Cypherdog Enterprise

Installation of proxy services and HashiCorp Vault on Linux Ubuntu server

1. General information

The manual presents the various steps to be followed to properly install and run the proxy service implemented by **Cypherdog** and **HashiCorp Vault** on **Ubuntu Server** (version **20.04 LTS** or **18.04 LTS**).

2. Installation

2.1. Script download

To download the script, run the following command on the server:

```
curl -L https://packer.cdn.cypher.dog/scripts/proxy.sh -o proxy.sh
```

The command will download the proxy.sh file and save it locally on the server. This file contains a script that allows to perform the necessary initialization and launching of services.

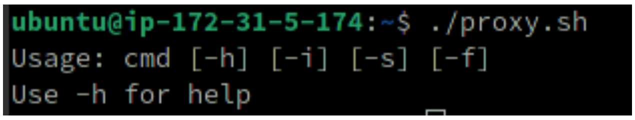
2.2. Giving the executable flag

For a file to run properly, it must be flagged as executable. We do this by calling the command:

```
chmod +x proxy.sh
```

2.3. Available commands

Just running the script by calling **./proxy.sh** without specifying a specific flag will not start the initialization process. Instead, it will display the available flags and how to use the script.



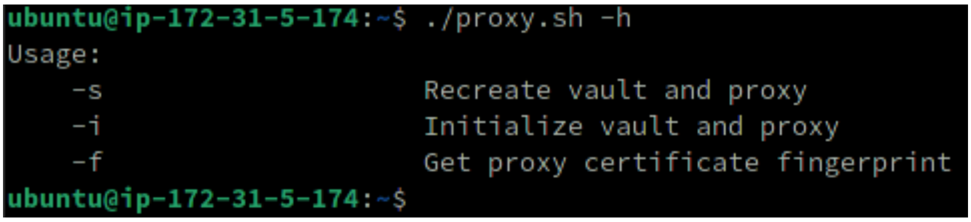
```
ubuntu@ip-172-31-5-174:~$ ./proxy.sh
Usage: cmd [-h] [-i] [-s] [-f]
Use -h for help
```

2.3.1. Overview of individual flags

Calling the command (help)

```
./proxy.sh -h
```

will display the available flags with a brief description of them.



```
ubuntu@ip-172-31-5-174:~$ ./proxy.sh -h
Usage:
    -s                        Recreate vault and proxy
    -i                        Initialize vault and proxy
    -f                        Get proxy certificate fingerprint
ubuntu@ip-172-31-5-174:~$
```

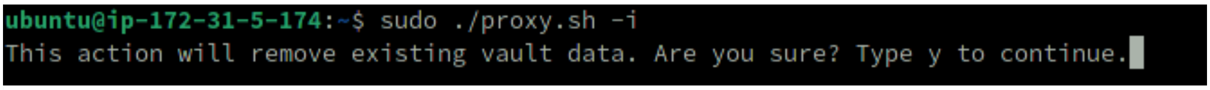
So, the flags:

- **-i** - Initializes and automatically installs and configures proxy and Vault services. This flag should only be used during the first run. Any re-triggering of this flag may result in the loss of Vault data.
- **-s** - In case the server is stopped for some reason, or one of the services requires a restart, this flag will allow the proxy and Vault to be restarted correctly.
- **-f** - Allows you to see the SHA-1 fingerprint of the proxy certificate.

2.4. Initialization

To start initialization, run the command below. The *sudo* command is necessary for proper initialization.

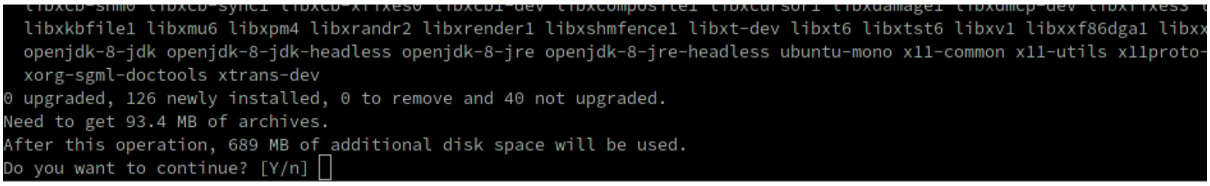
```
sudo ./proxy.sh -i
```



```
ubuntu@ip-172-31-5-174:~$ sudo ./proxy.sh -i
This action will remove existing vault data. Are you sure? Type y to continue.
```

At the beginning, we will receive information that the entire process will delete the existing data. Press "Y" to continue and press any other key to abort the process.

