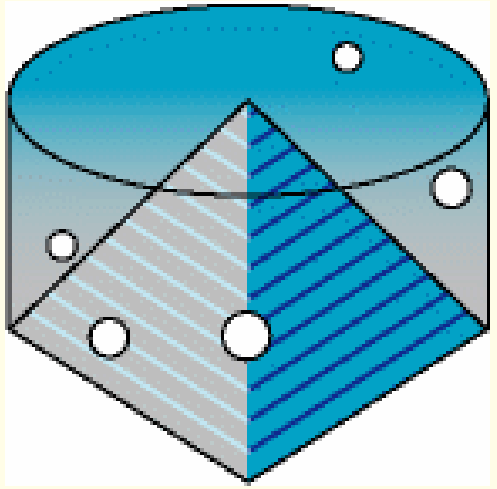
LogManager



Manage your security logs

Sommaire

L’équipe LogManager

L’équipe

- Raymond Mercier
  - Consultant sécurité Alcatel CIT
    - Audit sécurité
    - Responsable technique de l’offre SOC
  - Ancien responsable technique de produit
    - SecureScan NX et SP
    - VIGILANTe, NetVigilance

L’équipe

- Céline Charbonnaud
  - Equipe d'Audit en charge de la qualité des services Après Vente Fournisseurs
    - Service Direction Après Vente
    - Airbus Central Entity
  - Développeuse
    - Bases de données, PHP, C++
    - VIGILANTe, NetVigilance

Pour nous contacter

- Mail
  - lmcr@free.fr
- Web
  - http://lmcr.free.fr
- Forum/Faq
  - http://lmcr.forumactif.com/index.htm

La journalisation

- L'équipe LogManager
- La journalisation
- Le constat
- L'idée de base
- L'implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

Définitions et Motivations

- Définitions
  - Enregistrement d'événements
  - Enregistrement d'états
- Motivations
  - Reflet d'une activité
  - Etude de facteurs spécifiques
  - Détection de défaillances
  - Mémoire
  - Aide à la décision
  - Surveillance
  - Elément de preuve

Diversité de la journalisation

- Multitude d'équipements et d'applications
  - Matériels et systèmes d'exploitation
  - Système d'information
  - Diversité de la qualité de la journalisation
- Multitude de besoins
  - Surveillance
  - Analyse
  - Statistiques
- Diversité de mises en œuvre
  - Motivées par les besoins
  - Assujetties aux moyens
  - Corrélées par l'analyse

Les apports de la journalisation

- Surveillance
  - Activité continue / Surveillance discontinue
    - Recours aux journaux
- Audit
  - Analyse d'informations spécifiques
- Comptabilité
  - Surveillance par la statistique
  - Support d'information pour statistiques
- Etude sur incident
  - Dysfonctionnement de systèmes
  - Incidents sécurité

Contraintes induites

- Mise en place et administration
- Obligation légales (CNIL)
- Qualité de service relative à la Journalisation
- Exploitation des informations collectées
- Protection des informations de la Journalisation
- Responsabilités des administrateurs

Devoirs liés à la politique de Sécurité

- Journalisation : Moyen essentiel pour couvrir certains objectifs de la politique de Sécurité
  - Traçabilité
  - Imputatibilité des actions
  - Aide à l'audit
  - Conservation des traces
- Devoirs énoncés par la politique de Sécurité
- Obligation de moyens lors de la conception et mise en place
- Obligations de résultats lors de la production

Réponse sur incident

- Journaux : Supports indispensables aux travaux relatifs à la Sécurité
- Journaux : Prépondérants pour la gestion d'un incident de Sécurité
  - Qualification
  - Etude de l'incident
  - Mesure de l'étendue des dégâts
  - Réparation
- Journaux : Eléments fondamentaux dans le cadre du d'une réponse sur incident

Qualification de l'incident

- Incident de Sécurité / Anomalie / autre
  - Evénements et états
    - Support des journaux : Système, Etats, Applications
- Manifestations
  - Traces suspectes ou explicites
    - Support des journaux : Réseau, Système, Applications
  - Modification du référentiel
    - Support du journal : Etats
- Compréhension du contexte
  - Besoin de retracer l'activité, de surveiller
    - Support des journaux : Réseau, Système, Applications
  - Besoin de référentiels
    - Support du journal : Etats

Etude de l'incident

- Depuis quand est-ce dans cet état ?
  - Historique
    - Support des journaux : Système, Etats, Applications
  - Modifications récentes
    - Support des journaux : Réseau, Système, Applications
- Comment cela s'est-il produit ?
  - Déviation d'une utilisation normale
    - Utilisation volontaire/involontaire d'une faille
      - Support des journaux : Réseau, Système, Applications
    - Dérive
      - Support des journaux : Système, Applications

Etude de l'incident

- Comment cela s'est-il produit (suite) ?
  - Attaque transversale ?
    - Quels services sont utilisés ?
    - Quelle activité système ?
      - Support des journaux
- Qui est à l'origine de l'incident ?
  - Connexions détectées ?
    - Connexion réseau
    - Connexion sur la machine
    - Connexion aux applications
    - Chemin réseau
      - Support des journaux

Mesure de l'étendue des dégâts

- Etude à partir du point d'impact constaté
  - Dégâts sur les applications
    - Support des journaux : Système, Etats, Application
  - Dégâts sur la machine
    - Support des journaux : Système, Etats
  - Dégâts sur les points de passage
    - Support des journaux : Réseau, Système, Etats, Application
  - Rayonnement sur les points accessibles depuis les éléments utilisés ou altérés
    - Support des journaux : Réseau, Système, Etats, Application

Réparation

- Sur la base de la compréhension de l'incident
- Sur la base de l'étude de l'étendue des dégâts
- Restauration et modification
  - Réparation des dégâts
    - Support des journaux : Système, Etats, Applications
  - Renforcement du système
    - Support des journaux : Réseau, Système, Etats, Application
- Période d'alerte consécutive à l'incident
    - Support des journaux : Réseau, Système, Etats, Application

Exigences, besoins et responsabilités

- Obligations pour l'administrateur
  - Exigences relatives à la journalisation présentes parmi les exigences Sécurité d'un système
  - Mise à disposition des responsables Sécurité des journaux par les administrateurs
- Besoins à satisfaire
  - Besoins internes
  - Relations avec un CERT
- Responsabilités pour les administrateurs
  - Mise en place du système de Journalisation
  - Maintenance du système de Journalisation
  - Exploitation des journaux

