Nextcloud

docker-compose.yml

```
version: '2'

volumes:
  nextcloud:
  db:

services:
  db:
    image: mariadb
    command: --transaction-isolation=READ-COMMITTED --binlog-format=ROW
    restart: always
    volumes:
      - db:/var/lib/mysql
    environment:
      - MYSQL_ROOT_PASSWORD=rootpasword
      - MYSQL_PASSWORD=nextcloudpassword
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud

  app:
    image: nextcloud:fpm
    links:
      - db
    volumes:
      - /dades/nextcloud_fpm:/var/www/html
      - ${PWD}/www.conf:/usr/local/etc/php-fpm.d/www.conf
    restart: always

  web:
    image: nginx
    ports:
      - 9080:80
    links:
      - app
    volumes:
      - ./nginx.conf:/etc/nginx/nginx.conf:ro
    volumes_from:
      - app
    restart: always
```

www.conf

```
; Start a new pool named 'www'.
; the variable $pool can be used in any directive and will be replaced by
the
```

```
; pool name ('www' here)
[www]

; Per pool prefix
; It only applies on the following directives:
; - 'access.log'
; - 'slowlog'
; - 'listen' (unixsocket)
; - 'chroot'
; - 'chdir'
; - 'php_values'
; - 'php_admin_values'
; When not set, the global prefix (or NONE) applies instead.
; Note: This directive can also be relative to the global prefix.
; Default Value: none
;prefix = /path/to/pools/$pool

; Unix user/group of processes
; Note: The user is mandatory. If the group is not set, the default user's
group
;       will be used.
user = www-data
group = www-data

; The address on which to accept FastCGI requests.
; Valid syntaxes are:
;   'ip.add.re.ss:port'    - to listen on a TCP socket to a specific IPv4
address on
;                            a specific port;
;   '[ip:6:addr:ess]:port' - to listen on a TCP socket to a specific IPv6
address on
;                            a specific port;
;   'port'                 - to listen on a TCP socket to all addresses
;                            (IPv6 and IPv4-mapped) on a specific port;
;   '/path/to/unix/socket' - to listen on a unix socket.
; Note: This value is mandatory.
listen = 127.0.0.1:9000

; Set listen(2) backlog.
; Default Value: 511 (-1 on FreeBSD and OpenBSD)
;listen.backlog = 511

; Set permissions for unix socket, if one is used. In Linux, read/write
; permissions must be set in order to allow connections from a web server.
Many
; BSD-derived systems allow connections regardless of permissions. The owner
; and group can be specified either by name or by their numeric IDs.
; Default Values: user and group are set as the running user
;                 mode is set to 0660
;listen.owner = www-data
;listen.group = www-data
```

```
;listen.mode = 0660
; When POSIX Access Control Lists are supported you can set them using
; these options, value is a comma separated list of user/group names.
; When set, listen.owner and listen.group are ignored
;listen.acl_users =
;listen.acl_groups =

; List of addresses (IPv4/IPv6) of FastCGI clients which are allowed to
connect.
; Equivalent to the FCGI_WEB_SERVER_ADDRS environment variable in the
original
; PHP FCGI (5.2.2+). Makes sense only with a tcp listening socket. Each
address
; must be separated by a comma. If this value is left blank, connections
will be
; accepted from any ip address.
; Default Value: any
;listen.allowed_clients = 127.0.0.1

; Specify the nice(2) priority to apply to the pool processes (only if set)
; The value can vary from -19 (highest priority) to 20 (lower priority)
; Note: - It will only work if the FPM master process is launched as root
;       - The pool processes will inherit the master process priority
;         unless it specified otherwise
; Default Value: no set
; process.priority = -19

; Set the process dumpable flag (PR_SET_DUMPABLE prctl) even if the process
user
; or group is differrent than the master process user. It allows to create
process
; core dump and ptrace the process for the pool user.
; Default Value: no
; process.dumpable = yes

; Choose how the process manager will control the number of child processes.