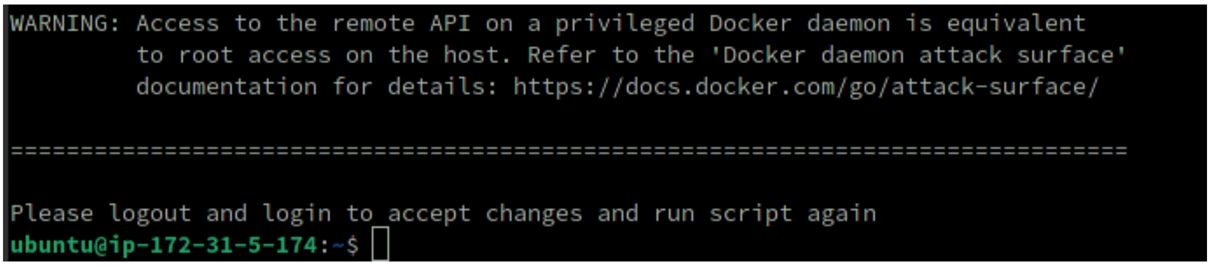
After hitting the "Y" key the script will start downloading and installing the necessary software. Be vigilant as some operations will require additional confirmation. An example in the photo below.



```
  libxcb-shm0 libxcb-sync1 libxcb-xfixes0 libxcb1-dev libxcomposite1 libxcursor1 libxdamage1 libxdmcp-dev libxfixes3
  libxkbfile1 libxmu6 libxpm4 libxrandr2 libxrender1 libxshmfence1 libxt-dev libxt6 libxtst6 libxv1 libxxf86dga1 libxx
  openjdk-8-jdk openjdk-8-jdk-headless openjdk-8-jre openjdk-8-jre-headless ubuntu-mono x11-common x11-utils x11proto-
  xorg-sgml-doctools xtrans-dev
0 upgraded, 126 newly installed, 0 to remove and 40 not upgraded.
Need to get 93.4 MB of archives.
After this operation, 689 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

In this case, to continue, type "Y" and click "Enter". The process will continue.

If **docker** was not installed on the server, at some point we will receive information about the need to log out and log back into the machine.



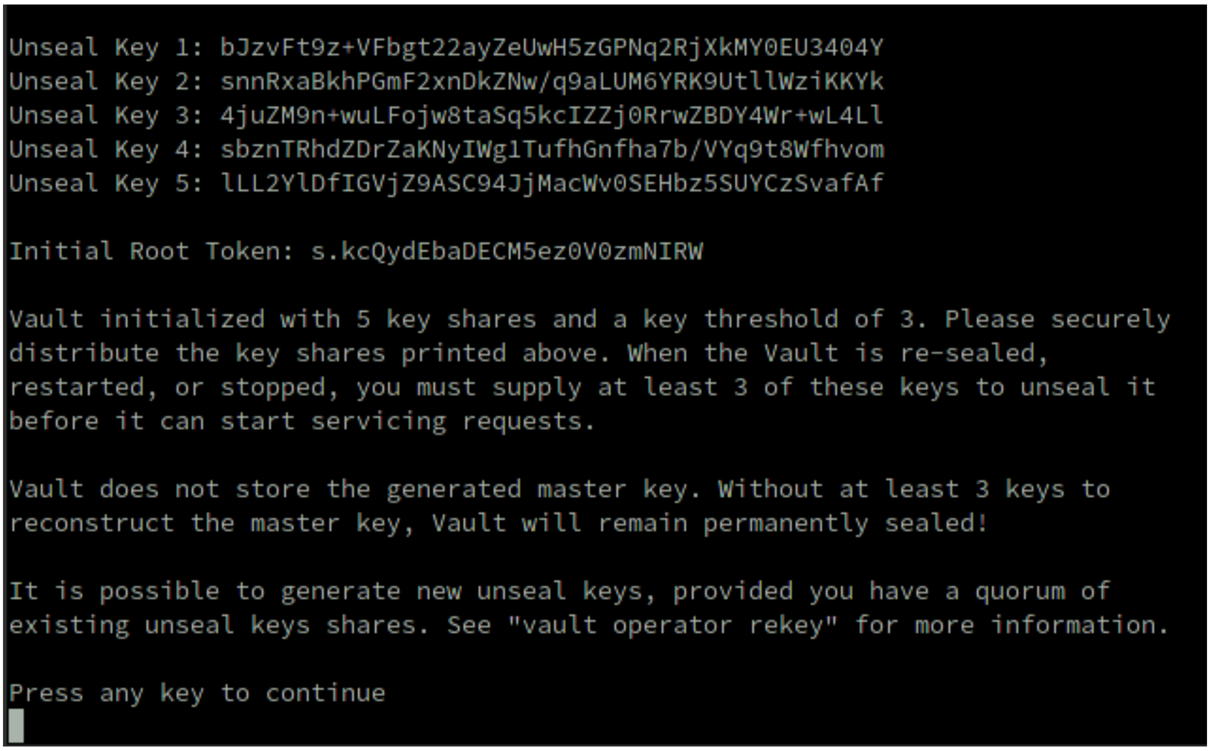
```
WARNING: Access to the remote API on a privileged Docker daemon is equivalent
         to root access on the host. Refer to the 'Docker daemon attack surface'
         documentation for details: https://docs.docker.com/go/attack-surface/

==========================================================================

Please logout and login to accept changes and run script again
ubuntu@ip-172-31-5-174:~$ 
```

The easiest way is to close the terminal and reconnect to the server. After logging back in, you should re-run the script with the -i flag as the superuser:

```
sudo ./proxy.sh -i
```

The script will continue to install the software as needed and begin downloading images of individual sites and their configuration.

At some point, information similar to the one below will appear in the terminal.



