РЕД СЛЁРМ

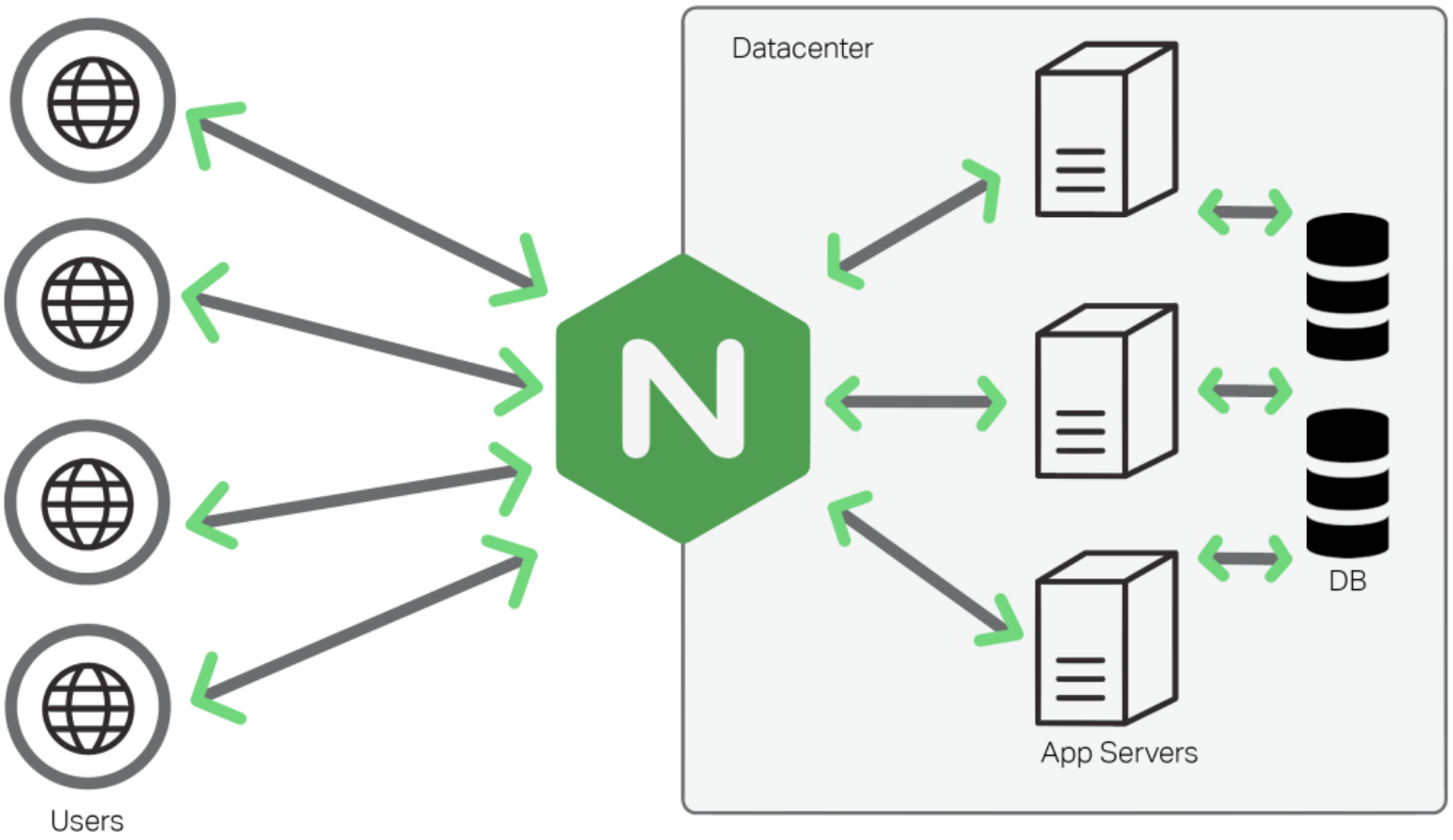
+

Southbridge

Веб-серверы. Опыт и практика Southbridge

slurm.io

Nginx – наше все



А что скрывается за nginx ?

