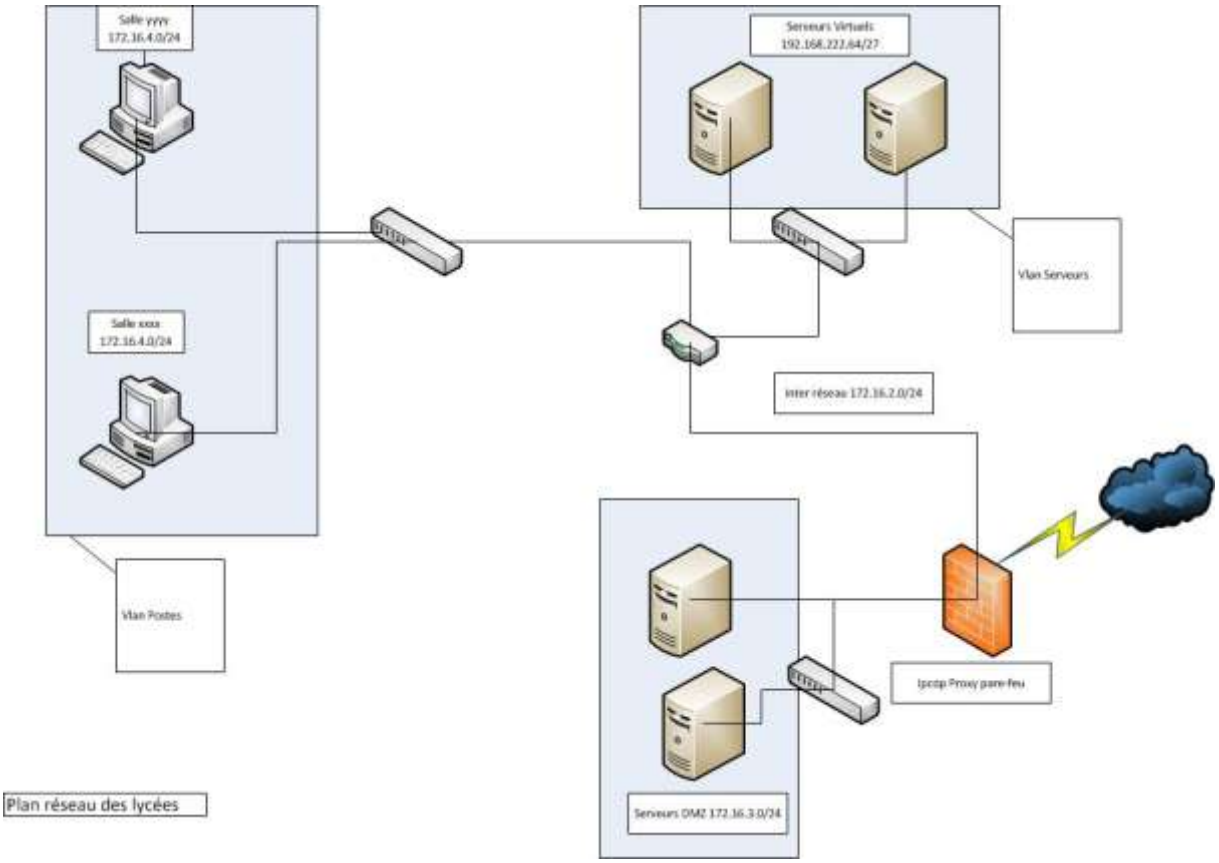
Exonet sur le protocole Syslog

Propriétés	Description
Intitulé long	Exonet sur le protocole Syslog
Formation concernée	BTS SIO
Matière	SISR3 - Exploitation des services
Présentation	L'objectif consiste à : - Analyser des fichiers de trace et repérer les lacunes du protocole syslog - Faciliter l'analyse de l'activité en proposant des améliorations
Notions du programme	**Activités supports de l'acquisition des compétences** **D2.1 - Exploitation des services** • A2.1.2 Évaluation et maintien de la qualité de service **D3.1 - Conception d'une solution d'infrastructure** • A3.1.3 Prise en compte du niveau de sécurité nécessaire à une infrastructure **D3.3 - Administration et supervision d'une infrastructure** • A3.3.5 Gestion des indicateurs et des fichiers d'activité **Savoir-faire** • Analyser le contenu des fichiers d'activité **Savoirs associés** • Continuité et sécurité de service, méthodes, technologies, techniques normes et standards associés
Pré-requis	Savoir lire une capture de trames, connaitre l'existence des serveurs de temps
Outils	
Mots-clés	Syslog, protocole, log, trace, criticité.
Durée	2 h 00
Auteur(es)	Marie-pascale Delamare
Version	v 1.0
Date de publication	Janvier 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 :



Plan réseau des lycées

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 composé de deux serveurs en cluster avec déplacement automatique des machines virtuelles en cas de problème sur un des deux serveurs ESX.

