Ottimizzare i parametri di rete nel kernel Linux

FONTE: < http://www.inforge.net/community/gnu-linux/119720-%5Bguida%5D-ottimizzare-i-parametri-di-rete-nel-kernel-linux.html >

Quando si parla di ottimizzazione di un webserver, di un server ftp o di un server DNS si pensa subito ai servizi tipici come apache, mysql, proftp, bind, ecc, ma visto che il denominatore comune dei vari demoni che devono rispondere alle richieste provenienti dalla rete è proprio l'interfaccia di rete, perchè non ottimizzare i vari parametri che la riguardano?

I parametri di rete nel kernel Linux modificabili tramite sysctl sono davvero molti, in questo thread vedremo come settarli a seconda dell'utilizzo principale del nostro server.

Cominciamo col prendere la mano con il comando **sysctl**, che gestisce la configurazione di tutti i parametri del kernel.

Per visualizzare la lista completa dei parametri coi loro rispettivi valori digitate questo comando da terminale:
sysctl -A

Oppure potete visualizzare solamente il valore di un determinato parametro digitando:
sysctl nomeparametro (per esempio: sysctl net.ipv4.route.gc_thresh)

Per modificare il valore di uno o più parametri dovremo inserire nel file /etc/sysctl.conf il nome del parametro seguito dal nuovo valore, ad esempio:
net.ipv4.tcp_keepalive_probes = 2

Infine, per applicare effettivamente le modifiche senza riavviare il server, usate il comando: **sysctl -p**

E, se i settaggi cambiati riguardano la parte network, flushate la routing table con questo comando:
sysctl -w net.ipv4.route.flush=1

Guida ai parametri di rete - Sicurezza:

net.ipv4.tcp_syncookies: Quando abilitato, protegge dagli attacchi SYN FLOOD

net.ipv4.icmp_echo_ignore_broadcasts: Quando abilitato, ignora tutte le richieste ICMP ECHO e TIMESTAMP dirette ad indirizzi broadcast e multi cast proteggendo il server da attacchi smurf.

net.ipv4.icmp_ignore_bogus_error_responses: Quando abilitato, protegge da errori ICMP maligni

I seguenti parametri, quando abilitati, permettono al server di inoltrare il traffico di rete da un'interfaccia ad un'altra, agendo come un router:

net.ipv4.ip_forward
net.ipv4.conf.all.send_redirects
net.ipv4.conf.default.send_redirects

I seguenti parametri, quando abilitati, proteggono dall'IP spoofing:

net.ipv4.conf.all.rp_filter
net.ipv4.conf.lo.rp_filter
net.ipv4.conf.eth0.rp_filter
net.ipv4.conf.default.rp_filter

I seguenti parametri, quando disabilitati, rifiutano i pacchetti ICMP con le route modificate:

net.ipv4.conf.all.accept_redirects
net.ipv4.conf.lo.accept_redirects
net.ipv4.conf.eth0.accept_redirects
net.ipv4.conf.default.accept_redirects

I seguenti parametri, quando abilitati, abilitano e loggano i pacchetti spoofed, source routed e redirect:

net.ipv4.conf.all.log_martians
net.ipv4.conf.lo.log_martians
net.ipv4.conf.eth0.log_martians
net.ipv4.conf.default.log_martians

I seguenti parametri, quando disabilitati, disabilitano i pacchetti source route:

net.ipv4.conf.all.accept_source_route
net.ipv4.conf.lo.accept_source_route
net.ipv4.conf.eth0.accept_source_route
net.ipv4.conf.default.accept_source_route

I seguenti parametri, quando abilitati, abilitano l'exec-shild:

kernel.exec-shield
kernel.randomize_va_space

Guida ai parametri di rete – Performance:

net.ipv4.tcp_fin_timeout: Definisce il numero di secondi che una connessione in stato FIN-WAIT-2 può restare appesa, le connessioni in questo stato occupano al massimo 1.5 kilobyte di RAM.

net.ipv4.tcp_keepalive_time: Definisce ogni quanti secondi inviare al client con una connessione keepalive aperta un pacchetto in modo tale da mantenerla aperta.

fs.file-max: Indica il numero massimo di file descriptor

kernel.pid_max: Indica il numero massimo di PID utilizzabili (un valore più alto di quello di default potrebbe generare qualche problema con alcuni programmi)

net.ipv4.ip_local_port_range: Indica il range di porte locali utilizzabili dalle connessioni di rete aperte

I seguenti parametri indicano i valori dei buffer per le connessioni e i socket TCP:

net.ipv4.tcp_rmem
net.ipv4.tcp_wmem

I seguenti parametri indicano i valori massimi per i buffer (ricezione e invio) che il sistema operativo avrà per ogni tipo di connessione:

net.core.rmem_max
net.core.wmem_max

net.core.netdev_max_backlog: Indica il numero massimo di pacchetti che si possono mettere in coda per essere processati quando il kernel non riesce a processare tutti i pacchetti in tempo reale.

net.ipv4.tcp_window_scaling: Dev'essere abilitato per poter settare valori di buffer più alti di quelli di default

Parametri ideali per trasferimenti di grossi files con poche connessioni:

net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
kernel.exec-shield = 1
kernel.randomize_va_space = 1
fs.file-max = 65535
kernel.pid_max = 65536
net.ipv4.ip_local_port_range = 2000 65000
net.ipv4.tcp_rmem = 4096 87380 8388608
net.ipv4.tcp_wmem = 4096 87380 8388608
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.core.netdev_max_backlog = 5000
net.ipv4.tcp_window_scaling = 1

Parametri ideali per tante connessioni (webserver, dns, mail):

net.ipv4.icmp_echo_ignore_broadcasts = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.tcp_syncookies = 1
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.secure_redirects = 0
net.ipv4.ip_forward = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
kernel.exec-shield = 1
kernel.randomize_va_space = 1
net.ipv4.tcp_fin_timeout = 15
net.ipv4.tcp_keepalive_time = 1800
fs.file-max = 65535
kernel.pid_max = 65536
net.ipv4.ip_local_port_range = 2000 65000
net.core.netdev_max_backlog = 5000
net.ipv4.tcp_window_scaling = 0

Fonte: Andrea Usuelli