Présentation du relais HTTP Open Source Vulture

Arnaud Desmons <ads@INTRINsec.com>
Jérémie Jourdin <jjn@INTRINsec.com>

Présentation

- Motivations
- Historique
- Démonstration
- Présentation fonctionnelle
- Présentation technique
- L'interface d'administration
- Roadmap

Motivations

- Ouvrir les applications web sur Internet
- Contrôler les accès
- Centraliser les accès
- Ne pas modifier l'existant

Historique (1/2)

- INTRINsec intègre de nombreux proxy inverse
- Utilisation quasi systématique d'Apache
  - Le client manque souvent de compétences Open Source
  - Besoin croissant d'authentification forte
  - Pas de solution simple pour gérer les accès
  - Chaque client est un cas particulier ⇨ configuration particulière
- Vulture sort en GPLv2 en août 2004
  - Utilisation d'Apache 2 / Interface d'administration Web
  - L'interface intègre une gestion simple des ACLs
  - Vulture = Interface de configuration d'Apache
  - Les limites de Vulture sont celles d'Apache

Historique (2/2)

- Des besoins non couverts par Apache
  - Nécessité du SSO
  - Nécessité de s'authentifier sur les applications
  - Contrôle d'accès unique, et indépendant du protocole
    - SQL, LDAP, RADIUS, X509...

- VultureNG sort en GPLv2 en mars 2005
  - Utilisation d'Apache 2 / Interface d'administration Web
  - mod_perl prend en charge l'authentification
  - Système de plugin pour les méthodes d'authentification
  - Vulture ≠ Interface de configuration d'Apache
  - Les limites de Vulture sont celles de Perl

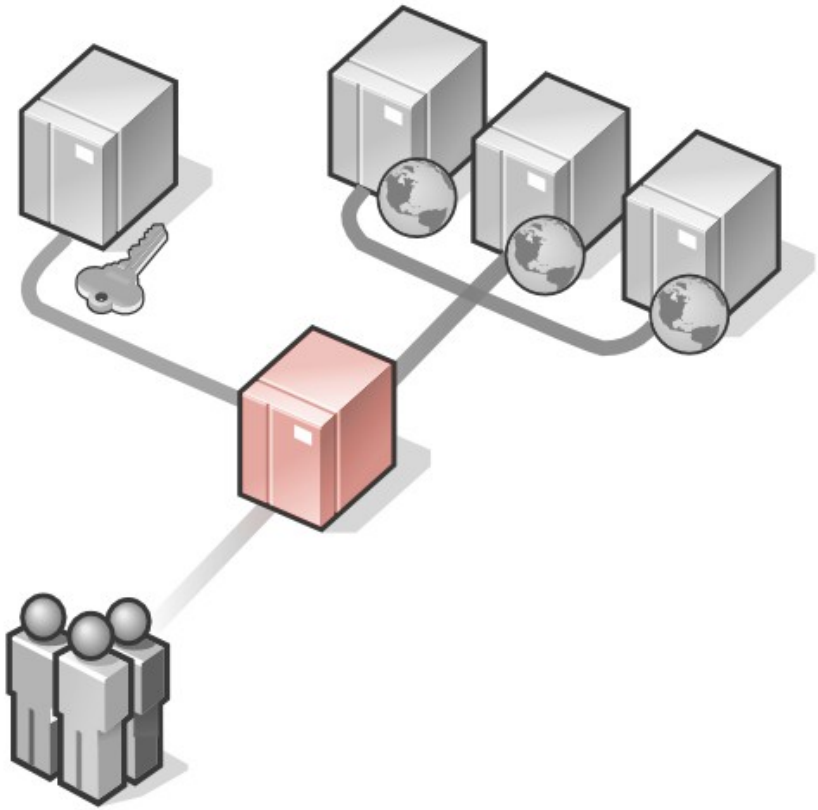
Présentation fonctionnelle

- Proxy Inverse
- Filtrage et réécriture
- Authentification
- Single Sign On
- Démonstration
- Propagation de l'authentification
- Démonstration