```
Unseal Key 1: bJzvFt9z+VFbgt22ayZeUwH5zGPNq2RjXkMY0EU3404Y
Unseal Key 2: snnRxaBkhPGmF2xnDkZNw/q9aLUM6YRK9UtllWziKKYk
Unseal Key 3: 4juZM9n+wuLFojw8taSq5kcIZZj0RrwZBDY4Wr+wL4Ll
Unseal Key 4: sbznTRhdZDrZaKNyIWg1TufhGnfha7b/VYq9t8Wfhvom
Unseal Key 5: lLL2YlDfIGVjZ9ASC94JjMacWv0SEHbz5SUYCzSvafAf

Initial Root Token: s.kcQydEbaDECM5ez0V0zmNIRW

Vault initialized with 5 key shares and a key threshold of 3. Please securely
distribute the key shares printed above. When the Vault is re-sealed,
restarted, or stopped, you must supply at least 3 of these keys to unseal it
before it can start servicing requests.

Vault does not store the generated master key. Without at least 3 keys to
reconstruct the master key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum of
existing unseal keys shares. See "vault operator rekey" for more information.

Press any key to continue
```

ATTENTION!

These are the most important keys and the root token for the Vault service. Keep the above information in a safe place. Losing your keys will prevent you from restarting the site, and losing your token will prevent you from logging into and administering the Vault.
It is impossible to recover the keys and the root of the token.

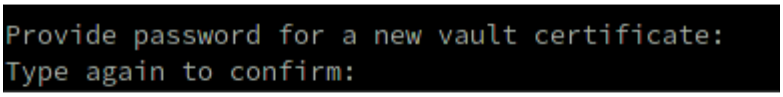
What are these keys for?

Vault creates the so-called *master key* with which it encrypts all its data. By default, the *master key* is divided into 5 smaller keys that must be kept safe. The use of 3 out of 5 keys allows you to recreate the entire *master key*, and thus - allows you to use the Vault after a restart.

The *master key* is volatile and is not stored anywhere. Therefore, after a restart, or after manual binding, Vault is not able to decode its data, and thus - it is impossible to use it.

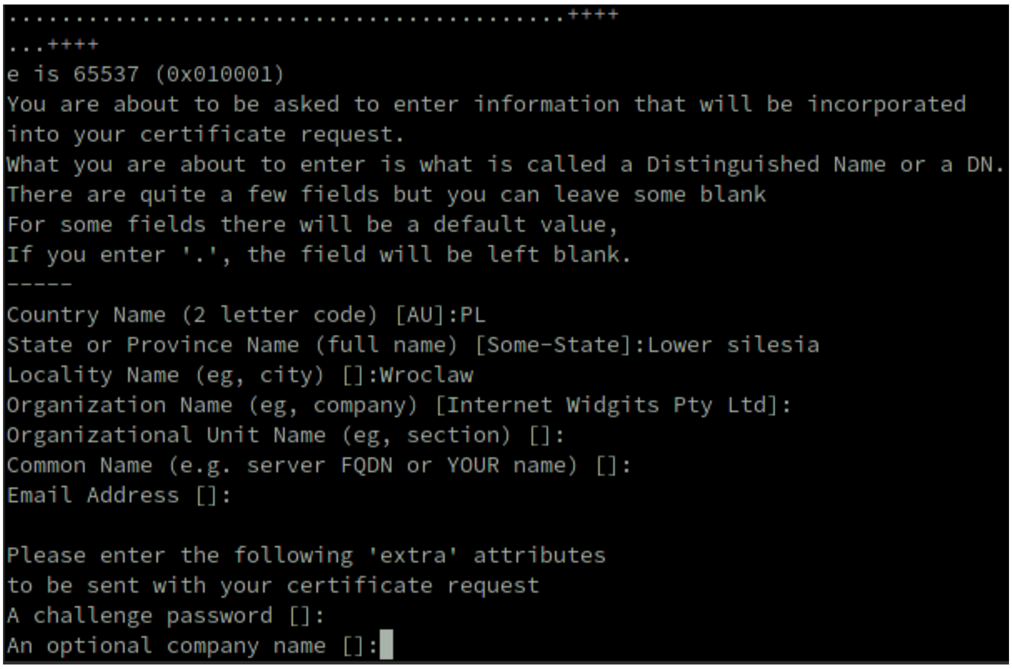
After copying the displayed information and saving it in a safe place, we can continue the initialization process by pressing any button.

The next step performed by the script that requires the user's intervention is to enter the password that will be used to protect the Vault server certificate. The password should be remembered as it is necessary during reboots.



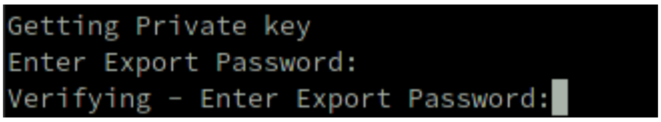
```
Provide password for a new vault certificate:
Type again to confirm:
```

In the penultimate step, the script will start generating a certificate for the proxy server. Depending on the needs, you can provide the indicated information, but it does not affect the further operation of the application.



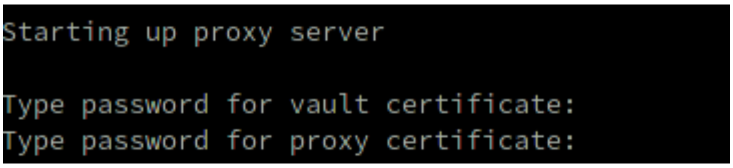
```
..........................................++++
...++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Lower silesia
Locality Name (eg, city) []:Wroclaw
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The last step is to enter the password with which the private key is to be encrypted. It is recommended that this password be different from the password used to encrypt the Vault certificate. Remember the password as it will be needed every time you start the proxy.



