Cypherdog Enterprise

Instalacja serwisów proxy oraz HashiCorp Vault na serwerze Linux Ubuntu

1. Ogólne informacje

W instrukcji zostały przedstawione poszczególne etapy, jakie należy wykonać, aby prawidłowo zainstalować oraz uruchomić serwis **proxy** zaimplementowany przez **Cypherdog** oraz **HashiCorp Vault** na serwerze **Ubuntu Server** (wersja **20.04 LTS** lub **18.04 LTS**).

2. Instalacja

2.1. Pobranie skryptu

Aby pobrać skrypt należy wywołać na serwerze poniższą komendę:

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

Komenda pobierze plik *proxy.sh* i zapisze go lokalnie na serwerze. Plik ten zawiera skrypt pozwalający dokonywać niezbędnej inicjalizacji oraz uruchomienia serwisów.

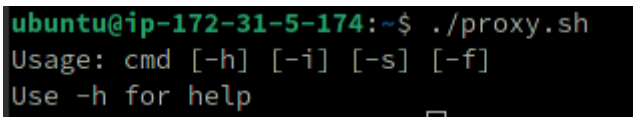
2.2. Nadanie flagi wykonywalności

Aby plik mógł być poprawnie uruchamiany, należy nadać mu flagę wykonywalności. Wykonujemy to wywołując polecenie:

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

2.3. Dostępne komendy

Samo uruchomienie skryptu poprzez wywołanie `./proxy.sh` bez podania konkretnej flagi nie rozpocznie procesu inicjalizacji. Zamiast tego, wyświetli dostępne flagi oraz sposób użycia skryptu.



2.3.1. Omówienie poszczególnych flag

Wywołanie komendy (help)

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

wyświetli dostępne flagi wraz z ich krótkim omówieniem

```
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:~$
```

Zatem flagi:

- **-i** - Inicjalizuje i automatycznie instaluje oraz konfiguruje serwisy proxy i Vault. Tej flagi powinno używać się jedynie podczas pierwszego uruchomienia. Każde ponowne wywołanie tej flagi może spowodować utratę danych serwisu Vault
- **-s** - W przypadku, gdyby z jakiegoś powodu serwer uległ zatrzymaniu, lub któryś z serwisów wymagał restartu, ta flaga pozwoli na poprawne, ponowne uruchomienie proxy oraz vault
- **-f** - Pozwala na wyświetlenie odcisku palca SHA-1 certyfikatu serwera proxy

2.4. Inicjalizacja

Aby rozpocząć inicjalizację należy wywołać poniższą komendę. Polecenie *sudo* jest niezbędne do poprawnego przeprowadzenia inicjalizacji.

```
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.
```

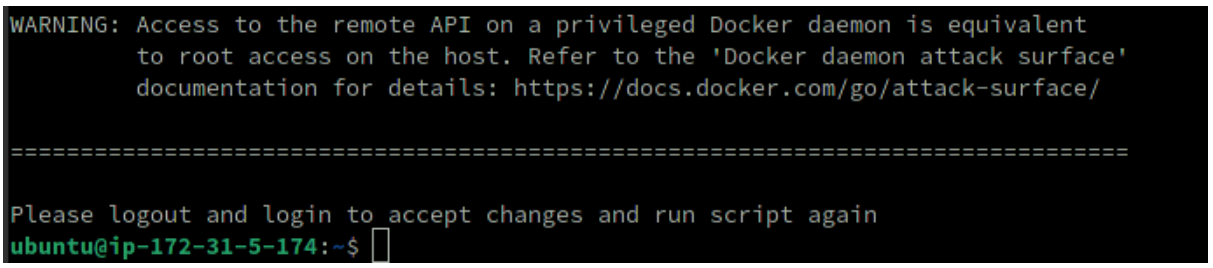
Na początku otrzymamy informację, że cały proces usunie istniejące dane. Aby kontynuować należy nacisnąć klawisz “Y”, zaś aby przerwać proces, należy nacisnąć dowolny, inny klawisz.