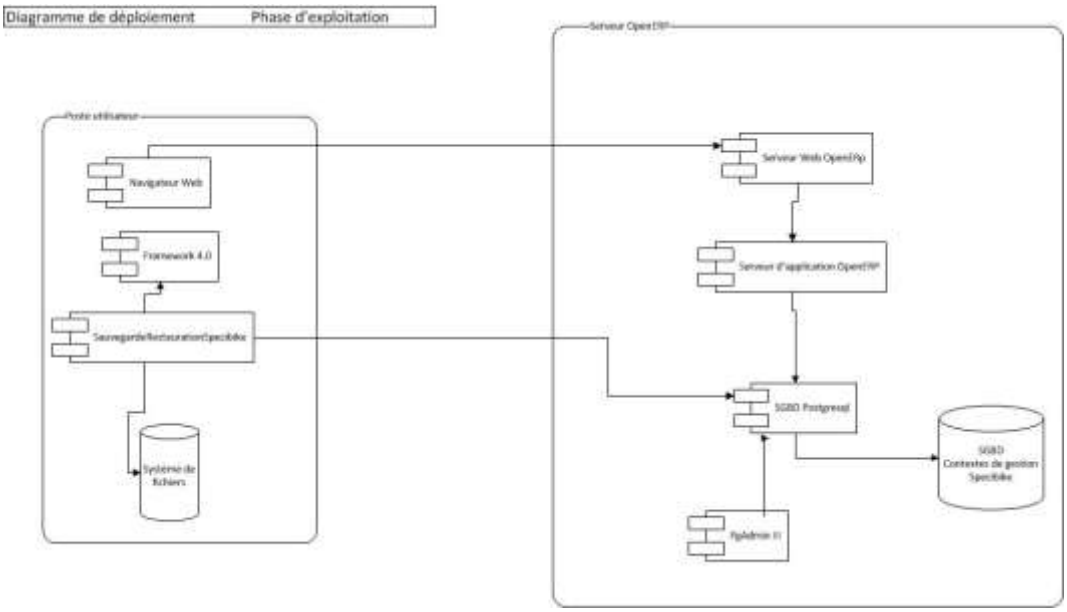
La filière STMG ne va utiliser pour le moment qu'un seul contexte : le contexte Specibike qui nécessite l'installation de la version 6.0.3 du PGI OpenERP. Dans ce PGI, chaque contexte de gestion, est une base de données

Chaque élève ou chaque groupe d'élèves ou 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.

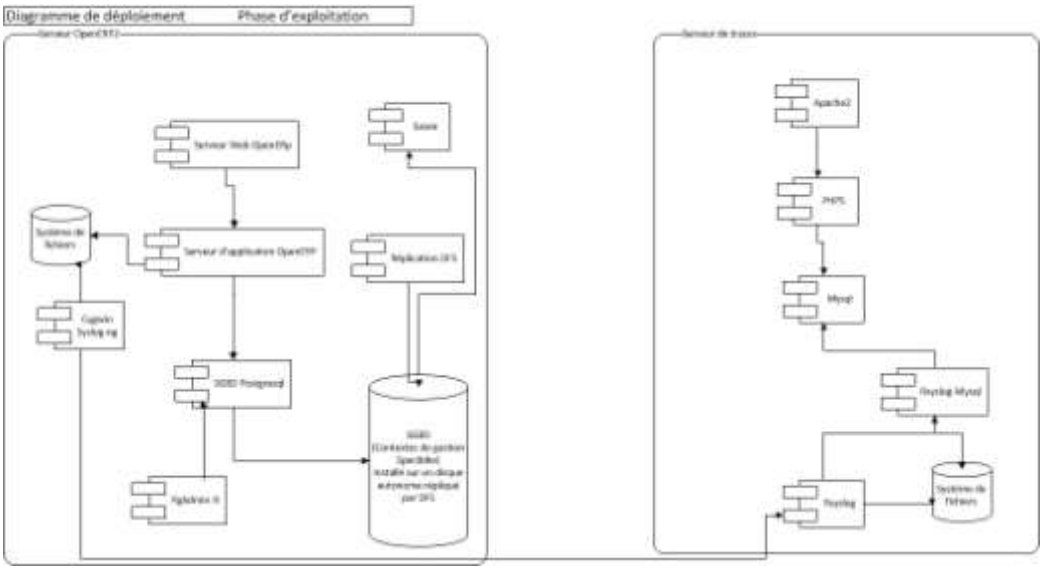
Pour différentier les bases de données entre elles, la codification suivante a été retenue :

- 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, vous aidez l'administrateur réseau à mettre point cette architecture.

