Ãåíåðàöèÿ îò÷åòîâ äëÿ squid

Ðàçäåë : Ñèñòåìà. Àäìèíèñòðèðîâàíèå
Îïóáëèêîâàíî NULL [14/08/2008]

Intro

Â äàííîì îò÷åòå ðàññìàòðèâàþòñÿ òîëüêî ïðîãðàììû/ñêðèïòû, äëÿ ðàáîòû êîòîðûõ íå íóæåí âåá-ñåðâåð. Ñâÿçàíî ýòî ïðåæäå âñåãî ñ òðåáîâàíèÿìè ê áåçîïàñíîñòè, à òàêæå ñ òåì, ÷òî äëÿ ïðîñòîãî èñïîëüçóþò íå î÷åíü ìíîãî êîìïüþòåðû, à ñëåäîâàòåëüíî äîñòàòî÷íî ïðîñòûå è/èëè íåóäîáíòâî ðàáîòû íà í¸ì.

Êîíå÷íî, ìîæíî ïîäíÿòü apache íà ñâîåé ðàáî÷åé ìàøèíå, íî ýòî òîæå ñâÿçàíî ñ îïðåäåëåííûìè íåóäîáñòâàìè. Ïëþñ êî âñåìó ãåíåðàòîðû îò÷åòîâ, ðàáîòàþùèå íà âåá-ñåðâåðå, äîñòàòî÷íî ìåäëåííû è íåýôôåêòèâíû.

Íó è ïîñëåäíåå — âñå âûøåñêàçàííîå îïðîáîâàíî â OpenSUSE 11.0. Âñå ïàêåòû áûëè óñòàíîâëåíû áåç îøèáîê ïðîáëåì. Äëÿ äðóãèõ äèñòðèáóòèâîâ Linux ìîãóò áûòü íåêîòîðûå ðàçëè÷èÿ, íàïðèìåð â ïóòÿõ êôàéëàì.

free-sa 1.4.4

Ïðî free-sa, êîòîðûé íàïèñàí íà C(++), ãîâîðÿò, ÷òî ýòî ïî÷òè ïîëíûé àíàëîã SARG'à. Free-sa çíà÷èò Ñâîáîäíûé Àíàëèçàòîð Ñòàòèñòèêè (free statistic analyzer). Free-sa ïîääåðæèâàåò Squid, CGP, CERN/NCSA, Postfix, Qmail. Ïîñëåäíèå äâà ñ ïîìåòêîé EXPERIMENTAL. À òàêæå Communigate pro 5.x ñ ïîìåòêîé VERY EXPERIMENTAL ;)

Âûêà÷èâàåì ïðîãðàììó ñ http://free-sa.sourceforge.net/. Óñòàíîâêà rpm-ïàêåòà íå âûçûâàåò íèêàêèõ òðóäíîñòåé. Åñëè íå óñòàíàâëèâàåòñÿ — ðàçðåøàåì çàâèñèìîñòè.

Òåïåðü íåîáõîäèìî íàñòðîèòü ôàéë êîíôèãóðàöèè free-sa.conf. Ïî-óìîë÷àíèþ îí íàõîäèòñÿ â êàòàëîãå /usr/local/etc/free-sa. Åñëè êîíôèã íåîáõîäèìî ïåðåìåùèòü â äðóãîé êàòàëîã, òî free-sa íàäî âûçûâàòü òàê:
free-sa -d year -f /home/admin/docs/free-sa.conf
Â ýòîì ñëó÷àå áóäåò ïîñòðîåí îò÷åò çà ïîñëåäíèé ãîä, à ôàéë êîíôèãóðàöèè áóäåò âçÿò èç /home/admin/docs.

Äëÿ ôîðìèðîâàíèÿ îò÷åòîâ íà îñíîâå squid'îâñêîãî access.log â ñåêöèè FILES ôàéëà free-sa.conf íåîáõîäèìî ðàñêîììåíòèðîâàòü ïàðàìåòð log è óêàçàòü ïîëíûé ïóòü ê access.log.

Òàêæå â ñåêöèè DIRECTORIES óêàçûâàåì targetdir= «ïóòü, êóäà ñîõðàíÿåòñÿ ñãåíåðèðîâàííûé îò÷åò» è tmpdir= «êàòàëîã äëÿ õðàíåíèÿ âðåìåííûõôàéëîâ». Áàçîâàÿ íàñòðîéêà free-sa çàêîí÷åíà.