Po wciśnięciu klawisza “Y” skrypt rozpocznie pobieranie i instalację niezbędnego oprogramowania. Należy zachować czujność, gdyż niektóre operacje będą wymagały dodatkowego potwierdzenia. Przykład na poniższym zdjęciu.

```
  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]
```

W takiej sytuacji, aby kontynuować wpisujemy “y” i klikamy klawisz “Enter”. Proces będzie kontynuowany.

Jeśli na serwerze nie był zainstalowany **docker**, w pewnym momencie otrzymamy informację o konieczności wylogowania oraz ponownego zalogowania się na maszynę



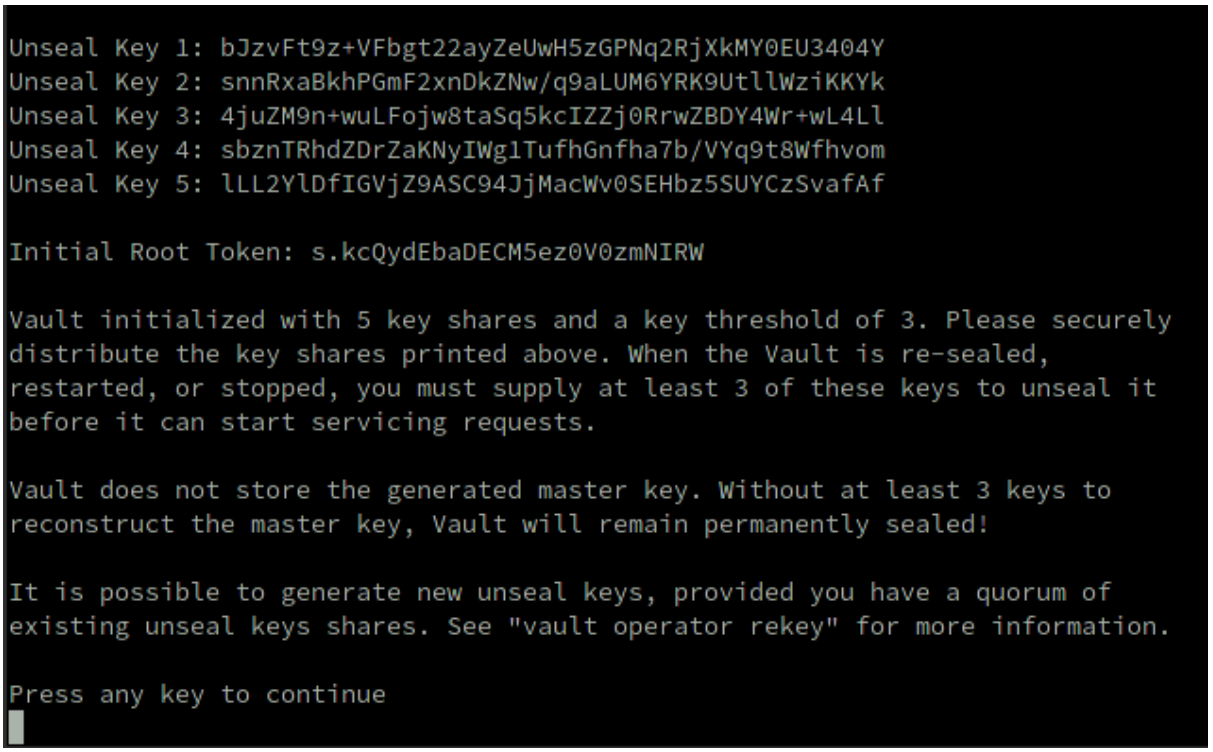
Najprostszym sposobem jest zamknięcie terminala i ponowne połączenie się z serwerem.

