JoSy
Journées
Systèmes

RESINFO

802.1X avec Certificats

Au centre d'Etudes Nucléaires de Bordeaux-Gradignan

Serge Bordères
(Centre d'Etudes Nucléaires de Bordeaux-Gradignan)

20 mars 2007

Institut d'Astrophysique de Paris

Environnement et historique du CENBG

- UMR CNSR/IN2P3 , Université Bordeaux 1
- 100 permanents
- Vingtaine de thésards, stagiaires, visiteurs
- Le réseau est également utilisé par le LCNAB qui représente environ 20 personnes

- 7 groupes de recherche
- 5 services
- Un accélérateur (instrumentation connectée sur le réseau)

Environnement et historique du CENBG

Epoque filaire

- Depuis 2001, segmentation du réseau en 20 sous-réseaux (VLAN)
  - ✓ Un sous-réseau par groupe/service
  - ✓ Sous-réseau “visiteurs”
  - ✓ Sous-réseau pour l'instrumentation de l'accélérateur
  - ✓ DMZs, serveurs
- Chaque PC est placé automatiquement dans son VLAN
- Utilisation de **VMPS** avec des commutateurs Cisco.

Epoque filaire et WIFI

- A partir de fin 2002, début du déploiement du WIFI avec le même objectif:
  - ✓ Chaque PC est placé dans son VLAN quelque soit sa méthode de connexion, filaire ou WIFI (PEAP)
- Installation d'un serveur **Freeradius**, mise en oeuvre de **802.1X** (Wifi)
- 2006 : Début du remplacement de VMPS par Radius sur le filaire
- 2007 : Authentification par certificat

Environnement et historique du CENBG

- 22 commutateurs (Cisco, HP) – 20 compatibles VMPS – 2 compatibles Radius
- 6 bornes Wifi (Cisco AP1230) compatibles Radius
- Environ 280 postes utilisateurs (hors visiteurs et postes persos) – Windows et Linux (machines de bureau/portables + petits calculateurs + instrumentation/acquisition)
- Dont environ 60 postes Wifi – essentiellement Windows
- Environ 50 postes « privés » + quinzaine de postes visiteurs
- Une vingtaine de serveurs
- Une dizaine d'imprimantes
- Sous contrôle de Radius

  ~ 60 postes Wifi
  ~ 30 postes filaires

- Le reste sous contrôle VMPS
- Evolution prévue de l'architecture

Usage de PEAP et problèmes

- Utilisation du login/password du domaine Windows
- Croisé avec l'adresse MAC du poste de travail

Pour se connecter il faut :

- ✓ Le bon login/password
- ✓ Le poste de travail associé (adresse MAC)

Problèmes

- Sur les clients Linux, le mot de passe est stocké en clair ⟶ Danger poste nomade
- La configuration du supplicant nécessite la présence de l'utilisateur
- Authentification à l'ouverture de session (pas de réseau avant et après)
- Authentification liée à l'utilisateur

La situation “idéale” souhaitée

- Mise en oeuvre du WiFi aussi proche et simple pour l'utilisateur que la mise en oeuvre du filaire (plug en play)
- Réseau disponible dès le boot, sans ouverture de session
- Authentification de la machine et positionnement sur un VLAN (le même en filaire et en sans-fil)
- Configuration simple sans présence de l'utilisateur

La solution des certificats

- **Certificat Utilisateur**

  ✓ Nécessite une gestion par l'utilisateur (demande, renouvellement)
  ✓ Nécessite la présence de l'utilisateur pour la configuration (installation du certificat)
  ✓ Authentifie l'utilisateur et pas la machine

Administration et usage compliqués

- **Certificat machine**

  ✓ Gérer par les administrateurs
  ✓ Pas de présence de l'utilisateur pour la configuration
  ✓ Lié à la machine et pas un utilisateur

Bon candidat

Utilisation des certificats CNRS ?

- Techniquement, pas de problème avec les certificats CNRS

Mais ….

- Expiration du certificat (CNRS: 2 ans pour machine)
  - ✓ Gestion lourde
  - ✓ Risque de bloquage des utilisateurs

- Création et renouvellement du certificat uniquement par les Autorités d'Enregistrement du labo
  - ✓ Problème : Les postes sont installés et configurés par un technicien qui n'est pas AE.

- Le supplicant Windows n'est pas compatible avec « la protection renforcée de la clé privée » (passphrase)
  - ➢ Ne pas fournir de passphrase sur des certificats CNRS présents sur des postes nomades n'est pas envisageable.

Peut-on lever ces problèmes ?

Création d'une IGC locale

- Créer une autorité de gestion de certificats spécifique au labo (**certificats réseau**)
- Ces certificats sont utilisables **uniquement** pour l'authentification sur le réseau local
- Pour toutes autres applications (accès depuis l'extérieur par ex) le certificat CNRS est utilisé

Réponses aux problèmes précédents

- Expiration

On peut décider que les certificats réseau n'expire pas
parce qu'ils sont à usage interne uniquement

- Création/renouvellement

Le technicien peut créer les certificats réseau (exécution d'un script)

- Authentification de la machine

Le certificat est croisé avec l'adresse MAC. Il faut le certificat + l'adresse MAC correspondante

- Protection renforcée

Les certificats réseau n'ont pas de passphrase parce qu'ils sont à usage interne uniquement et qu'il faut les utiliser avec le poste d'adresse MAC correspondante.