Proxy Inverse

Présentation fonctionnelle

- Pare-feu applicatif
- Point d'accès unique
- Filtrage au niveau IP
- Répartition de charge possible



Filtrage et réécriture

Présentation fonctionnelle

- Réécriture des URL
  - Redirection interne
  - Redirection externe
  - Redirection vers un code d'erreur
- Réécriture des entêtes permettant de transférer de l'information
  - IP du client
  - Variables du certificat
  - Constantes

Authentification

Présentation fonctionnelle

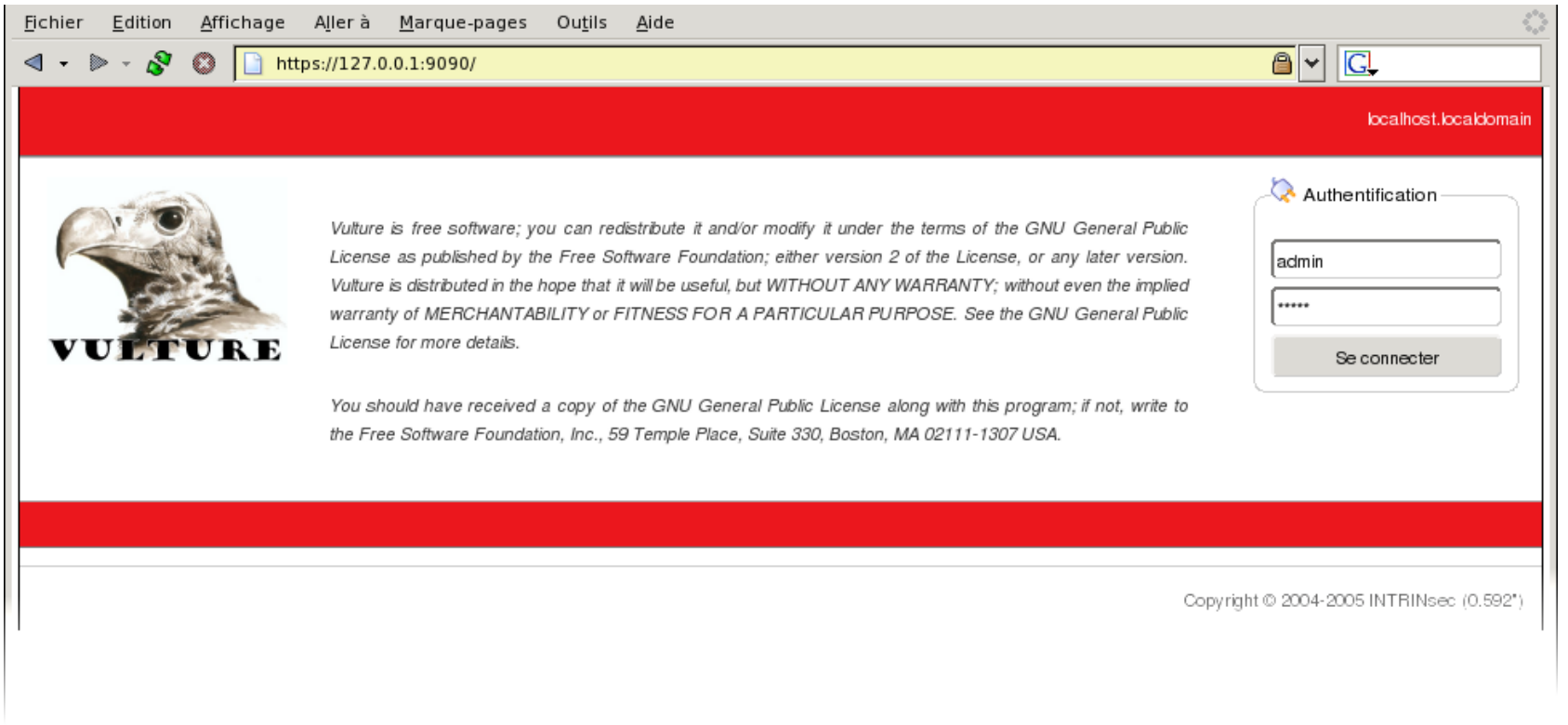
- Modules d'authentification intégrés
  - SQL
  - LDAP / Active Directory
  - Par certificat numérique
- ACL possibles pour chaque module
  - Configurables depuis l'interface
  - Par utilisateur, par groupe, par champs du certificat