Le constat

- L'équipe LogManager
- La journalisation
- Le constat
- L'idée de base
- L'implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

Constat

- Des mondes très différents
  - Unix et Syslog
  - Microsoft et EventLog
  - SNMP et ses trap
  - CheckPoint et LEA
  - …
- Des sources très disparates
  - Équipements réseau (routeur, firewall, …),
  - Équipements Système (Unix, Microsoft, …),
  - Applications (mail, web, backup, …)
  - …

Vision locale/globale

- Chacun son domaine
  - Log réseau analysés par des admin réseau
  - Log système analysés par des admin système
  - Log applicatifs analysés par des admin application
- Pas de centralisation
  - Les logs restent à l'endroit de leur génération
  - Impossibilité de détecter une attaque d'envergure sur une société
  - Pas de politique de conservation globale

Le protocole Syslog

- Syslog devient limité
  - UDP
    - Pas de garantie d'acheminement
  - Non crypté
    - Informations « sensibles » par rapport à Internet
  - 24 facilités uniquement
    - Pas de place pour les nouveaux venus
  - 8 sévérités uniquement
    - Cela peut s'avérer un peu juste dans certains cas

Le protocole EventLog

- Spécifique au monde Microsoft
  - 3 facilités par défaut
    - Application, System, Security
  - chaque application peut créer sa facilité
    - DNS, MimeSweeper, …
  - 5 sévérités différentes
    - Error, Warning, Information, AuditSuccess, AuditFailure

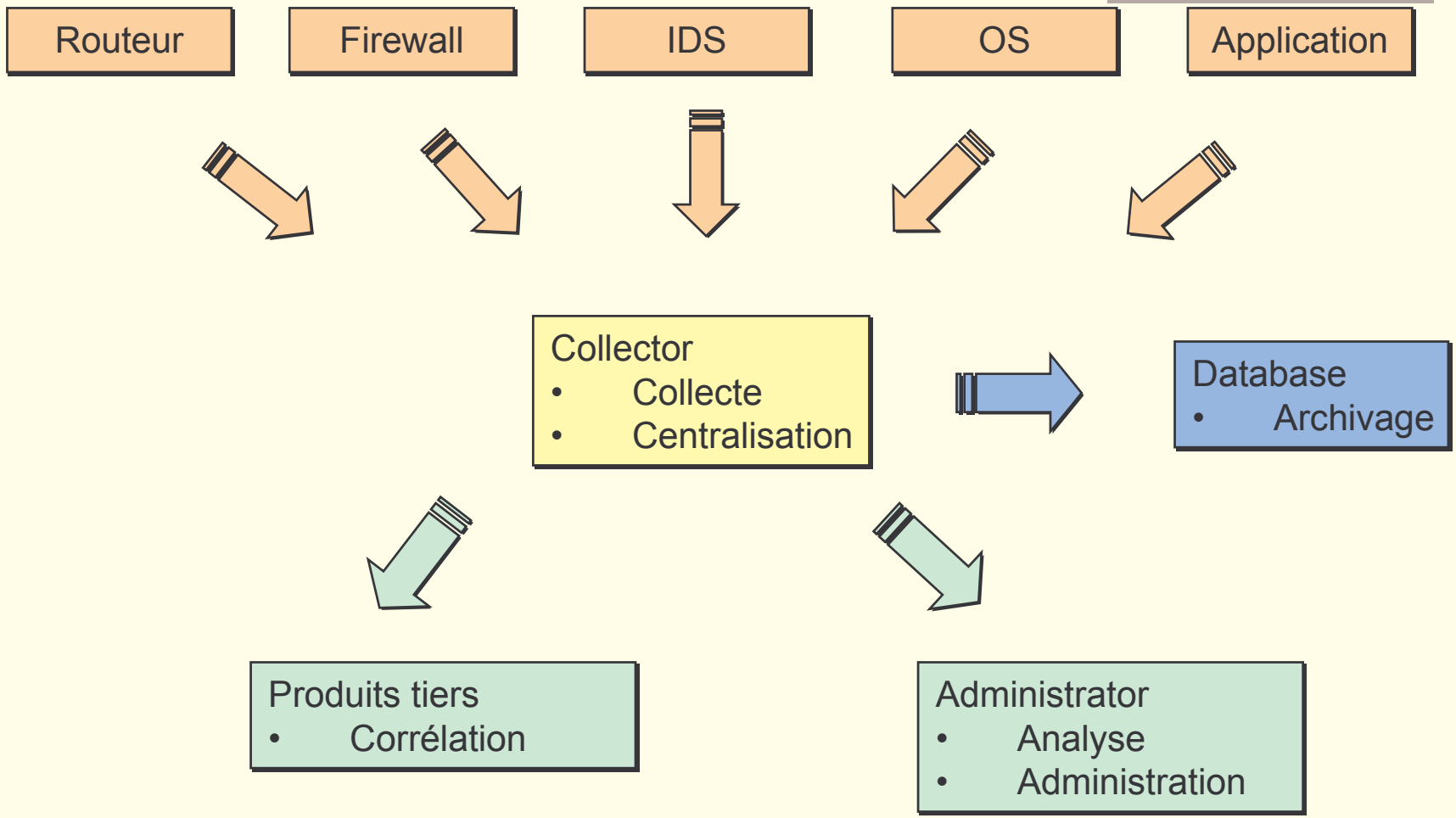
L’idée de base

- L’équipe LogManager
- La journalisation
- Le constat
- L’idée de base
- L’implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

