Selecció i configuració de programari lliure per a xarxes de servidors

VIII Jornades de Programari Lliure

Sergio Talens-Oliag
sto@iti.upv.es

3 de juliol de 2009

En aquest document parlarem del disseny i la implementació d'infraestructures basades en programari lliure, centrant-nos en la selecció d'eines i la configuració dels sistemes i serveis.

Per a l'exposició començarem definint els requisits de la infraestructura TIC d'una organització fictícia, indicant el conjunt de serveis a proporcionar, l'abast de cadascú (els serveis poden ser interns, externs o estructurals) i els nivells d'accés als mateixos (restringits o públics).

A partir del model definit farem un xicotet anàlisi de les eines lliures disponibles per a proporcionar els serveis i ens centrarem en la descripció del procés de selecció del programari, comentant algunes de les opcions de configuració en relació amb les nostres necessitats.

Contingut

1 Introducció

En aquest document parlarem de la selecció i configuració de programari lliure per a fer-lo servir en infraestructures TIC; per començar donarem alguns criteris per a la selecció de programari i definirem els requisits d'una infraestructura d'exemple.

A partir de l'anàlisi dels requisits plantejarem un model de configuració per als sistemes i serveis i donarem la nostra selecció de programari, explicant les alternatives disponibles i les raons per a fer servir un programa o un altre.

2 Criteris de selecció de programari (1)

Per a seleccionar un producte *software* per a integrar-lo dins d'una infraestructura TIC farem servir alguns dels següents criteris:

- *Complexitat*: ha de tindre la justa, si realitza una tasca senzilla la configuració ha de ser trivial i si la tasca és complicada la configuració i el manteniment han de ser fàcils.
- *Comunitat al voltant del producte*: ¿hi ha actualitzacions (noves característiques, correcció d'errors funcionals i de seguretat, etc.) i suport (llistes i fòrums, documentació, sistemes de gestió d'errors, etc.)?

3 Criteris de selecció de programari (2)

- *Documentació disponible*: guies (*HOWTOs*), llibres, llistes de correu i fòrums, wikis, etc.
- *Experiència del personal*: Si tenim coneixements previs (*know how*) sobre un producte el fer-lo servir ens estalviarà temps i diners.
- *Funcionalitats*: cal revisar la quantitat i qualitat de les mateixes, les possibilitats d'habilitar i inhabilitar selectivament el que necessitem, etc.

4 Criteris de selecció de programari (3)

- *Interoperabilitat*: suport de mecanismes d'integració amb altres productes.
- *Llenguatge de la implementació*: ens interessa per les possibilitats de revisar i escriure pedaços o *plugins* per part del personal i per a minimitzar el requisits dels sistemes (reduir el nombre de intèrprets i biblioteques amb funcionalitat similar).
- *Qualitat del producte*: històric de errors, procés de prova i validació, consum de recursos, grau de configurabilitat, mecanismes d'expansió, llegibilitat del codi, qualitat de la documentació, etc.

5 Descripció de la infraestructura d'exemple

- Organització amb xarxa local de màquines d'usuaris amb múltiples sistemes operatius (Linux, MacOS X i Windows).
- Els usuaris han de tindre accés a Internet.
- Els servidors han de proporcionar serveis estructurals (serveis per a la xarxa de servidors), interns (només accessibles des dels equips dels usuaris) i externs (accessibles des de Internet). Alguns serveis tindran l'accés restringit i altres seran públics per a tots els equips del seu àmbit.

6 Serveis interns a proporcionar

- *Serveis de directori*: DHCP (assignació adreces IP), DNS (mapa de noms i adreces) i LDAP (informació d'usuaris, incloent-hi l'autenticació)
- *Serveis de correu*: SMTP (eixida de missatges) i POP o IMAP (recepció)
- *Compartició de impressores*: CUPS i SAMBA
- *Compartició d'arxius*: NFS, NFSv4, SAMBA, SSHFS, etc.

7 Serveis externs a proporcionar

- *Servidor de correu d'entrada*: SMTP
- *Servidor de noms públic*: DNS
- *Servidor web de la organització*: HTTP i HTTPS
- *Altres serveis accessibles via HTTP o HTTP* d'accés públic (fòrums de discussió, bloc públic, etc.) i restringit (client de correu web per als usuaris interns, aplicació de gestió de projectes, etc.)

