

ImageMagick

Commando's en policy voorbeeld voor gebruik/instellen van ImageMagick op de server

- [Commando's](#)
- [policy.xml](#)
- [Standaard policy.xml van imagemagick 7](#)
- [policy.xml die Combell nabootst](#)

Commando's

ImageMagick 7 installeren op ddev project

Bewerk: .ddev/web-build/Dockerfile

```
# Use ImageMagick 7 instead of 6
# See: https://github.com/ddev/ddev/issues/5332
RUN apt update
RUN apt remove "*imagemagick*" --purge -y && apt autoremove --purge -y
RUN apt install -y php-pear php8.3-dev libaom-dev aom-tools cmake build-essential libltdl-dev
libjpeg-dev libpng-dev libtiff-dev libgif-dev libfreetype6-dev liblcms2-dev libxml2-dev

ENV IMAGEMAGICK_DIR=/usr/local/imagemagick7
RUN mkdir -p $IMAGEMAGICK_DIR

RUN git clone https://github.com/SoftCreatR/imei $IMAGEMAGICK_DIR
RUN chmod +x $IMAGEMAGICK_DIR/imei.sh
RUN bash $IMAGEMAGICK_DIR/imei.sh

# install the Imagick PHP Extension
RUN apt-get update \
    && pecl install imagick
```

dan: .ddev/php/php.ini bewerken en toevoegen:

```
extension = imagick.so
```

Dan herstarten:

```
ddev restart
```

Om te controleren:

```
ddev ssh
magick -version
```

Nu kan je een custom policy maken door de originele van imagemagick 7 te kopiëren:

```
cp /usr/local/etc/ImageMagick-7/policy.xml ~/.config/ImageMagick
nano ~/.config/ImageMagick/policy.xml
```

Overige ddev commando's

```
magick convert -list resource
magick identify -list policy
```

In ddev:

```
.ddev/.webimageBuild/policy.xml
.ddev/web-build/policy.xml
dan ddev restart
```

```
ddev ssh
convert identify -list policy
convert identify -list resource
```

----- demo commandos -----

```
ddev exec magick /var/www/html/web/modules/custom/dam_media_adjustments/assets/demo-input-
2.png -resize 650x650 /var/www/html/tmp/demo-output.png
magick convert -resample 72x72 -units PixelsPerInch -strip -resize 460x
/data/sites/web/damagfaradiologysolutionscom/test/test-5000x4681.jpg -density 72
/data/sites/web/damagfaradiologysolutionscom/test/test-result-1.png
magick convert -resample 72x72 -units PixelsPerInch -strip -resize 460x
/data/sites/web/damagfaradiologysolutionscom/test/AGFA-RADIOLOGY_conceptbeeld_X-Ray.jpg -
density 72 /data/sites/web/damagfaradiologysolutionscom/test/test-result-2.png
```

```
magick convert
/data/sites/web/damagfaradiologysolutionscom/production/private/assets/graphic_files/AGFA-
RADIOLOGY_conceptbeeld_X-Ray.psd
/data/sites/web/damagfaradiologysolutionscom/production/private/psd_previews/media_321/AGFA-
RADIOLOGY_conceptbeeld_X-Ray.jpg/AGFA-RADIOLOGY_conceptbeeld_X-Ray.jpg
magick convert -units PixelsPerInch
/data/sites/web/damagfaradiologysolutionscom/production/private/assets/graphic_files/AGFA-
RADIOLOGY_conceptbeeld_X-Ray.psd -density 72
/data/sites/web/damagfaradiologysolutionscom/production/private/psd_previews/media_321/AGFA-
```

RADIOLOGY_conceptbeeld_X-Ray-72-dpi.png

magick convert -units PixelsPerInch

/data/sites/web/damagfaradiologysolutionscom/production/private/assets/graphic_files/AGFA-

RADIOLOGY_conceptbeeld_X-Ray.psd[0] -density 72

/data/sites/web/damagfaradiologysolutionscom/production/private/psd_previews/media_321/AGFA-