Êàê ïîêàçûâàåò ïðàêòèêà ëó÷øå ñêîìèðîâàòü access.log squid'à íà äðóãóþ ìàøèíó, è ãåíåðèðîâàòü îò÷åò íà íåé. Êîððåêòíàÿ ðàáîòà íà ðàáîòàþùåì squid ïîêà íå ïðîâåðÿëàñü. ß ñêîìèðîâàë àðõèâû ëîãîâ

ê ñåáå â äîìàøíþþ äèðåêòîðèþ /home/null/squid. Âûãëÿäèò ýòî òàê: access.log-DATE.bz2.
Ðàíüøå ÿ äóìàë, ÷òî squid ñàì çèïóåò ôàéëû ëîãîâ, íî îêàçàëîñü, ÷òî ýòî äåëàåò logrotate. Ïîäðîáíàÿ èíôà â man logrotate. Êàê îêàçàëîñü ýòî î÷åíü ïîëåçíàÿ âåùü, îñîáåííî äëÿ ñåðâåðíûõ ñèñòåì.
Äëÿ îòêðûòèÿ ôàéëîâ òèïà bz2 êà÷àåì bzip2 http://www.bzip.org/. Íà ìîìåíò íàïèñàíèÿ ñòàòüè ñàìàÿ ñâåæàÿ âåðñèÿ áûëà bzip2-1.0.5. Äëÿ óñòàíîâêè ïàêåòà íåîáõîäèìî çàïóñòèòü:

make
make install
Åñòåñòâåííî, äëÿ óñòàíîâêè íóæíû ïðàâà root. Ïîñëå óñòàíîâêè ïåðåõîäèì â äèðåêòîðèþ ñ àðõèâàìè ëîãîâ, è âûïîëíÿåì:
bunzip2 -fkvsVL access.log*.bz2
èëè â ìîåì ñëó÷àå:
bunzip2 -fkvsVL /home/null/squid/access.log*.bz2
Ïîñëå ýòîãî â êàòàëîãå ïîÿâèòñÿ ìíîæåñòâî ôàéëîâ access.log-ÄÀÒÀ Ò.ê. free-sa ðàáîòàåò òîëüêî ñ îäíèì ôàéëîì access.log âûïîëíÿåì:
cat access.log* > access.log
ìîæíî èñïîëüçîâàòü àáñîëþòíûå ïóòè:
cat /home/null/squid/access.log* > /home/null/squid/access.log
Òåïåðü ó íàñ åñòü îáùèé ëîã-ôàéë squid'à çà íåîáõîäèìûé ïåðèîä âðåìåíè. Ïðîâåðÿåì ñìîæåò ëè ñ íèì ðàáîòàòü free-sa:
free-sa -s

Ïîñëå ýòîé êîìàíäû äîëæíî ïîÿâèòñÿ íå÷òî ïîäîáíîå:

Åñëè îøèáîê íåò, òî ìîæíî ãåíåðèðîâàòü îò÷åò.
free-sa -d [year][month][day]
Îò÷åò ìîæíî ñãåíåðèðîâàòü çà äåíü, ìåñÿö èëè ãîä.
Î÷åíü âàæíî, ÷òî íåëüçÿ óêàçûâàòü ïðîèçâîëüíûé ïåðèîä âðåìåíè, ò.å. íóæíî âûáðàòü èëè çàðåçåðâèðîâàííûå ñëîâî èëè óêàçàòü äàòó íà÷àëà èëè îêîí÷àíèÿ. Âðåìÿ íåîáõîäèìî óêàçûâàòü â òåêóùåé ëîêàëèçàöèè Linux. Íàïðèìåð:
free-sa -d 01.01.20008-
èëè
free-sa -d -01.08.2008

Â ïåðâîì ñëó÷àå îò÷åò áóäåò ñãåíåðèðîâàí ñ 01.01.2008, à âî âòîðîì, ñ äàòû íà÷àëà âåäåíèÿ ëîãà, äî 01.08.2008.

Îò÷åò ãåíåðèðóåòñÿ íåñêîëüêî ×òîáû àâòîìàòèçèðîâàòü âñÿêèå ðóòèííûå ïîðàöèè ÿ íàïèñàë ñêðèïò, êîòîðûé ñàì ðàñïàêîâûâàåò access.log'è, îáúåäèíÿåò èõ â îäèí, âûâîäèò èíôîðìàöèþ î íåì, è ãåíåðèðóåò îò÷åò.

Êîìàíäû echo îïîâåùàþò àäìèíà î òåêóùåì äéñòâèè ñêðèïòà. Íåìíîãî ïîèçâðàùàëñÿ ñ öâåòîì òåêñòà ;)

Åù¸ õî÷åòñÿ îòìåòèòü
man free-sa
man cat
è

man bzip2
êîòîðûå î÷åíü ïîìîãëè, è âîîáùå RTFM!

calamaris v. 2.59

Calamaris ýòî ñêðèïò íà perl, êîòîðûé ãåíåðèðóåò íà îñíîâå access.log squid'à îò÷åò î ïîñåùåíèÿõ è ò.ï. Îò÷åò óäîáåí ïðåæäå âñåãî äëÿ àíàëèçà ñòàòèñòèêè «â öåëîì» ïî ïîñåùåíèÿì ñàéòîâ. Îñîáåííî èíòåðåñíû ñåêöèè Request-destinations by 2nd-level-domain, TCP-Request-protocol, Incoming TCP-requests by host è Requested extensions. À äëÿ äåòàëüíîãî àíàëèçà ïî îòäåëüíûì ïîëüçîâàòåëÿì ëó÷øå èñïîëüçîâàòü free-sa.