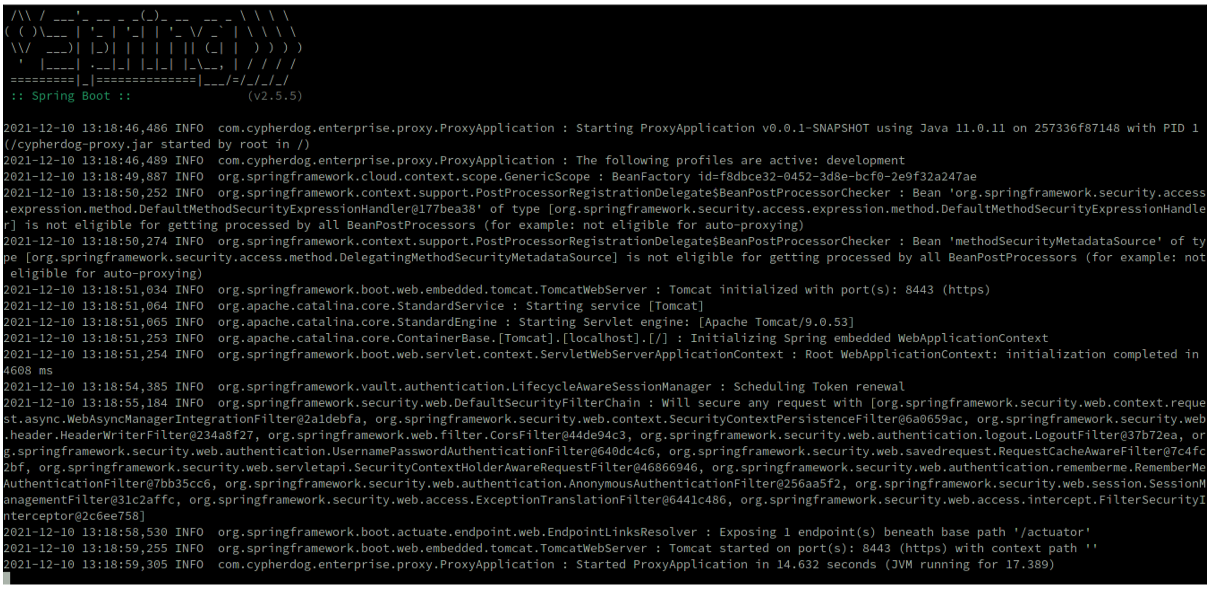
```
Getting Private key
Enter Export Password:
Verifying - Enter Export Password:
```

The initialization process is now completed and the script will start the startup process of the proxy server. We will be asked to provide passwords for Vault and proxy certificates.



```
Starting up proxy server

Type password for vault certificate:
Type password for proxy certificate:
```