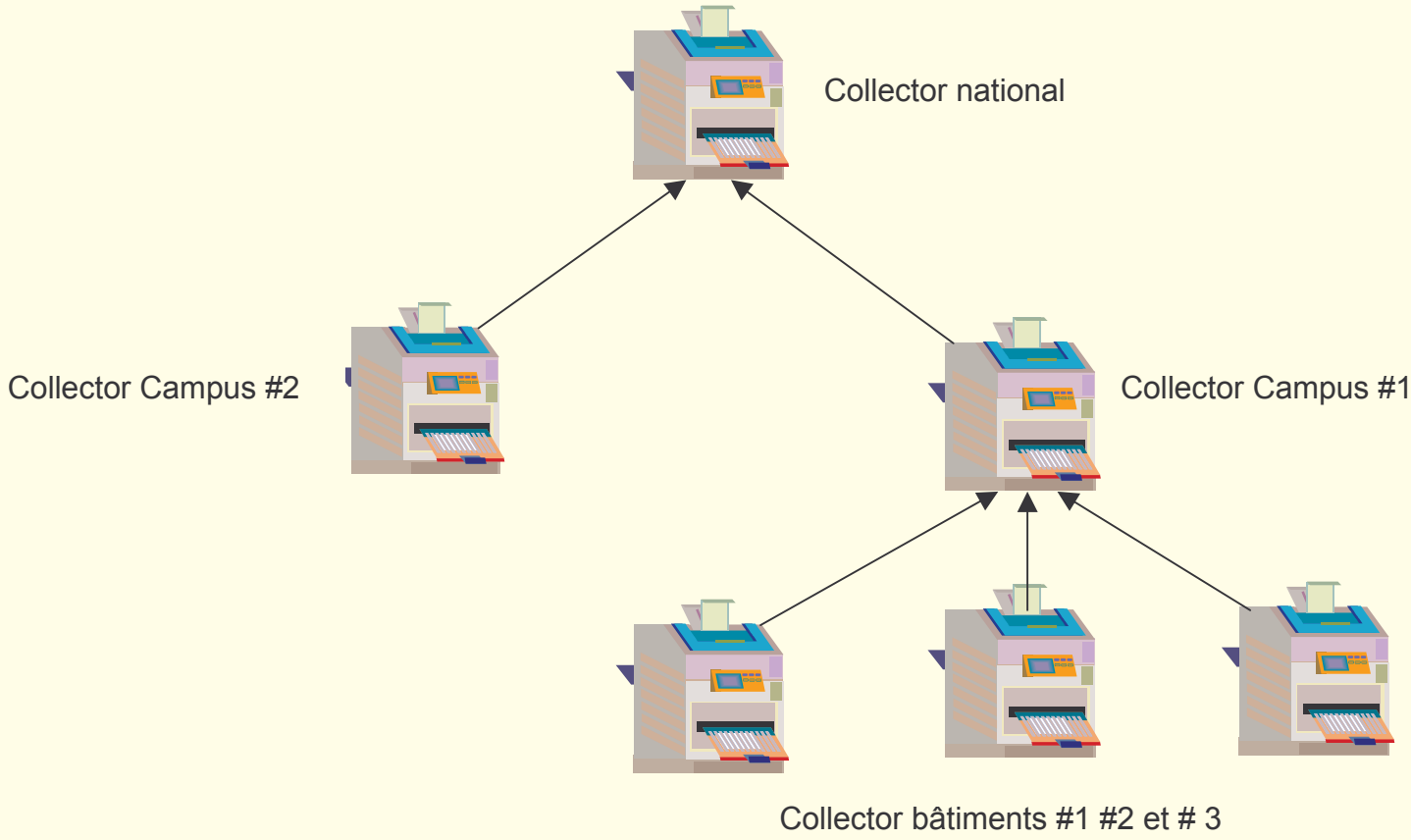
Un fédérateur de logs

- Des agents
  - Collecte
  - Centralisation
- Une base de données
  - Archivage
- Des clients
  - Analyse
  - Corrélation
  - Administration

Architecture



Une hiérarchie de collecte



Le protocole VipLog

- Protocole TCP ou UDP
  - UDP non crypté
  - TCP compressé (LZW) et crypté (SSL V3)
- Encapsule plusieurs protocoles
  - Syslog
  - EventLog
  - VipLog natif