Po ponownym zalogowaniu, należy ponownie wywołać skrypt z flagą -i jako superużytkownik

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

Skrypt będzie kontynuował instalację oprogramowania w zależności od potrzeb i rozpocznie pobieranie obrazów poszczególnych serwisów i ich konfigurację.

W pewnym momencie w terminalu pojawią się informacje podobne do tych zamieszczonych poniżej



UWAGA!
Są to najważniejsze klucze oraz główny token do serwisu Vault. Powyższe informacje należy przechowywać w bezpiecznym miejscu. Utrata kluczy uniemożliwi restartowanie serwisu, zaś utrata tokenu uniemożliwi zalogowanie do serwisu Vault oraz administrowanie nim.

Odzyskanie kluczy oraz root tokenu jest niemożliwe.

Po co te klucze?

Vault podczas inicjalizacji tworzy tzw. *master key*, którym szyfruje wszystkie swoje dane. *Master key* dzielony jest domyślnie na 5 mniejszych kluczy, które należy przechowywać bezpiecznie. Użycie 3 z 5 kluczy pozwala na odtworzenie całego *master key*, a co za tym idzie - pozwala na korzystanie z Vaulta po restarcie.

Klucz *master key* jest ulotny i nie jest on nigdzie zapisany. Dlatego Vault po restarcie, albo po manualnym związaniu, nie jest w stanie rozszyfrować swoich danych, a co za tym idzie - niemożliwe jest korzystanie z niego.

Po skopiowaniu wyświetlonych informacji i zapisaniu ich w bezpiecznym miejscu, możemy kontynuować proces inicjalizacji wciskając dowolny przycisk.

Kolejnym krokiem wykonywanym przez skrypt, który wymaga ingerencji użytkownika jest podanie hasła jakim zostanie zabezpieczony certyfikat serwera Vault. Hasło należy zapamiętać, gdyż jest ono niezbędne przy restartach.

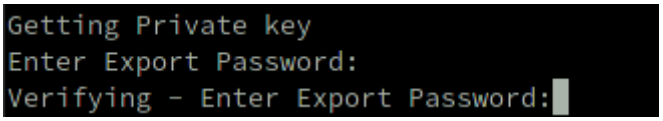
```
Provide password for a new vault certificate:
Type again to confirm:
```

W przedostatnim kroku, skrypt rozpocznie generowanie certyfikatu dla serwera proxy. W zależności od potrzeb, można podać wskazane informację, lecz nie mają one wpływu na dalsze działanie aplikacji.

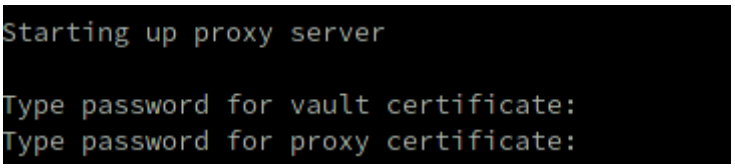
```
.........................................++++
...++++
e is 65537 (0x010001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can 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 []:
```

