Network Daemons

Giuseppe Augiero

Apache

Storia

- E' un webserver per il protocollo HTTP.
- Il suo sviluppo e' curato da un' organizzazione not-for-profit quale la *Apache Software Foundation*. (ASF - fondata nel 1999 dal team di volontari denominato Apache Group).
- Nasce come evoluzione del webserver httpd 1.3 sviluppato dal NCSA (National Center for Supercomputing Applications); ne ingloba le carrateristiche, risolvendo i problemi ed implementando nuove features.

Risorse

- Protocollo applicativo: http
- Protocollo di trasporto: tcp
- Porta utilizzata: 80

Configurazione

- I file di configurazione principali sono:
- Httpd.conf
- Srm.conf

Direttive di configurazione

Principali direttive:

- *ServerType standalone*
- *ServerRoot /etc/apache*
- *Port 80*
- *User www-data*
- *Group www-data*
- *ServerName www.dominio.it*
- *DocumentRoot /var/www*

Direttive di config. (2)

- *<Directory /var/www/>*

  Options Indexes Includes FollowSymLinks MultiViews

  Order allow,deny

  Allow from all

  </Directory>

Gestione degli errori

- ErrorDocument 400 “Errore 400 -
- ErrorDocument 500 “Accesso Denied
- ErrorDocument 402 “Fatal Error
- ErrorDocument 403 “Not Found!

Demone o Servizio?

- Apache normalmente gira come demone.
- E’ possibile farlo girare anche come servizio, ma solo nel caso di poco traffico web.

Tools Grafici

- I due tools più famosi sono:
- Comanche - Comanche è un **tool grafico** open-source per la configurazione di **Apache**. E' multi piattaforma, ossia gira su molti dei sistemi operativi Unix-based (compreso Linux) e anche su Windows.
- Webmin - Potente strumento di configurazione web-based che permette, attraverso un interfaccia web user-friendly ed una struttura a moduli espandibile, di poter amministrare praticamente l'intero sistema, quindi anche la configurazione di **Apache**.

Sicurezza

- Apache ha una lunga storia di aggiornamenti, bug e patch.
- Consigliato l'utilizzo di mod_security.

Documentazione

- La documentazione ufficiale di Apache e' disponibile all'url:

  http://httpd.apache.org/docs-project/

Postfix

Storia

- Successore e antagonista di Sendmail.
- E’ stato scritto da un ricercatore olandese che ora lavora per l’IBM.
- Famoso per la sua sicurezza, robustezza e scalabilità.

Risorse

- Protocollo applicativo: smtp
- Protocollo di trasporto: tcp
- Porta utilizzata: 25

Configurazione

- I file di configurazione principali sono:
- main.cf
- master.cf
- virtual

Direttive di configurazione

Principali direttive:

- *myhostname = mail.dominio.it*
- *mydomain = dominio.it*
- *mydestination = mail.dominio.it*
- *relayhost = 1.1.1.1*
- *virtual_mailbox_maps = hash:/etc/postfix/virtual*
- *mailbox_size_limit = 0*
- *message_size_limit = 20480000*

Direttive di config. (2)

- *smtpd_sender_restrictions = permit_mynetworks, reject_unknown_sender_domain*
- *smtpd_client_restrictions = permit_mynetworks, reject_unknown_hostname, reject_non_fqdn_hostname*
- *smtpd_helo_required = yes*
- *smtpd_helo_restriction = reject_invalid_hostname, reject_unknown_hostname*

Virtual domain

- dominio.it domain
- mario@dominio.it mario
- server@dominio.it roberto
- Webmaster@dominio.it giulia antonio
- @dominio.it info

Demone o Servizio?

- Postfix normalmente gira come demone.

Tools Grafici

- Esistono molti tools grafici per PostFix, alcuni di questi sono stati scritti ad hoc per un utilizzo particolare.
- Uno dei tool grafici più famoso e' WebMin che attraverso un modulo specifico gestisce le opzioni di base ed alcune avanzate di Postfix.

