Projekt: Zdalny Dostęp do Terminali przez przeglądarke

1. Cel Projektu

Projekt umożliwia zdalny dostęp do terminali dwóch maszyn (Debian i Rocky Linux) poprzez przeglądarkę internetową. Dostęp jest zabezpieczony mechanizmem uwierzytelniania opartym o OIDC (OpenID Connect) z wykorzystaniem serwera Keycloak. Po zalogowaniu użytkownik trafia do strony wyboru, gdzie wybiera maszynę, z którą chce się połączyć (Debian lub Rocky Linux). Terminale udostępniane są za pomocą narzędzia ttyd, a cały ruch kierowany jest przez Nginx działający jako reverse proxy.

---

2. Zastosowane Technologie

Frontend

- **HTML, CSS, JavaScript**
  Strony logowania oraz wyboru terminala (choose.php) są napisane w HTML i stylizowane przy użyciu CSS. Animacja unoszącego się nagłówka dodaje interaktywności oraz nowoczesnego wyglądu.

Backend

- **PHP**
  Skrypty PHP, takie jak login.php, auth_check.php, choose.php oraz logout.php, zarządzają logiką uwierzytelniania, obsługą sesji użytkowników oraz przekierowywaniem.

- **OIDC (OpenID Connect)**
  Uwierzytelnianie jest realizowane przy użyciu biblioteki PHP (np. Jumbojett\OpenIDConnectClient), która inicjuje przepływ OIDC, przekierowując użytkownika do serwera Keycloak.

Uwierzytelnianie

- **Keycloak Server**
  Serwer Keycloak służy do zarządzania użytkownikami oraz procesem autoryzacji. Po poprawnym uwierzytelnieniu użytkownik otrzymuje token, który jest zapisywany w sesji PHP, umożliwiając dostęp do zabezpieczonych zasobów.

Keycloak Deployment:
Kluczowy serwer uwierzytelniania jest uruchomiony jako kontener Docker, zarządzany przy użyciu docker-compose. Konfiguracja docker-compose obejmuje usługi Keycloak, PostgreSQL (jako bazę danych) oraz Nginx. Dzięki temu wdrożenie jest łatwe w utrzymaniu, skalowalne oraz umożliwia szybkie aktualizacje. Pełna konfiguracja docker-compose znajduje się w osobnym pliku.

Serwer WWW i Reverse Proxy

- **Nginx**
  Nginx pełni rolę serwera WWW oraz reverse proxy. Ruch z internetu jest kierowany na odpowiednie ścieżki:
  - Na „/" – do strony logowania.
  - Na „/debian/" – do ttyd działającego na maszynie Debian (IP: 10.0.0.4, port: 7681).
  - Na „/rocky/" – do ttyd działającego na maszynie Rocky Linux (IP: 10.0.0.10, port: 7681).
    Konfiguracja zawiera mechanizm auth_request, który sprawdza, czy użytkownik posiada aktywną sesję, oraz obsługę WebSocket dzięki ustawieniom proxy_set_header Upgrade oraz Connection.

Terminal w Przeglądarce

- **ttyd**
  Narzędzie ttyd umożliwia udostępnienie terminala w przeglądarce. Na obu maszynach (Debian oraz Rocky Linux) ttyd jest uruchamiany na porcie LAN (np. 7681), a dostęp do niego jest możliwy dzięki reverse proxy Nginx.

