AP : ArchiSite

Groupe: 5

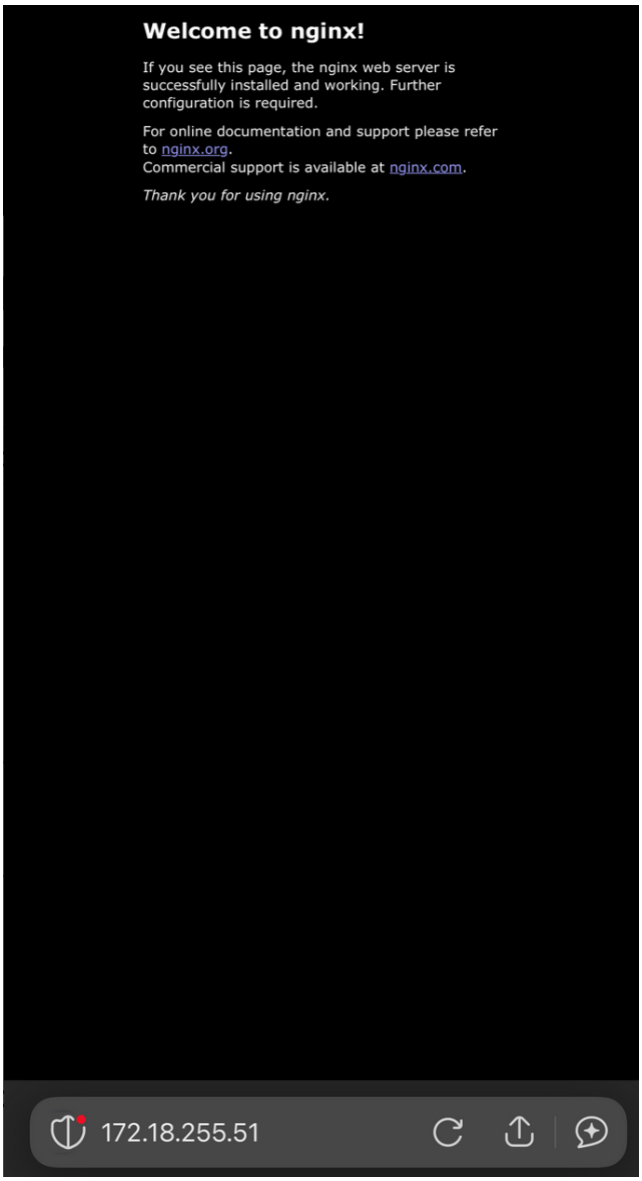
Adrien Zakaria

A.1 Créer et configurer VM Debian serveur Web (IP, réseau, accès)

```
web@web:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-11-12 12:39:08 CET; 1 day 20h ago
       Docs: man:nginx(8)
    Process: 560 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
    Process: 582 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Main PID: 583 (nginx)
      Tasks: 3 (limit: 4615)
     Memory: 4.3M
        CPU: 31ms
     CGroup: /system.slice/nginx.service
             ├─583 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             ├─584 "nginx: worker process"
             └─585 "nginx: worker process"

Warning: some journal files were not opened due to insufficient permissions.
```

```
web@web:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:0a:01:03 brd ff:ff:ff:ff:ff:ff
    inet 10.51.10.11/16 brd 10.51.255.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe0a:103/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

A.2 Déployer site web et tester fonctionnement HTTP basique et NAT



Router Net 1 :

ip nat inside source static tcp 10.51.10.11 80 172.18.255.51 80 extendable

ip nat inside source static tcp 10.51.10.11 443 172.18.255.51 443 extendable

Router Net 2

ip nat inside source static tcp 10.51.10.11 80 172.18.255.51 80 extendable

ip nat inside source static tcp 10.51.10.11 443 172.18.255.51 443 extendable

A.3 Configurer nginx en HTTPS/TLS et forcer redirection

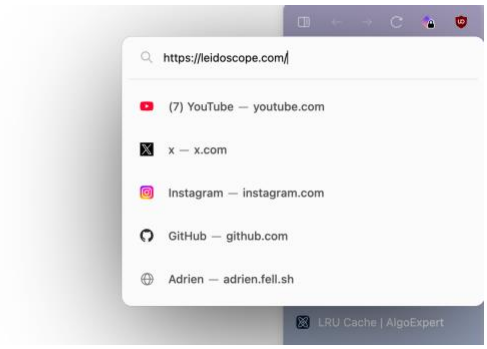
```
web@web:~$ openssl x509 -in /etc/ssl/ca/certs/ca-cert.pem -noout -subject -issuer -dates
subject=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
issuer=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
notBefore=Nov  4 14:13:09 2025 GMT
notAfter=Nov  2 14:13:09 2035 GMT
```

