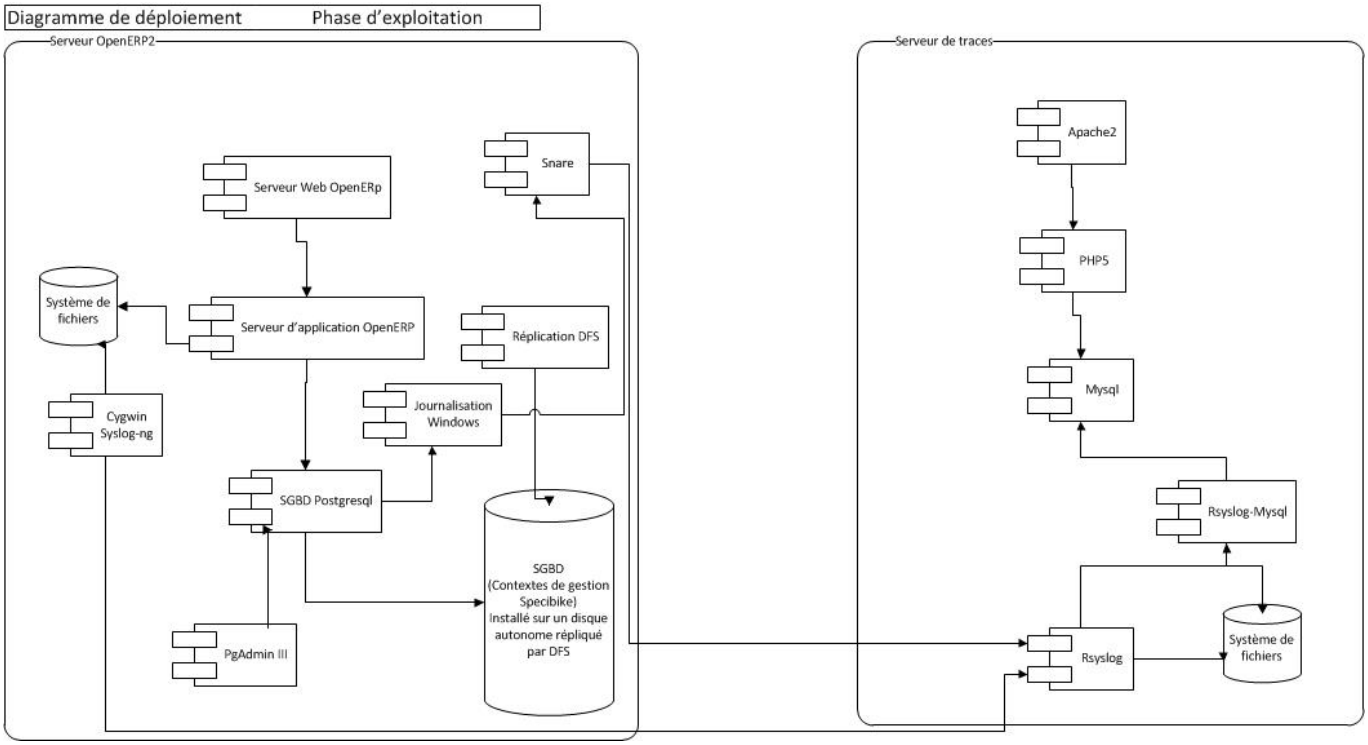
Syslog : Comprendre le protocole Syslog

Ressources

- Exonet sur le protocole Syslog
- https://www.fr.paessler.com/it-explained/syslog

Présentation de l'architecture

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 :