; Possible Values:
;   static  - a fixed number (pm.max_children) of child processes;
;   dynamic - the number of child processes are set dynamically based on the
;             following directives. With this process management, there will
be
;             always at least 1 children.
;             pm.max_children      - the maximum number of children that can
;                                    be alive at the same time.
;             pm.start_servers     - the number of children created on
startup.
;             pm.min_spare_servers - the minimum number of children in
'idle'
;                                    state (waiting to process). If the
number
;                                    of 'idle' processes is less than this
```

```
;                                   number then some children will be
created.
;             pm.max_spare_servers - the maximum number of children in
'idle'
;                                   state (waiting to process). If the
number
;                                   of 'idle' processes is greater than
this
;                                   number then some children will be
killed.
;  ondemand - no children are created at startup. Children will be forked
when
;             new requests will connect. The following parameter are used:
;             pm.max_children           - the maximum number of children
that
;                                         can be alive at the same time.
;             pm.process_idle_timeout   - The number of seconds after which
;                                         an idle process will be killed.
; Note: This value is mandatory.
pm = dynamic

; The number of child processes to be created when pm is set to 'static' and
the
; maximum number of child processes when pm is set to 'dynamic' or
'ondemand'.
; This value sets the limit on the number of simultaneous requests that will
be
; served. Equivalent to the ApacheMaxClients directive with mpm_prefork.
; Equivalent to the PHP_FCGI_CHILDREN environment variable in the original
PHP
; CGI. The below defaults are based on a server without much resources.
Don't
; forget to tweak pm.* to fit your needs.
; Note: Used when pm is set to 'static', 'dynamic' or 'ondemand'
; Note: This value is mandatory.
pm.max_children = 120

; The number of child processes created on startup.
; Note: Used only when pm is set to 'dynamic'
; Default Value: (min_spare_servers + max_spare_servers) / 2
pm.start_servers = 12

; The desired minimum number of idle server processes.
; Note: Used only when pm is set to 'dynamic'
; Note: Mandatory when pm is set to 'dynamic'
pm.min_spare_servers = 6

; The desired maximum number of idle server processes.
; Note: Used only when pm is set to 'dynamic'
; Note: Mandatory when pm is set to 'dynamic'
pm.max_spare_servers = 18
```

```
; The number of seconds after which an idle process will be killed.
; Note: Used only when pm is set to 'ondemand'
; Default Value: 10s
;pm.process_idle_timeout = 10s;

; The number of requests each child process should execute before
respawning.
; This can be useful to work around memory leaks in 3rd party libraries. For
; endless request processing specify '0'. Equivalent to
PHP_FCGI_MAX_REQUESTS.
; Default Value: 0
;pm.max_requests = 500

; The URI to view the FPM status page. If this value is not set, no URI will
be
; recognized as a status page. It shows the following informations:
;   pool                 - the name of the pool;
;   process manager      - static, dynamic or ondemand;
;   start time           - the date and time FPM has started;
;   start since          - number of seconds since FPM has started;
;   accepted conn        - the number of request accepted by the pool;
;   listen queue         - the number of request in the queue of pending
;                          connections (see backlog in listen(2));
;   max listen queue     - the maximum number of requests in the queue
;                          of pending connections since FPM has started;
;   listen queue len     - the size of the socket queue of pending
connections;
;   idle processes       - the number of idle processes;
;   active processes     - the number of active processes;
;   total processes      - the number of idle + active processes;
;   max active processes - the maximum number of active processes since FPM
;                          has started;
;   max children reached - number of times, the process limit has been
reached,
;                          when pm tries to start more children (works only
for
;                          pm 'dynamic' and 'ondemand');
; Value are updated in real time.
