#

# From oslo.middleware

#

# Indicate whether this resource may be shared with the domain received in the

# requests "origin" header. Format: "<protocol>://<host>[:<port>]", no trailing

# slash. Example: https://horizon.example.com (list value)

#allowed\_origin = <None>

{%- if \_data.allowed\_origin is defined %}

allowed\_origin = {{ \_data.allowed\_origin }}

{%- endif %}

# Indicate that the actual request can include user credentials (boolean value)

#allow\_credentials = true

{%- if \_data.allow\_credentials is defined %}

allow\_credentials = {{ \_data.allow\_credentials }}

{%- endif %}

# Indicate which headers are safe to expose to the API. Defaults to HTTP Simple

# Headers. (list value)

#expose\_headers = X-Auth-Token,X-Openstack-Request-Id,X-Subject-Token

{%- if \_data.expose\_headers is defined %}

expose\_headers = {{ \_data.expose\_headers }}

{%- endif %}

# Maximum cache age of CORS preflight requests. (integer value)

#max\_age = 3600

{%- if \_data.max\_age is defined %}

max\_age = {{ \_data.max\_age }}

{%- endif %}

# Indicate which methods can be used during the actual request. (list value)

#allow\_methods = GET,PUT,POST,DELETE,PATCH

{%- if \_data.allow\_methods is defined %}

allow\_methods = {{ \_data.allow\_methods }}

{%- endif %}

# Indicate which header field names may be used during the actual request.

# (list value)

#allow\_headers = X-Auth-Token,X-Openstack-Request-Id,X-Subject-Token,X-Project-Id,X-Project-Name,X-Project-Domain-Id,X-Project-Domain-Name,X-Domain-Id,X-Domain-Name

{%- if \_data.allow\_headers is defined %}

allow\_headers = {{ \_data.allow\_headers }}

{%- endif %}