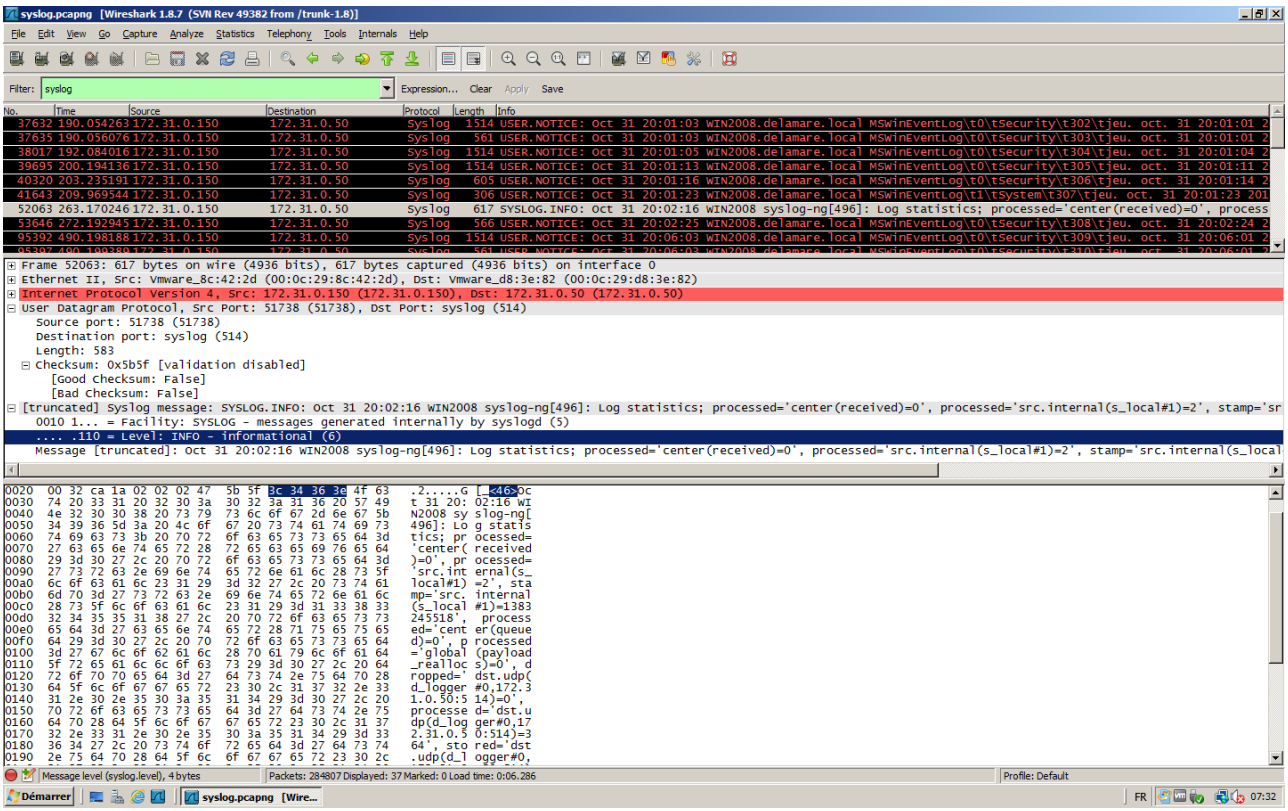
Travail à faire

En vous appuyant sur le cours concernant le protocole syslog (http://ram-0000.developpez.com/tutoriels/reseau/Syslog/) et les documents fournis ci-dessous, répondez aux questions suivantes :

