

## Тема: "Элементы безопасности информационных систем"

1. Установил Hashicorp Vault на виртуальной машине Vagrant/VirtualBox (Ubuntu 20.04.1 LTS).

Для получения и хранения сертификатов и ключей для web-сервера Nginx.

2. Запустил vault в dev- режиме, (т.е. только для разработки или экспериментов).





```
vagrant@vagrant:~$ VAULT_UI=true vault server -dev -dev-listen-address="0.0.0.0:8200" -dev-root-token-id="root"
=> Vault server configuration:

  Api Address: http://0.0.0.0:8200
    Cgo: disabled
  Cluster Address: https://0.0.0.0:8201
    Go Version: go1.15.13
  Listener 1: tcp (addr: "0.0.0.0:8200", cluster address: "0.0.0.0:8201", max_request_duration: "1m30s", max_request_size: "33554432", tls: "disabled")
    Log Level: info
    Mlock: supported: true, enabled: false
  Recovery Mode: false
    Storage: inmem
    Version: Vault v1.7.3
    Version Sha: 5d517c864c8f10385bf65627891bc7ef55f5e827

=> Vault server started! Log data will stream in below:
```

3. Создадим цепочку сертификатов (CA Bundle): корневой (Root CA) и промежуточный (Intermediate CA) сертификаты.  
Результат в программе Vault:

### Secrets Engines

 <a href="#">cubbyhole/</a> cubbyhole_f13155e9
 <a href="#">pki/</a> pki_b29689ce
 <a href="#">pki_int/</a> pki_775e4baf
 <a href="#">secret/</a> v2 kv_6af6f839

Промежуточный удостоверяющий центр (CA) может подписывать сертификаты от имени корневого удостоверяющего центра. Корневой удостоверяющий центр подписывает промежуточный сертификат, формируя цепочку доверия.

4. Подписываем промежуточный сертификат Intermediate CA для тестового домена (netology.example.com), чтобы можно было установить защищенное https соединение

[pki\\_int](#) [creds](#) [example-dot-com](#)

## Issue Certificate

**Common Name**

netology.example.com

**Format**

pem

[^ Hide Options](#)

< pki\_int < creds < example-dot-com

## Issue Certificate



You will not be able to access this information later, so please copy the information below.

### Certificate

[illegible]

- Установил и настроил `consul-template` для автоматического подтягивания сертификата из Vault.

```
root@vagrant:~# systemctl start consul-template.service
root@vagrant:~# systemctl status consul-template.service
● consul-template.service - consul-template
   Loaded: loaded (/etc/systemd/system/consul-template.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-06-23 07:54:00 UTC; 4s ago
     Main PID: 22738 (consul-template)
        Tasks: 6 (limit: 1074)
       Memory: 1.6M
      CGroup: /system.slice/consul-template.service
              └─22738 /usr/local/bin/consul-template -config=/etc/consul-template.d/pki-demo.hcl

Jun 23 07:54:00 vagrant systemd[1]: Started consul-template.
```

