关于 pages 在现有中讯云上的情况说明

Pages 前提

- 有一个单独的域名为 GitLab Pages 服务。假设它是 example.io

- **配置一条通配符 DNS 记录**

- 还有一些可选的，比如：配置 https、添加一个 Shared Runner、对于自定义

  域名有一个第二个 IP

GitLab Pages 期望运行在 GitLab 的虚拟机上，在 DNS 服务器或者 DNS 提供商那里需要配置一个通配符 DNS 记录指向 GitLab 运行的机器。例如一个条目类似如下：

`*.example.io.  1800  IN  A  1.1.1.1`

其中 example.io 是为 Gitlab Pages 服务的域名，1.1.1.1 是 GitLab 实例的 IP

中讯云的中间 IP 特殊情况

中讯云，主机的实际监听 IP 是内网 172.X.X.X 的地址，但是对外通信都是通过 NAT 的方式，使用的是中间 IP，比如 10.10.58.77 这样的 10.10 的地址，**特点是不同主机间彼此使用 10.10.的地址访问不通，甚至主机访问自己内网对应的 10.10 的地址也不通。如果我们在配置中监听 10.10 的地址，在 pages 发布中会直接报错**

```
 1  Running with gitlab-runner 15.3.0 (bbcb5aba)
 2    on 508eaa26f975 SuFqK3VW
 3  Preparing the "docker" executor
 4  Using Docker executor with image kubesphere/builder-maven:v3.1.0 ...
 5  Pulling docker image kubesphere/builder-maven:v3.1.0 ...
 6  Using docker image sha256:667c7f488fce03ee410c787e8b773d66743120ad8d2ad337626bc0df912ce093 for kubesphere/builder-maven:v3.1.0 with digest kubesp
    -maven@sha256:a05fadfa0ec6333a7e51b176a80fd15fb3cfe76c2a5955b8362af92d1ed13508 ...
 8  Preparing environment
 9  Running on runner-sufqk3vw-project-2-concurrent-0 via 508eaa26f975...
11  Getting source from Git repository
12  Fetching changes with git depth set to 20...
13  Reinitialized existing Git repository in /builds/root/pages-test/.git/
14  fatal: unable to access 'http://10.10.58.77/root/pages-test.git/': Failed to connect to 10.10.58.77 port 80 after 127204 ms: Operation timed out
15  ERROR: Job failed: exit code 1
```