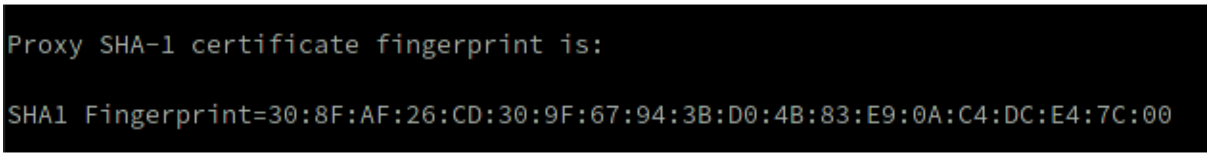
After the docker downloads the proxy server image in the terminal, you should see logs similar to the ones below.



```
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.5.5)

2021-12-10 13:18:46,486 INFO  com.cypherdog.enterprise.proxy.ProxyApplication : Starting ProxyApplication v0.0.1-SNAPSHOT using Java 11.0.11 on 257336f87148 with PID 1
(/cypherdog-proxy.jar started by root in /)
2021-12-10 13:18:46,489 INFO  com.cypherdog.enterprise.proxy.ProxyApplication : The following profiles are active: development
2021-12-10 13:18:49,887 INFO  org.springframework.cloud.context.scope.GenericScope : BeanFactory id=f8dbce32-0452-3d8e-bcf0-2e9f32a247ae
2021-12-10 13:18:50,252 INFO  org.springframework.context.support.PostProcessorRegistrationDelegate$BeanPostProcessorChecker : Bean 'org.springframework.security.access
.expression.method.DefaultMethodSecurityExpressionHandler@177bea38' of type [org.springframework.security.access.expression.method.DefaultMethodSecurityExpressionHandle
r] is not eligible for getting processed by all BeanPostProcessors (for example: not eligible for auto-proxying)
2021-12-10 13:18:50,274 INFO  org.springframework.context.support.PostProcessorRegistrationDelegate$BeanPostProcessorChecker : Bean 'methodSecurityMetadataSource' of ty
pe [org.springframework.security.access.method.DelegatingMethodSecurityMetadataSource] is not eligible for getting processed by all BeanPostProcessors (for example: not
 eligible for auto-proxying)
2021-12-10 13:18:51,034 INFO  org.springframework.boot.web.embedded.tomcat.TomcatWebServer : Tomcat initialized with port(s): 8443 (https)
2021-12-10 13:18:51,064 INFO  org.apache.catalina.core.StandardService : Starting service [Tomcat]
2021-12-10 13:18:51,065 INFO  org.apache.catalina.core.StandardEngine : Starting Servlet engine: [Apache Tomcat/9.0.53]
2021-12-10 13:18:51,253 INFO  org.apache.catalina.core.ContainerBase.[Tomcat].[localhost].[/] : Initializing Spring embedded WebApplicationContext
2021-12-10 13:18:51,254 INFO  org.springframework.boot.web.servlet.context.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in
4608 ms
2021-12-10 13:18:54,385 INFO  org.springframework.vault.authentication.LifecycleAwareSessionManager : Scheduling Token renewal
2021-12-10 13:18:55,184 INFO  org.springframework.security.web.DefaultSecurityFilterChain : Will secure any request with [org.springframework.security.web.context.reque
st.async.WebAsyncManagerIntegrationFilter@2a1debfa, org.springframework.security.web.context.SecurityContextPersistenceFilter@6a0659ac, org.springframework.security.web
.header.HeaderWriterFilter@234a8f27, org.springframework.web.filter.CorsFilter@44de94c3, org.springframework.security.web.authentication.logout.LogoutFilter@37b72ea, or
g.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@640dc4c6, org.springframework.security.web.savedrequest.RequestCacheAwareFilter@7c4fc
2bf, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@46866946, org.springframework.security.web.authentication.rememberme.RememberMe
AuthenticationFilter@7bb35cc6, org.springframework.security.web.authentication.AnonymousAuthenticationFilter@256aa5f2, org.springframework.security.web.session.SessionM
anagementFilter@31c2affc, org.springframework.security.web.access.ExceptionTranslationFilter@6441c486, org.springframework.security.web.access.intercept.FilterSecurityI
nterceptor@2c6ee758]
2021-12-10 13:18:58,530 INFO  org.springframework.boot.actuate.endpoint.web.EndpointLinksResolver : Exposing 1 endpoint(s) beneath base path '/actuator'
2021-12-10 13:18:59,255 INFO  org.springframework.boot.web.embedded.tomcat.TomcatWebServer : Tomcat started on port(s): 8443 (https) with context path ''
2021-12-10 13:18:59,305 INFO  com.cypherdog.enterprise.proxy.ProxyApplication : Started ProxyApplication in 14.632 seconds (JVM running for 17.389)
```

These are logs coming directly from the container in which the proxy server is located. If you do not see any errors, the initialization and start-up process was successful. To leave these logs and complete the installation process, use the following button combinations in turn: **Ctrl + P** and then **Ctrl + Q**.

Finally, the SHA-1 thumbprint of the proxy certificate will be displayed.



```
Proxy SHA-1 certificate fingerprint is:

SHA1 Fingerprint=30:8F:AF:26:CD:30:9F:67:94:3B:D0:4B:83:E9:0A:C4:DC:E4:7C:00
```

Thus, the installation, initialization and commissioning process is completed, and the Vault and proxy services are ready for use.