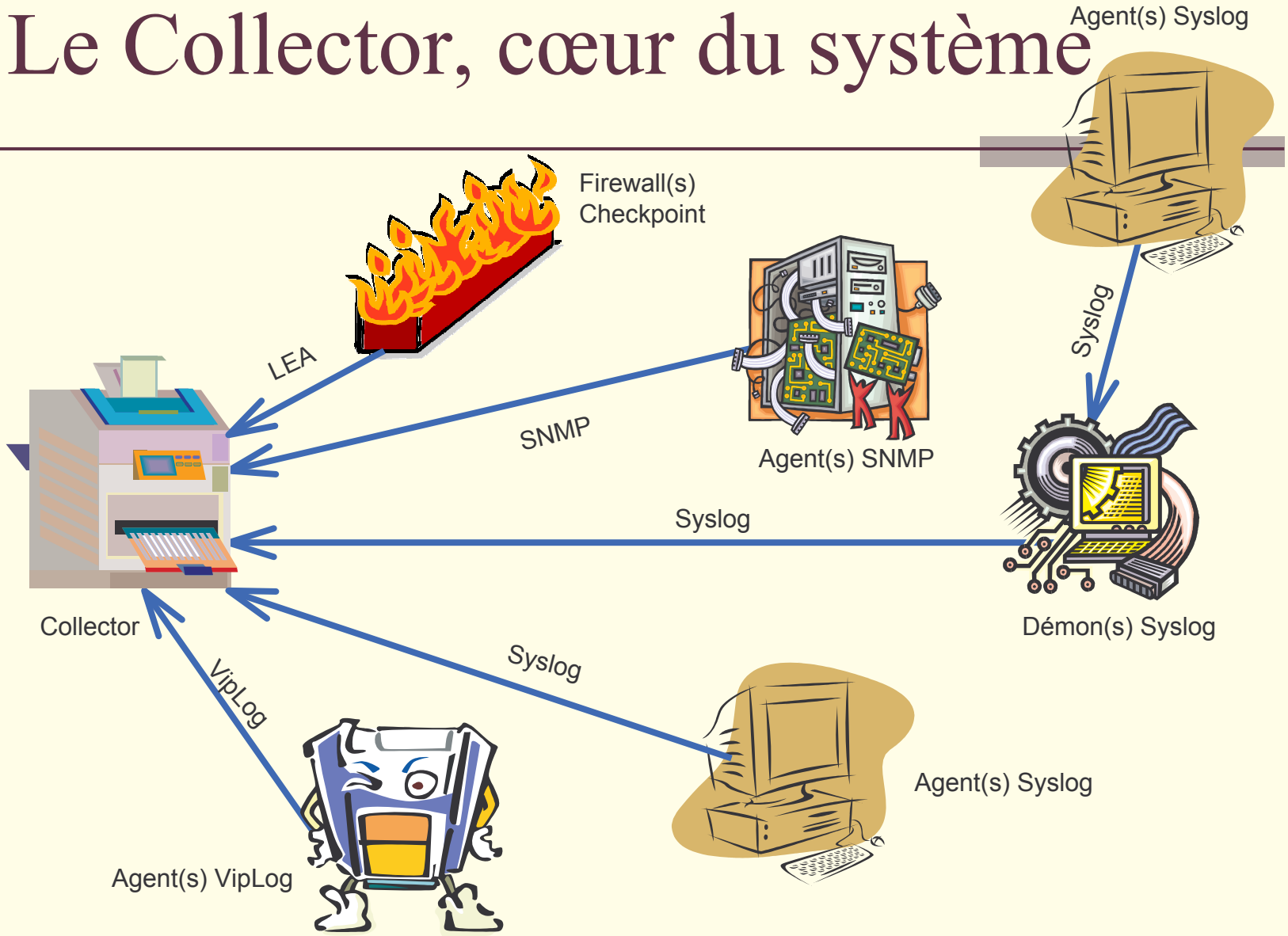
Le protocole VipLog

- Plus de possibilités que Syslog
  - Un numéro d'ordre
    - Pour détecter les messages de log perdus
  - Un tag horaire « complet » en UTC
    - Pour la corrélation transcontinentale
  - 4 milliards de facilités et autant de sévérités
  - Notions de thread, de process et d'utilisateur émetteur

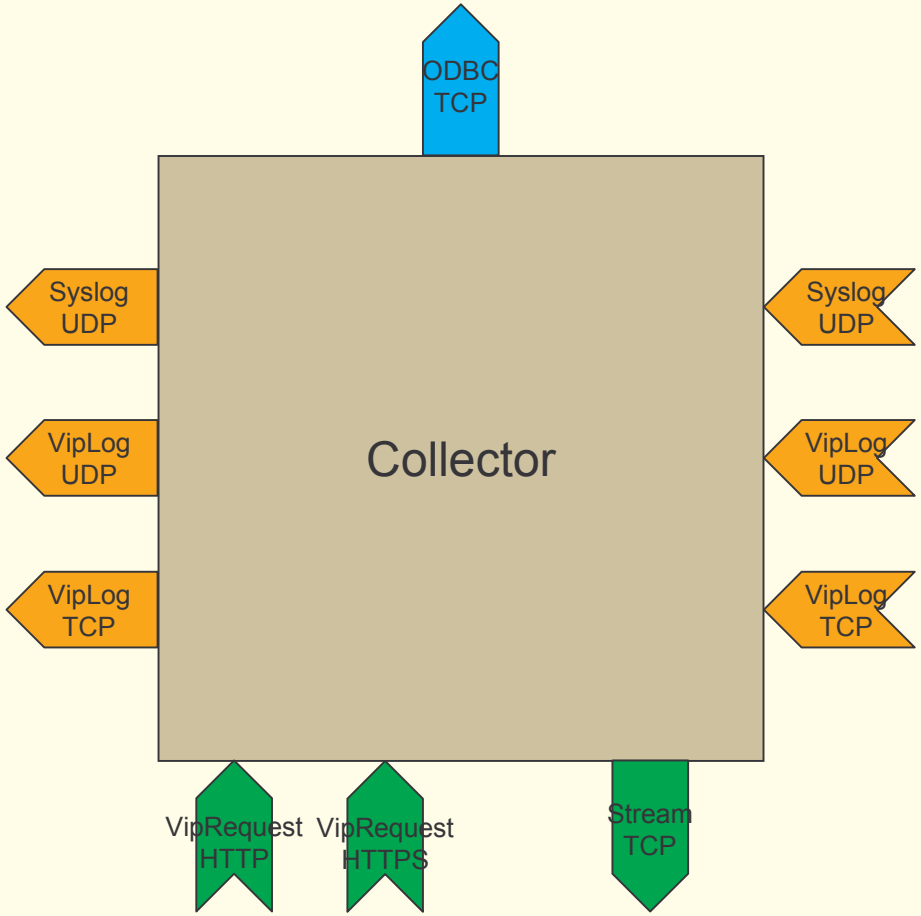
L'implémentation

- L'équipe LogManager
- La journalisation
- Le constat
- L'idée de base
- L'implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

Le Collector, cœur du système



Le Collector, cœur du système



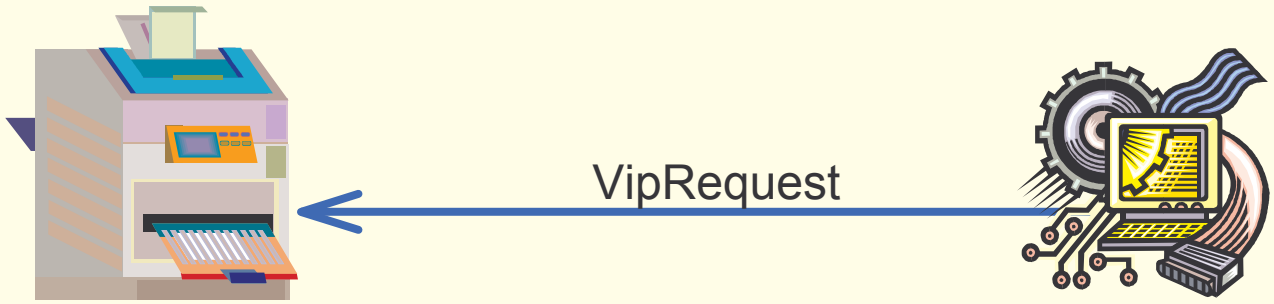
Protocoles de collecte et de relais

- Protocoles supportés
  - Syslog
    - UDP port 514
  - VipLog
    - TCP compressé et crypté
    - UDP non crypté
  - EventLog
    - Messages EventLog transformés en VipLog
    - Nécessite le composant EventCatch

