GRUPA WYDAWNICZA
polskapresse

HaProxy – możliwości i zastosowania

Marek Oszczapiński
m.oszczapiński@polskapresse.pl

Agenda

- Wstęp
- HaProxy
- Konfiguracja i zastosowani
- Podsumowanie

Load Balancing

- Sprzętowe – F5, Cisco LD, loadbalancer.org
- Sieciowe – L2 i L3
- Softwarowe

Softwarowe LB

- HaProxy
- Pound
- Varnish
- Squid
- Nginx
- Pen
- I wiele innych...

HaProxy

- Darmowy
- Bardzo szybki
- HA
- Load Balancing
- Proxy TCP i HTTP(s)
- Multisystemowy
- Bezpieczny

Konfiguracja HaProxy

- global
- defaults
- backend
- frontend
- listen

Konfiguracja – global

```
global
        log 127.0.0.1:520       local1 debug
        maxconn 4096
        uid www
        gid www
        daemon
        pidfile /var/run/haproxy.pid
        stats socket /tmp/haproxy mode 0600 level admin
```

Konfiguracja – defaults

```
defaults
        log             global
        mode            http
        balance         roundrobin
        option          httplog
        maxconn         8192
        contimeout      30s
        clitimeout      30s
        srvtimeout      30s
```

Konfiguracja – backend, frontend, listen

```
backend apache
        server  www   192.168.0.1:80 inter 3000 fall 2 rise 2

frontend web.example.tld
        bind 1.1.1.1:80
        default_backend apache

listen web.example.tld 1.1.1.1:80
        server www    192.168.0.1:80 inter 3000 fall 2 rise 2
```

Konfiguracja – HaProxy HA

```
peers haproxy
        peer haproxy1 192.168.0.1:1024
        peer haproxy2 192.168.0.2:1024

backend apache
        stick-table type ip size 20k expires 10m store cont_cur peers
haproxy
        stick or src
```

Konfiguracja – HTTP

```
frontend web.example.tld
        bind 1.1.1.1:80
        balance roundrobin
        default_backend apache

backend apache
        option  httpchk HEAD /check.txt HTTP/1.0
        server  www1        192.168.0.1:80 inter 3000 cookie 1 check
        server  www2        192.168.0.2:80 inter 3000 cookie 2 check 81
        server  www3        192.168.0.3:80 inter 3000 cookie 3 check
        server  www-bkp1    192.168.0.4:80 inter 3000 cookie 1 check backup
```

Konfiguracja – HTTP acl

```
fronted web.example.tld
        bind 1.1.1.1:80
        acl static              path_end .flv .js .css .ico .jpeg .jpg .png

        use_backend static if static
        default_backend apache

fronted web.example.tld
        bind 1.1.1.1:80

        use_backend static if { path_end .flv .js .css .ico .jpeg .jpg .png }
        default_backend apache
```

Zastosowania – HTTP acl

```
fronted web.example.tld
        bind 1.1.1.1:80
        acl static          path_end .flv .js .css .ico .jpeg .jpg .png
        acl static          hdr_reg(host) -i ^(s|m|img).web.example.tld
        acl bot             hdr_reg(user-agent) -i -f /etc/haproxy/bot.txt
        acl blokada         src 192.168.100.0/24
        acl wyjatek         src 192.168.100.100

        block if blokada !wyjatek

        use_backend bot if bot
        use_backend static if static
        default_backend apache
```

GRUPA WYDAWNICZA polskapresse

Zastosowania – HTTP acl c.d.

```
redirect code 301 prefix http://www.naszemiasto.pl  if { hdr(host) -i
naszemiasto.pl } || { hdr_end(host) naszemiasto.com.pl }

redirect location http://prasa24.pl  if { hdr_reg(host) -i ^(www.)?
naszemiasto.pl } { path_beg /gazety }

redirect location http://www.gratka.pl                if { hdr_reg(host) (.*) }

reqirep ^Host:\ www.(.*) Host:\ \1 if { hdr_beg(host) -i www. }
```

