	DATE TIME	MESSAGE
33167	WIN2008.delamare.local	user-notice	2013-11-02 09:06:03	nov. 02 09:06:01 20140114689011Microsoft-Windows-Security-Auditing[01DELA.MAREWIN2008S011NA011Success Audit#011WIN2008.delamare.local#011Un nouveau processus a été créé. Sujet : ID de sécurité : S:1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du nouveau processus : 0x038 Nom du nouveau processus : C:\Windows\System32\cmd.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0x58 Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif ou pour toujours exiger les privilèges maximum, et que l'utilisateur est membre du groupe Administrateurs. Le type 3 est un jeton limité dont les privilèges administratifs sont supprimés et les groupes administratifs désactivés. Le jeton limité est utilisé lorsque le contrôle de compte d'utilisateur est activé, que l'application n'exige pas le privilège administratif et que l'utilisateur ne choisit pas de démarrer le programme en tant qu'administrateur.011325
33168	WIN2008.delamare.local	user-notice	2013-11-02 09:06:03	nov. 02 09:06:01 20140114689011Microsoft-Windows-Security-Auditing[01DELA.MAREWIN2008S011NA011Success Audit#011WIN2008.delamare.local#011Fin du processus#011WIN2008.delamare.local#011Un processus est terminé. Sujet : ID de sécurité : S:1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du processus : 0x038 Nom du processus : C:\Windows\System32\cmd.exe Etat de fin : 0x00011325
33164	WIN2008.delamare.local	user-notice	2013-11-02 09:01:03	nov. 02 09:01:01 20140114689011Microsoft-Windows-Security-Auditing[01DELA.MAREWIN2008S011NA011Success Audit#011WIN2008.delamare.local#011Création du processus#011WIN2008.delamare.local#011Un nouveau processus a été créé. Sujet : ID de sécurité : S:1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du nouveau processus : 0x038 Nom du nouveau processus : C:\Windows\System32\cmd.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0x58 Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif ou pour toujours exiger les privilèges maximum, et que l'utilisateur est membre du groupe Administrateurs. Le type 3 est un jeton limité dont les privilèges administratifs sont supprimés et les groupes administratifs désactivés. Le jeton limité est utilisé lorsque le contrôle de compte d'utilisateur est activé, que l'application n'exige pas le privilège administratif et que l'utilisateur ne choisit pas de démarrer le programme en tant qu'administrateur.011323
33165	WIN2008.delamare.local	user-notice	2013-11-02 09:01:03	nov. 02 09:01:01 20140114689011Microsoft-Windows-Security-Auditing[01DELA.MAREWIN2008S011NA011Success Audit#011WIN2008.delamare.local#011Fin du processus#011WIN2008.delamare.local#011Un processus est terminé. Sujet : ID de sécurité : S:1-5-18 Nom du compte : WIN2008S Domaine du compte : DELAMARE ID d'ouverture de session : 0x3e7 Informations sur le processus : ID du processus : 0x038 Nom du processus : C:\Windows\System32\cmd.exe Etat de fin : 0x00011324
33162	WIN2008.delamare.local	user-notice	2013-11-02 09:00:56	nov. 02 09:00:55 20140114689011Microsoft-Windows-Security-Auditing[011WIN2008Administrateur#011NA011Success Audit#011WIN2008.delamare.local#011Création du processus#011WIN2008.delamare.local#011Un nouveau processus a été créé. Sujet : ID de sécurité : S:1-5-21-241459311-4228339857-3661958750-500 Nom du compte : Administrateur Domaine du compte : WIN2008 ID d'ouverture de session : 0x526da Informations sur le processus : ID du nouveau processus : 0x44 Nom du nouveau processus : C:\Program Files\Internet Explorer\iexplore.exe Type d'élevation du jeton : Type d'élevation de jeton par défaut (1) ID du processus créateur : 0xcfc Le type d'élevation du jeton indique le type de jeton qui a été attribué au nouveau processus conformément à la stratégie de contrôle du compte d'utilisateur. Le type 1 est un jeton complet sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton complet est uniquement utilisé si le contrôle du compte d'utilisateur est désactivé, ou si l'utilisateur est le compte d'administrateur intégré ou un compte de service. Le type 2 est un jeton aux droits élevés sans aucun privilège supprimé ni aucun groupe désactivé. Un jeton aux droits élevés est utilisé lorsque le contrôle de compte d'utilisateur est activé et que l'utilisateur choisit de démarrer le programme en tant qu'administrateur. Un jeton aux droits élevés est également utilisé lorsqu'une application est configurée pour toujours exiger un privilège administratif

## Partie 3

### a) Extrait du fichier syslog du serveur de traces centralisé

The screenshot shows a terminal window displaying the contents of a syslog file named 'syslog.1 - Kate'. The log entries include timestamps and messages such as 'Sending failed: Host not found', 'Starting delivery: protocol: smtp host: mail. file: 1370366884\_2521', and 'Delivery complete: B message(s) remain'. The messages are related to email delivery attempts from 'kubuntuMarie nullmailer[1341]'.