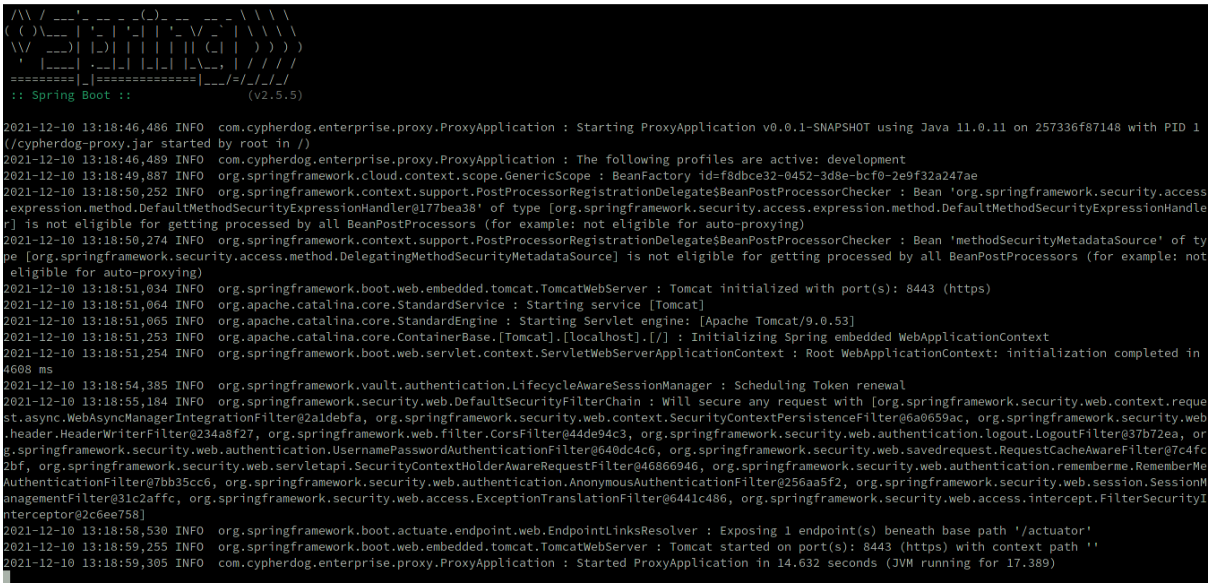
Ostatnim krokiem jest podanie hasła, jakim ma zostać zaszyfrowany klucz prywatny. Zalecane jest, aby to hasło różniło się od hasła, jakim został zaszyfrowany certyfikat Vaulta. Hasło należy zapamiętać, gdyż będzie niezbędne przy każdym uruchomieniu proxy.



Tym samym proces inicjalizacji został zakończony i skrypt rozpocznie proces uruchamiania serwera proxy. Zostaniemy poproszeni o podanie haseł do certyfikatów Vault oraz proxy

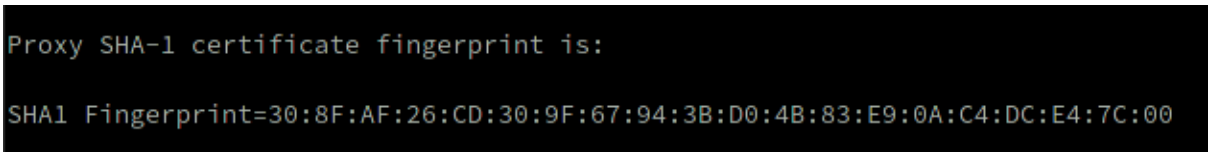


Po pobraniu przez dockera obrazu serwera proxy w terminalu powinny wyświetlić się logi podobne do tych poniżej



Są to logi pochodzące bezpośrednio z kontenera, w którym znajduje się serwer proxy. Jeśli nie widać żadnych błędów, oznacza to, że proces inicjalizacji i uruchomienia przebiegł pomyślnie. Aby opuścić te logi i zakończyć proces instalacji, należy kolejno użyć następujących kombinacji przycisków: **Ctrl + P** a następnie **Ctrl + Q**.

Na końcu zostanie wyświetlony odcisk palca SHA-1 certyfikatu serwera proxy.



Tym samym, proces instalacji, inicjalizacji oraz uruchomienia dobiegł do końca, a serwisy Vault oraz proxy są gotowe do użycia