Konfiguracja – HTTPs

```
fronted web.example.tld
        bind 1.1.1.1:80
        bind 1.1.1.1:443 ssl crt /etc/haproxy/ssl/cert.pem

        reqadd X-Forwarded-Proto:\ https if { dst_port 443 }
        reqadd X-Forwarded-Proto:\ http unless { dst_port 443 }

        http-request redirect scheme https if !{ ssl_fc }

        default_backend apache
```

Zastosowania – HTTPs htaccess

```
userlist admin
        user admin1 insecure-password 123456
        user admin2 password $6$k6y3o.eP$JlKBx9za966xHSwRv6J.C0/D7cV91

fronted web.example.tld
        bind 1.1.1.1:80
        bind 1.1.1.1:443 ssl crt /etc/haproxy/ssl/cert.pem

        http-request auth realm Restricted_Area if !{ http_auth(admin) } { dst_port
443 }
        default_backend apache
```

Konfiguracja – sticky session, hit ratio

```
backend apache
        balance source
        server  cache1   192.168.0.1:80 check
        server  cache2   192.168.0.2:80 check

backend apache
        balance roundrobin
        cookie JSESSIONID prefix indirect nocache
        server  cache1   192.168.0.1:80 check cookie c1
        server  cache2   192.168.0.2:80 check cookie c2

backend apache
        stick store-request src
        stick-table type ip size 200k expires 30m
        server  cache1   192.168.0.1:80 inter 3000 fall 2 rise 2
        server  cache2   192.168.0.2:80 inter 3000 fall 2 rise 2
```

Konfiguracja – IPv6

```
listen naszemiasto.pl 2a02:1320:ffff:0:195:8:99:2:80
        mode tcp

        server  naszemiasto.pl          195.8.99.2:80 check inter 3000
```

Zastosowania – TCP, DDoS

```
listen 1.1.1.1:22
        mode tcp
        stick-table type ip size 200k expires 60s store conn_cur
        tcp-request connection reject if { sc1_conn_cur gt 10 }
        tcp-request connection track-sc1 src

        server ssh1    192.168.0.1:22 inter 3000 fall 2 rise 2

listen 1.1.1.1:80
        stick-table type ip size 200k expires 60s store conn_cur
        acl abuser sc1_conn_cur gt 100
        tcp-request connection track-sc1 src if ! { sc1_conn_cur gt 100 }

        use_backend  slow if abuser
        server ssh1    192.168.0.1:80 inter 3000 fall 2 rise 2
```

Konfiguracja – TCP smtp, imap

```
listen 1.1.1.1:25
        mode tcp
        option tcplog
        balance roundrobin
        tcp-request connection reject if { src 192.168.100.0/24 }
        server smtp1    192.168.0.1:25 inter 3000
        server smtp2    192.168.0.2:25 inter 3000

listen 1.1.1.1:143
        mode tcp
        balance lastconn
        option tcp-check
        tcp-check connect port 143
        tcp-check expect string *\ OK\ IMAP4\ ready
        server imap1    192.168.0.1:143 check inter 3000
        server imap2    192.168.0.2:143 check inter 3000
```

Zastosowania – MySQL

```
listen mysql 192.168.0.1:3306
        mode tcp
        option   tcplog
        server   mysql1  10.0.0.1:3306 check
```

Zastosowania – MySQL

```
# DB write cluster
#       Failure scenarios:
#       - replication 'up' on db01 & db02          = writes to db01
#       - replication 'down' on db02               = writes to db01
#       - replication 'down' on db01               = writes to db02
#       - replication 'down' on db01 & db02        = go nowhere, split-
brain, cluster FAIL!
#       - mysql 'down' on db02                     = writes to db01_backup
#       - mysql 'down' on db01                     = writes to db02_backup
#       - mysql 'down' on db01 & db02              = go nowhere, cluster
FAIL!
```