8 Model de configuració

El model inclourà:

- Descripció de l'organització de la xarxa, models d'accés entre diferents segments amb restriccions a nivell IP,
- Descripció dels elements de la infraestructura (components estructurals, serveis interns i serveis externs) amb la llista de serveis a instal·lar i notes sobre com els configurarem.

9 Organització de la xarxa

A partir dels requisits agrupem els dispositius en tres subxarxes:

- **DMZ interna**: serveis per a la LAN (connecta servidors i dispositius amb accés controlat com impressores, faxes, escànners, etc.).
- **DMZ externa**: serveis accessibles des de la LAN i des de Internet, amb accés públic o restringit.
- **LAN**: subxarxa per als equips d'usuari.

L'entrada i eixida a **Internet** i la interconnexió de les subxarxes es gestionarà amb un tallafocs.

10 Model d'accés entre xarxes

- Les restriccions d'accés entre xarxes a nivell IP es defineixen i apliquen en el tallafoc; quan un servei és d'accés restringit els servidors també incorporen mecanismes per a limitar l'accés a nivell IP (és pot fer amb `iptables`, `tcpwrappers` o amb opcions pròpies del programari en qüestió).
- La xarxa d'usuaris no té limitacions en l'eixida (accés complet a Internet i controlat cap a les DMZ) però està prohibit establir connexions des de qualsevol altra xarxa cap a la xarxa dels usuaris.
- Les DMZ tenen restringit l'accés d'entrada (només s'accepten connexions externes per a alguns serveis) com d'eixida (control de l'inici de connexions des dels servidors).

11 Resum de les restriccions d'accés

Xarxa objectiu	**LAN**		**DMZ Int**		**DMZ Ext**		**Internet**	
Tipus de connexió	**--> SYN**	**<-- S-A**	**--> SYN**	**<-- S-A**	**--> SYN**	**<-- S-A**	**--> SYN**	**<-- S-A**
LAN	O	O	~	X	~	X	O	X

Xarxa objectiu	LAN		DMZ Int		DMZ Ext		Internet	
Tipus de connexió	**--> SYN**	**<-- SYN-A**	**--> SYN**	**<-- SYN-A**	**--> SYN**	**<-- SYN-A**	**--> SYN**	**<-- SYN-A**
DMZ Int	X	~	~	~	~	X	~	X
DMZ Ext	X	~	X	~	~	~	~	~
Internet	X	X	X	X	~	O	O	O

On O vol dir accés total, ~ vol dir accés restringit i X vol dir accés prohibit.

12 Elements de la infraestructura

Elements de la infraestructura en funció del seu tipus i abast:

- *Components estructurals*: elements *hardware* i *software* necessaris per al bon funcionament de la xarxa de servidors; el programari inclou eines d'ús intern en els servidors com serveis que no fan servir directament els usuaris.
- *Serveis interns*: serveis per a la xarxa d'àrea local (LAN); la idea és que aquest tipus de serveis només es fan servir dins de la xarxa interna de l'organització.
- *Serveis externs*: serveis accessibles des de Internet; poden ser totalment públics o restringir l'accés tant a nivell IP com a nivell d'aplicació (accés amb identificació).

13 Components estructurals (1)

Hardware:

- Servidors amb arquitectures **Intel** o **AMD** de 64 bits

Distribució i nucli:

- **Debian GNU/Linux**

Eines de virtualització:

- **OpenVZ**: virtualització a nivell de sistema operatiu, útil per a sistemes Linux
- **KVM**: virtualització completa amb suport hardware, suporta qualsevol sistema.

14 Components estructurals (2)

Sistemes d'emmagatzematge:

- Discos interns o sistemes RAID amb interfície SCSI, FC o iSCSI,
- Configuració dels discos amb RAID-1 o RAID-5 hardware o software,
- Fem ús del gestor de volums lògics (LVM): ens permet redimiensionar volums i fer *snapshots*,
- Sistemes d'arxius en format `ext3` (és el més estàndard en Linux),
- Ús de *swap*: si tenim molta memòria RAM no és molt necessari, però generalment ho configurem amb la mateixa mida que la RAM per a poder fer servir l'**uswsusp**.

15 Components estructurals (3)

Monitorització local i remota:

- *Anàlisi de logs*: **logcheck**
- *Detecció de canvis en fitxers*: **changetrack**, **filetrack**, **integrit**, ...
- *Històric de configuracions*: **etckeeper**,
- *Monitorització i reinici de serveis*: **monit**, **mon**, **god**, ...
- *Monitorització dels SAI*: **nut**,
- *Monitors per a serveis remots*: **zabbix**, **nagios**, ...