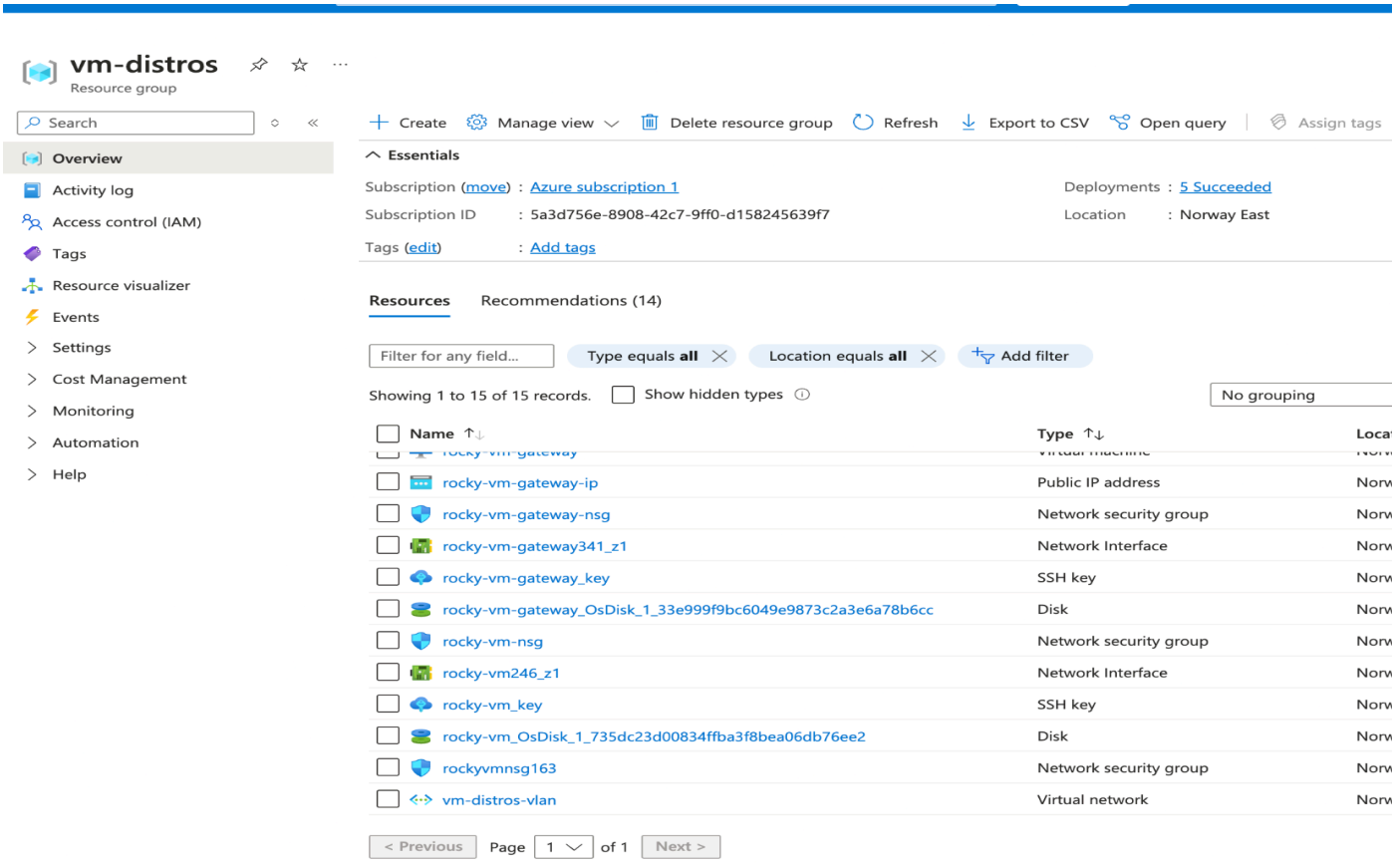
Certyfikaty SSL

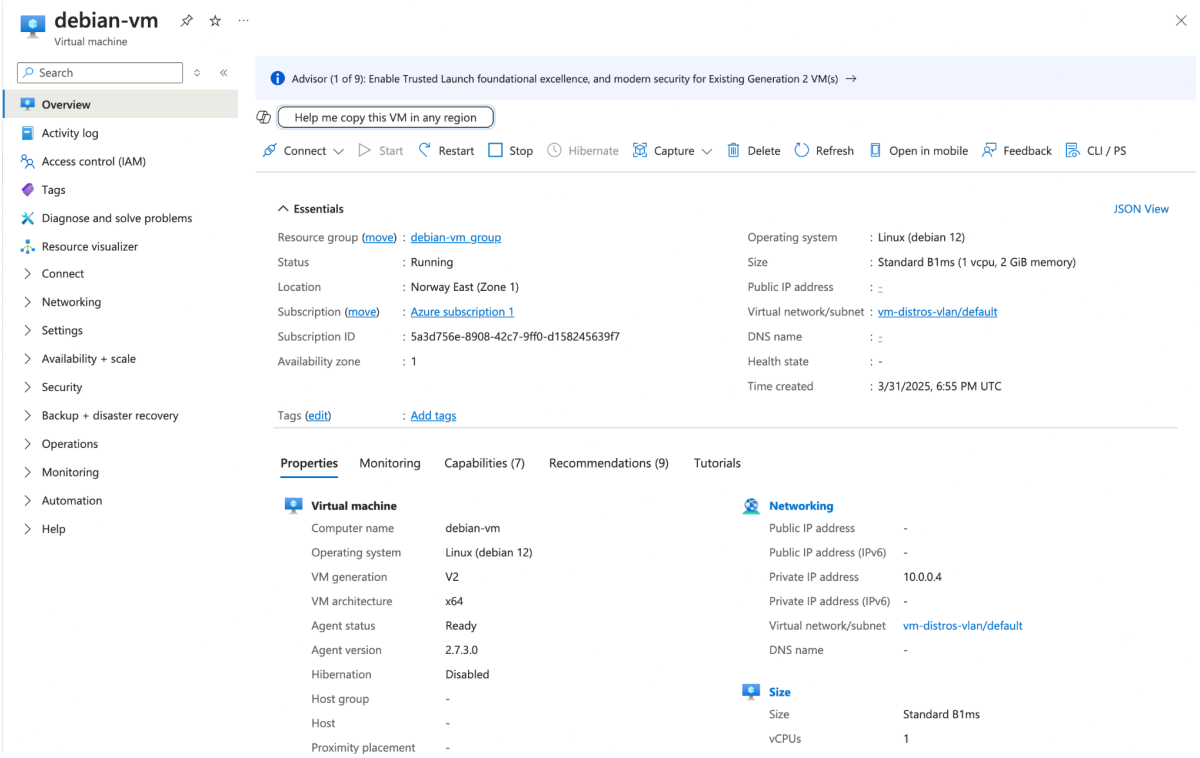
- **Certbot / Let's Encrypt**
  Certbot generuje certyfikaty SSL dla domeny, co umożliwia bezpieczny dostęp przez HTTPS.