Zastosowania – MySQL

```
backend cluster_db_write
        mode    tcp
        option  tcpka
        balance roundrobin
        option httpchk GET /dps

        server  db01 172.16.0.60:3306 weight 1 check port 9201 inter 1s rise 2 fall 1
        server  db02 172.16.0.61:3306 weight 1 check port 9201 inter 1s rise 2 fall 1
backup
        server  db01_backup 172.16.0.60:3306 weight 1 check port 9301 inter 1s rise
2 fall 2 addr 127.0.0.1 backup
        server  db02_backup 172.16.0.61:3306 weight 1 check port 9302 inter 1s rise
2 fall 2 addr 127.0.0.1 backup
```

Zastosowania – FTP

```
listen ftp-lb00
    bind 2.2.2.2:21
    mode tcp
    option tcplog
    balance leastconn
    server ftp-serv00 192.168.1.1:21 check
    server ftp-serv01 192.168.1.2:21 check
    server ftp-serv02 192.168.1.3:21 check
```

- **ACTIVE**

```
iptables -A POSTROUTING -s 192.168.1.1/32 -o eth1 -j SNAT --to-source 2.2.2.2
iptables -A POSTROUTING -s 192.168.1.2/32 -o eth1 -j SNAT --to-source 2.2.2.2
iptables -A POSTROUTING -s 192.168.1.3/32 -o eth1 -j SNAT --to-source 2.2.2.2
```

Zastosowania – FTP c.d.

- **PASSIVE**

Bind 192.168.1.1
Port 21
MasqueradeAddress 2.2.2.2
PassivePorts 1025 2048

Bind 192.168.1.2
Port 21
MasqueradeAddress 2.2.2.2
PassivePorts 2049 3072

iptables -A PREROUTING -d 2.2.2.2/32 -i eth1 -p tcp -m tcp --dport 1025:2048 -j DNAT --to-destination 192.168.1.1
iptables -A PREROUTING -d 2.2.2.2/32 -i eth1 -p tcp -m tcp --dport 2049:3072 -j DNAT --to-destination 192.168.1.2

Zastosowania – RDP

```
listen RDP_Test
        bind 192.168.67.30:3389
        mode tcp
        balance leastconn
        option tcpka
        tcp-request inspect-delay 5s
        tcp-request content accept if RDP_COOKIE
        stick-table type string size 10240k expire 12h peers haproxy
        timeout client 12h
        timeout server 12h

        server Win2k8-1 192.168.0.11:3389 check inter 2000 rise 2 fall 3
        server Win2k8-2 192.168.0.12:3389 check inter 2000 rise 2 fall 3
```

GRUPA WYDAWNICZA polskapresse

Statystyki

```
listen stats 192.168.0.1:8080
        mode http
        stats enable
        stats hide-version
        stats realm Haproxy\ Statistics
        stats uri /
```

GRUPA WYDAWNICZA polskapresse

Narzędzia

Backend	0	0		0	0		0	0	1	0	0	0	0	0	0		0	0	0	0	8h14m UP		1	1	0		0	0s	

polskatimes_www

	Queue			Session rate			Sessions					Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
	0	0	-	33	82		13	145	-	1 259 614	1 259 614	963 056 823	30 869 414 093		0		0	1	0	0	8h14m UP	L4OK in 1ms	50	Y	-	0	0	0s	-
	0	0	-	16	41		6	33	-	629 807	629 807	452 416 105	15 441 267 039		0		0	0	0	0	8h14m UP	L4OK in 0ms	25	Y	-	0	0	0s	-
	0	0	-	20	49		5	52	-	755 769	755 769	579 368 216	18 572 278 081		0		0	0	0	0	8h14m UP	L4OK in 0ms	30	Y	-	0	0	0s	-
	0	0	-	10	25		5	25	-	376 310	376 310	297 451 716	9 196 606 621		0		0	0	0	0	8h14m UP	L4OK in 0ms	15	Y	-	0	0	0s	-
	0	0	-	16	41		4	29	-	629 807	629 807	468 513 525	15 455 844 544		0		0	0	0	0	8h14m UP	L4OK in 0ms	25	Y	-	0	0	0s	-
	0	0	-	17	40		4	26	-	629 807	629 807	489 751 841	15 424 987 652		0		0	1	0	0	8h14m UP	L4OK in 0ms	25	Y	-	0	0	0s	-
	0	0	-	13	33		5	25	-	503 846	503 846	395 906 794	12 339 082 276		0		0	0	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
	0	0	-	12	33		4	28	-	503 845	503 845	387 822 733	12 386 811 838		0		0	0	0	0	8h14m UP	L4OK in 1ms	20	Y	-	0	0	0s	-
Backend	0	0		141	344		46	186	1 639	5 288 822	5 288 805	4 034 307 031	129 686 293 161	0	0		0	2	0	0	8h14m UP		210	8	0		0	0s	