3. Service

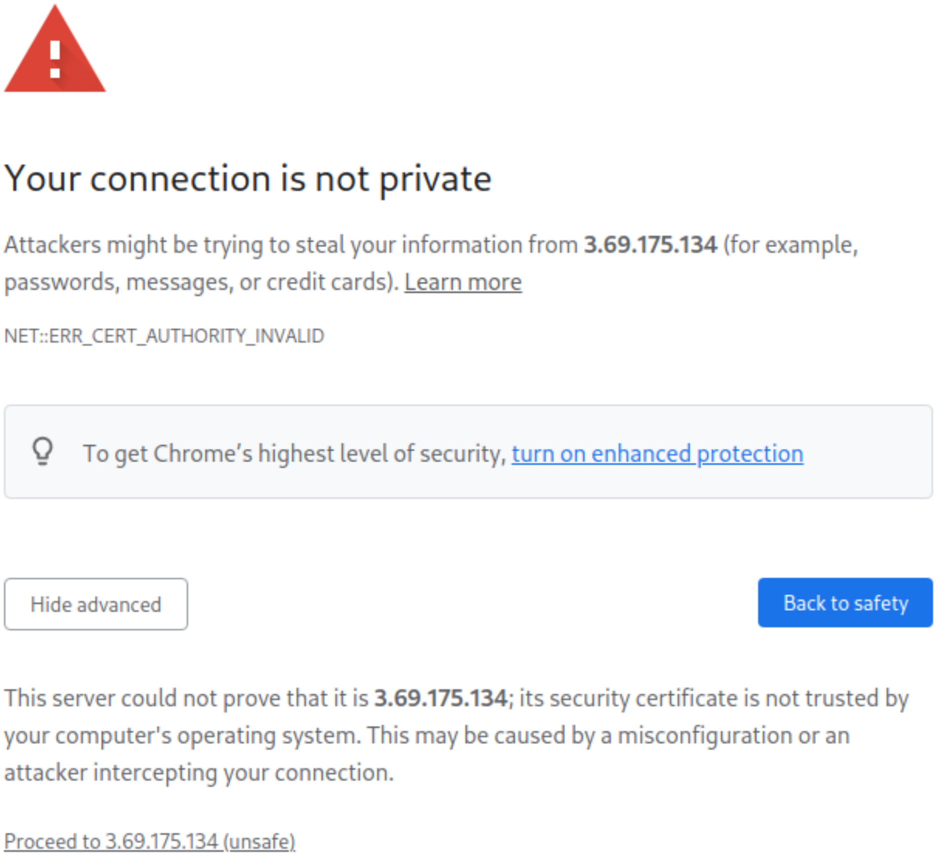
The proxy service will be run on port **443 (HTTPS)**, and Vault on port **8200**. Any web browser can be used for the basic operation of these services.

3.1. Vault login

To open the Vault panel, enter the following address in the browser:

```
https://<server_ip_address>:8200/
```

Probably the first thing that will appear is the information about an invalid certificate. This is normal because the certificate attached to the Vault site was not created by any authorized CA, but was created by the user when the Vault site was initialized.



Your connection is not private

Attackers might be trying to steal your information from **3.69.175.134** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

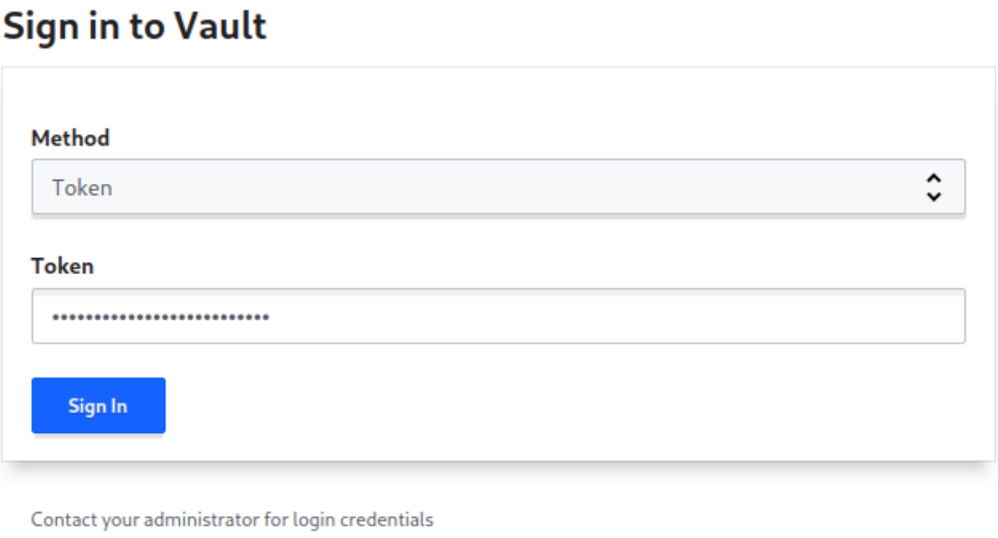
To get Chrome's highest level of security, turn on enhanced protection

This server could not prove that it is **3.69.175.134**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 3.69.175.134 (unsafe)

Continue to the indicated address.

At this point, the Vault login panel will be displayed in the browser. To gain access, select the **Token** method and provide the root token that was generated during Vault initialization.