Protocoles de collecte et de relais

- Protocoles pas encore supportés
  - Trap Snmp
    - UDP 162
  - LEA CheckPoint Firewall I
    - TCP crypté

VipRequest : protocole de requête



VipRequest : protocole de requêtes

- HTTP et/ou HTTPS
  - SSL Version 3 (si HTTPS)
  - Données formatées en XML
- Afficher les logs
  - En temps réel
  - En temps différé
- Administrer le Collector
  - Gérer les utilisateurs
  - Gérer la configuration

Requêtes existantes

- Connexion
  - Login
  - Logout
- Configuration
  - Getconfiguration
  - Setconfiguration
- Analyse des logs
  - Querydata
  - Querystream
- Gestion des utilisateurs
  - Adduser
  - Deluser
  - Getuser
  - Getuserlist
  - Getcommandlist
  - Setuser
  - Setpassword
- Informations diverses
  - Getversion
  - Getdatabaseinfo

Système ouvert

- Par la base de données
  - Le schéma de la base est disponible
- Par le protocole VipRequest
  - XML sur HTTP ou HTTPS
  - Le format des requêtes XML est disponible

Technologies utilisées

- Windows 2000 SP 4 ou XP SP2
- Visual C++ 6.0 / Visual Source Safe SP6
- SDK Microsoft (XP SP2)
- MFC 4.2
- API système Windows « standard »
- XML 3.0
- ODBC
- SqlServer 2000 / MSDE / MySQL 3.x et 4.x

Les composants de LogManager

- L'équipe LogManager
- La journalisation
- Le constat
- L'idée de base
- L'implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

Le composant Setup

- Utilise le compilateur de setup InnoSetup
  - http://www.jrsoftware.org/isinfo.php
- Prérequis
  - nécessite l'existence d'une base de données (MySql ou SqlServer ou MSDE)
  - nécessite des privilèges sur la base de données (mot de passe administrateur)

Le composant Collector

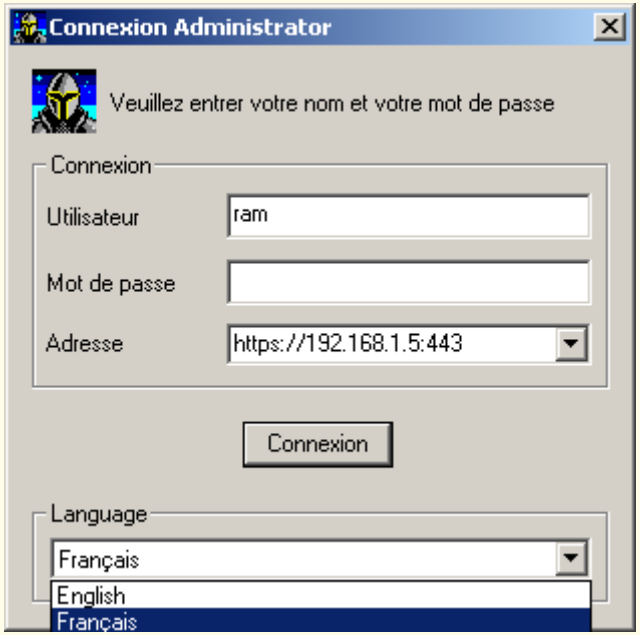
- C‘est le cœur du système
- OS supportés
  - Windows 2000 / XP
  - Tourne en tant que service
  - La communication avec la database utilise ODBC

Le composant EventCatch

- Passerelle Microsoft EventLog vers VipLog
- OS supportés
  - Windows 2000 / XP
  - Tourne en tant que service
- Mapping EventLog vers VipLog configurable
  - facilité et sévérité
- Un composant EventCatch par machine à superviser
  - DLL de décodage des messages installée spécifiquement par l'application
  - Utilisateur par forcément global/domain