那使用域名呢？ 假设，我们每个 pages 项目都手动改自己电脑本地的 hosts 是否可以使用 ？ 测试如下，以现在的域名 git.software.dimpt.com 为例，在内部的 proxy 转发中，依然会面临同样的访问不通问题
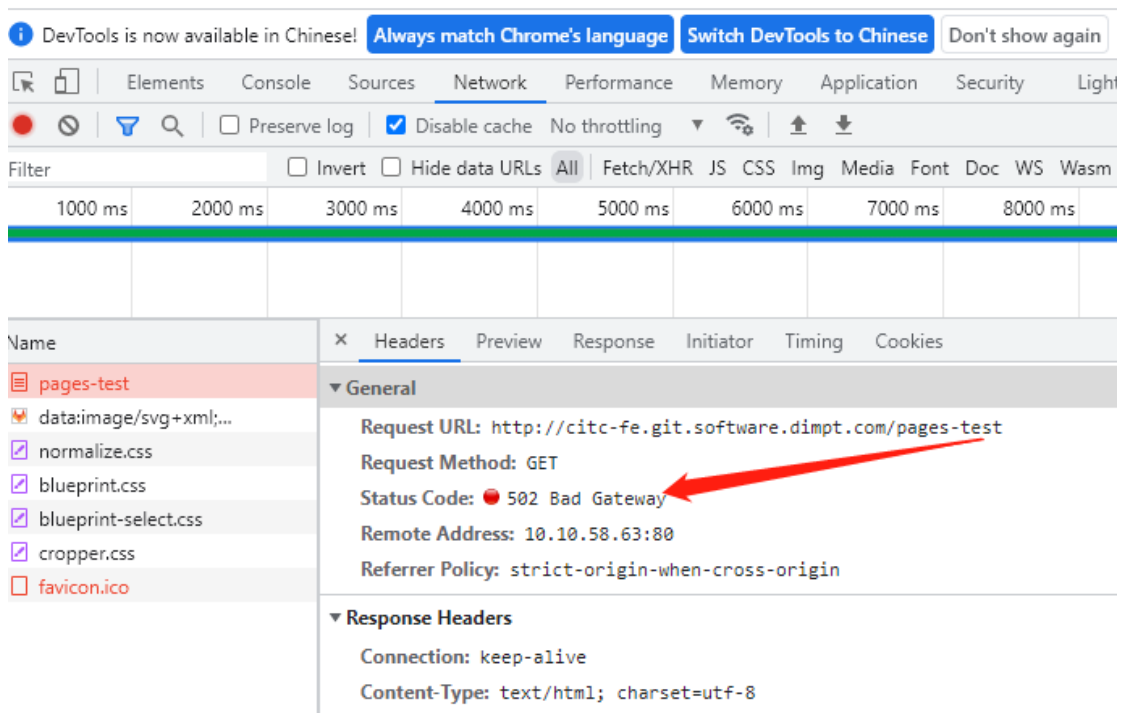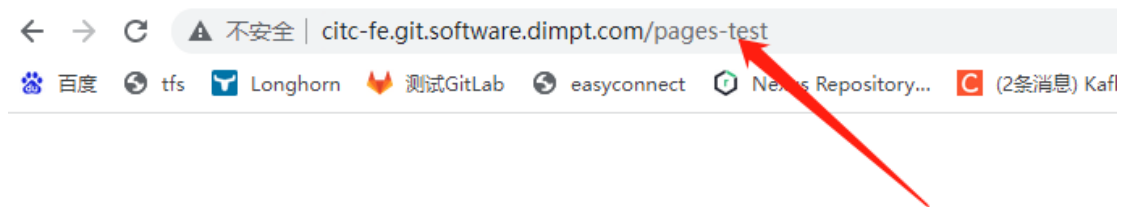
如下是配置 pages 部分对应的内部 nginx 配置

```
server {
  listen *:80;
  server_name  ~^(?<group>.*)\.git\.software\.dimpt\.com$;
  server_tokens off; ## Don't show the nginx version number, a security best practice

  ## Disable symlink traversal
  disable_symlinks on;


  ## Real IP Module Config
  ## http://nginx.org/en/docs/http/ngx_http_realip_module.html

  ## HSTS Config
  ## https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/
  add_header Strict-Transport-Security "max-age=63072000";

  ## Individual nginx logs for this GitLab vhost
  access_log  /var/log/gitlab/nginx/gitlab_pages_access.log gitlab_access;
  error_log   /var/log/gitlab/nginx/gitlab_pages_error.log error;

  # Pass everything to pages daemon
  location / {
    proxy_set_header Host $http_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 http;

    # Prevent NGINX from caching pages in response to the pages `Cache-Control`
    # header.
    #
    # Browsers already respect this directive and Pages can handle the request
    # volume without help from NGINX.
    #
    # If this changes in the future, ensure `proxy_cache_key` is set to a value
    # like `$scheme$host$request_uri`, as the default value does not take the
    # Pages hostname into account, leading to incorrect responses being served.
    #
    # See https://gitlab.com/gitlab-org/gitlab-pages/issues/73
    proxy_cache off;


    proxy_pass            http://localhost:8090;
```

8090 相关的代理实现中，ruby 程序的配置中，依然需要内部解析 http://citc-fe.git.software.dimpt.com/,

```
root@aaf150fc25b5:/var/opt/gitlab# cat /var/opt/gitlab/gitlab-pages/gitlab-pages-config
pages-domain=git.software.dimpt.com
pages-root=/var/opt/gitlab/gitlab-rails/shared/pages
api-secret-key=/var/opt/gitlab/gitlab-pages/.gitlab_pages_secret
listen-proxy=localhost:8090
log-format=json
use-http2=true
artifacts-server=http://git.software.dimpt.com/api/v4
artifacts-server-timeout=10
gitlab-server=http://git.software.dimpt.com
root@aaf150fc25b5:/var/opt/gitlab# ping git.software.dimpt.com
PING git.software.dimpt.com (10.10.58.63): 56 data bytes
^C
--- git.software.dimpt.com ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss
root@aaf150fc25b5:/var/opt/gitlab#
```

但即使是内部到内部，10.10 依然是不通 的

以下是日志表现

10.220.8.38 - - [08/Sep/2022:15:09:05 +0800] "GET /pages-test HTTP/1.1" 502 2917 "" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36" -
10.220.8.38 - - [08/Sep/2022:15:09:05 +0800] "GET /favicon.ico HTTP/1.1" 502 2917 "http://citc-fe.git.software.dimpt.com/pages-test" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36" -