Sign in to Vault

Method: Token

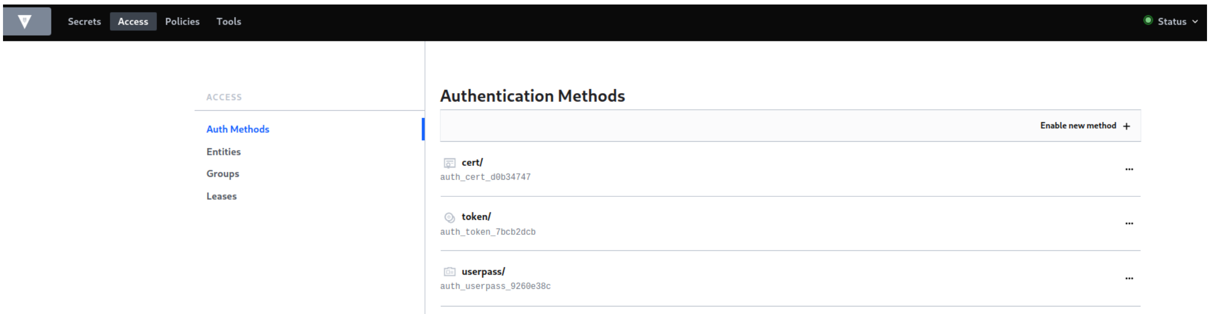
Token: ••••••••••••••••••••••••••

Contact your administrator for login credentials

3.2. Creating administrator accounts

The main task of an administrator with a root token should be to create accounts for other administrators who have the right to create one-time tokens for Cypherdog Enterprise users wanting to restore their key backup.

To create such an account, go to the **Access** tab and then select **userpass/**



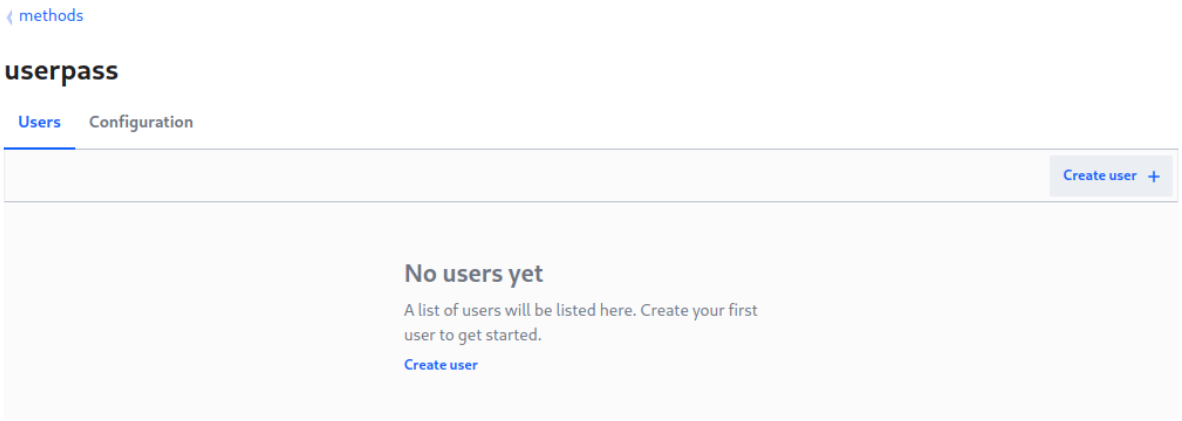
Authentication Methods

cert/
auth_cert_d0b34747

token/
auth_token_7bcb2dcb

userpass/
auth_userpass_9260e38c

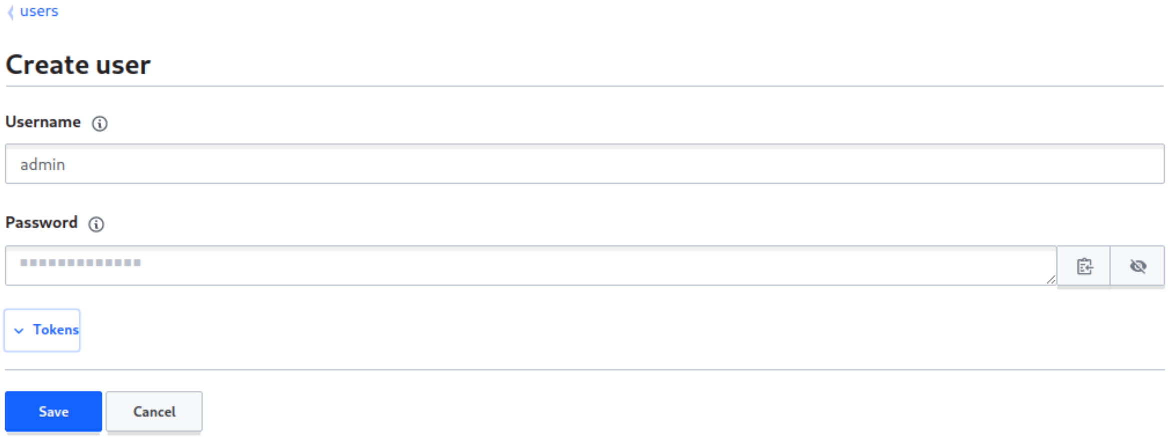
Then press the option **Create new user +**



No users yet

A list of users will be listed here. Create your first user to get started.

Now complete the form with the login and password that the administrator is to use.