; Example output:
;   pool:                 www
;   process manager:      static
;   start time:           01/Jul/2011:17:53:49 +0200
;   start since:          62636
;   accepted conn:        190460
;   listen queue:         0
;   max listen queue:     1
;   listen queue len:     42
;   idle processes:       4
;   active processes:     11
;   total processes:      15
;   max active processes: 12
```

```
;   max children reached: 0
;
; By default the status page output is formatted as text/plain. Passing
either
; 'html', 'xml' or 'json' in the query string will return the corresponding
; output syntax. Example:
;   http://www.foo.bar/status
;   http://www.foo.bar/status?json
;   http://www.foo.bar/status?html
;   http://www.foo.bar/status?xml
;
; By default the status page only outputs short status. Passing 'full' in
the
; query string will also return status for each pool process.
; Example:
;   http://www.foo.bar/status?full
;   http://www.foo.bar/status?json&full
;   http://www.foo.bar/status?html&full
;   http://www.foo.bar/status?xml&full
; The Full status returns for each process:
;   pid                  - the PID of the process;
;   state                - the state of the process (Idle, Running, ...);
;   start time           - the date and time the process has started;
;   start since          - the number of seconds since the process has
started;
;   requests             - the number of requests the process has served;
;   request duration     - the duration in µs of the requests;
;   request method       - the request method (GET, POST, ...);
;   request URI          - the request URI with the query string;
;   content length       - the content length of the request (only with
POST);
;   user                 - the user (PHP_AUTH_USER) (or '-' if not set);
;   script               - the main script called (or '-' if not set);
;   last request cpu     - the %cpu the last request consumed
;                          it's always 0 if the process is not in Idle state
;                          because CPU calculation is done when the request
;                          processing has terminated;
;   last request memory  - the max amount of memory the last request
consumed
;                          it's always 0 if the process is not in Idle state
;                          because memory calculation is done when the
request
;                          processing has terminated;
; If the process is in Idle state, then informations are related to the
; last request the process has served. Otherwise informations are related to
; the current request being served.
; Example output:
;   ************************
;   pid:                   31330
;   state:                 Running
;   start time:            01/Jul/2011:17:53:49 +0200
```

```
;   start since:          63087
;   requests:             12808
;   request duration:     1250261
;   request method:       GET
;   request URI:          /test_mem.php?N=10000
;   content length:       0
;   user:                 -
;   script:               /home/fat/web/docs/php/test_mem.php
;   last request cpu:     0.00
;   last request memory:  0
;
; Note: There is a real-time FPM status monitoring sample web page available
;       It's available in: /usr/local/share/php/fpm/status.html
;
; Note: The value must start with a leading slash (/). The value can be
;       anything, but it may not be a good idea to use the .php extension or
it
;       may conflict with a real PHP file.
; Default Value: not set
;pm.status_path = /status

; The ping URI to call the monitoring page of FPM. If this value is not set,
no
; URI will be recognized as a ping page. This could be used to test from
outside
; that FPM is alive and responding, or to
; - create a graph of FPM availability (rrd or such);
; - remove a server from a group if it is not responding (load balancing);
; - trigger alerts for the operating team (24/7).
; Note: The value must start with a leading slash (/). The value can be
;       anything, but it may not be a good idea to use the .php extension or
it
;       may conflict with a real PHP file.
; Default Value: not set
;ping.path = /ping

; This directive may be used to customize the response of a ping request.
The
; response is formatted as text/plain with a 200 response code.
; Default Value: pong
;ping.response = pong

; The access log file
; Default: not set
;access.log = log/$pool.access.log

; The access log format.
; The following syntax is allowed
;  %%: the '%' character
;  %C: %CPU used by the request
;      it can accept the following format:
```

```
;      - %{user}C for user CPU only
;      - %{system}C for system CPU only
;      - %{total}C  for user + system CPU (default)
;  %d: time taken to serve the request
;      it can accept the following format:
;      - %{seconds}d (default)
;      - %{miliseconds}d
;      - %{mili}d
;      - %{microseconds}d
;      - %{micro}d
;  %e: an environment variable (same as $_ENV or $_SERVER)
;      it must be associated with embraces to specify the name of the env
;      variable. Some exemples:
;      - server specifics like: %{REQUEST_METHOD}e or %{SERVER_PROTOCOL}e
;      - HTTP headers like: %{HTTP_HOST}e or %{HTTP_USER_AGENT}e
;  %f: script filename
;  %l: content-length of the request (for POST request only)
;  %m: request method
;  %M: peak of memory allocated by PHP
;      it can accept the following format:
;      - %{bytes}M (default)
;      - %{kilobytes}M
;      - %{kilo}M
;      - %{megabytes}M
;      - %{mega}M
;  %n: pool name
;  %o: output header
;      it must be associated with embraces to specify the name of the
header:
;      - %{Content-Type}o
;      - %{X-Powered-By}o
;      - %{Transfert-Encoding}o
;      - ....