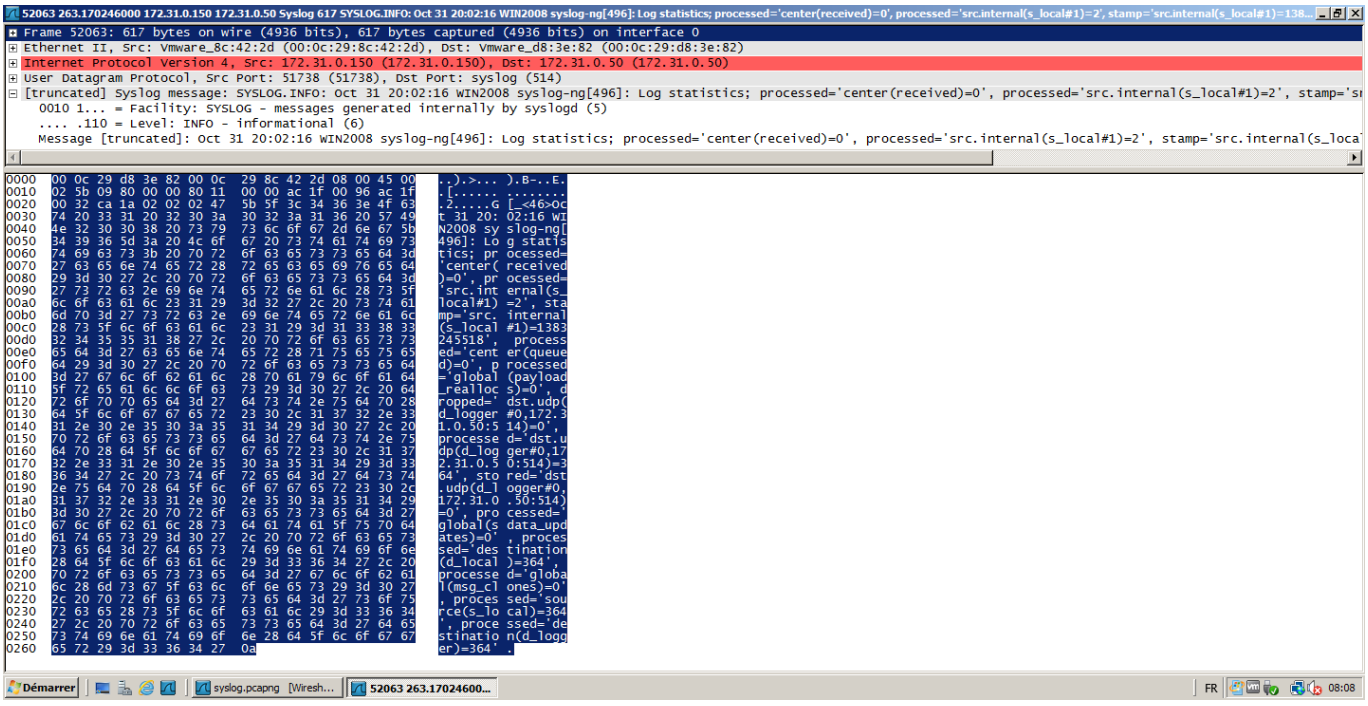
- 1) Donner l'adresse du serveur syslog récepteur, l'adresse du serveur émetteur, le port d'écoute utilisé par le serveur syslog et les protocoles utilisés pour le transfert.
- 2) Dire quelle est la priorité du message (en base 10).
- 3) Vérifier que la priorité est bien fonction de la fonctionnalité 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.

Documents

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, ce fichier est conservé car il est en fait géré par OpenERP). * destination : indique où envoyer les messages * destination dlocal : 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.. Les paragraphes « log » active les paramétrages réalisés. d) Message retrouvé dans le fichier syslog du serveur de traces centralisé : <code> Oct 31 20:02:16 WIN2008 syslog-ng[496]: Log statistics; processed='center(received)=0', processed='src.internal(slocal#1)=2', stamp='src.internal(slocal#1)=1383245518', processed='center(queued)=0', processed='global(payloadreallocs)=0', dropped='dst.udp(dlogger#0,172.31.0.50:514)=0', processed='dst.udp(dlogger#0,172.31.0.50:514)=364', stored='dst.udp(dlogger#0,172.31.0.50:514)=0', processed='global(sdataupdates)=0', processed='destination(dlocal)=364', processed='global(msgclones)=0', processed='source(slocal)=364', processed='destination(d_logger)=364' </code>**