16 Components estructurals (4)

Control d'accés a nivell IP:

- *Control a nivell d'aplicació*: **tcpwrappers**.
- *Tallafoc*: **iptables** amb scripts propis, ús d'**iptables-save** i **iptables-restore** o ús de sistemes de configuració més avançats com **shorewall**.
- *Xarxes privades virtuals*: **tinc** i **openvpn**.

17 Components estructurals (5)

Eines de configuració i manteniment:

- *Servidors de sessió remota*: **openssh** (eliminem totalment sistemes com el **rsh** i **telnet**); els fem servir amb claus RSA i per a gestionar múltiples servidors al mateix temps fem servir programes com **clusterssh** i **kanif/taktuk**.
- *Sistemes de gestió de configuracions*: podem fer servir programes com **cfengine**, **puppet** o **STAF**.
- *Sistemes de gestió de clusters* (gestió de recursos i planificació i distribució de treballs): **torque** i **maui**.

18 Components estructurals (6)

Sistemes de còpia de seguretat en disc dur amb suport de xarxa:

- **rdiff-backup** (amb snapshots LVM); gestió amb **backupninja**.
- **duplicity** (amb snapshots LVM): per a fer backups xifrats.
- **partimage**: especialitzat, el fem servir per a clonar sistemes.

Sistemes de còpia de seguretat a nivell local:

- **dar**: còpia en disc que es pot copiar en qualsevol suport (CD, DVD, cintes, etc.)
- **tar**: còpia en cinta.

19 Components estructurals (7)

Utilitats en els servidors:

- *pager*: **less**
- *mua*: **mutt**
- *gestió de consoles*: **screen**
- *editor*: **vim**
- *scm*: **subversion**; en el futur **mercurial** i **git**.

20 Serveis interns: assignació d'adreces IP

Eines per a assignar de manera dinàmica les adreces IP i moltes dades de configuració interessants (servidors de DNS, servidors WINS, etc.).

- **dnsmasq**: Servidor senzill i ràpid, es pot configurar per a fer servir els fitxers `/etc/hosts` i `/etc/ethers` per a l'assignació d'adreces IP a adreces MAC. El producte inclou també un servidor de DNS (podem habilitar selectivament els serveis proporcionats per el programa).
- **isc-dhcpd**: estàndard de facto, l'hem abandonat perquè amb dnsmasq ja tenim tot el que ens fa falta.

21 Serveis interns: DNS intern (1)

Tots el servidors dels que parlarem funcionen com a sistema de resolució recursiu, tenen la possibilitat de definir servidors concrets per a les consultes de dominis específics (útil per a muntar un sistema de *split DNS*) i inclouen suport per a servir el domini intern sense fer servir un servidor addicional.

Els programes a triar són:

- **dnsmasq**: fa servir el fitxer `/etc/hosts` per a servir el domini intern i genera la resolució inversa.

22 Serveis interns: DNS intern (2)

- **pdnsd**: té un sistema de *caching* en disc que estalvia consultes fins i tot després de reiniciar el servei.
- **pdns-recursor**: semblant als anteriors, bon rendiment.
- **bind**: abandonat per la complexitat de configuració i els requisits de funcionament.

23 Components estructurals: Proxy HTTP/FTP

Servidors proxy i proxy-caché:

- **tinyproxy**: senzill i lleuger, sense memòria cau en disc, útil si es vol tancar l'eixida directa dels servidors a Internet.
- **apt-catcher**: sistema especialitzat en *caching* de paquets Debian, estalvia connexions de xarxa i transferències quan no fem servir un mirror local i centralitza l'eixida a Internet.

24 Serveis interns: Relay SMTP

Relay SMTP:

- **postfix**: el nostre servidor de correu preferit; el fem servir com a servidor local dels sistemes (hi ha una copia en cada servidor per tindre cues i logs locals) i un d'ells es fa servir com a *relay* de tota la xarxa de servidors (el fem servir per a enviar correus a l'exterior, ens permet filtrar el correu per reescriure les capçaleres o el contingut, detectar spam i virus d'eixida i encaminar el correu intern com siga més convenient).