Mission 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.

Mission 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, représenter les parcours possibles des messages syslog.

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

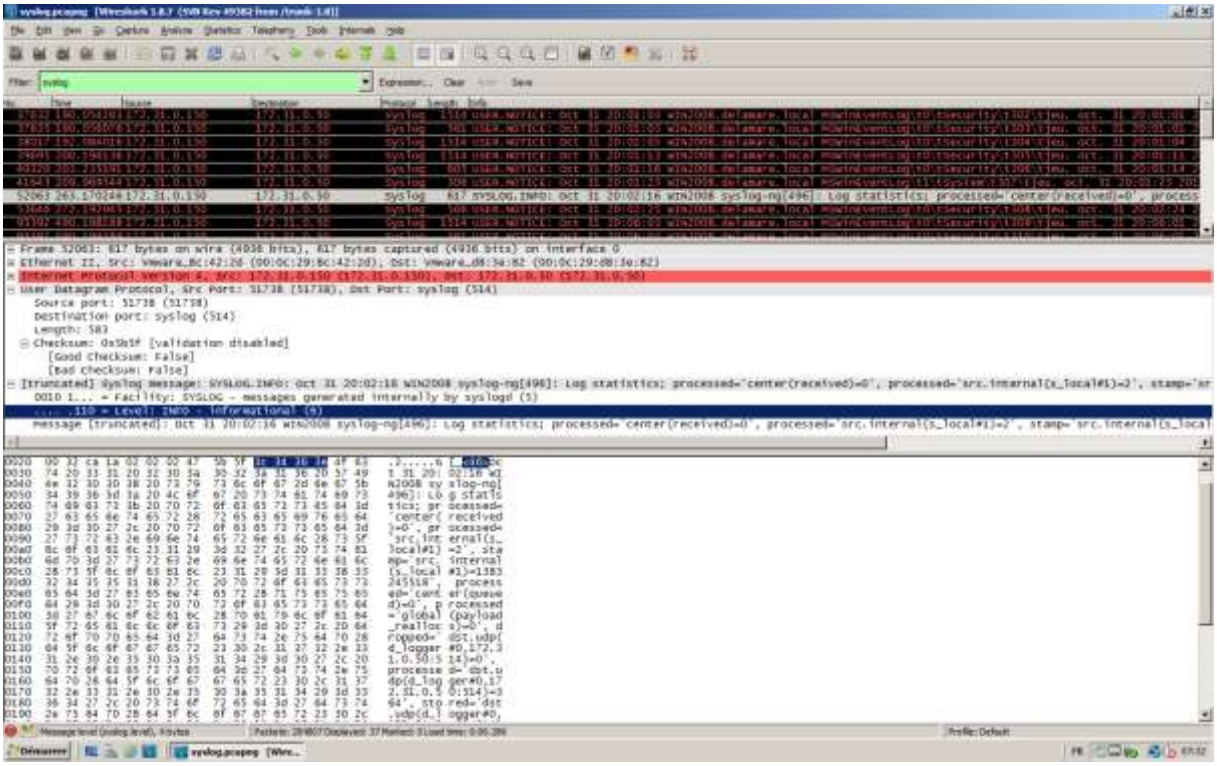
Documents à utiliser : Partie 3

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

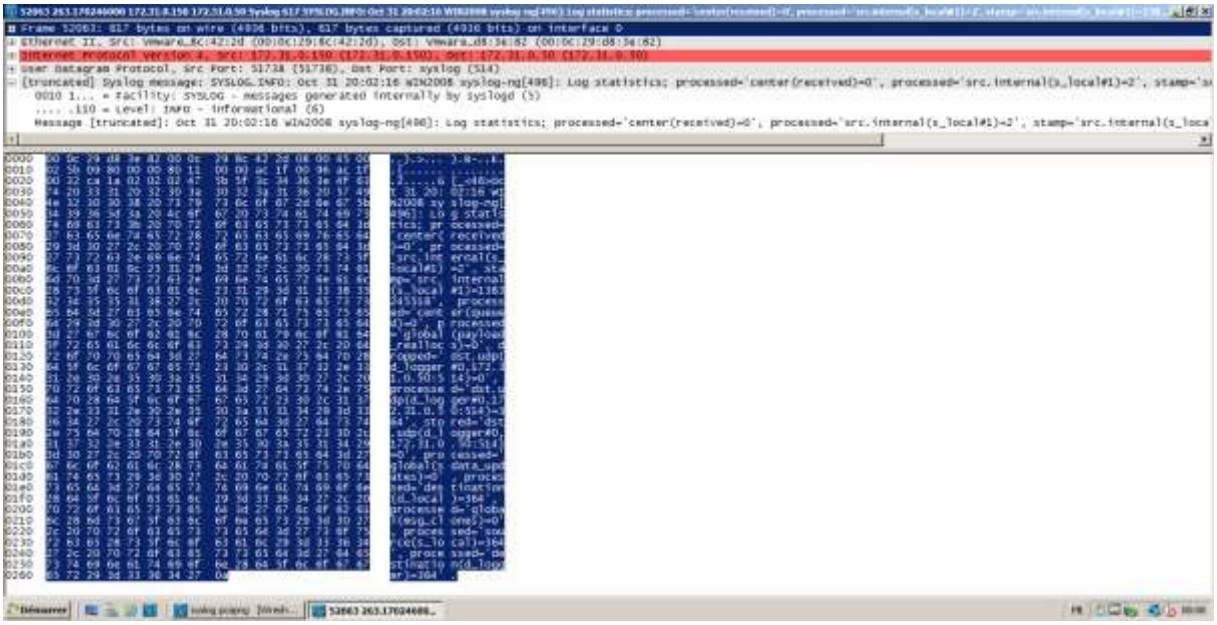
Dossier documentaire

Partie 1 :