```
web@web:~$ openssl crl2pkcs7 -nocrl -certfile /etc/nginx/ssl/server-fullchain.pem | openssl pkcs7 -print_certs -noout
subject=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = IT, CN = leidoscope.com
issuer=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA

subject=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
issuer=C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
```

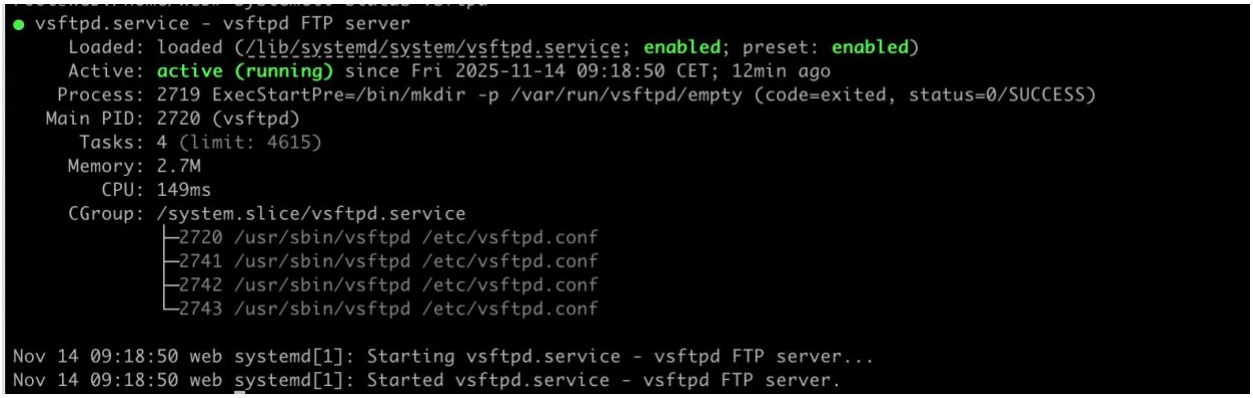
```
root@web:/home/web# cat /etc/nginx/sites-available/leidoscope
server {
    listen 80;
    listen [::]:80;
    server_name leidoscope.com www.leidoscope.com web.leidoscope.com 10.51.10.11;
    root /var/www/leidoscope;
    index index.php index.html index.htm;
    access_log /var/log/nginx/leidoscope_access.log;
    error_log /var/log/nginx/leidoscope_error.log;
    location / { try_files $uri $uri/ =404; }
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
    location ~ /\.ht { deny all; }
}
root@web:/home/web# cat /etc/nginx/sites-available/leidoscope-ssl
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name leidoscope.com www.leidoscope.com web.leidoscope.com;
    root /var/www/leidoscope;
    index index.php index.html index.htm;

    ssl_certificate /etc/nginx/ssl/server-fullchain.pem;
    ssl_certificate_key /etc/nginx/ssl/server-key.pem;

    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384';
    ssl_prefer_server_ciphers off;

    add_header Strict-Transport-Security "max-age=31536000" always;
    add_header X-Frame-Options "SAMEORIGIN" always;
    add_header X-Content-Type-Options "nosniff" always;

    access_log /var/log/nginx/leidoscope_ssl_access.log;
    error_log /var/log/nginx/leidoscope_ssl_error.log;

    location / { try_files $uri $uri/ =404; }
    location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.2-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
    location ~ /\.ht { deny all; }
}
```