;  %p: PID of the child that serviced the request
;  %P: PID of the parent of the child that serviced the request
;  %q: the query string
;  %Q: the '?' character if query string exists
;  %r: the request URI (without the query string, see %q and %Q)
;  %R: remote IP address
;  %s: status (response code)
;  %t: server time the request was received
;      it can accept a strftime(3) format:
;      %d/%b/%Y:%H:%M:%S %z (default)
;      The strftime(3) format must be encapsuled in a %{<strftime_format>}t
tag
;      e.g. for a ISO8601 formatted timestring, use: %{%Y-%m-%dT%H:%M:%S%z}t
;  %T: time the log has been written (the request has finished)
;      it can accept a strftime(3) format:
;      %d/%b/%Y:%H:%M:%S %z (default)
;      The strftime(3) format must be encapsuled in a %{<strftime_format>}t
tag
```

```
;      e.g. for a ISO8601 formatted timestring, use: %{%Y-%m-%dT%H:%M:%S%z}t
;  %u: remote user
;
; Default: "%R - %u %t \"%m %r\" %s"
;access.format = "%R - %u %t \"%m %r%Q%q\" %s %f %{mili}d %{kilo}M %C%%"

; The log file for slow requests
; Default Value: not set
; Note: slowlog is mandatory if request_slowlog_timeout is set
;slowlog = log/$pool.log.slow

; The timeout for serving a single request after which a PHP backtrace will
be
; dumped to the 'slowlog' file. A value of '0s' means 'off'.
; Available units: s(econds)(default), m(inutes), h(ours), or d(ays)
; Default Value: 0
;request_slowlog_timeout = 0

; Depth of slow log stack trace.
; Default Value: 20
;request_slowlog_trace_depth = 20

; The timeout for serving a single request after which the worker process
will
; be killed. This option should be used when the 'max_execution_time' ini
option
; does not stop script execution for some reason. A value of '0' means
'off'.
; Available units: s(econds)(default), m(inutes), h(ours), or d(ays)
; Default Value: 0
;request_terminate_timeout = 0

; The timeout set by 'request_terminate_timeout' ini option is not engaged
after
; application calls 'fastcgi_finish_request' or when application has
finished and
; shutdown functions are being called (registered via
register_shutdown_function).
; This option will enable timeout limit to be applied unconditionally
; even in such cases.
; Default Value: no
;request_terminate_timeout_track_finished = no

; Set open file descriptor rlimit.
; Default Value: system defined value
;rlimit_files = 1024

; Set max core size rlimit.
; Possible Values: 'unlimited' or an integer greater or equal to 0
; Default Value: system defined value
;rlimit_core = 0
```

```
; Chroot to this directory at the start. This value must be defined as an
; absolute path. When this value is not set, chroot is not used.
; Note: you can prefix with '$prefix' to chroot to the pool prefix or one
; of its subdirectories. If the pool prefix is not set, the global prefix
; will be used instead.
; Note: chrooting is a great security feature and should be used whenever
;       possible. However, all PHP paths will be relative to the chroot
;       (error_log, sessions.save_path, ...).
; Default Value: not set
;chroot =

; Chdir to this directory at the start.
; Note: relative path can be used.
; Default Value: current directory or / when chroot
;chdir = /var/www

; Redirect worker stdout and stderr into main error log. If not set, stdout
and
; stderr will be redirected to /dev/null according to FastCGI specs.