3. Obsługa

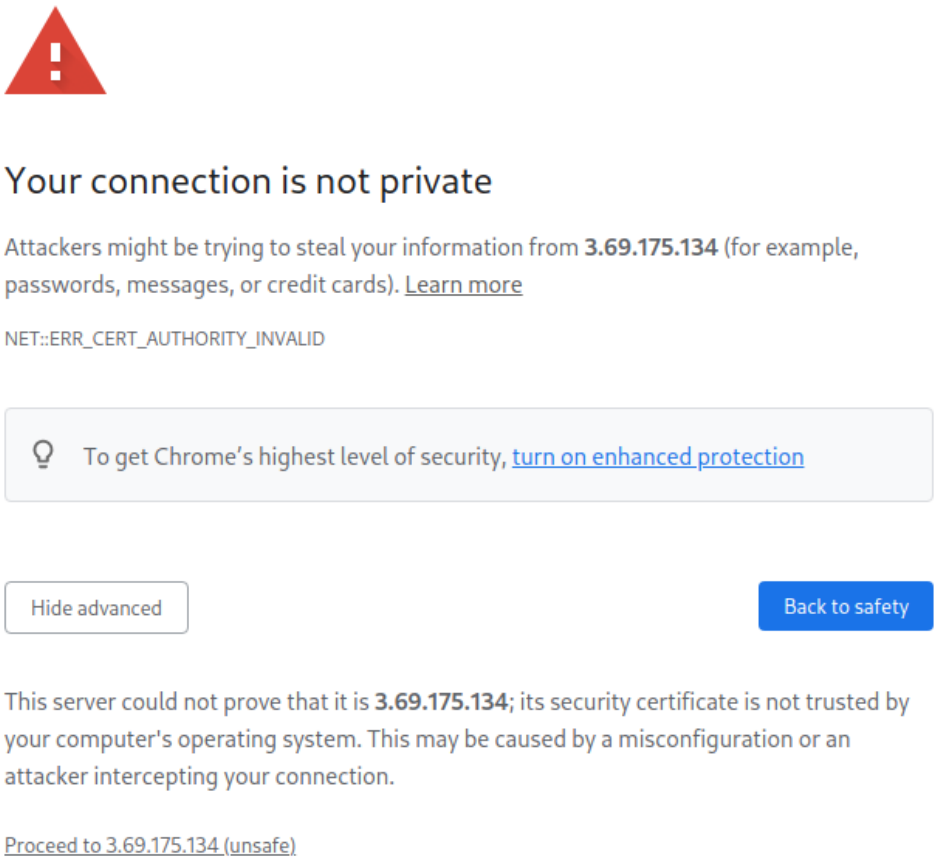
Serwis proxy zostanie uruchomiony na porcie **443** (**HTTPS**), zaś Vault na porcie **8200**. Do podstawowej obsługi tych serwisów może zostać użyta dowolna przeglądarka internetowa.

3.1. Logowanie do Vault

Aby otworzyć panel Vault'a należy w przeglądarce wpisać następujący adres:

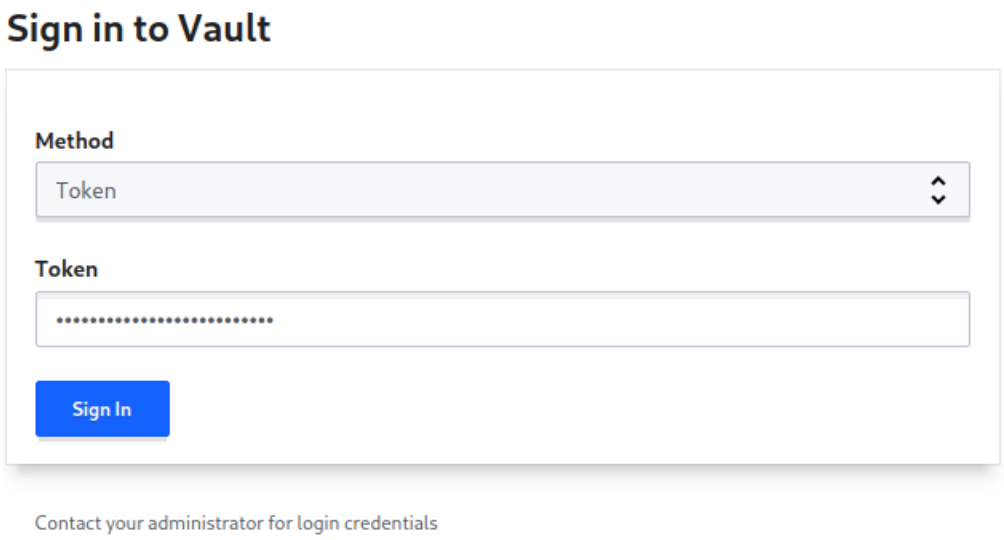
```
https://<adres_ip_serwera>:8200/
```