25 Serveis interns: Servei de directori

Serveis de directori:

- **openldap**: Per a autenticar els usuaris en els servidors Linux fem servir el mòdul **libpam-ldap**; la informació dels usuaris UNIX també està centralitzada fent servir el mòdul **libnss-ldap**, tot i que per temes de rendiment en molts casos ho hem reemplaçat pel mòdul **libnss-extrausers** i un script que exporta les dades de LDAP i distribueix els fitxers resultants als servidors. Per a gestionar als usuaris de **Windows** fem servir **Samba** com a controlador de domini i el configurem per a que lligue la informació amb **LDAP**, de manera que les dades dels usuaris estiguen unificades.

26 Serveis interns: compartir arxius

Compartició d'arxius:

- *Per a sistemes Unix*: NFS i NFSv4, tot i que aquest últim necessita que la informació d'usuaris i grups siga coherent entre tots els sistemes (ús de **libnss-ldap** o similar),
- *Per a sistemes Windows*: Samba

27 Serveis interns: impressió per xarxa

Impressió per xarxa:

- **cups**: estàndard de facto actual, inclou compatibilitat lpr, però els clients ja fan servir IPP i similars.
- **lpr/lprng**: eines estàndard antigues, hui en dia no paga la pena.
- **samba**: integració CUPS per a xarxes de Windows.

28 Serveis interns: proxy FTP/HTTP(S)

Servidors proxy:

- **squid**: si volem optimitzar l'ús de la xarxa fent *caching* o controlar l'eixida externa, és l'estàndard de facto; és complicat configurar-lo correctament, però està molt provat i documentat.
- **tinyproxy**: servidor sense *caching* amb una configuració senzilla, útil com a proxy per a túnels **ssh**.

29 Serveis externs: correu electrònic

Eines de correu:

- *SMTP*: **postfix**.
- *IMAP/POP3*: fem servir **Dovecot**, el vam instal·lar com a migració des de **uw-imapd** per temes de rendiment i el vam triar davant d'alternatives com **Courier** i **Cyrus** per la seua simplicitat (la migració inicial només va requerir canviar el fitxer de subscripcions IMAP dels usuaris).
- *Llistes*: **mailman**.
- *Webmail*: Per raons històriques fem servir **IMP** i com a solució lleugera hem fet servir **Ilohamail** (només necessita PHP, sense base de dades).

30 Serveis externs: intercanvi de fitxers

Lectura anònima:

- FTP: **vsftp**
- HTTP: **nginx**
- RSYNC: **rsyncd**

Lectura/escriptura autenticada:

- FTP: **vsftp amb TLS**
- RSYNC: **openssh** i **rsync** instal·lat a la màquina remota.
- SCP/SFTP: **openssh**

En alguns casos es fa servir la web, però fa falta una aplicació PHP o similar.

31 Serveis externs: servidors web

Servidors HTTP i HTTPS:

- **nginx**: el nostre favorit, molt ràpid, no té tantes funcionalitats com l'Apache, però amb fastcgi es pot fer servir per a gairebé tot (de fet no implementa ni CGI, tot i que existeix un servidor fastcgi per a llançar scripts de CGI quan fa falta).
- **apache2**: servidor estàndard de facto, el fem servir quan els es fan servir funcionalitats específiques com fitxers `.htaccess` o mòduls que no funcionen en altres servidors com els de suport de subversion via http / https (mòduls `mod_dav_svn` i `mod_authz_svn`).

32 Serveis externs: servidors web (2)

Altres servidors:

- **lighttpd**: semblant a **nginx**, la configuració no ens agrada massa, té històric d'errades de seguretat, el rendiment no és tan alt com nginx, només el fèiem servir per a tindre suport per a CGI, però resulta més econòmic fer servir nginx amb el gnosek-fcgiwrap.

33 Serveis externs: proxy invers

Servidor proxy invers:

- **nginx**: servidor HTTP i HTTPS lleuger amb funcionalitats com reescriptura d'URLs, proxy invers amb balanceig o generació de *caches* estàtiques. Actualment és la nostra opció per defecte pel seu rendiment i baix consum de recursos.
- **apache2**: servidor web de referencia, inclou mòdul per a funcionar com a proxy invers; és un producte madur i molt documentat però generalment fem servir **nginx** per temes de rendiment i consum de recursos.
- **pound**: servidor limitat amb menys potència i rendiment que les alternatives.
- **squid**: la configuració és complicada i el consum de recursos elevat.