; Note: on highloaded environement, this can cause some delay in the page
; process time (several ms).
; Default Value: no
;catch_workers_output = yes

; Decorate worker output with prefix and suffix containing information about
; the child that writes to the log and if stdout or stderr is used as well
as
; log level and time. This options is used only if catch_workers_output is
yes.
; Settings to "no" will output data as written to the stdout or stderr.
; Default value: yes
;decorate_workers_output = no

; Clear environment in FPM workers
; Prevents arbitrary environment variables from reaching FPM worker
processes
; by clearing the environment in workers before env vars specified in this
; pool configuration are added.
; Setting to "no" will make all environment variables available to PHP code
; via getenv(), $_ENV and $_SERVER.
; Default Value: yes
;clear_env = no

; Limits the extensions of the main script FPM will allow to parse. This can
; prevent configuration mistakes on the web server side. You should only
limit
; FPM to .php extensions to prevent malicious users to use other extensions
to
; execute php code.
; Note: set an empty value to allow all extensions.
; Default Value: .php
```

```
;security.limit_extensions = .php .php3 .php4 .php5 .php7

; Pass environment variables like LD_LIBRARY_PATH. All $VARIABLEs are taken
from
; the current environment.
; Default Value: clean env
;env[HOSTNAME] = $HOSTNAME
;env[PATH] = /usr/local/bin:/usr/bin:/bin
;env[TMP] = /tmp
;env[TMPDIR] = /tmp
;env[TEMP] = /tmp

; Additional php.ini defines, specific to this pool of workers. These
settings
; overwrite the values previously defined in the php.ini. The directives are
the
; same as the PHP SAPI:
;   php_value/php_flag             - you can set classic ini defines which
can
;                                    be overwritten from PHP call 'ini_set'.
;   php_admin_value/php_admin_flag - these directives won't be overwritten
by
;                                     PHP call 'ini_set'
; For php_*flag, valid values are on, off, 1, 0, true, false, yes or no.

; Defining 'extension' will load the corresponding shared extension from
; extension_dir. Defining 'disable_functions' or 'disable_classes' will not
; overwrite previously defined php.ini values, but will append the new value
; instead.

; Note: path INI options can be relative and will be expanded with the
prefix
; (pool, global or /usr/local)

; Default Value: nothing is defined by default except the values in php.ini
and
;                specified at startup with the -d argument
;php_admin_value[sendmail_path] = /usr/sbin/sendmail -t -i -f
www@my.domain.com
;php_flag[display_errors] = off
;php_admin_value[error_log] = /var/log/fpm-php.www.log
;php_admin_flag[log_errors] = on
;php_admin_value[memory_limit] = 32M
```

nginx.conf

```
user www-data;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;
```

```
events {
    worker_connections  1024;
}


http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request"
'
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    set_real_ip_from  10.0.0.0/8;
    set_real_ip_from  172.16.0.0/12;
    set_real_ip_from  192.168.0.0/16;
    real_ip_header    X-Real-IP;

    #gzip  on;

    upstream php-handler {
        server app:9000;
    }

    server {
        listen 80;

        # Add headers to serve security related headers
        # Before enabling Strict-Transport-Security headers please read into
this
        # topic first.
        # add_header Strict-Transport-Security "max-age=15768000;
        # includeSubDomains; preload;";
        #
        # WARNING: Only add the preload option once you read about
        # the consequences in https://hstspreload.org/. This option
        # will add the domain to a hardcoded list that is shipped
        # in all major browsers and getting removed from this list
        # could take several months.
        add_header X-Content-Type-Options nosniff;
        add_header X-XSS-Protection "1; mode=block";
        add_header X-Robots-Tag none;
        add_header X-Download-Options noopen;
```

```
        add_header X-Permitted-Cross-Domain-Policies none;
        add_header Referrer-Policy no-referrer;

        # Remove X-Powered-By, which is an information leak
        fastcgi_hide_header X-Powered-By;

        root /var/www/html;

        location = /robots.txt {
            allow all;
            log_not_found off;
            access_log off;
        }