Single Sign On

Présentation fonctionnelle

- Si plusieurs applications partagent la même méthode d'authentification, Vulture ne demande le mot de passe qu'une seule fois à la première connexion de l'utilisateur et ce, sans configuration particulière.

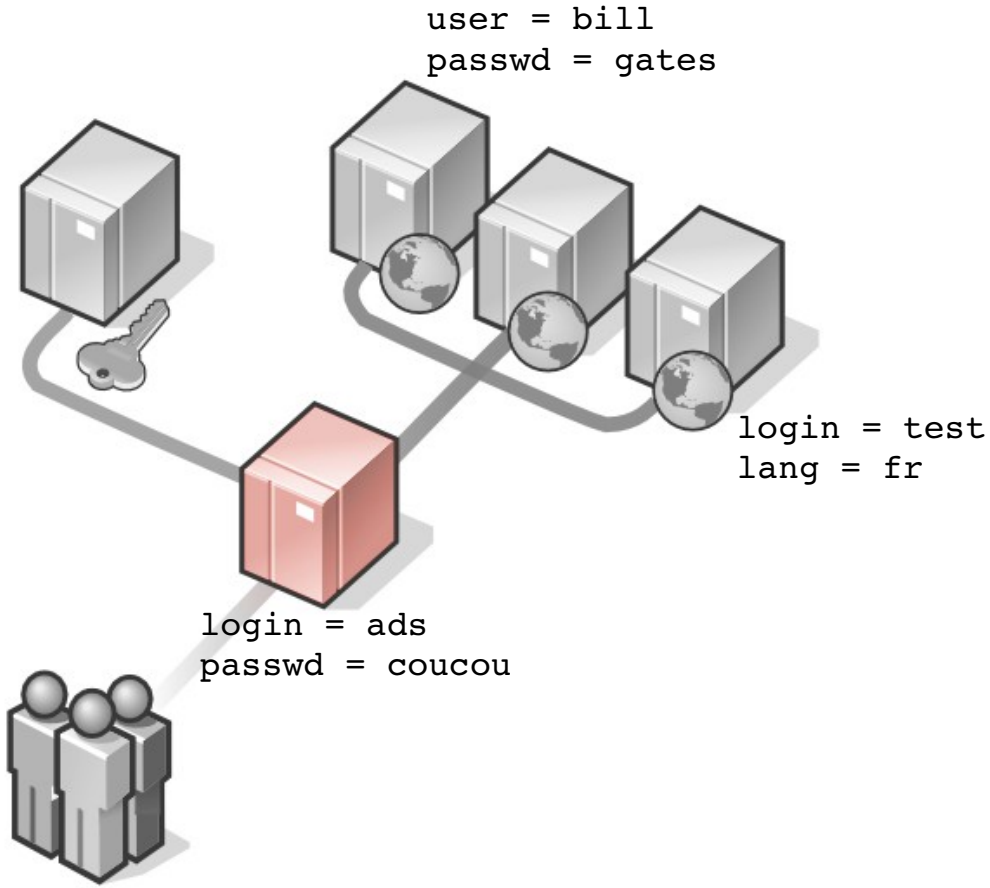
Démonstration



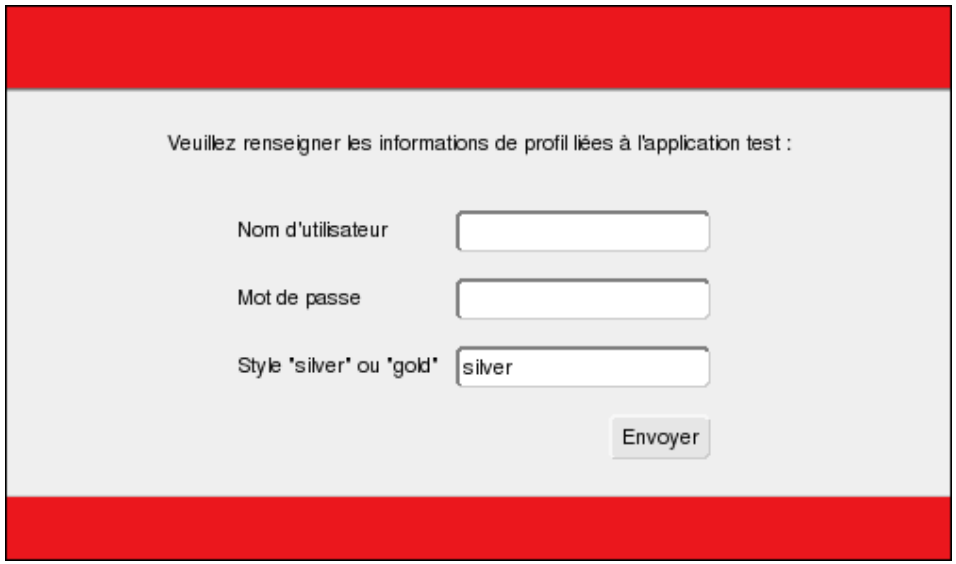
Propagation de l'authentification

Présentation fonctionnelle

- Permet d'associer un profil applicatif à une authentification
- Permet avec le SSO de centraliser l'authentification des applications sans modifications



Démonstration



Présentation technique

intrinsec. SÉCURITÉ INFORMATIQUE

- Architecture
- Proxy Inverse
- Filtrage et réécriture
- Authentification
- Single Sign On
- Propagation de l'authentification
- Packaging et installation
- Interface d'administration

Architecture

Présentation technique

- Interface d'administration
  - mod_php (avec support SQLite)
- Fichier de configuration Vulture
  - Fichier de base de données SQLite
- Proxy inverse Apache
  - mod_perl + DBD::SQLite
  - mod_proxy

Proxy inverse

Présentation technique

- Utilisation de mod_proxy
  - Robuste et performant
  - Supporte les protocoles FTP, HTTP et CONNECT (pour le SSL).
  - Accessible depuis mod_perl...
- Répartition de charge
  - Vulture choisit aléatoirement une URL privée parmis plusieurs définies pour une application

Filtrage et réécriture

intrinsec. SÉCURITÉ INFORMATIQUE

Présentation technique

- Utilisation de mod_perl
  - Permet d'accéder à la plupart des données traitées par Apache
    - Requêtes
    - Réponses
    - Entêtes
    - IP du client
    - Accès au module mod_ssl
  - Permet de profiter de la puissance des expressions régulières
    - `^/redirect=(.*) => http://$1 [R]`
    - `^/redirect=(.*) => http://$1 [P]`
    - `admin => [403]`
    - `^/admin => /enroll.php [NOCERT,P]`

Authentification (1/2)

Présentation technique

- Authentification LDAP
- Authentification SQL
- Authentification par certificat
- ACL
  - Stockage en base SQLite des ACL
  - Cumul avec l'authentification normal
  - Utilisation de la PKI Rooster

Authentification (2/2)