RADIOLOGY_conceptbeeld_X-Ray-72-dpi.png

policy.xml

Policy bewerken:

```
nano /.config/ImageMagick/policy.xml
magick identify -list policy
nano /data/sites/web/damagfaradiologysolutionscom//.config/ImageMagick/policy.xml
```

Policy aanmaken:

```
voor ddev: eerst: ddev ssh
cd ~/.config
mkdir ImageMagick
cd ImageMagick
touch policy.xml
nano ~/.config/ImageMagick/policy.xml
(plakken van wiki?)

testen:
magick identify -list policy
ddev exec magick identify -list policy
```

Inhoud:

```
<policymap>
  <policy domain="resource" name="temporary-path"
value="/data/sites/web/damagfaradiologysolutionscom/current/tmp"/>
  <policy domain="resource" name="memory" value="512MiB"/>
  <policy domain="resource" name="map" value="1GiB"/>
  <policy domain="resource" name="width" value="32KP"/>
  <policy domain="resource" name="height" value="32KP"/>
  <policy domain="resource" name="area" value="1.0737GP"/>
  <policy domain="resource" name="disk" value="100GiB"/>
  <policy domain="resource" name="file" value="768"/>
  <policy domain="resource" name="thread" value="4"/>
  <policy domain="resource" name="throttle" value="0"/>
```

```
<policy domain="resource" name="time" value="unlimited"/>
<policy domain="coder" rights="read|write"
pattern="{GIF,JPEG,PNG,WEBP,AI,PSD,PDF,PS,PS2,PS3,EPS,XPS}" /> -->
<policy domain="delegate" rights="none" pattern="URL" />
<policy domain="delegate" rights="none" pattern="HTTPS" />
<policy domain="delegate" rights="none" pattern="HTTP" />
<!-- in order to avoid to get image with password text -->
<policy domain="path" rights="none" pattern="@*" />
<!-- disable ghostscript format types -->
</policymap>
```

Andere settings als voorbeeld:

```
policy domain="resource" name="memory" value="1GiB"
policy domain="resource" name="map" value="2GiB"
policy domain="resource" name="width" value="64KP"
policy domain="resource" name="height" value="64KP"
policy domain="resource" name="area" value="200MP"
policy domain="resource" name="disk" value="5GiB"
policy domain="coder" rights="read|write" pattern="{AI, PSD, PDF, PS, PS2, PS3, EPS, XPS}"
```

Standaard policy.xml van imagemagick 7

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE policymap [
<!ELEMENT policymap (policy)*>
<!ATTLIST policymap xmlns CDATA #FIXED "">
<!ELEMENT policy EMPTY>
<!ATTLIST policy xmlns CDATA #FIXED "">
<!ATTLIST policy domain NMTOKEN #REQUIRED>
<!ATTLIST policy name NMTOKEN #IMPLIED>
<!ATTLIST policy pattern CDATA #IMPLIED>
<!ATTLIST policy rights NMTOKEN #IMPLIED>
<!ATTLIST policy stealth NMTOKEN #IMPLIED>
<!ATTLIST policy value CDATA #IMPLIED>
]>
<!--
```

Creating a security policy that fits your specific local environment before making use of ImageMagick is highly advised. You can find guidance on setting up this policy at <https://imagemagick.org/script/security-policy.php>, and it's important to verify your policy using the validation tool located at <https://imagemagick-secevaluator.doyensec.com/>.

Open ImageMagick security policy:

The default policy for ImageMagick installations is the open security policy. This policy is designed for usage in secure settings like those protected by firewalls or within Docker containers. Within this framework, ImageMagick enjoys broad access to resources and functionalities. This policy provides convenient and adaptable options for image manipulation. However, it's important to note that it might present security vulnerabilities in less regulated conditions. Thus, organizations should thoroughly assess the appropriateness of the open policy according to their particular use case and security prerequisites.

ImageMagick security policies in a nutshell:

Domains include system, delegate, coder, filter, module, path, or resource.

Rights include none, read, write, execute and all. Use | to combine them, for example: "read | write" to permit read from, or write to, a path.

Use a glob expression as a pattern.

Suppose we do not want users to process MPEG video images, use this policy:

```
<policy domain="delegate" rights="none" pattern="mpeg:decode" />
```

Here we do not want users reading images from HTTP:

```
<policy domain="coder" rights="none" pattern="HTTP" />
```

The /repository file system is restricted to read only. We use a glob expression to match all paths that start with /repository:

```
<policy domain="path" rights="read" pattern="/repository/*" />
```

Prevent users from executing any image filters:

```
<policy domain="filter" rights="none" pattern="*" />
```

Cache large images to disk rather than memory:

```
<policy domain="resource" name="area" value="1GP"/>
```

Use the default system font unless overridden by the application:

```
<policy domain="system" name="font" value="/usr/share/fonts/favorite.ttf"/>
```

Define arguments for the memory, map, area, width, height and disk resources with SI prefixes (.e.g 100MB). In addition, resource policies are maximums for each instance of ImageMagick (e.g. policy memory limit 1GB, -limit 2GB exceeds policy maximum so memory limit is 1GB).

Rules are processed in order. Here we want to restrict ImageMagick to only

read or write a small subset of proven web-safe image types:

```
<policy domain="delegate" rights="none" pattern="*" />
<policy domain="filter" rights="none" pattern="*" />
<policy domain="coder" rights="none" pattern="*" />
<policy domain="coder" rights="read|write" pattern="{GIF,JPEG,PNG,WEBP}" />
```

See <https://imagemagick.org/script/security-policy.php> for a deeper understanding of ImageMagick security policies.

-->

<polycymap>

```
<policy domain="Undefined" rights="none"/>
<!-- Set maximum parallel threads. -->
<!-- <policy domain="resource" name="thread" value="2"/> -->
<!-- Set maximum time to live in seconds or mnemonics, e.g. "2 minutes". When
      this limit is exceeded, an exception is thrown and processing stops. -->
<!-- <policy domain="resource" name="time" value="120"/> -->
<!-- Set maximum number of open pixel cache files. When this limit is
      exceeded, any subsequent pixels cached to disk are closed and reopened
      on demand. -->
<!-- <policy domain="resource" name="file" value="768"/> -->
<!-- Set maximum amount of memory in bytes to allocate for the pixel cache
      from the heap. When this limit is exceeded, the image pixels are cached
      to memory-mapped disk. -->
<!-- <policy domain="resource" name="memory" value="256MiB"/> -->
<!-- Set maximum amount of memory map in bytes to allocate for the pixel
      cache. When this limit is exceeded, the image pixels are cached to
      disk. -->
<!-- <policy domain="resource" name="map" value="512MiB"/> -->
<!-- Set the maximum width * height of an image that can reside in the pixel
      cache memory. Images that exceed the area limit are cached to disk. -->
<!-- <policy domain="resource" name="area" value="16KP"/> -->
<!-- Set maximum amount of disk space in bytes permitted for use by the pixel
      cache. When this limit is exceeded, the pixel cache is not be created
      and an exception is thrown. -->
<!-- <policy domain="resource" name="disk" value="1GiB"/> -->
<!-- Set the maximum length of an image sequence. When this limit is
      exceeded, an exception is thrown. -->
<!-- <policy domain="resource" name="list-length" value="32"/> -->
<!-- Set the maximum width of an image. When this limit is exceeded, an
```