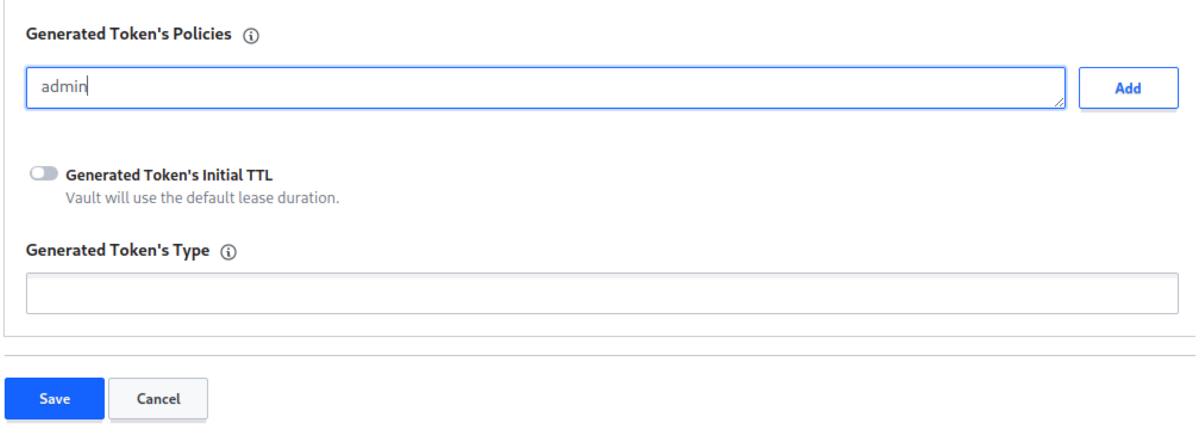
Create user

Username: admin

Password: ■■■■■■■■■■■■■■

The next step is to develop Tokens and assign the appropriate role to the administrator.To do so, enter **admin** in the **Generated Token's Policies** field.

Without this value, the administrator account will be useless.



Generated Token's Policies: admin

Generated Token's Initial TTL

Vault will use the default lease duration.

Generated Token's Type

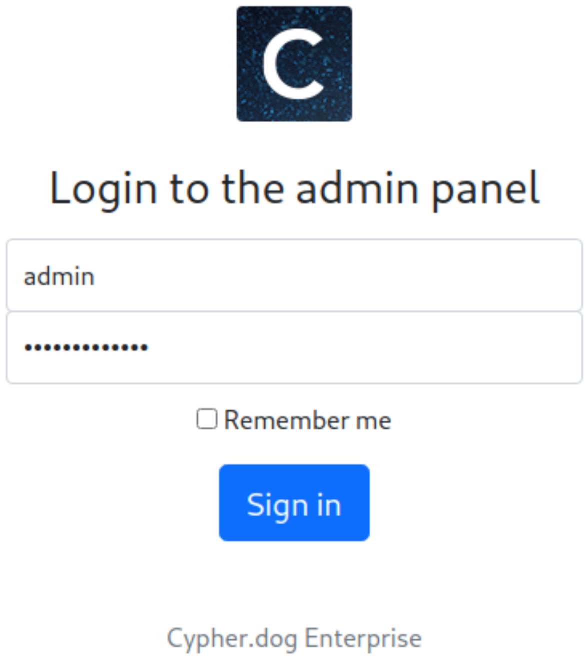
Now save the changes by pressing the **Save** button. The login and password should be provided to the administrator in a safe manner.

3.3. Creating one-time tokens

To open the panel that allows you to generate tokens, enter the following address in your browser:

`https://<server_ip_address>/`

As in the case of entering the address where the Vault panel is located, we will receive information about an incorrect certificate. As in the previous case, continue to the provided address.



Login to the admin panel

admin

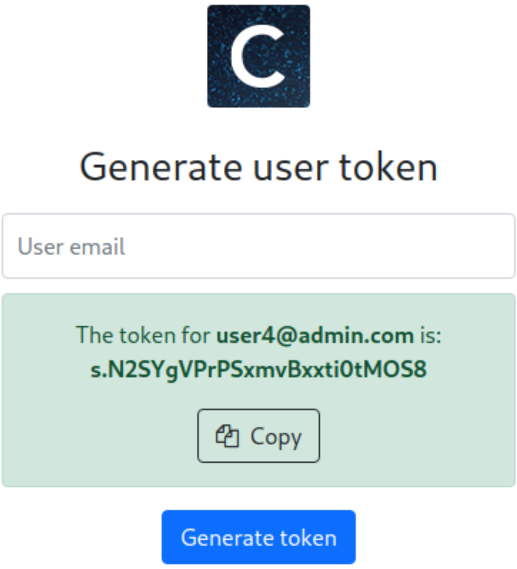
••••••••••••••

☐ Remember me

Cypher.dog Enterprise

To log in, use the account data created in create administrator accounts.

Then enter the email address of the user who wants to get his backup. The necessary condition is that the user has his backup in the Vault. Without it, generating the token will not be possible.



Generate user token

The token for **user4@admin.com** is:
s.N2SYgVPrPSxmvBxxti0tMOS8

The token generated in this way should be handed over to the user. The token is a one-time use and will only allow the backup to be restored to the user with the specified email address.