Sicurezza

- Postfix è un mail server robusto e sicuro.
- E’ importante configurare nel modo più opportuno la direttiva relayhost.

Documentazione

- La documentazione ufficiale di Postfix e' disponibile all'url:

  http://www.postfix.org/documentation.html

Bind

Storia

- **Bind**, conosciuto anche come *named*, è un pezzo fondamentale della **storia** di internet e di ogni sistema che lavora sulla rete internet, i server che risolvono i nomi su internet rappresentano uno dei più grandi database distribuiti sulla rete.
- Gestisce la risoluzione dei nomi di dominio, in particolare questo applicativo si occupa di mappare uno o più nomi di dominio su un'indirizzo IP e, nella risoluzione inversa, un indirizzo IP ad un nome univoco di host.

Risorse

- Protocollo applicativo: domain
- Protocollo di trasporto: udp (tcp)
- Porta utilizzata: 53

Configurazione

- I file di configurazione principali sono:
- named.conf
- file di zona

Direttive di configurazione

- Da ricordare: Ogni direttiva termina con un ";". Tra parentesi graffe si inseriscono le direttive relative ad una direttiva principale. I commenti sono gli stessi che si utilizzano in linguaggio C, "//"per aprire e chiudere o "/*" per aprire e "*/" per chiudere.

Direttive di config. (2)

- *zone “dominio.it" {*

  type master;

  file "/etc/bind/db.dominio";

  };

- *zone "255.in-addr.arpa" {*

  type master;

  file "/etc/bind/db.255";

  };

File di zona

- $ORIGIN dominio.it
- $TTL 172800 ; 2 days
- Dominio.it. IN SOA ns. dominil.it. root.dominio.it. (
- 200501163 ; serial
- 28800 ; refresh (8 hours)
- 7200 ; retry (2 hours)
- 604800 ; expire (1 week)
- 86400 ; minimum (1 day)
-)
- NS ns. dominio.it.
- 1 PTR localhost.

- ns.domini.it. A 172.16.1.10
- zeus.dominio.it. A 172.16.1.10
- ;Aliases
- www.dominio.it. CNAME zeus.dominio.it.

- Dominio.it. MX 10 mail.dominio.it.

Demone o Servizio?

- Bind deve girare come demone.

Tools Grafici

- Uno dei tool grafici più famoso e' WebMin che attraverso un modulo specifico gestisce le opzioni di base di Bind.

Sicurezza

- Bind, in passato, e' stato colpito da molti problemi di sicurezza. Spesso attraverso di lui si e' riuscito a guadagnare un accesso alla macchina sul quale girava.

Documentazione

- La documentazione ufficiale di Bind e' disponibile all'url:

  http://www.isc.org/index.pl?/sw/bind/

SSH

Storia

- OpenSSH è una versione libera della suite di tool per la connettività di rete basati sul protocollo SSH .
- Molti utenti che utilizzano telnet, rlogin, ftp e simili programmi forse non sanno che la loro password viene trasmessa attraverso la rete non criptata. OpenSSH cripta tutto il traffico (password compresa) per eliminare a tutti gli effetti l'ascolto passivo, l'hijacking della connessione e altri attacchi a livello di rete.

Risorse

- Protocollo applicativo: ssh
- Protocollo di trasporto: tcp
- Porta utilizzata: 22

Configurazione

- I file di configurazione principali sono:
- sshd_config

Direttive di configurazione

- *Port 22*
- *Protocol 2*
- *KeyRegenerationInterval 3600*
- *ServerKeyBits 768*
- *RSAAuthentication yes*
- *PubkeyAuthentication yes*

Comandi ssh

- Nella suite di tool ssh troviamo:
- Scp
- Sftp
- Sshd
- Ssh
- Utility di base

Demone o Servizio?

- SSHD deve girare come demone.

Tools Grafici

- Normalmente non e' necessario utilizzare un tool grafico per configurare sshd.

Sicurezza

- Occorre utilizzare ssh al posto dei comandi che non cifrano il canale di comunicazione (telnet, rcp, rlogin).
- Il protocollo 1 di ssh e' insicuro, il traffico prodotto dalla versione 1 e', in alcuni casi, decifrabile.
- In passato le implementazioni di openssh hanno sofferto di alcuni bug di sicurezza.