[root@ZFRJKF_KFHJ_VMC1_0002241 logs]# tail -f -n 50 gitlab-pages/current
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:08+08:00"}
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:19+08:00"}
{"content_type":"text/html; charset=utf-8","correlation_id":"01GCDHWQ863Y801GA1ZT0CK868","duration_ms":24092,"host":"citc-fe.git.software.dimpt.com","level":"info","method":"GET","msg":"access","pages_https":false,"proto":"HTTP/1.0","referrer":"","remote_addr":"10.220.8.38","remote_ip":"10.220.8.38","status":404,"system":"http","time":"2022-09-08T11:22:22+08:00","ttfb_ms":24085,"uri":"/pages-test","user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36","written_bytes":3067}
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:28+08:00"}
{"correlation_id":"01GCDHXMGSXP307B1Q47AKXWFG","error":"retrieval context done: context deadline exceeded","host":"citc-fe.git.software.dimpt.com","level":"error","msg":"could not fetch domain information from a source","path":"/pages-test","time":"2022-09-08T11:22:28+08:00"}
{"content_type":"text/html; charset=utf-8","correlation_id":"01GCDHXMGSXP307B1Q47AKXWFG","duration_ms":38,"host":"citc-fe.git.software.dimpt.com","level":"info","method":"GET","msg":"access","pages_https":false,"proto":"HTTP/1.0","referrer":"","remote_addr":"10.220.8.38","remote_ip":"10.220.8.38","status":502,"system":"http","time":"2022-09-08T11:22:28+08:00","ttfb_ms":37,"uri":"/pages-test","user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36","written_bytes":2905}
{"correlation_id":"01GCDHXN5KKPZZJGW07CFCKY1B","error":"retrieval context done: context deadline exceeded","host":"citc-fe.git.software.dimpt.com","level":"error","msg":"could not fetch domain information from a source","path":"/favicon.ico","time":"2022-09-08T11:22:28+08:00"}
{"content_type":"text/html; charset=utf-8","correlation_id":"01GCDHXN5KKPZZJGW07CFCKY1B","duration_ms":0,"host":"citc-fe.git.software.dimpt.com","level":"info","method":"GET","msg":"access","pages_https":false,"proto":"HTTP/1.0","referrer":"http://citc-fe.git.software.dimpt.com/pages-test","remote_addr":"10.220.8.38","remote_ip":"10.220.8.38","status":502,"system":"http","time":"2022-09-08T11:22:28+08:00","ttfb_ms":0,"uri":"/favicon.ico","user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36","written_bytes":2905}
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:38+08:00"}
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:49+08:00"}
{"address":"10.10.58.63:80","error":"dial tcp 10.10.58.63:80: i/o timeout","level":"error","msg":"httptrace.ClientTrace.ConnectDone","network":"tcp","time":"2022-09-08T11:22:58+08:00"}

结论:

目前在现有情况下使用 pages 的两大问题分别是:

- **没有通配的 DNS 域名解析 A 记录支持**

- **中讯云中间 IP 的存在,导致无论是监听域名,还是中间 IP,都会导致 pages 功能部署失败或访问不成功**

即使每个使用者都手动改自己电脑的 hosts,而且每添加一个 pages 站点都要手动改一次,来"克服"DNS 问题,还是会因中间 IP 而无法访问。
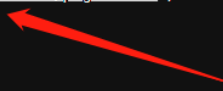
如果以前 pages 部署成功过,或使用过,那应该是五楼机房,内部部署的情况下

以下是一个正常案例,供参考使用

以下是实际测试截图,实际搭建了另外一套与现有 gitlab 版本,runner 版本都一致的环境,配置也完全一致,唯一不同是监听的私有地址

在完成 gitlab ci 配置, pages 正常发布后

```
$ echo "The site will be deployed to $CI_PAGES_URL $PWD"
The site will be deployed to http://root.172.22.0.77/pages-test /builds/root/pages-test
Uploading artifacts for successful job
Uploading artifacts...
public: found 4 matching files and directories
Uploading artifacts as "archive" to coordinator... 201 Created  id=3 responseStatus=201 Created token=Ux_dXsD8
Job succeeded
```

域名如 http://root.172.22.0.77/pages-test 在本地电脑手动加 hosts 解析后，使

用浏览器可以看到 pages 被成功部署