



Cypherdog Enterprise

Instalacja serwisów proxy oraz HashiCorp Vault na serwerze Linux Ubuntu

| | |
|---------------------------------|----------|
| Ogólne informacje | 3 |
| Instalacja | 3 |
| Pobranie skryptu | 3 |
| Nadanie flagi wykonywalności | 3 |
| Dostępne komendy | 3 |
| Omówienie poszczególnych flag | 3 |
| Inicjalizacja | 4 |
| Obsługa | 8 |
| Logowanie do Vault | 8 |
| Tworzenie kont administratorów | 10 |
| Tworzenie jednorazowych tokenów | 12 |

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.

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

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 libxxf86dgal 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

```
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:~$ █
```

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

```
Unseal Key 1: bJzvFt9z+VFbgt22ayZeUwH5zGPNq2RjXkMY0EU3404Y
Unseal Key 2: snnRxaBkhPGmF2xnDkZnw/q9aLUM6YRK9UtlWziKKYk
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
█
```

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.

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

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

```
Starting up proxy server
Type password for vault certificate:
Type password for proxy certificate:
```

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

```

  ____ _
 / ___| | | | |
 \___ \| |_| | | |
  ___) | | | | | |
 |___) | | | | | |
      |_| |_| |_|_|_|
:: 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=f8dbc32-0452-3d8e-bcf0-2e9f32a247ae
2021-12-10 13:18:50,252 INFO org.springframework.context.support.PostProcessorRegistrationDelegate$BeanPostProcessorChecker : Bean 'org.springframework.security.access.expression.method.DefaultMethodSecurityExpressionHandler@177bea38' of type [org.springframework.security.access.expression.method.DefaultMethodSecurityExpressionHandler] is not eligible for getting processed by all BeanPostProcessors (for example: not eligible for auto-proxying)
2021-12-10 13:18:50,274 INFO org.springframework.context.support.PostProcessorRegistrationDelegate$BeanPostProcessorChecker : Bean 'methodSecurityMetadataSource' of type [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.request.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@837b72ea, org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@6460dc4c6, org.springframework.security.web.savedrequest.RequestCacheAwareFilter@7c4fc2bf, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@46866946, org.springframework.security.web.authentication.rememberme.RememberMeAuthenticationFilter@7bb35cc6, org.springframework.security.web.authentication.AnonymousAuthenticationFilter@256aa5f2, org.springframework.security.web.session.SessionManagementFilter@31c2affc, org.springframework.security.web.access.ExceptionTranslationFilter@6441c486, org.springframework.security.web.access.intercept.FilterSecurityInterceptor@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)

```

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.

```
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
```

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 podpisany do serwisu Vault nie został wytworzony przez żadne autoryzowane CA, lecz został utworzony przez użytkownika w momencie przeprowadzania inicjalizacji serwisu Vault.



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](#)

Hide advanced

Back to safety

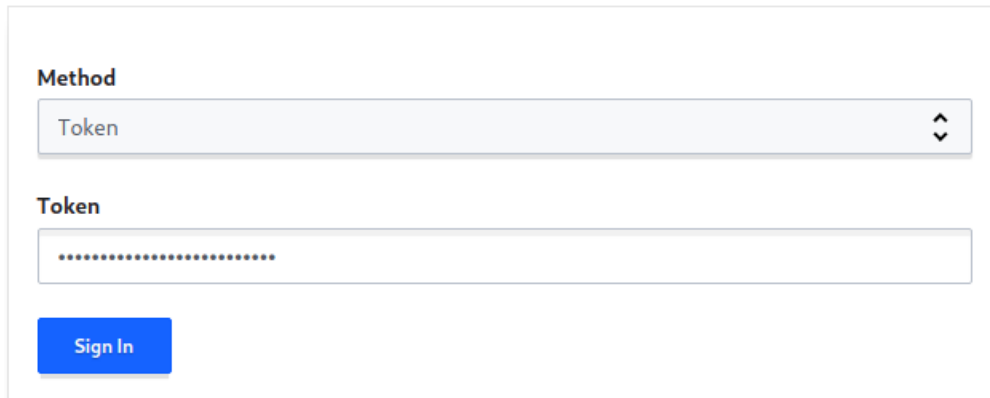
This server could not prove that it is **3.69.175.134**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 3.69.175.134 \(unsafe\)](#)

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.