6. Сервер nginx получил подписанный сертификат Vault Intermediate CA и успешно запустился.

```
root@vagrant:/home/vagrant/vault# systemctl start nginx.service
root@vagrant:/home/vagrant/vault# systemctl status nginx.service
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-06-23 08:08:23 UTC; 8s ago
     Docs: man:nginx(8)
   Process: 22869 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Process: 22880 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Main PID: 22881 (nginx)
    Tasks: 2 (limit: 1074)
   Memory: 2.6M
   CGroup: /system.slice/nginx.service
           └─22881 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             └─22882 nginx: worker process

Jun 23 08:08:23 vagrant systemd[1]: Starting A high performance web server and a reverse proxy server...
Jun 23 08:08:23 vagrant systemd[1]: Started A high performance web server and a reverse proxy server.
```

```
root@vagrant:/home/vagrant/vault# openssl x509 -in /etc/nginx/certs/yet.crt -noout -text -purpose
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            43:2f:a2:70:4b:2a:99:73:18:64:3b:e0:c9:f5:61:92:31:55:37:45
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = pki-ca-int
        Validity
            Not Before: Jun 22 10:27:43 2021 GMT
            Not After : Jun 22 10:30:13 2021 GMT
        Subject: CN = example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:d6:58:1e:59:4f:98:87:49:d1:d1:5e:37:12:99:
                12:6a:aa:3e:20:ac:3e:ea:76:58:10:f7:37:02:62:
                ba:41:17:d5:1b:20:fe:aa:23:f7:d1:24:e0:27:de:
                92:79:bf:df:41:b3:4c:a8:37:7c:87:31:8a:3a:13:
                d1:ec:2b:a5:18:d2:fe:e8:66:1b:00:94:61:81:58:
                6e:cb:7d:8f:5f:03:01:48:a0:33:ea:a9:6d:08:ca:
                32:d2:4b:33:84:d7:36:e7:99:98:e4:7e:6a:dd:1c:
                66:06:00:90:a9:67:71:e1:dd:5b:f9:40:34:f4:7c:
                b1:9e:e8:d4:ac:ce:7a:9d:f5:3d:db:ab:c9:a9:5d:
                ac:e6:af:4d:a0:d8:23:19:47:15:7d:ab:df:6f:a0:
                42:bd:91:2e:4b:70:06:72:b7:5f:5f:13:d9:5b:57:
                5d:96:ce:e3:80:5c:5b:4d:af:4a:83:a7:78:e2:6e:
                71:46:8f:56:d3:85:d7:ba:c1:ae:87:31:78:eb:b6:
                46:65:f2:ce:bf:b8:53:42:9e:6e:d1:c9:54:99:e7:
                8f:43:ad:59:31:81:a9:38:8c:ea:34:cc:4f:3a:b4:
                4a:4d:95:fd:93:ec:e1:fb:ad:bf:a6:26:6b:ba:f3:
                f8:54:f9:8c:23:a8:54:c7:15:b4:f1:4a:94:b4:52:
                2a:3f
```

```
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment, Key Agreement
  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Subject Key Identifier:
    62:DB:93:3E:05:FF:3B:62:56:7E:B2:89:2D:01:2A:D6:8F:71:10:D2
  X509v3 Authority Key Identifier:
    keyid:C1:4D:58:9F:A3:55:C6:8B:98:F5:D8:40:AD:F8:6F:67:67:E1:4B:7D

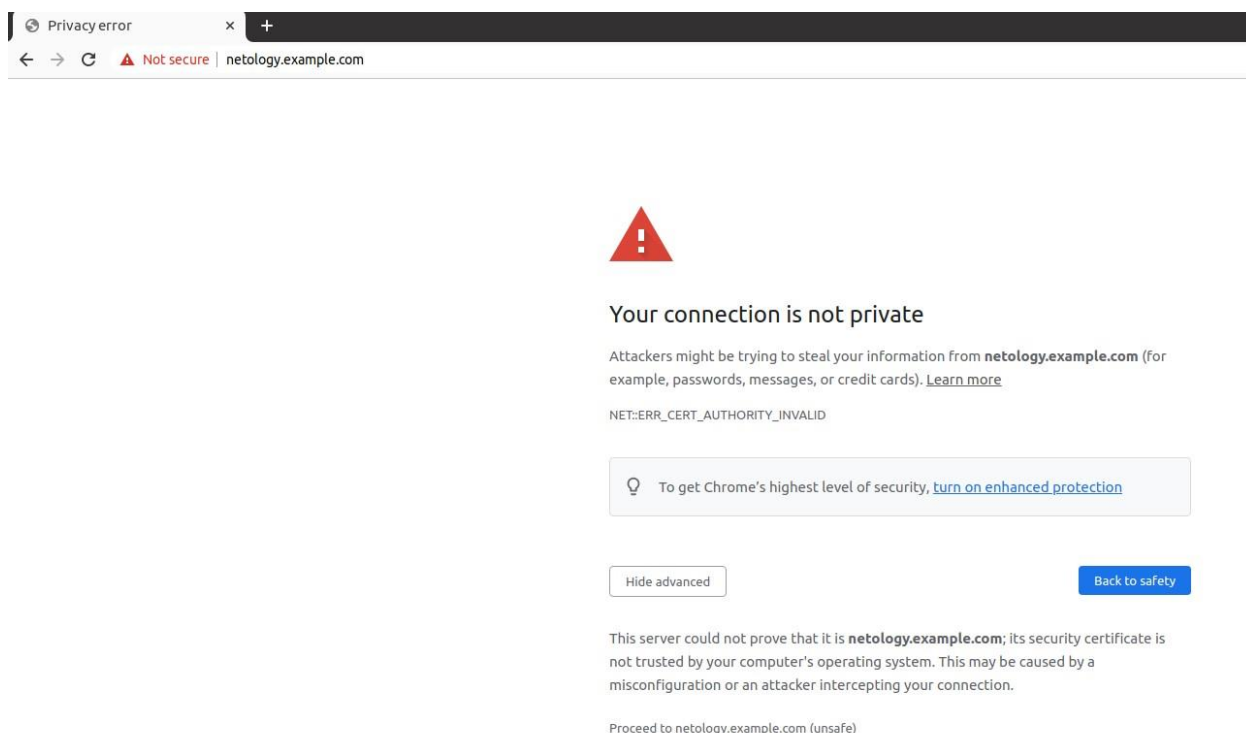
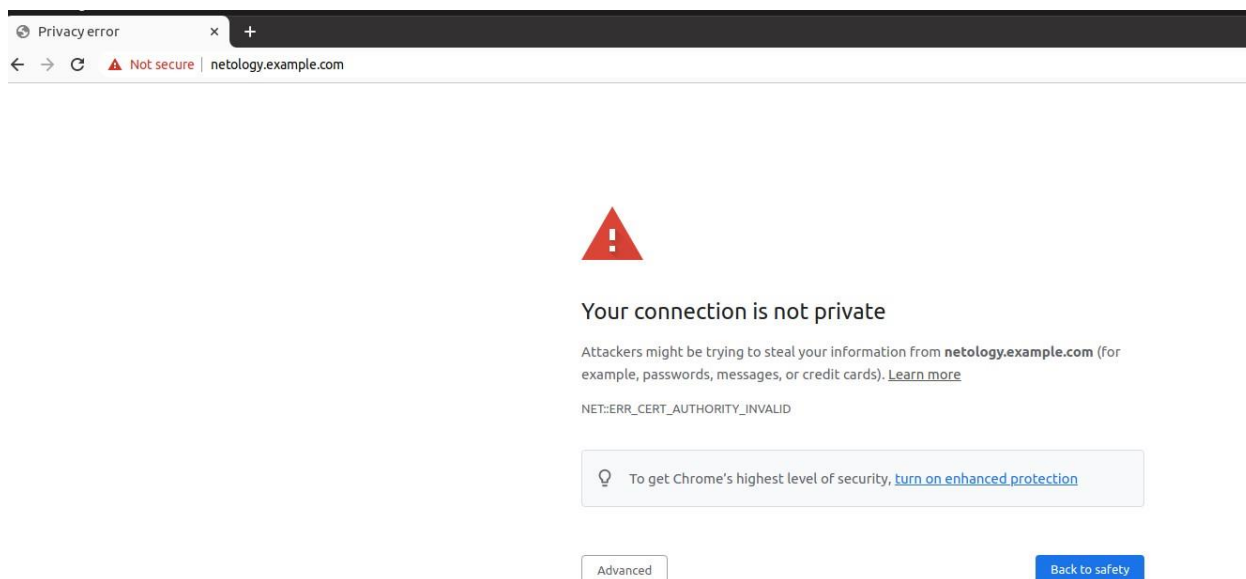
Authority Information Access:
  CA Issuers - URI:http://127.0.0.1:8200/v1/pki_int/ca

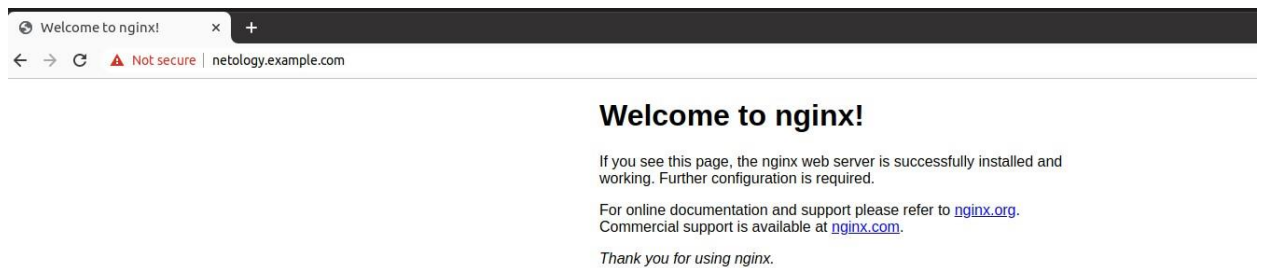
X509v3 Subject Alternative Name:
  DNS:example.com
X509v3 CRL Distribution Points:

  Full Name:
    URI:http://127.0.0.1:8200/v1/pki_int/crl
```

```
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : No
S/MIME signing CA : No
S/MIME encryption : No
S/MIME encryption CA : No
CRL signing : No
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No
```