Prawdopodobnie pierwszą rzeczą jaka się ukaże, jest informacja o błędnym certyfikacie. Jest to normalna sytuacja, ponieważ certyfikat podpięty do serwisu Vault nie został wytworzony przez żadne autoryzowane CA, lecz został utworzony przez użytkownika w momencie przeprowadzania inicjalizacji serwisu Vault.



Należy kontynuować przejście pod wskazany adres.

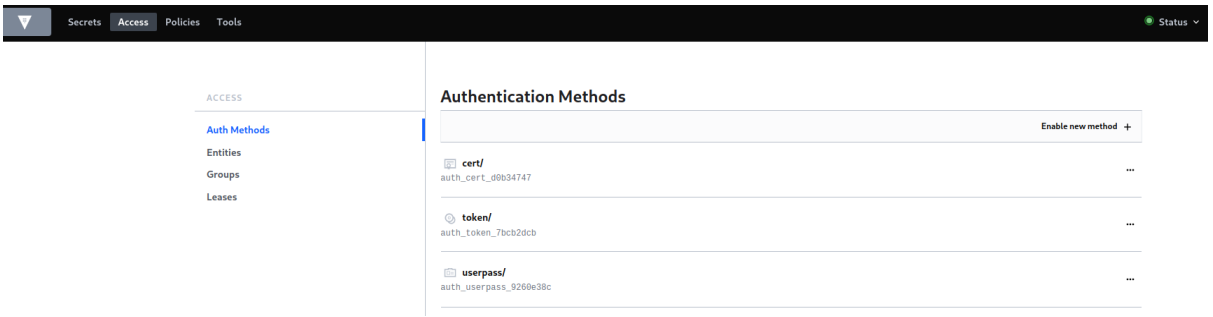
W tym momencie w przeglądarce zostanie wyświetlony panel logowania do Vault'a. Aby uzyskać dostęp, należy wybrać metodę **Token** i podać root token, który został wygenerowany podczas inicjalizacji Vault'a.



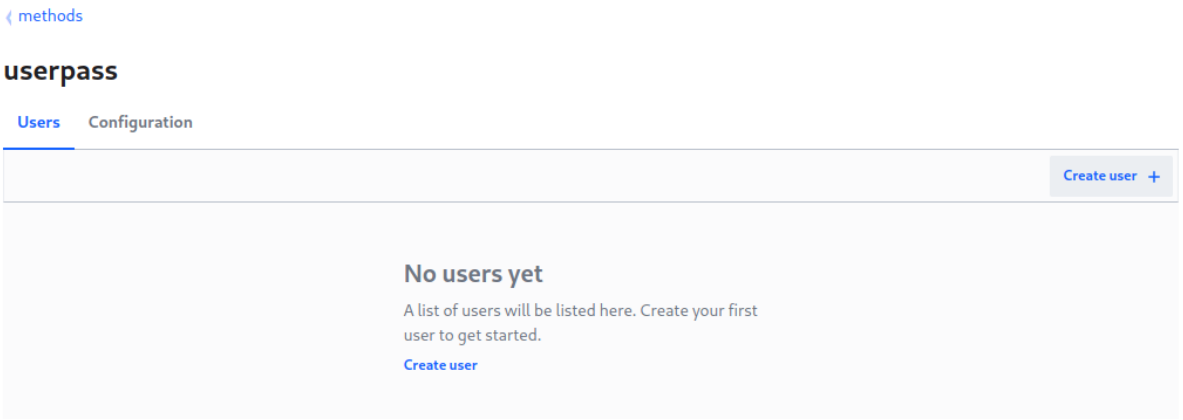
3.2. Tworzenie kont administratorów

Głównym zadaniem administratora posiadającego root token, powinno być tworzenie kont dla innych administratorów, którzy mają mieć uprawnienia do tworzenia jednorazowych tokenów dla użytkowników Cypherdog Enterprise, chcących przywrócić backup swojego klucza.