naszemiasto

	Queue			Session rate			Sessions					Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
	0	0	-	31	54		15	92	-	914 994	914 994	1 051 362 332	18 557 798 039		0		0	318	0	0	8h14m UP	L4OK in 1ms	60	Y	-	0	0	0s	-
	0	0	-	20	36		15	117	-	609 998	609 996	701 397 030	12 375 931 561		0		0	220	2	0	8h14m UP	L4OK in 0ms	40	Y	-	0	0	0s	-
	0	0	-	31	54		23	121	-	914 994	914 994	1 040 011 071	18 583 415 286		0		0	345	0	0	8h14m UP	L4OK in 0ms	60	Y	-	0	0	0s	-
	0	0	-	26	45		21	63	-	762 495	762 495	869 825 155	15 466 998 189		0		0	189	0	0	8h14m UP	L4OK in 0ms	50	Y	-	0	0	0s	-
	0	0	-	10	18		11	26	-	304 998	304 998	340 231 446	6 184 242 086		0		0	70	0	0	8h14m UP	L4OK in 1ms	20	Y	-	0	0	0s	-
	0	0	-	10	18		7	24	-	304 998	304 998	351 692 502	6 186 497 798		0		0	65	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
	0	0	-	17	31		18	42	-	533 746	533 746	617 218 625	10 806 952 374		0		0	156	0	0	8h14m UP	L4OK in 0ms	35	Y	-	0	0	0s	-
	0	0	-	18	32		17	49	-	533 746	533 746	629 663 129	10 831 692 315		0		0	160	0	0	8h14m UP	L4OK in 0ms	35	Y	-	0	0	0s	-
	0	0	-	18	32		16	45	-	533 746	533 746	596 118 685	10 847 752 635		0		0	164	0	0	8h14m UP	L4OK in 0ms	35	Y	-	0	0	0s	-
Backend	0	0		186	320		144	326	820	5 413 737	5 413 713	6 197 563 792	109 841 280 283	0	0		0	1 687	2	0	8h14m UP		355	9	0		0	0s	

dom_gratka_pl

	Queue			Session rate			Sessions					Bytes		Denied		Errors			Warnings		Server								
	Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Dwntme	Thrtle
	0	0	-	27	68		9	137	-	1 195 157	1 195 157	3 334 854 823	22 055 780 038		0		0	31	0	0	8h14m UP	L4OK in 0ms	60	Y	-	0	0	0s	-
	0	0	-	9	22		2	21	-	398 386	398 386	1 114 536 883	7 358 878 368		0		0	15	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
	0	0	-	8	23		3	18	-	398 385	398 385	1 156 596 876	7 297 398 988		0		0	12	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
	0	0	-	9	22		3	17	-	398 385	398 385	1 098 258 351	7 446 264 459		0		0	9	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
	0	0	-	9	23		4	19	-	398 385	398 385	1 102 380 437	7 342 767 679		0		0	10	0	0	8h14m UP	L4OK in 0ms	20	Y	-	0	0	0s	-
Backend	0	0		64	157		21	153	820	2 788 713	2 788 698	7 806 656 878	51 501 089 532	0	0		0	77	0	0	8h14m UP		140	5	0		0	0s	