7. На рабочем компьютере (Ubuntu 21.04) в Google Chrome перешел на сайт: <https://netology.example.com>





С помощью команды `curl` со своего рабочего компьютера проверил статус сертификата NGINX:

```
user@ubuntu: ~/netology/3.1$ curl --cacert /home/user/pki_ca.pem --insecure -v https://netology.example.com 2>&1 | awk 'BEGIN { cert=0 } /^* SSL connection/ { cert=1 } /^*/ { if (cert) print }'
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
* ALPN, server accepted to use h2
* Server certificate:
* subject: CN=example.com
* start date: Jun 22 10:27:43 2021 GMT
* expire date: Jun 22 10:30:13 2021 GMT
* issuer: CN=pki-ca-int
* SSL certificate verify result: unable to get local issuer certificate (20), continuing anyway.
* Using HTTP2, server supports multi-use
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x55ff5cde9580)
* Connection state changed (MAX_CONCURRENT_STREAMS == 120)!
* Connection #0 to host netology.example.com left intact
user@ubuntu: ~/netology/3.1$
user@ubuntu: ~/netology/3.1$ cat /etc/os-release
NAME="Ubuntu"
VERSION="21.04 (Hirsute Hippo)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 21.04"
VERSION_ID="21.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=hirsute
UBUNTU_CODENAME=hirsute
user@ubuntu: ~/netology/3.1$
```

Выполненные команды в файле README.md,  
Конфигурационные файлы (nginx, consul-template) и сертификаты от Valut в  
git-репозитории