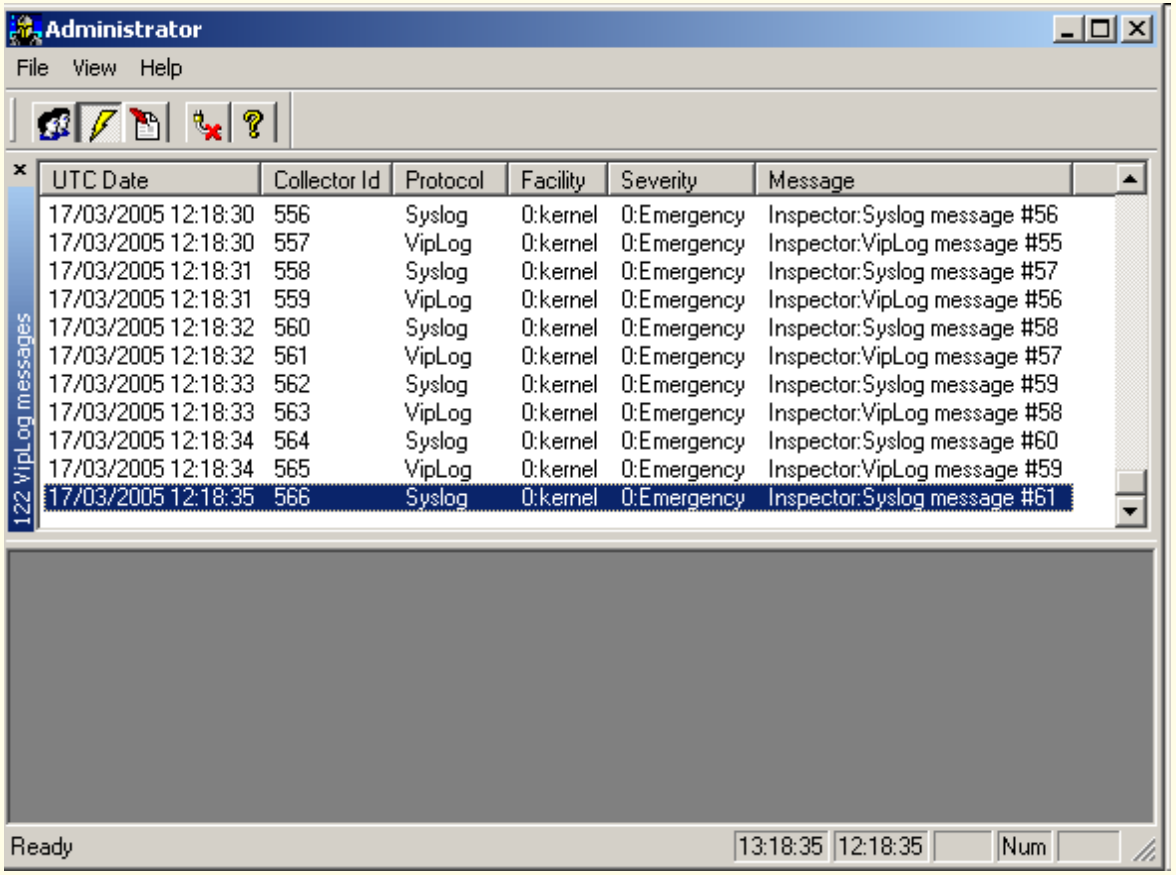
Le composant Administrator

- Support multi language unicode
  - Actuellement Français et Anglais



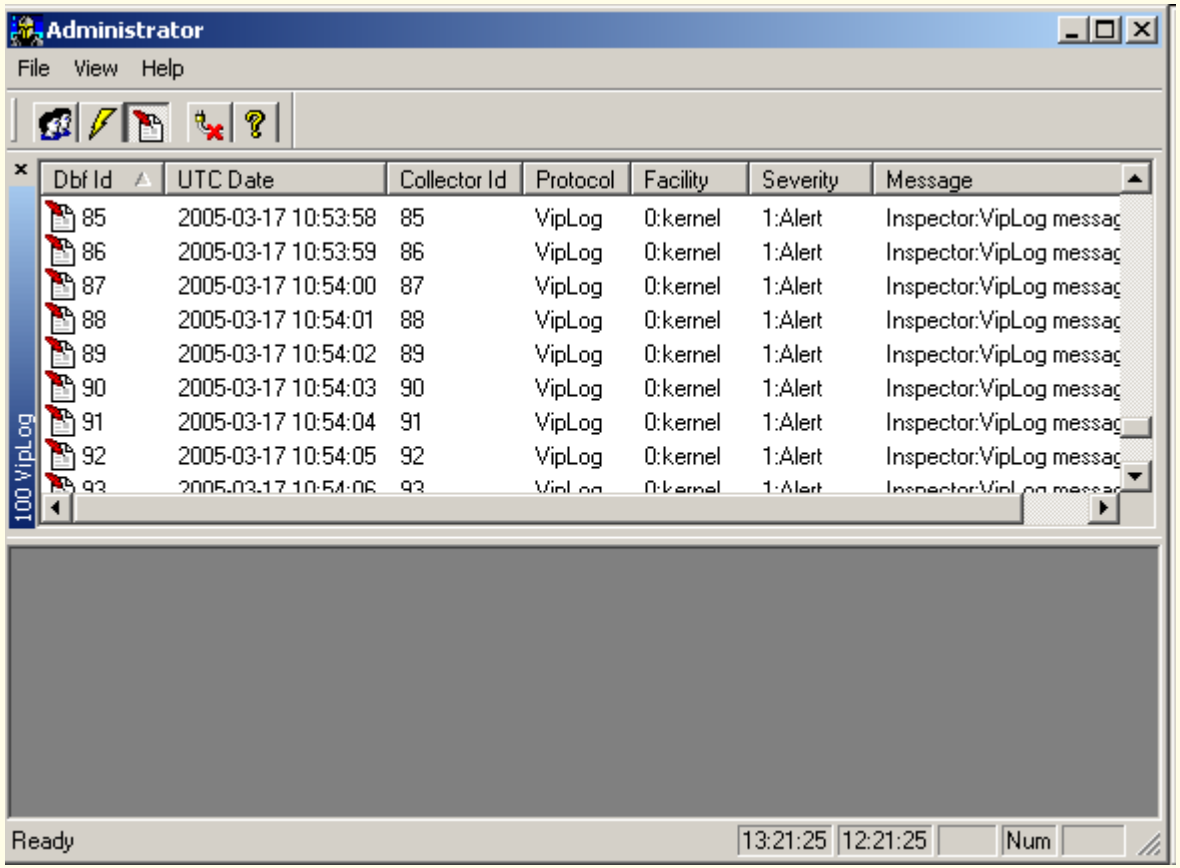
Le composant Administrator

- Suivi en temps réel des messages de log



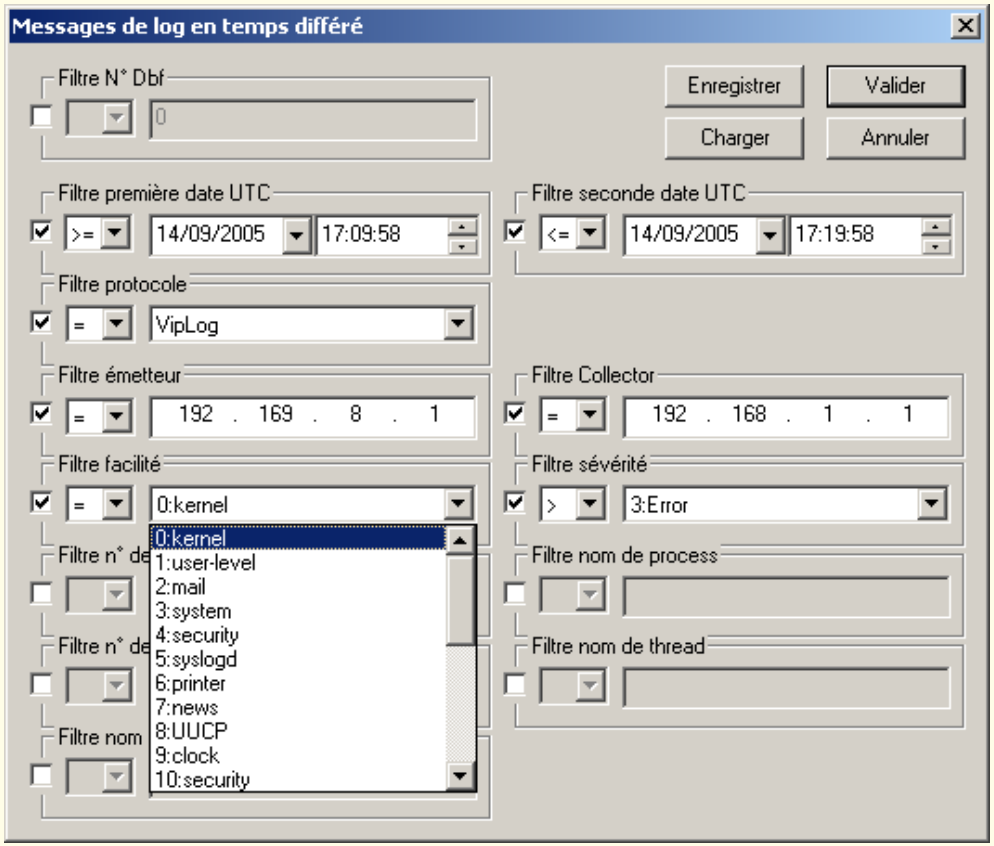
Le composant Administrator

- Analyse en temps différé des messages de log



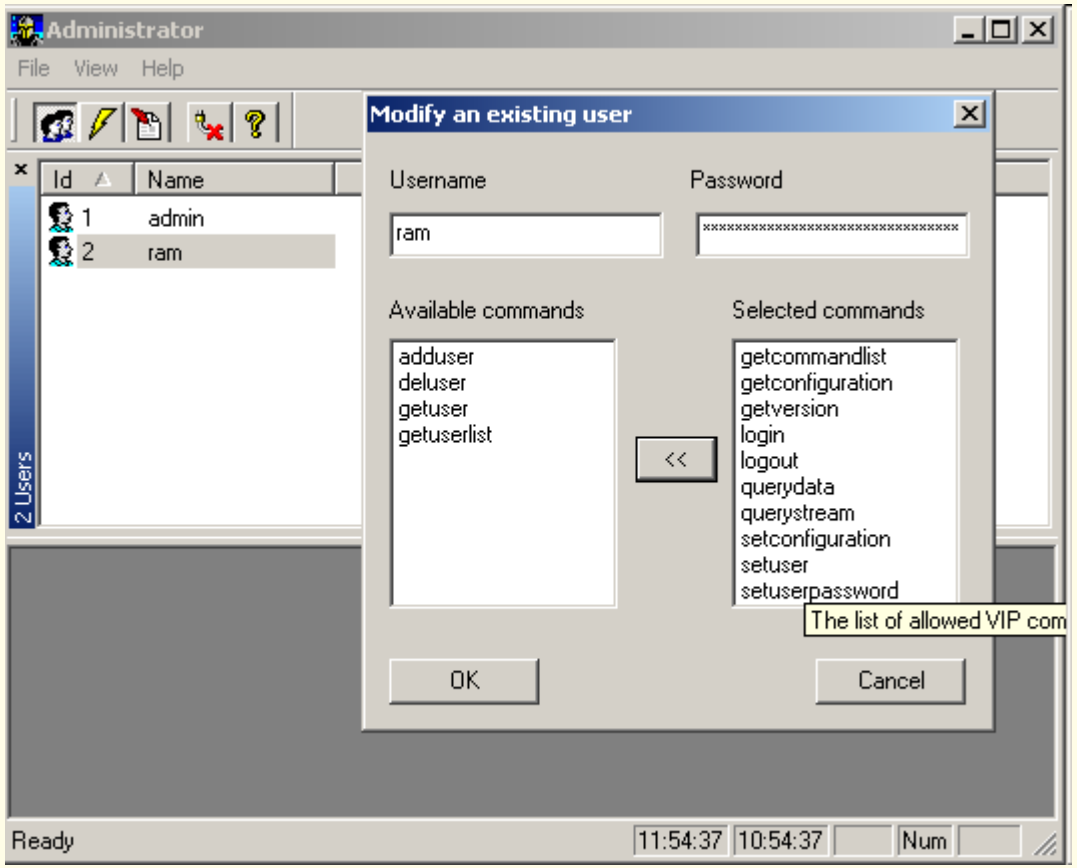
Le composant Administrator

- Filtrage des messages de log



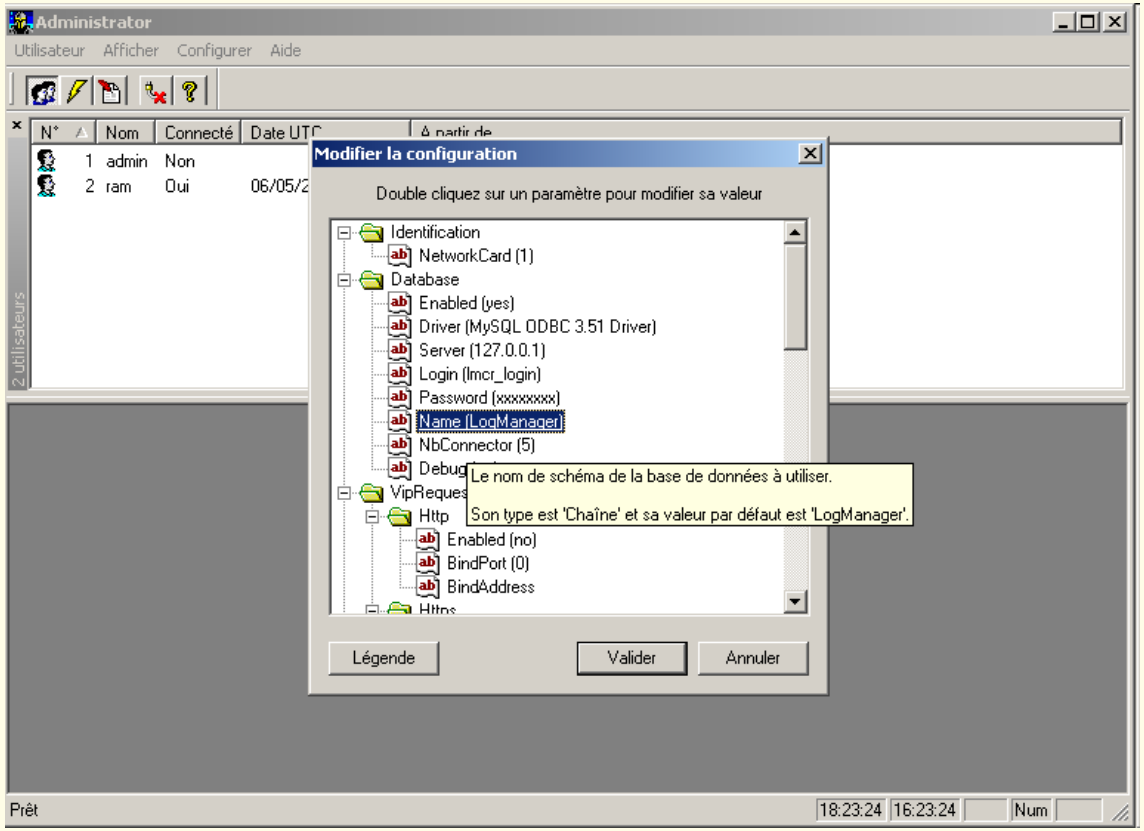
Le composant Administrator

- Gestion des utilisateurs



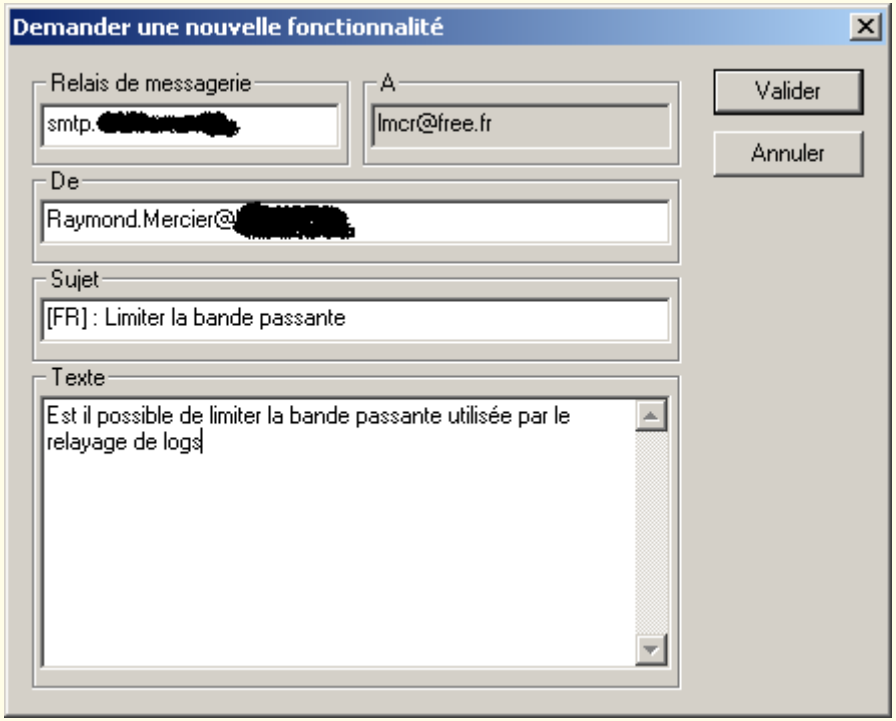
Le composant Administrator

- Gestion de la configuration



Le composant Administrator

- Contacter le support



Les autres composants

- API VipLog
  - Utilisable par des produits tiers
  - Permet de générer des événements VipLog UDP
  - OS supportés : Windows 2000 / XP
  - Format : librairie, DLL ou sources
- Inspector
  - Outil utilisé pour tester et debugger le produit
  - Livré « en l'état »
- Documentation
  - Manuel de référence format PDF
  - En anglais

Exemple de déploiement

Déploiement réel

- Equipement générant des logs