Comment créer une IGC locale (Linux) ?

- Récupération de l'utilitaire CA
http://www.formation.ssi.gouv.fr/stages/documentation/architecture_securisee/igc.html

- Adaptation pour automatiser la création des certificats

- Création du certificat de l'autorité locale

- Création des certificats réseau (CN=nom de la machine)
(exécution de CA avec le nom de la machine en paramètre)

- Le résultat : un fichier PKCS12

Intégration de l'autorité locale dans Freeradius

Question :

Qu'elle doit être l'autorité de certification du serveur, CNRS ou locale ?

Réponse : CNRS

- Le client a besoin **uniquement** du certificat de l'autorité qui certifie le certificat du serveur.
- Il est plus intéressant pour le client de disposer du certificat de l'autorité du CNRS parce qu'il peut en avoir besoin pour d'autres applications.
- Le certificat de l'autorité locale n'est pas utile sur le poste client.

Intégration de l'autorité locale dans Freeradius

Question :

Le serveur doit t'il pouvoir authentifier des certificats CNRS en plus des certificats réseau ?

Réponse : Oui, éventuellement

- Pour conserver la possibilité de traiter des cas où un certificat CNRS devrait être utilisé pour le client
- Un serveur Freeradius sait valider les certificats émis par différentes autorités

Configuration du serveur FreeRadius

Le module tls du module eap doit être configuré ainsi :

```
tls {
      private_key_file = ${raddbdir}/certs/serveur-radius.key
      certificate_file = ${raddbdir}/certs/serveur-radius.crt
            .
            .
            .
      CA_path=/etc/raddb/CA
      check_crl = yes ou no

      check_cert_cn=%{Stripped-User-Name:-%{User-Name:-None}

  }
```

Certificat du serveur

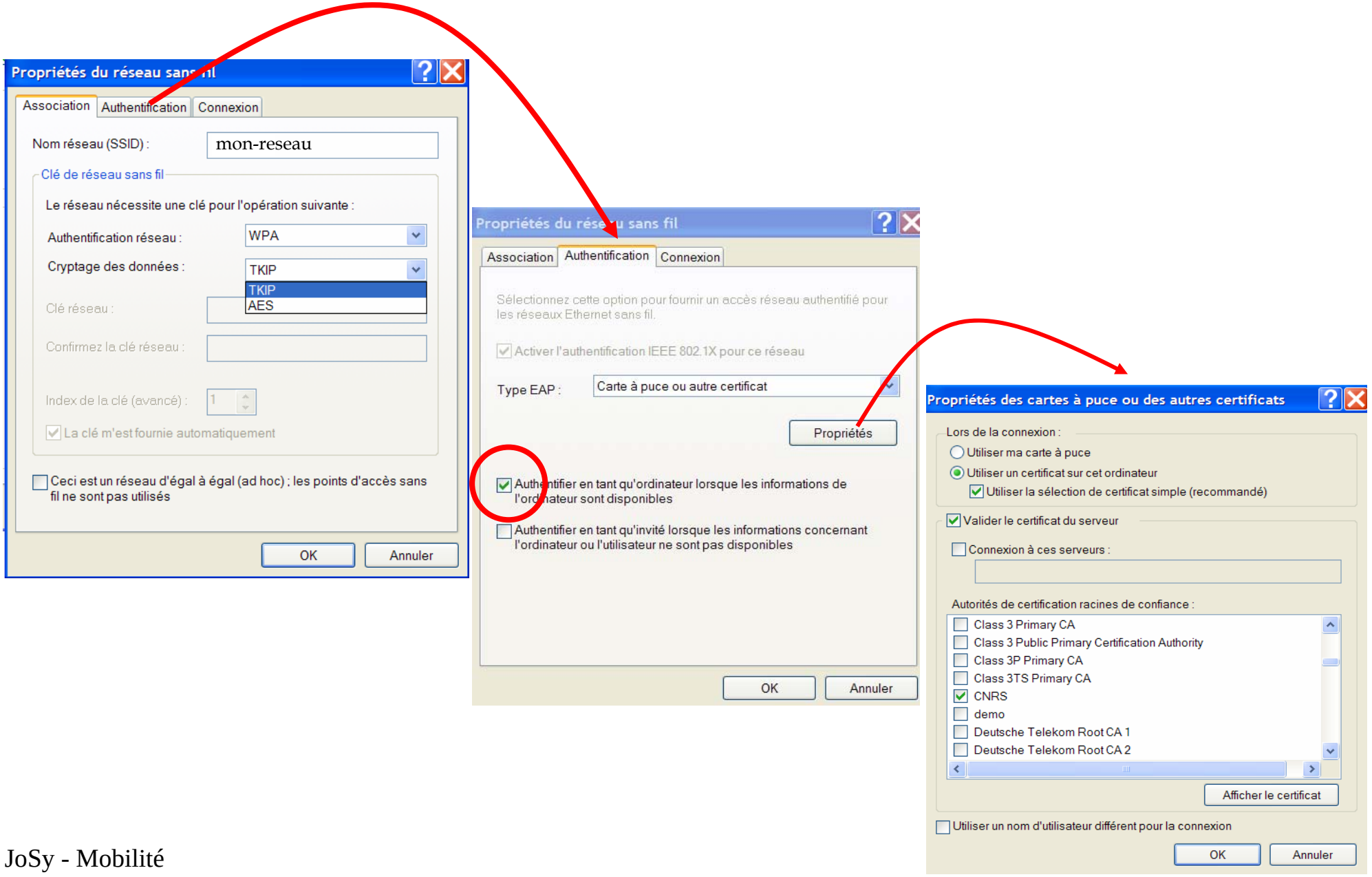
Ce répertoire contient les certificats des autorités reconnues et, les listes de révocation.