Narzedzia

```
global
        stats socket /tmp/haproxy mode 0600 level admin
```

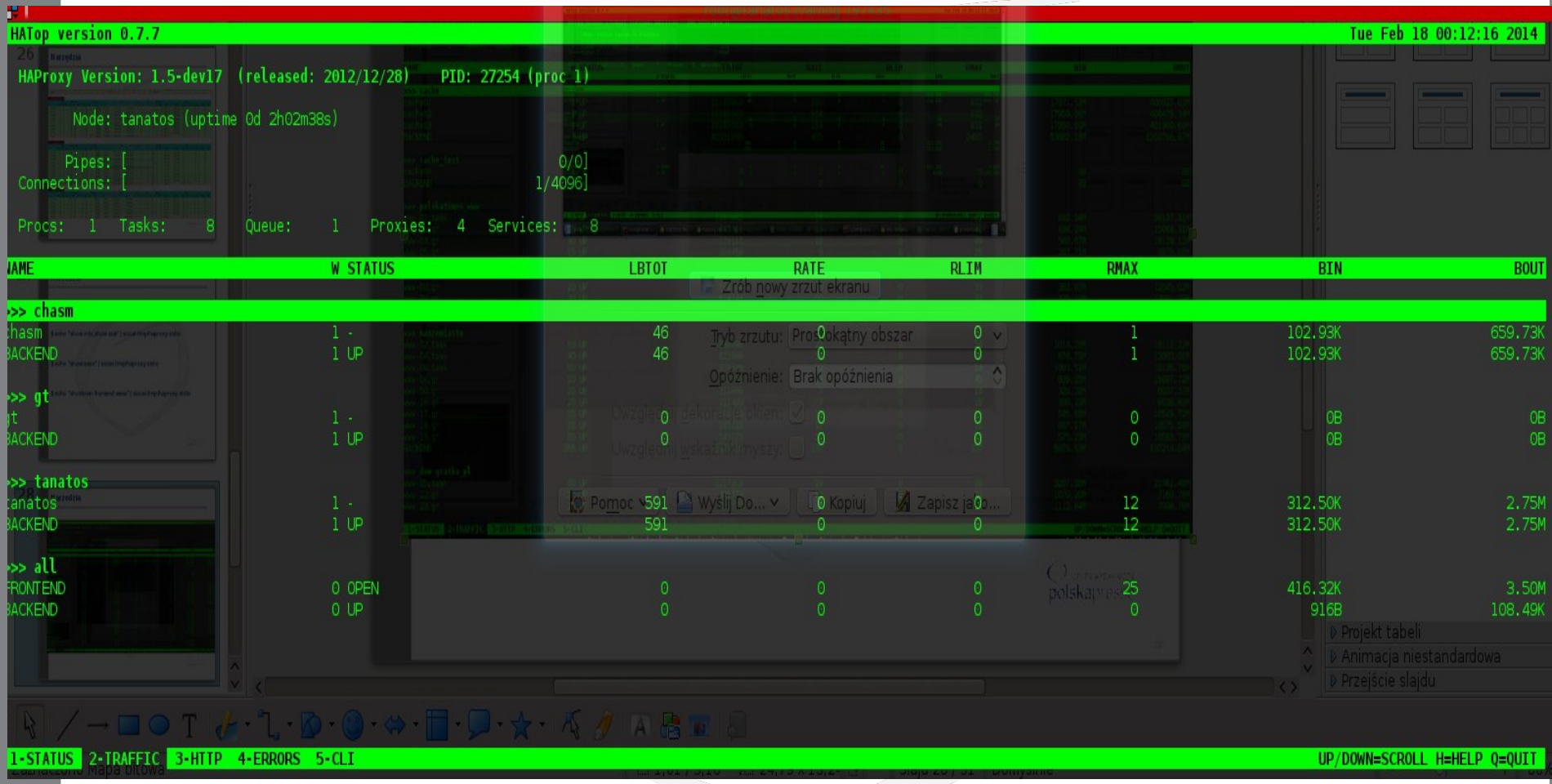
```
$ echo "show info;show stat" | socat /tmp/haproxy stdio
```

```
$ echo "show sess" | socat /tmp/haproxy stdio
```

```
$ echo "shutdown frontend www" | socat /tmp/haproxy stdio
```