Ñêðèïò ìîæíî óñòàíîâèòü (!) èç rpm èëè èç àðõèâà. Ïðè óñòàíîâêå èç àðõèâà äîñòàòî÷íî ïðîñòî ðàñïàêîâàòü èìåþùèåñÿ â íåì ôàéëû, è ðàçðåøèòü âûïîëíåíèå calamaris.pl. Â ïåðâîé ñòðî÷êå ýòîãî ôàéëà íåîáõîäèìî óêàçàòü êîððåêòíûé ïóòü ê èíòåðïðåòàòîðó perl. Óñòàíîâêà èç rpm òàêæå ïðîïèñàíî áåç êàêèõ-ëèáî òðóäíîñòåé. Äëÿ èñïîëüçîâàíèÿ ãðàôèêè â îò÷åòàõ íåîáõîäèìà óñòàíîâêà áèáëèîòåêè gd.

Õîòÿ â èíòåðíåòå è áûëè ïðåäñòàâëåíû êðàñèâûå îò÷åòû ñ ãðàôèêîé è äèàãðàììàìè, ìíå èõ ñîçäàòü íå óäàëîñü. Èôàéë /etc/calamaris.conf ïî-ìîåìó òîæå íèêàê íå èñïîëüçóåòñÿ. Ìîæåò áûòü ýòî ñâÿçàíî ñ âåðñèåé ìîåãî ñêðèïòà, íî ïàðàìåòðà graph ïðè âûâîäå íà ýêðàí â ñêðèïòå ÿ íå íàø¸ë, è ññûëêè íà /etc/calamaris.conf òîæå.

Ñãåíåðèðîâàòü îò÷åò óäàëîñü âîò òàêèì îáðàçîì:

cat /home/null/squid/access.log | calamaris -asvH 'lookup' -f squid-old -F html > /home/null/squid/report.html

Áîëüøå âñåãî óäèâèëî òî, ÷òî äëÿ squid 2.5stable12 ïîòðåáîâàëñÿ ïàðàìåòð squid-old, ðåêîìåíäîâàííûé äëÿ squid 1.2 è ìëàäøå. Òåïåðü êëþ÷è:

-a — âûâîäèò âñå âîçìîæíûå îò÷åòû;

-s — äåëàåò áîëåå èíôîðìàòèâíûì ñãåíåðèðîâàííûé îò÷åò;

-v — äåëàåò áîëåå èíôîðìàòèâíûì ïðîöåññ ãåíåðàöèè îò÷åòà;

-H — äîáàâëÿåò â çàãîëîâîê îò÷åòà èìÿ õîñòà, ò.å. ñ ïàðàìåòðîì 'lookup' âûäàñò èìÿ âàøåé ìàøèíû;

-f — âõîäíîé ôîðìàò ôàéëà ëîãà;

-F — âûõîäíîé ôîðìàò ôàéëà îò÷åòà.

Ñòîèò îòìåòèòü, ÷òî èçó÷èâ man calamaris è ïîèãðàâøèñü ñ ïàðàìåòðàìè ìîæíî ñãåíåðèðîâàòü î÷åíü êðàñèâûé îò÷åò (áåç ãðàôèêè).

Outro
Áûë ïîðîáîâàí ñêðèïò ïîä íàçâàíèåì Squid-log-analyzer 0.6 ååðñèè. Èñïîëüçîâàòü êàòåãîðè÷åñêè íå ðåêîìåíäóåòñÿ, ò.ê. îí ïðîñòî ïåðåâîäèò access.log squid'à â áîëåå ÷èòàáåëüíûé html. Ñ òàêèì æå óñïåõîì access.log ìîæíî îòêðûòü â MS Excel, ò.å. ïðîñòèòå â OpenOffice Calc. Íèçà÷îò òàêîìó

àíàëèç¸ðó.

Ñïàñèáî âñåì, êòî äî÷èòàë äî êîíöà. Åñëè äàííûé ìàòåðèàë êîìó-íèáóäü ïðèãîäèòñÿ — áóäó î÷åíü ðàä. Ïðèíèìàåòñÿ êîíñòðóêòèâíàÿ êðèòèêà — íà å¸ îñíîâå áóäó óëó÷øàòü ñòàòüþ. Òàêæå ïðèíèìàþòñÿ ññûëêè íà ïîäîáíûå ïðîãè/ñêðèïòû — áóäåì èçó÷àòü.

Îáñóæäåíèå ñòàòüè "ãåíåðàöèÿ îò÷åòîâ â squid"

July-august 2008
© NULL