```
root@web:/home/web# openssl s_client -connect localhost:443 -servername leidoscope.com -CAfile /etc/ssl/ca/certs/ca-cert.pem
CONNECTED(00000003)
depth=1 C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
verify return:1
depth=0 C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = IT, CN = leidoscope.com
verify return:1
---
Certificate chain
 0 s:C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = IT, CN = leidoscope.com
   i:C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Nov  7 09:04:54 2025 GMT; NotAfter: Nov  7 09:04:54 2027 GMT
 1 s:C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
   i:C = FR, ST = Normandie, L = Vernon, O = Leidoscope, OU = Interne, CN = Leidoscope Root CA
   a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
   v:NotBefore: Nov  4 14:13:09 2025 GMT; NotAfter: Nov  2 14:13:09 2035 GMT
---
Server certificate
```

leidoscope


https://leidoscope.com/
(7) YouTube — youtube.com
x — x.com
Instagram — instagram.com
GitHub — github.com
Adrien — adrien.fell.sh
LRU Cache | AlgoExpert

A.4 Installer et configurer vsftpd en FTPS



```
root@web:/home/web# cat /etc/vsftpd.conf
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
local_root=/var/www/leidoscope

ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.crt
rsa_private_key_file=/etc/ssl/private/vsftpd.key
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH

pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000

allow_writeable_chroot=YES
```

```
root@web:/etc/ssl/private# ls -ld  vsftpd.key
-rw------- 1 root root 1708 Nov  4 14:28 vsftpd.key
root@web:/etc/ssl/private#
```

```
root@web:/etc/ssl/certs# cat vsftpd.crt
-----BEGIN CERTIFICATE-----
MIIDeTCCAmGgAwIBAgIUR2kC2xqsUPyFZ7InqGk/YpV8tj8wDQYJKoZIhvcNAQEL
BQAwTDELMAkGA1UEBhMCRlIxDDAKBgNVBAgMA1ZybjEMMAoGA1UEBwwDVnJuMSEw
HwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwHhcNMjUxMTA0MTMyODQw
WhcNMjYxMTA0MTMyODQwWjBMMQswCQYDVQQGEwJGUjEMMAoGA1UECAwDVnJuMQww
CgYDVQQHDANWcm4xITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK1mhW18O8Nrpyi8Vn7ury/J
FAmy5o0HpD/9T7wpiJC7IikAmujLDwL0BYUxVlwmIvNkSOUvQM5gCKFQFE3KJ5Ke
eVMpKC84XGHLu/SDSAC/dxeUoINFQ1mF/cjnz3R7pYB0+2jbO4JVsD8gd7px0Rq0
L3HxVjqU7FwVyr9+TSz8Gyxl+uooNwhCFXwDP8WoREfONabHM92mLUDN1oD0zx6b
HGlNgBmxxtJiaFz2OHavAHiJ8FgPJqUnM8/dJhsZQfEM9vCRvXJUwSA9WfPQdnOs
Q7q3rNADQqKHqrnFwPy0yXLgYCtKT2i4RUE3Lh6NLqthbWDI5nsFK4Lkwr9z0UsC
AwEAAaNTMFEwHQYDVR0OBBYEFIx87hZ7KooxqkulB0yZouEOHmNKMB8GA1UdIwQY
MBaAFIx87hZ7KooxqkulB0yZouEOHmNKMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZI
hvcNAQELBQADggEBAFVQWp706N7gZuREczAFMKpSK7778FtWH9tYZnB9Kxeradf+
eF0DqUC3Ik/75trtuwBigoAi5qzUZ4Dh+JZi8aVabrJoHu4bzqUv3z6U7j11c1lG
nXNTaC3BlcDnwWld/51wI+F8TqGnf3CAcLU+eVxFtZALRHdhreUllT9vQsPXSWRr
z9eqcpeY04YIZLYHcfej0kfymw9C65fGr2TbBj9PWr9y0AvAgIIkoS7pX9NB04T6
dgyGFTUkhx17FHdD2+VQFQL741bvqOaK08Ur9ooZmHibWZJEjc0J6WV5KnzxpRh1
7tPjufJ2nfSAFCv9+zsLGM09CSgfJKPK/WrVkAU=
-----END CERTIFICATE-----
```

/

Filter

Name	Size	Date
info.php	20 bytes	7 Nov 2025 at 10:01:00
index.html	20 bytes	7 Nov 2025 at 10:10:00

A.5 Installer et configurer bind9 pour le site