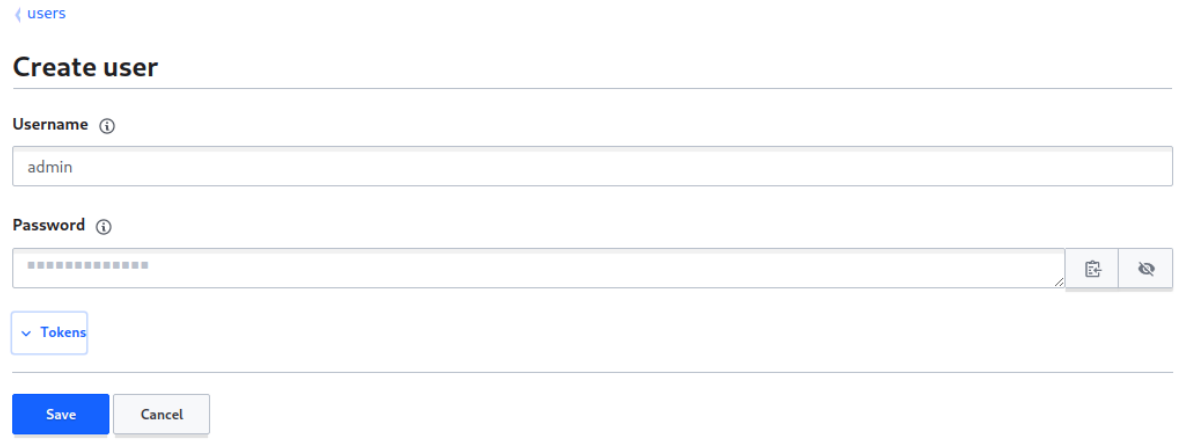
Aby utworzyć takie konto, należy przejść do zakładki *Access* a następnie wybrać **userpass/**



Następnie należy nacisnąć opcję **Create new user +**

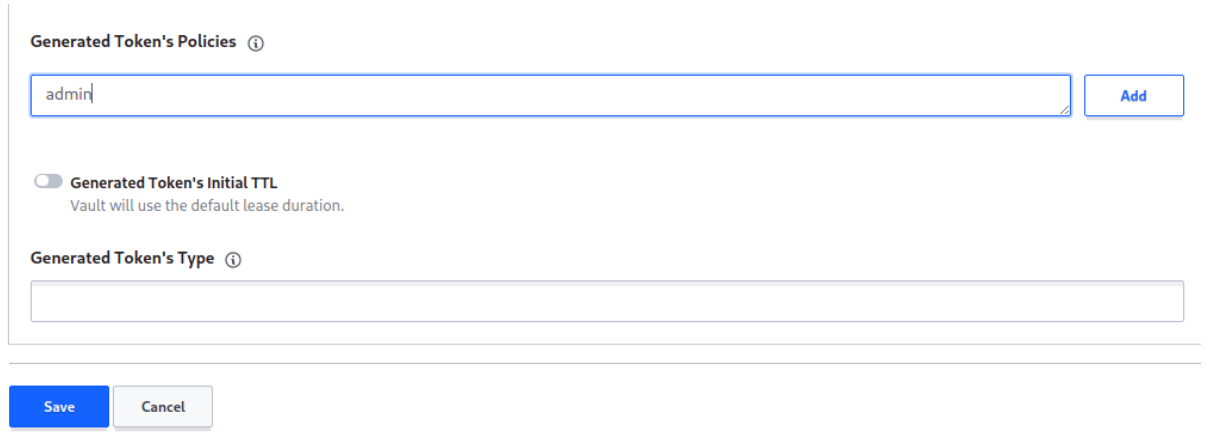


Teraz należy wypełnić formularz podając login oraz hasło, jakim administrator ma się posługiwać.