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



b) Détail de la trame sélectionnée



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 entre autre).

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.

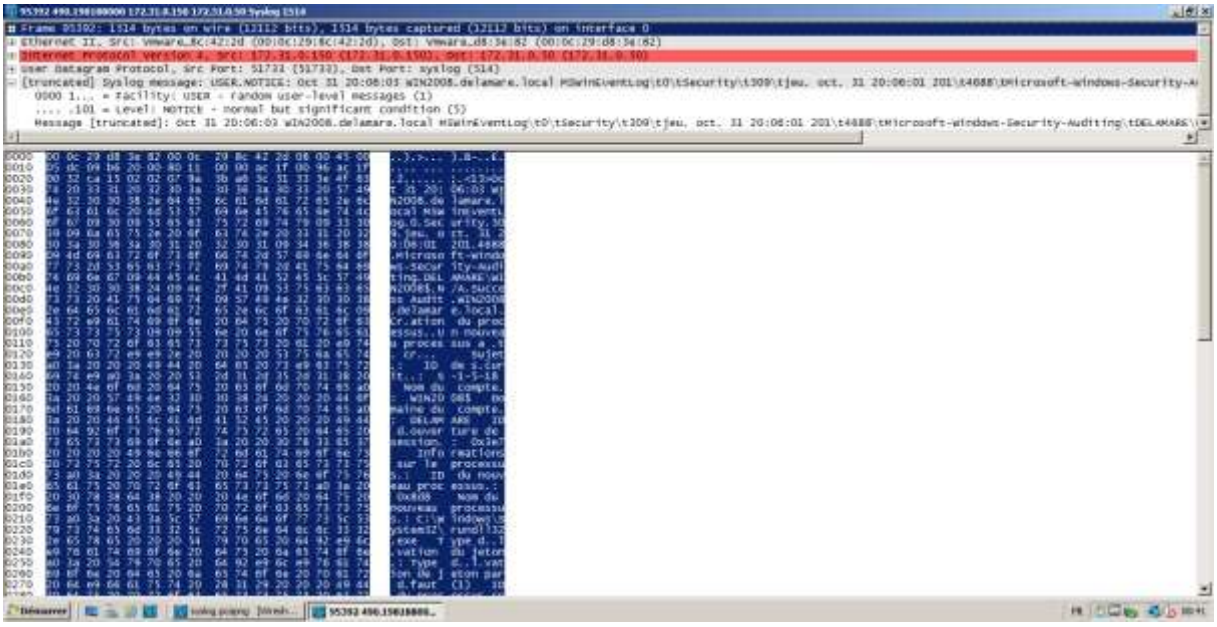
Les paragraphes « log » activent les paramétrages réalisés.

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

Partie 3

a) Extrait du fichier syslog du serveur de traces centralisé