```
root@web:/etc/ssl/private# systemctl status bind9
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-11-12 12:39:07 CET; 1 day 21h ago
       Docs: man:named(8)
   Main PID: 496 (named)
     Status: "running"
      Tasks: 8 (limit: 4615)
     Memory: 90.7M
        CPU: 8.099s
     CGroup: /system.slice/named.service
             └─496 /usr/sbin/named -f -u bind

Nov 14 09:49:41 web named[496]: client @0x7fe5dadec898 172.20.60.5#49545 (api.honeycomb.io): view internal: query: api.honeycomb.io IN A + (10.51.10.11)
Nov 14 09:49:41 web named[496]: client @0x7fe5dad35c98 172.20.60.5#34987 (api.honeycomb.io): view internal: query: api.honeycomb.io IN HTTPS + (10.51.10.11)
Nov 14 09:49:42 web named[496]: client @0x7fe5db039098 172.20.60.5#55860 (francecentral-pa03.augloop.office.com): view internal: query: francecentral-pa03.augloop.office.com IN HTTPS>
Nov 14 09:49:42 web named[496]: client @0x7fe5db074898 172.20.60.5#51807 (francecentral-pa03.augloop.office.com): view internal: query: francecentral-pa03.augloop.office.com IN A + (>
Nov 14 09:49:50 web named[496]: client @0x7fe5dadec898 172.20.60.5#57688 (jdasa2-my.sharepoint.com): view internal: query: jdasa2-my.sharepoint.com IN HTTPS + (10.51.10.11)
Nov 14 09:49:50 web named[496]: client @0x7fe5dad35c98 172.20.60.5#50704 (jdasa2-my.sharepoint.com): view internal: query: jdasa2-my.sharepoint.com IN A + (10.51.10.11)
Nov 14 09:49:50 web named[496]: client @0x7fe5db039098 172.20.60.5#53790 (188211-ipv4v6.farm.dprodmgd104.aa-rt.sharepoint.com.dual-spo-0005.spo-msedge.net): view internal: query: 188>
Nov 14 09:49:50 web named[496]: client @0x7fe5db039098 172.20.60.5#64354 (dual-spo-0005.spo-msedge.net): view internal: query: dual-spo-0005.spo-msedge.net IN HTTPS + (10.51.10.11)
Nov 14 09:49:53 web named[496]: client @0x7fe5db039098 172.20.60.5#53128 (eu-teams.events.data.microsoft.com): view internal: query: eu-teams.events.data.microsoft.com IN HTTPS + (10>
Nov 14 09:49:53 web named[496]: client @0x7fe5dad35c98 172.20.60.5#61902 (eu-teams.events.data.microsoft.com): view internal: query: eu-teams.events.data.microsoft.com IN A + (10.51.>
lines 1-22/22 (END)
```

```
root@web:/etc/bind# cat named.conf.local
view "internal" {
    match-clients { 10.0.0.0/8; 172.20.0.0/16; 192.168.3.0/29; localhost; };
    recursion yes;
    allow-query { any; };

    zone "localhost" {
        type master;
        file "/etc/bind/db.local";
    };

    zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
    };

    zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
    };

    zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
    };

    zone "leidoscope.com" {
        type master;
        file "/etc/bind/zones/db.leidoscope.com.internal";
    };

    zone "10.51.10.in-addr.arpa" {
        type master;
        file "/etc/bind/zones/db.10.51.10";
    };
};
```