Présentation technique

- Les différentes méthodes d'authentification se basent sur les modules Perl :
  - `Net::LDAP`
  - `DBD::SQLite`
  - `DBD::Pg`
  - `Apache::SSLLookup`
- Pour la gestion des ACL depuis l'interface PHP :
  - Support LDAP/AD
  - PEAR
  - XML-RPC pour l'interrogation de la PKI Rooster

SSO (1/2)

Présentation technique

```
GET / HTTP/1.1
Host: app1:4242

HTTP/1.x 200 OK
Set-Cookie: vulture=5e18a8702397dd0fbf235fea96e6b123; path=/
Location: https://secure/?vulture=5e18a8702397dd0fbf235fea96e6b123
```

```
GET /?vulture=5e18a8702397dd0fbf235fea96e6b123 HTTP/1.1
Host: secure

HTTP/1.x 401 Authorization Required

GET /?vulture=5e18a8702397dd0fbf235fea96e6b123 HTTP/1.1
Host: secure
Authorization: Basic YWRtaW46YWRtaW4=

HTTP/1.x 200 OK
Set-Cookie: vulture=cccf9f0264cc644faf03ec9c6a79aced; path=/
Location: http://app1:4242
```

```
GET / HTTP/1.1
Host: app1:4242
Cookie: vulture=5e18a8702397dd0fbf235fea96e6b123

HTTP/1.x 200 OK
...
```

SSO (2/2)

Présentation technique

```
GET / HTTP/1.1
Host: app2:4242

HTTP/1.x 200 OK
Set-Cookie: vulture=32b61b6e70237dd0f97dd0feaf6b1b69; path=/
Location: https://secure/?vulture=32b61b6e70237dd0f97dd0feaf6b1b69
```

```
GET /?vulture=32b61b6e70237dd0f97dd0feaf6b1b69 HTTP/1.1
Host: secure
Cookie: vulture=cccf9f0264cc644faf03ec9c6a79aced
```

```
GET / HTTP/1.1
Host: app2:4242
Cookie: vulture=32b61b6e70237dd0f97dd0feaf6b1b69

HTTP/1.x 200 OK
...
```

SSO Forward

Présentation technique

- Les informations sensibles du profil sont chiffrées avec le mots de passe de l'authentification associée (ou un code PIN si par certificat)
- Les informations non sensible des profils sont accessibles depuis l'interface

- Authentification par formulaire
  - Utilisation de la libwww dans mod_perl pour poster les informations et récupérer un cookie à la volée

- Authentification htaccess
  - Génération du digest directement dans mod_perl

Packaging et installation

Présentation technique

- Gentoo (dans l'arborescence officielle)

```
# emerge vultureng
# echo "apache ALL=NOPASSWD:/usr/sbin/apache2" >> /etc/sudoers
# /etc/init.d/vultureng start
```

- Mandriva (dans les contribs)

```
# urpmi VultureNG
```

- Windows
  - http://groups.open-source.fr/viewtopic.php?t=25
- RPM INTRINsec-common

```
# rpm -i INTRINsec-common.rpm VultureNG.rpm
```

- Sources
  - http://docs.open-source.fr/doku.php?id=vultureng:install

Interface d'administration

- Utilisation de phpmvc
  - Portage en PHP de Struts
  - Egalement utilisé pour Rooster et Owl
  - Abstraction de la base de données
  - Protection contre l'injection SQL
- Démonstration
  - Gestion des interfaces réseau
    - Portail SSO
  - Méthodes d'authentification
  - Règles de réécriture
  - Répartition de charge
  - Gestion des filtres applicatifs
  - Gestion des formats de journalisation

Roadmap

- Cumul des méthodes d'authentification
  - Opérateurs logiques entre les méthodes d'authentification (ET, OU)
- Haute disponibilité
  - Combinaison de la répartition de charge et de la détection d'indisponibilité
- Module d'apprentissage
  - Génération de whitelist
- Système de plugin pour les modules d'authentification
- Authentification Radius et SecureID

Questions