GRUPA WYDAWNICZA polskapresse

Narzedzia


HATop version 0.7.7
Tue Feb 18 00:12:16 2014
HAProxy Version: 1.5-dev17 (released: 2012/12/28) PID: 27254 (proc 1)
Node: tanatos (uptime 0d 2h02m38s)
Pipes: [0/0]
Connections: [1/4096]
Procs: 1 Tasks: 8 Queue: 1 Proxies: 4 Services: 8
NAME W STATUS LBTOT RATE RLIM RMAX BIN BOUT
>>> chasm
chasm 1 - 46 0 0 1 102.93K 659.73K
BACKEND 1 UP 46 0 0 1 102.93K 659.73K
>>> gt
gt 1 - 0 0 0 0 0B 0B
BACKEND 1 UP 0 0 0 0 0B 0B
>>> tanatos
tanatos 1 - 591 0 0 12 312.50K 2.75M
BACKEND 1 UP 591 0 0 12 312.50K 2.75M
>>> all
FRONTEND 0 OPEN 0 0 0 25 416.32K 3.50M
BACKEND 0 UP 0 0 0 0 916B 108.49K
1-STATUS 2-TRAFFIC 3-HTTP 4-ERRORS 5-CLI
UP/DOWN=SCROLL H=HELP Q=QUIT

Podsumowanie

- Wydajne: 108k req/s, 16kb per session
- Konfigurowalne
- Bardzo dobra dokumentacja
  - http://haproxy.1wt.eu/download/1.5/doc/configuration.txt
  - http://marc.info/?l=haproxy
- Multisystemowa
- Proxy TCP i HTTP
- Obsługa SSL

GRUPA WYDAWNICZA polskapresse

praca.gratka.pl/lista/fr_polskapresse

INTERNET polskapresse

Polskapresse, wiodąca grupa mediowa działająca na rynkach wydawniczym, internetowym i usług poligraficznych, wydawca 9 największych dzienników regionalnych w Polsce, właściciel portalu ogłoszeniowego Gratka.pl, NaszeMiasto.pl oraz ponad 30 serwisów informacyjnych, w związku z dynamicznym rozwojem, poszukuje kandydatów na stanowisko:

ADMINISTRATOR SYSTEMÓW

Data publikacji: **2014-02-14**
Miejsce: **Gdańsk**
Nr referencyjny: **AS/02/14**

Obowiązki:

- utrzymanie i rozwój infrastruktury sieciowej i serwerowej
- utrzymanie i rozwój systemów serwerowych opartych o architekturę LAMP
- dbanie o bezpieczeństwo systemów
- rozwiązywanie bieżących problemów serwerowych
- monitorowanie bieżącej konfiguracji systemów serwerowych i zasobów sieciowych
- prowadzenie dokumentacji infrastruktury sieciowej i serwerowej

Wymagania:

- wykształcenie wyższe kierunkowe
- doświadczenie w administrowaniu systemami
- znajomość sieci LAN/WLAN oraz znajomość protokołów sieciowych
- znajomość tematyki zewnętrznych macierzy dyskowych oraz sieci SAN
- doświadczeniu w administrowaniu MySQL (strojenie, replikacja)
- znajomość języków skryptowych
- znajomość produktów i technologii: Linux, Apache, nginx, Varnish, PHP, MySQL, Solr, NFS, HAProxy, KVM, puppet
- znajomość aktualnych technologii i trendów internetowych
- umiejętność pracy w zespole
- samodzielność i inicjatywa

GRUPA WYDAWNICZA polskapresse

Dziękuję za uwagę!
Pytania?

GRUPA WYDAWNICZA
polskapresse