```
root@web:/etc/bind/zones# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-11-14 10:08:41 CET; 54s ago
       Docs: man:named(8)
   Main PID: 2825 (named)
     Status: "running"
      Tasks: 8 (limit: 4615)
     Memory: 51.6M
        CPU: 99ms
     CGroup: /system.slice/named.service
             └─2825 /usr/sbin/named -f -u bind

Nov 14 10:09:18 web named[2825]: client @0x7fc199276098 172.20.60.5#53526 (roaming.svc.cloud.microsoft): view internal: query: roaming.svc.cloud.microsoft IN A + (10.51.10.11)
Nov 14 10:09:19 web named[2825]: client @0x7fc19b078098 172.20.60.5#58766 (github.com): view internal: query: github.com IN A + (10.51.10.11)
Nov 14 10:09:20 web named[2825]: client @0x7fc19b078098 172.20.60.5#33878 (gew1-spclient.spotify.com): view internal: query: gew1-spclient.spotify.com IN HTTPS + (10.51.10.11)
Nov 14 10:09:20 web named[2825]: client @0x7fc199276098 172.20.60.5#24427 (gew1-spclient.spotify.com): view internal: query: gew1-spclient.spotify.com IN A + (10.51.10.11)
Nov 14 10:09:21 web named[2825]: client @0x7fc19b078098 172.20.60.5#54643 (api.github.com): view internal: query: api.github.com IN HTTPS + (10.51.10.11)
Nov 14 10:09:21 web named[2825]: client @0x7fc19b079c98 172.20.60.5#27700 (api.github.com): view internal: query: api.github.com IN A + (10.51.10.11)
Nov 14 10:09:25 web named[2825]: client @0x7fc199276098 172.20.60.5#6505 (spclient.wg.spotify.com): view internal: query: spclient.wg.spotify.com IN A + (10.51.10.11)
Nov 14 10:09:25 web named[2825]: client @0x7fc19b079c98 172.20.60.5#53353 (spclient.wg.spotify.com): view internal: query: spclient.wg.spotify.com IN HTTPS + (10.51.10.11)
Nov 14 10:09:31 web named[2825]: client @0x7fc199276098 172.20.60.5#59151 (jdasa2-my.sharepoint.com): view internal: query: jdasa2-my.sharepoint.com IN HTTPS + (10.51.10.11)
Nov 14 10:09:31 web named[2825]: client @0x7fc19b079c98 172.20.60.5#56186 (jdasa2-my.sharepoint.com): view internal: query: jdasa2-my.sharepoint.com IN A + (10.51.10.11)
root@web:/etc/bind/zones#
```

```
root@web:/etc/bind/zones# cat db.leidoscope.com.internal
$TTL 86400
@ IN SOA ns1.leidoscope.com. admin.leidoscope.com. (2025110408 3600 1800 604800 86400)
@ IN NS ns1.leidoscope.com.
ns1 IN A 10.51.10.11
@ IN A 10.51.10.11
root@web:/etc/bind/zones#
```

```
root@web:/etc/bind/zones# cat db.10.51.10
$TTL 86400
@ IN SOA ns1.leidoscope.com. admin.leidoscope.com. (2025110408 3600 1800 604800 86400)
@ IN NS ns1.leidoscope.com.
11 IN PTR leidoscope.com.
11 IN PTR www.leidoscope.com.
root@web:/etc/bind/zones#
```

```
root@web:/etc/bind/zones# ls
db.10.51.10  db.leidoscope.com.internal
root@web:/etc/bind/zones#
```

```
❯ nslookup leidoscope.com
Server:         10.51.10.11
Address:        10.51.10.11#53

Name:   leidoscope.com
Address: 10.51.10.11
```