Configuration du supplicant Windows

- Copier le certificat de la machine (certificat réseau) sur le poste client
- Copier le certificat du CNRS sur le poste client
- Depuis le compte administrateur
  - ✓Charger le certificat réseau dans le magasin de certificats « ordinateur local »
  - ✓Charger le certificat de l'autorité du CNRS dans le magasin de certificats « ordinateur local »
  - ✓Configurer le supplicant Windows

Configuration du supplicant Windows

Configuration du supplicant



Configuration du supplicant Windows

Déroulement d'une connexion au réseau

- Lorsque la machine boot le **CN du certificat réseau** se trouvant dans le magasin « ordinateur Local » est envoyé comme identité au serveur FreeRadius (via les protocoles EAP/802.1X/Radius)

- Le serveur trouve une entrée dans sa base égale à ce CN (cad le nom de la machine)

- Dialogue EAP/TLS entre le serveur FreeRadius et le poste client (Authentification mutuelle des certificats)

- Initialisation du chiffrement TKIP ou AES

Le poste dispose alors du réseau

Que se passe t'il lorsque l'utilisateur ouvre une session ?

Configuration du supplicant Windows

Ouverture d'une session

Ce qui se passe à l'ouverture d'une session dépend de la valeur de la clé de registre :

HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode

0 : Authentification au boot (valeur par défaut)
Si impossible, l'authentification aura lieu à l'ouverture de session

1 : Authentification au boot, puis à l'ouverture de session

2 : Authentification au boot uniquement

Configuration du supplicant Windows

Ouverture d'une session

Problème :

Lorsque l'utilisateur est connecté s'il coupe puis rallume sa carte WiFi, il ne peut plus s'authentifier car il n'a pas accès au certificat réseau qui se trouve dans le magasin « ordinateur local » (sauf s'il est administrateur)

Deux solutions :

- Se déconnecter et se reconnecter. Le système refait alors l'authentification
- Installer le certificat réseau dans son magasin de certificat (double-clic sur le fichier p12)

Configuration d'un supplicant Linux

- Actuellement peu de postes WiFi avec Linux
(le plus souvent Windows natif et machine virtuelle Linux)

- Problèmes de drivers, chaque poste est un cas particulier (version noyau, carte wifi, procédures)

- Tests avec wpa_supplicant et NDISWRAPPER

wpa_supplicant.conf

```
network={
      ssid="nom-du-reseau"
      scan_ssid=0
      proto=WPA
      key_mgmt=WPA-EAP
      eap=TLS
      pairwise=TKIP
      group=TKIP
      anonymous_identity="nom-de-la-machine"
      ca_cert="/cert/ca/cacnrs.pem"
      private_key="/cert/nom-de-la-machine.p12"
      private_key_passwd="xxxxxxx"
}
```

CN du certificat

Configuration d'un supplicant Linux

Démarrage du supplicant

- Manuellement

wpa_supplicant -D ndiswrapper –i wlan0 –c /etc/wpa_supplicant/wpa_supplicant.conf

- Ou bien au boot

Autres cas

- Postes « privées »
  - ✓Sur un sous-réseau dédié, avec accès restreint
  - ✓Filaire => VMPS
  - ✓Sans-fil => Radius/802.1X avec PEAP – Evolution vers TLS à voir

- Postes visiteurs

  - ✓Un sous-réseau dédié, aucun accès vers le réseau interne
  - ✓Filaire => VMPS
  - ✓Sans-fil => Portail captif (Chillispot) + radius
    - ▪Longue durée : enregistrés, authentifiifiés par login/passwd + adresse MAC
    - ▪Courte durée : Auto-enregistrés (utilisation de Exec-Program-Wait Freeradius)

Futur : Peut-être Eduroam mais nécessité d'une autre solution.

Questions ?