Documentazione

- La documentazione ufficiale di Openssh e' disponibile all'url:

  http://www.openssh.org/it/

FTP

Storia

- **FTP** è lo storico protocollo per lo scambio di file.
- Esistono molti server ftp.
- Alcuni di questi hanno rappresentato un serio problema per la sicurezza della macchina che li ospitava.

Risorse

- Protocollo applicativo: ftp
- Protocollo di trasporto: tcp
- Porta utilizzata: 20-21

Configurazione

- I file di configurazione principali sono:
- vsftpd.conf

Direttive di configurazione

- *listen=YES*
- *anonymous_enable=YES*
- *write_enable=YES*

Root directory

- Normalmente viene creato l'utente ftp con shell /bin/false e con home in /home/ftp
- /home/ftp rappresenta la root directory del ftp server.

Demone o Servizio?

- Vsftpd può essere installato in modalità "classca" con un demone in esecuzione e uno script di start e di stop , o in modalità “superserver" che si attiva automaticamente quando arriva una richiesta.

Tools Grafici

- Esistono vari tool grafici tra cui un modulo per Webmin.

Sicurezza

- Vsftpd risulta essere un prodotto alquanto sicuro.
- E’ da segnalare che può supportare anche SSL.

Documentazione

- La documentazione Vsftpd e' disponibile all'url:

  http://www.vsftpdrocks.org/

Proxy

Storia

- Squid è il più conosciuto nonchè il più utilizzato dei Proxy Server attualmente in commercio, fornisce funzionalità di *caching* e *proxing* per il traffico HTTP, FTP.
- Il progetto nasce come evoluzione di CERN HTTP Server che già nel lontano 1994 includeva un modulo per la gestione della cache.

Risorse

- Protocollo applicativo: proxy
- Protocollo di trasporto: tcp
- Porta utilizzata: 3128

Configurazione

- I file di configurazione principali sono:
- squid.conf

Direttive di configurazione

- *http_port 8080*
- *cache_mem 100 MB*
- *maximum_object_size 409600 KB*
- *minimum_object_size 0 KB*
- *cache_dir ufs /var/spool/squid 2000 16 256*
- *dns_children 5*

Autenticazione

- *auth_param digest program <uncomment and complete this line>*
- *auth_param digest children 5*
- *auth_param digest realm Squid proxy-caching web server*
- *auth_param digest nonce_garbage_interval 5 minutes*
- *auth_param digest nonce_max_duration 30 minutes*
- *auth_param digest nonce_max_count 50*
- *auth_param ntlm program <uncomment and complete this line to activate>*
- *auth_param ntlm children 5*
- *auth_param ntlm max_challenge_reuses 0*
- *auth_param ntlm max_challenge_lifetime 2 minutes*
- *auth_param ntlm use_ntlm_negotiate off*
- *auth_param basic program <uncomment and complete this line>*
- *auth_param basic children 5*
- *auth_param basic realm Squid proxy-caching web server*
- *auth_param basic credentialsttl 2 hours*

AccessList

- acl all src 0.0.0.0/0.0.0.0
- acl manager proto cache_object
- acl casa src 172.16.0.0/255.255.0.0
- acl localhost src 127.0.0.1/255.255.255.255
- acl to_localhost dst 127.0.0.0/8

- http_access allow manager localhost
- http_access deny manager
- http_access allow purge localhost
- http_access deny purge
- http_access deny !Safe_ports
- http_access deny CONNECT !SSL_ports

Demone o Servizio?

- Squid deve girare come demone.

Tools Grafici

- Uno dei tool grafici più famoso e' WebMin che attraverso un modulo specifico gestisce le opzioni di base di Squid.

Sicurezza

- Squid non ha mai sofferto di grandi problemi di sicurezza.

Documentazione

- La documentazione ufficiale di Squid e' disponibile all'url:

http://www.squid-cache.org/Doc/

Domande?