- apache + mod+php (php)
- php-fpm (php)
- unicorn, puma (ruby)
- uwsgi (python)
- pm2 (node.js)
- unit

Структура конфигов

Общая часть – раскладывается системой конфигурации. Может быть изменена централизовано и массово

Описание виртуального хоста-сервера – отдельный файл в каталоге с проектом, симлинком прокинут в каталог с конфигами веб-сервера

Общая часть NGINX

Настройки, влияющие на производительность, на безопасность.
Настройки default-сайта.
Настройки для метрик мониторинга.

Общая часть Apache

Listen 127.0.0.1:8080

Лимиты для prefork

```
    StartServers            5
    MinSpareServers         5
    MaxSpareServers        15
    ServerLimit           150
    MaxClients            150
    MaxRequestsPerChild  4000
```

mod_rpaf или mod_remoteip

Шаблон настроек NGINX

```
 location ~*
\.(jpg|jpeg|gif|png|tif|tiff|bmp|svg|ico|js|css|zip|tgz|gz|tar|rar|bz2|rtf|doc|docx|x
ls|xlsx|ppt|pptx|exe|pdf|txt|mid|midi|swf|flv|avi|djvu|wav|mp3|ogg|mp4|mpg|m
peg|mov|wmv|wma|webm|ogv|ogg|3gp|otf|woff|woff2|eot)$ {
        expires 7d;
        access_log off;
        log_not_found off;
    }

location ~ /\.git { deny all; }

location ~ /\.ht { deny all; }

location ~ /\.svn { deny all; }
```

Шаблон настроек NGINX

```
location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Proxy "";
        proxy_redirect off;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        proxy_read_timeout 300;
        proxy_buffer_size 16k;
        proxy_buffers 32 16k;
    }
```

Шаблон настроек NGINX

```
 location / {
        try_files $uri/ =404;
# or rewrite to index
#       try_files $uri/ /index.php$is_args$args;
    }

 location ~ \.php$ {
        try_files $uri =404;
        fastcgi_pass $fpmpool;
        fastcgi_param HTTP_PROXY "";
        include fastcgi_params;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_read_timeout 300;
        fastcgi_buffer_size 16k;
        fastcgi_buffers 32 16k;
    }
```

Общая часть php

Php.ini:
disable_functions =
dl,shell_exec,exec,system,passthru,popen,proc_open,proc_nice,proc_get_status,proc_close,proc_terminate,posix_mkfifo,show_source,pcntl_fork
expose = off
error_reporting = E_ALL & ~E_DEPRECATED & ~E_STRICT & ~E_NOTICE - не выводить E_NOTICE в лог

Per virtual host/php-fpm pool:

open_basedir “/srv/www/project/:/usr/share/php"
upload_tmp_dir “/srv/www/project/tmp"
session.save_path "/srv/www/project/tmp"
upload_max_filesize "256M"
post_max_size "256M"
memory_limit "256M"
short_open_tag "On"
date.timezone "Europe/Moscow"

Шифрование

SSL – устарел и скомпрометирован. Версии 2 и 3

TLS – то же SSL, но лучше и без ошибок. Версии 1.0, 1.1, 1.2

HTTPS – HTTP с шифрованием

Цели и задачи

Аутентификация – удостоверится, что на другой стороне канала именно тот, к кому мы хотим обратится

Решение: Система доверия сертификатов, основанных на технологии шифрования с открытым ключом

Защита – предотвратить перехват информации

Решение: Шифрование трафика быстрым симметричным алгоритмом с одноразовыми или краткоживущими ключами

Let’s encrypt

Бесплатные сертификаты

Только для доменов

Открытый протокол ACME для верификации владельца домена

Множество различных клиентов

Сертификаты Organization Validation (OV) или Extended Validation (EV) не планируются

Проверка настройки SSL

http://www.ssllabs.com/ssltest

openssl dhparam -out dhparams.pem 2048; chmod 600 dhparams.pem

```
ssl_dhparam /etc/nginx/ssl/dhparams.pem;
ssl_prefer_server_ciphers on;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_session_cache shared:SSL:20m;
ssl_session_timeout 10m;

add_header Strict-Transport-Security "max-age=31536000;";
```

РЕД СЛЁРМ

+

Southbridge

slurm.io