Présentation du réseau et des services Cr@ns

Olivier Iffrig

Cachan Réseau à Normale Sup'

Mardi 23 octobre 2012

Sommaire

Sommaire

Connexion avec l'extérieur

Trois réseaux entre nous et Internet :

- l'ENS (DSI)
- Rubis (Val de Bièvre)
- Renater (Education Recherche National)

Les débits en jeu :

- Renater $\leftrightarrow$ ENS : 100 Mbps (supporte physiquement 1 Gbps)
- ENS $\leftrightarrow$ Cr@ns : 1 Gbps

Notre matériel

- 20 serveurs physiques
- 21 serveurs virtuels
- 53 switchs
- 107 bornes wifi
- 4 caméras

Notre réseau

- Un routeur/firewall : `komaz`
- Entre chaque bâtiment : fibres en Gigabit
- Dans chaque bâtiment : switchs manageables en étoile
- Dans chaque chambre : 100Mb
- Un serveur de secours dans un datacenter d'Ovh (Ovh)

Notre réseau

Plan du réseau

Le wifi

- Anciennes bornes Linksys WRT-54G
- Nouvelles bornes Ubiquiti {Nano,Pico}Station
- Couverture étendue
  - Env. 40 bornes actives sur le campus
  - Amélioration de la couverture en cours
- Points techniques
  - Linux embarqué (OpenWRT)
  - WPA2 Enterprise
  - Antennes
  - PoE

Le wifi

Plan du wifi

Sommaire

Le DHCP

- Permet la configuration automatique des machines sur le réseau
- Présent sur `sable` pour les machines fixes et sur `gordon` pour le wifi
- En test sur `dhcp` pour une gestion centralisée

Le DNS

- Permet la résolution des noms en IP et inversement
- Exemple : zamok.crans.org $\leftrightarrow$ 138.231.136.1
- Gestion des zones crans.org, crans.ens-cachan.fr, clubs.ens-cachan.fr
- Sous-domaines : adm, wifi, ferme, tv, v6
- Gestion des IPv4 de 138.231.136.0 à 138.231.151.255
- Gestion des IPv6 dans la plage 2a01:240:fe3d::/48
- Plusieurs serveurs : `sable` (maître), `charybde`, `titanic`, `ovh` et `gordon` (wifi uniquement)

Services aux adhérents

- Mails
- Pages personnelles
- Compte ssh sur `zamok`
- Impression
- Compte à vie (ou presque)

Stockage des données

- Espace disque : env. 2Go par adhérent (stockage des fichiers et des mails)
- Centralisation sur la baie de disques (`nols`), environ 700 Go utilisés
- Renvoyées par iSCSI sur `daath`
- Distribution des fichiers par NFS
- Authentification grâce à une base LDAP (avec réplicats sur différents serveurs)

La gestion des mails

- Utilisation exclusive de Postfix
- Utilisation d’une greylist pour réduire le spam
- Serveur principal : `redisdead`
- Livraison des mails par `zamok`
- Possibilité aux adhérents d’utiliser Procmail et Spamassasin
- Serveurs secondaires : Freebox (`titanic`) et `ovh` (forwardent uniquement les mails à `redisdead`)
- Pour lire ses mails : POP/IMAP (dovecot), Webmails (horde, roundcube et sogo), disponibles sur `owl` et `sogo` (domU)

Les pages perso

- Utilisation d’apache2
- Sites perso et de clubs servis par `zamok`, PHP disponible (mais restrictions)
- Autres sites de l’association sur `niomniom` (domU)

L’impression

- Impression laser couleur
- Imprimante : Canon iRC 3580
- Facturation : coût réel, compte prépayé
- Bac de sortie : séparation des travaux, agrafage, brochures
- Accès par digicode (génération aléatoire de code) → `vigile`

Le wiki

- Site web collaboratif
- Première source d'informations pour tout ce qui concerne le campus
- Pages publiques (accessibles sur `http://www.crans.org`)
- Utilisation de MoinMoin sur `niomniom`

Les news

- Serveur installé sur un domU, `news`
- Utilisation d'Inn
- Passerelle Web $\leftrightarrow$ News

IRC

- Serveur installé sur un domU, `irc`
- Utilisation de dancer-ircd
- Passerelle Web $\leftrightarrow$ IRC

La TV

- Quatre serveurs de diffusion : `canard`, `dindon`, `lapin` et `oie`
- Un serveur pour les vignettes et le DNS : `vache`
- Un serveur de test : `poulet`
- 5 cartes TNT, 11 cartes Satellite
- Diffusion en multicast
- Utilisation de MumuDvb développé par une nounou

Divers services

- Messagerie Jabber (`xmpp`, domU)
- Listes de diffusion (mailman) (`redisdead`, domU)
- FTP public (miroir Videolan, OpenBSD, images ISO de différentes distributions) (`charybde`)
- Nombreux logiciels disponibles sur `zamok` (aussi à la demande)
- Serveur de temps (ntp.crans.org, `sable`)
- Intranet (gestion de son compte et accès au service d'impression) (`zamok` et `o2`)
- Paypal (rechargement des comptes impression)

Sommaire

Sécurité

- Filtrage MAC sur toutes les prises des bâtiments (serveurs RADIUS `sable` et `radius`)
- Nombreux services disponibles en SSL
- Six sous réseaux séparés (VLans)
  - réseau filaire (adhérents)
  - réseau WiFi
  - réseau serveurs (transit des données d'administration)
  - réseau appartements de fonction
  - réseau d'isolement (virus et annonces IPv6 pirates)
  - réseau d'accueil (pas encore inscrits)

Surveillance

- Monitoring à l'aide de Munin
- Surveillance des services par Monit
- Surveillance des tentatives d'usurpation d'identité
- Surveillance du trafic sortant (upload, p2p, virus...)
- Surveillance de l'état des services : munin, monit, autostatus
- Surveillance des locaux sensibles par caméras et enregistrement
- Conservation de certains fichiers journaux conformément aux lois en vigueur.

Questions ?