  - Syslog
    - 2 routeurs Cisco sur Internet
    - 3 serveur de mail linux
    - 3 serveur DNS linux
  - EventLog
    - 1 serveur antivirus messagerie
- Volumétrie
  - 1 log par seconde environ
  - 100 000 logs par jour environ
  - Effacement des logs plus vieux que 2 mois
  - 5 000 000 logs dans la base de données

Déploiement réel

- Machine utilisée
  - Machine dédiée (Collector + EventCatch)
  - Pentium III
  - 600 Mhz
  - 128 Mo RAM
  - Quelques % de CPU

Déploiement réel

- Quelques statistiques d'utilisation

Paramètre	Valeur
Version des composants	
Administrator	1.2.123.334
Collector	1.2.134.418
Base de données	3
Protocole VipRequest	1.0
Protocole VipLog	1
Date & heure des composants	
Date UTC du Collector	14/09/2005 15:27:20
Date locale du Collector	14/09/2005 17:27:20
Date UTC de la base de données	14/09/2005 15:27:20
Date locale de la base de données	14/09/2005 17:27:20
Démarrage du Collector	
Date UTC de démarrage	02/08/2005 07:46:36
Démarré depuis	1 month 12 days 7 hours 40 minutes 44 seconds
Base de données	
Driver ODBC	MySQL ODBC 3.51 Driver
LMCR_LogData	4 899 958
LMCR_Facility	25
LMCR_Severity	8
LMCR_Protocol	3
LMCR_User	3
LMCR_Command	15
LMCR_Right	30
LMCR_Configuration	2

Conclusions

- L'équipe LogManager
- La journalisation
- Le constat
- L'idée de base
- L'implémentation
- Les composants de LogManager
- Exemple de déploiement
- Conclusions

Droits d'utilisation

- Usage libre
  - Même pour des utilisations commerciales

- Copyright sur les sources
  - Copyright © 2004-2005 C.Charbonnaud & R.Mercier.

Roadmap

- Agrégation et corrélation des logs
  - Support IDMEF
- Génération de rapports
- Ajout de nouveaux protocoles de collecte
  - Checkpoint LEA
  - Trap Snmp ?
- Importation d'événements ?
- Support Base de données
  - Oracle, Sybase
- Haute disponibilité
- Portage sous Linux
- Signature « à la volée » des logs en base

Aujourd'hui

- Première version stable (version 1.2)
  - Les fonctions de collecte, d'archivage et d'analyse « temps réel et temps différé » sont assurées
- Le produit doit être confronté au monde réel
  - Attente de feedback
  - Utilisation dans différents environnements

Ambition

- Faire que LogManager devienne une référence dans la gestion, l'analyse et la corrélation de logs

- Questions ?