        # The following 2 rules are only needed for the user_webfinger app.
        # Uncomment it if you're planning to use this app.
        #rewrite ^/.well-known/host-meta /public.php?service=host-meta last;
        #rewrite ^/.well-known/host-meta.json /public.php?service=host-meta-
json
        # last;

        location = /.well-known/carddav {
            return 301 $scheme://$host/remote.php/dav;
        }
        location = /.well-known/caldav {
            return 301 $scheme://$host/remote.php/dav;
        }

        # set max upload size
        client_max_body_size 10G;
        fastcgi_buffers 64 4K;

        # Enable gzip but do not remove ETag headers
        gzip on;
        gzip_vary on;
        gzip_comp_level 4;
        gzip_min_length 256;
        gzip_proxied expired no-cache no-store private no_last_modified
no_etag auth;
        gzip_types application/atom+xml application/javascript
application/json application/ld+json application/manifest+json
application/rss+xml application/vnd.geo+json application/vnd.ms-fontobject
application/x-font-ttf application/x-web-app-manifest+json
application/xhtml+xml application/xml font/opentype image/bmp image/svg+xml
image/x-icon text/cache-manifest text/css text/plain text/vcard
text/vnd.rim.location.xloc text/vtt text/x-component text/x-cross-domain-
policy;

        # Uncomment if your server is build with the ngx_pagespeed module
        # This module is currently not supported.
        #pagespeed off;
```

```
        location / {
            rewrite ^ /index.php$uri;
        }

        location ~ ^/(?:build|tests|config|lib|3rdparty|templates|data)/ {
            deny all;
        }
        location ~ ^/(?:\.|autotest|occ|issue|indie|db_|console) {
            deny all;
        }

        location ~
^/(?:index|remote|public|cron|core/ajax/update|status|ocs/v[12]|updater/.+|o
cs-provider/.+)\.php(?:$|/) {
            fastcgi_split_path_info ^(.+\.php)(/.*)$;
            include fastcgi_params;
            fastcgi_param SCRIPT_FILENAME
$document_root$fastcgi_script_name;
            fastcgi_param PATH_INFO $fastcgi_path_info;
            # fastcgi_param HTTPS on;
            #Avoid sending the security headers twice
            fastcgi_param modHeadersAvailable true;
            fastcgi_param front_controller_active true;
            fastcgi_pass php-handler;
            fastcgi_request_buffering off;
        }

        location ~ ^/(?:updater|ocs-provider)(?:$|/) {
            try_files $uri/ =404;
            index index.php;
        }

        # Adding the cache control header for js and css files
        # Make sure it is BELOW the PHP block
        location ~ \.(?:css|js|woff|svg|gif)$ {
            try_files $uri /index.php$uri$is_args$args;
            add_header Cache-Control "public, max-age=15778463";
            # Add headers to serve security related headers (It is intended
to
            # have those duplicated to the ones above)
            # Before enabling Strict-Transport-Security headers please read
into
            # this topic first.
            # add_header Strict-Transport-Security "max-age=15768000;
            #  includeSubDomains; preload;";
            #
            # WARNING: Only add the preload option once you read about
            # the consequences in https://hstspreload.org/. This option
            # will add the domain to a hardcoded list that is shipped
            # in all major browsers and getting removed from this list
            # could take several months.
```

```
            add_header X-Content-Type-Options nosniff;
            add_header X-XSS-Protection "1; mode=block";
            add_header X-Robots-Tag none;
            add_header X-Download-Options noopen;
            add_header X-Permitted-Cross-Domain-Policies none;
            # Optional: Don't log access to assets
            access_log off;
        }

        location ~ \.(?:png|html|ttf|ico|jpg|jpeg)$ {
            try_files $uri /index.php$uri$is_args$args;
            # Optional: Don't log access to other assets
            access_log off;
        }
    }

}
```

docker exec -u www-data nextcloud_app_1 php occ app:disable richdocumentscode