Kolejnym krokiem jest rozwinięcie **Tokens** i nadanie odpowiedniej roli administratorowi. Aby to uczynić, należy w polu **Generated Token's Policies** wpisać **admin**.

Bez podania tej wartości, konto administratora będzie bezużyteczne.



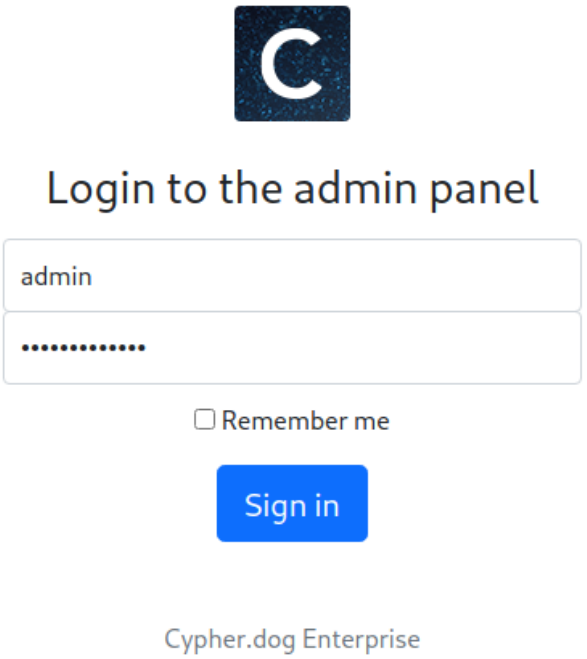
Teraz należy zapisać zmiany wciskając przycisk **Save**. Login oraz hasło powinny zostać przekazane administratorowi w bezpieczny sposób.

3.3. Tworzenie jednorazowych tokenów

Aby otworzyć panel umożliwiający generowanie tokenów, należy podać w przeglądarce następujący adres:

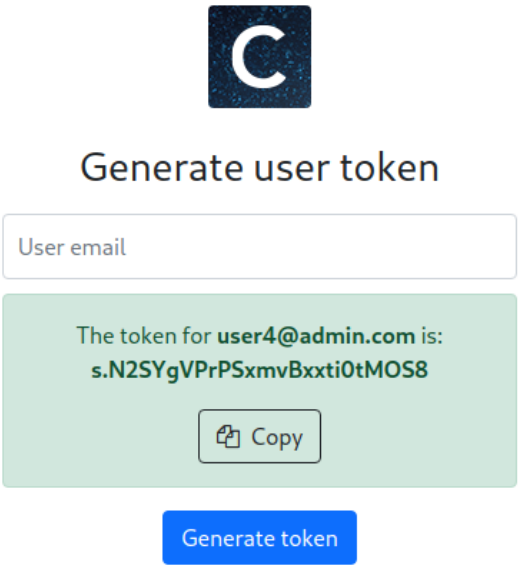
```
https://<adres_ip_serwera>/
```

Podobnie jak w przypadku wejścia na adres pod którym znajduję się panel Vault'a, otrzymamy informację o błędnym certyfikacie. Tak samo jak w poprzednim przypadku, należy kontynuować przejście pod wskazany adres.



Aby się zalogować, należy skorzystać z danych konta utworzonego w Tworzenie kont administratorów.

Następnie należy podać adres email użytkownika, który chce uzyskać swój backup. Warunkiem koniecznym jest, aby użytkownik posiadał swój backup w Vault. Bez tego, wygenerowanie tokenu nie będzie możliwe.



Tak wygenerowany token należy przekazać użytkownikowi. Token jest jednorazowy i pozwoli na przywrócenie backupu jedynie użytkownikowi ze wskazanym adresem email.