```
        exception is thrown. -->
<!-- <policy domain="resource" name="width" value="8KP"/> -->
<!-- Set the maximum height of an image. When this limit is exceeded, an
        exception is thrown. -->
<!-- <policy domain="resource" name="height" value="8KP"/> -->
<!-- Periodically yield the CPU for at least the time specified in
        milliseconds. -->
<!-- <policy domain="resource" name="throttle" value="2"/> -->
<!-- Do not create temporary files in the default shared directories, instead
        specify a private area to store only ImageMagick temporary files. -->
<!-- <policy domain="resource" name="temporary-path" value="/magick/tmp/"> -->
<!-- Force memory initialization by memory mapping select memory
        allocations. -->
<!-- <policy domain="cache" name="memory-map" value="anonymous"/> -->
<!-- Ensure all image data is fully flushed and synchronized to disk. -->
<!-- <policy domain="cache" name="synchronize" value="true"/> -->
<!-- Replace passphrase for secure distributed processing -->
<!-- <policy domain="cache" name="shared-secret" value="secret-passphrase" stealth="true"/>
-->
<!-- Do not permit any delegates to execute. -->
<!-- <policy domain="delegate" rights="none" pattern="*"> -->
<!-- Do not permit any image filters to load. -->
<!-- <policy domain="filter" rights="none" pattern="*"> -->
<!-- Don't read/write from/to stdin/stdout. -->
<!-- <policy domain="path" rights="none" pattern="-"/> -->
<!-- don't read sensitive paths. -->
<!-- <policy domain="path" rights="none" pattern="/etc/*"/> -->
<!-- Indirect reads are not permitted. -->
<!-- <policy domain="path" rights="none" pattern="@*"> -->
<!-- These image types are security risks on read, but write is fine -->
<!-- <policy domain="module" rights="write" pattern="{MSL,MVG,PS,SVG,URL,XPS}"/> -->
<!-- This policy sets the number of times to replace content of certain
        memory buffers and temporary files before they are freed or deleted. -->
<!-- <policy domain="system" name="shred" value="1"/> -->
<!-- Enable the initialization of buffers with zeros, resulting in a minor
        performance penalty but with improved security. -->
<!-- <policy domain="system" name="memory-map" value="anonymous"/> -->
<!-- Set the maximum amount of memory in bytes that are permitted for
        allocation requests. -->
<!-- <policy domain="system" name="max-memory-request" value="256MiB"/> -->
```

</policymap>

policy.xml die Combell nabootst

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE policymap [
<!ELEMENT policymap (policy)*>
<!ATTLIST policymap xmlns CDATA #FIXED "">
<!ELEMENT policy EMPTY>
<!ATTLIST policy xmlns CDATA #FIXED "">
<!ATTLIST policy domain NMTOKEN #REQUIRED>
<!ATTLIST policy name NMTOKEN #IMPLIED>
<!ATTLIST policy pattern CDATA #IMPLIED>
<!ATTLIST policy rights NMTOKEN #IMPLIED>
<!ATTLIST policy stealth NMTOKEN #IMPLIED>
<!ATTLIST policy value CDATA #IMPLIED>
]>
<policymap>
  <policy domain="Undefined" rights="none"/>
  <policy domain="resource" name="thread" value="4"/>
  <policy domain="resource" name="time" value="1800"/>
  <policy domain="resource" name="file" value="768"/>
  <policy domain="resource" name="memory" value="256MiB"/>
  <policy domain="resource" name="map" value="512MiB"/>
  <policy domain="resource" name="area" value="16KP"/>
  <policy domain="resource" name="disk" value="1GiB"/>
  <!-- <policy domain="resource" name="list-length" value="32"/> -->
  <policy domain="resource" name="width" value="8KP"/>
  <policy domain="resource" name="height" value="8KP"/>
  <policy domain="resource" name="throttle" value="2"/>
  <!-- <policy domain="resource" name="temporary-path" value="/magick/tmp/" /> -->
  <!-- <policy domain="cache" name="memory-map" value="anonymous"/> -->
  <!-- <policy domain="cache" name="synchronize" value="true"/> -->
  <!-- <policy domain="cache" name="shared-secret" value="secret-passphrase" stealth="true"/> -->
  <!-- <policy domain="delegate" rights="none" pattern="*" /> -->
  <!-- <policy domain="filter" rights="none" pattern="*" /> -->
  <!-- <policy domain="path" rights="none" pattern="-" /> -->
  <!-- <policy domain="path" rights="none" pattern="/etc/*" /> -->
```

```
<!-- <policy domain="path" rights="none" pattern="*" /> -->
<!-- <policy domain="module" rights="write" pattern="{MSL,MVG,PS,SVG,URL,XPS}" /> -->
<!-- <policy domain="system" name="shred" value="1" /> -->
<!-- <policy domain="system" name="memory-map" value="anonymous" /> -->
<!-- <policy domain="system" name="max-memory-request" value="256MiB" /> -->
</policymap>
```