Sign in to Vault



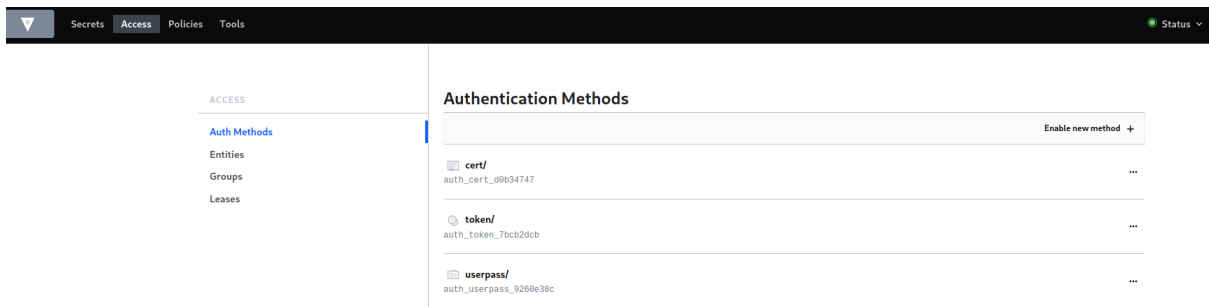
The image shows a web form titled "Sign in to Vault". It contains a dropdown menu labeled "Method" with "Token" selected. Below it is a text input field labeled "Token" containing a series of dots. At the bottom left of the form is a blue button labeled "Sign In".

Contact your administrator for login credentials

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 +**

[methods](#)

userpass

[Users](#) [Configuration](#)

[Create user +](#)

No users yet

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

[Create user](#)

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

[users](#)

Create user

Username ⓘ

Password ⓘ

▼ Tokens

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.

Generated Token's Policies ⓘ

Generated Token's Initial TTL
Vault will use the default lease duration.

Generated Token's Type ⓘ

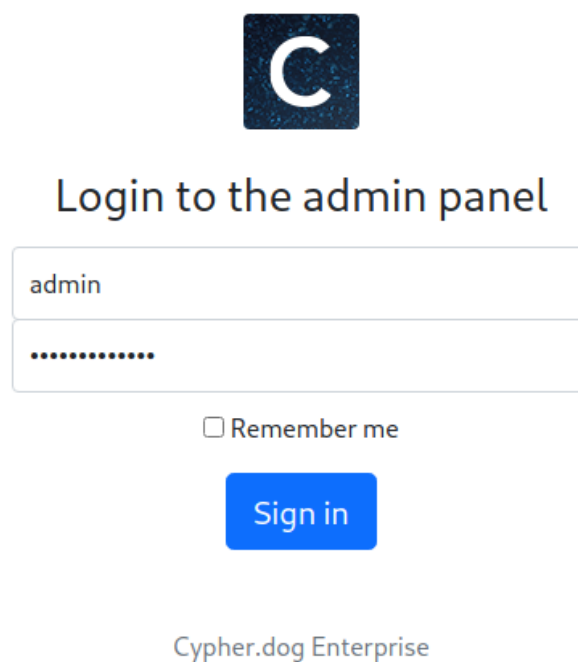
Teraz należy zapisać zmiany wciskając przycisk **Save**. Login oraz hasło powinny zostać przekazane administratorowi w bezpieczny sposób.

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



admin

.....

Remember me

Sign in

Cypher.dog Enterprise


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.



Generate user token

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

 Copy

Generate token

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