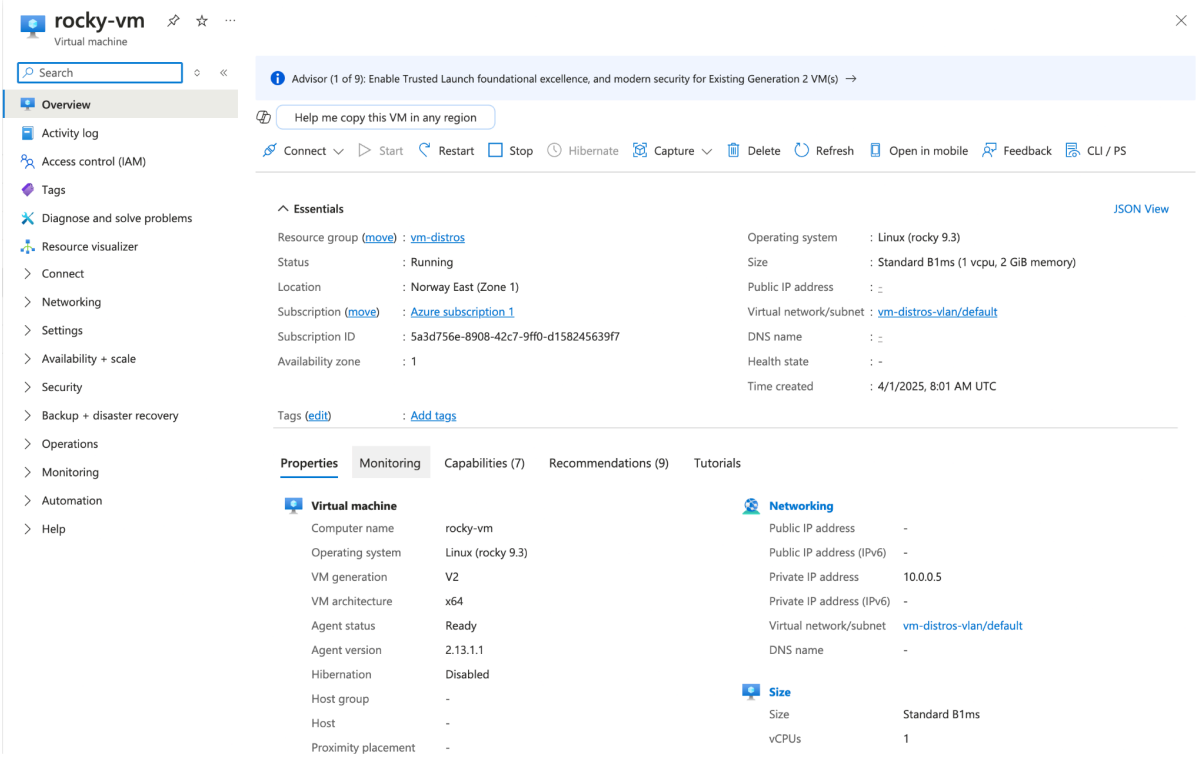
Infrastruktura Chmurowa

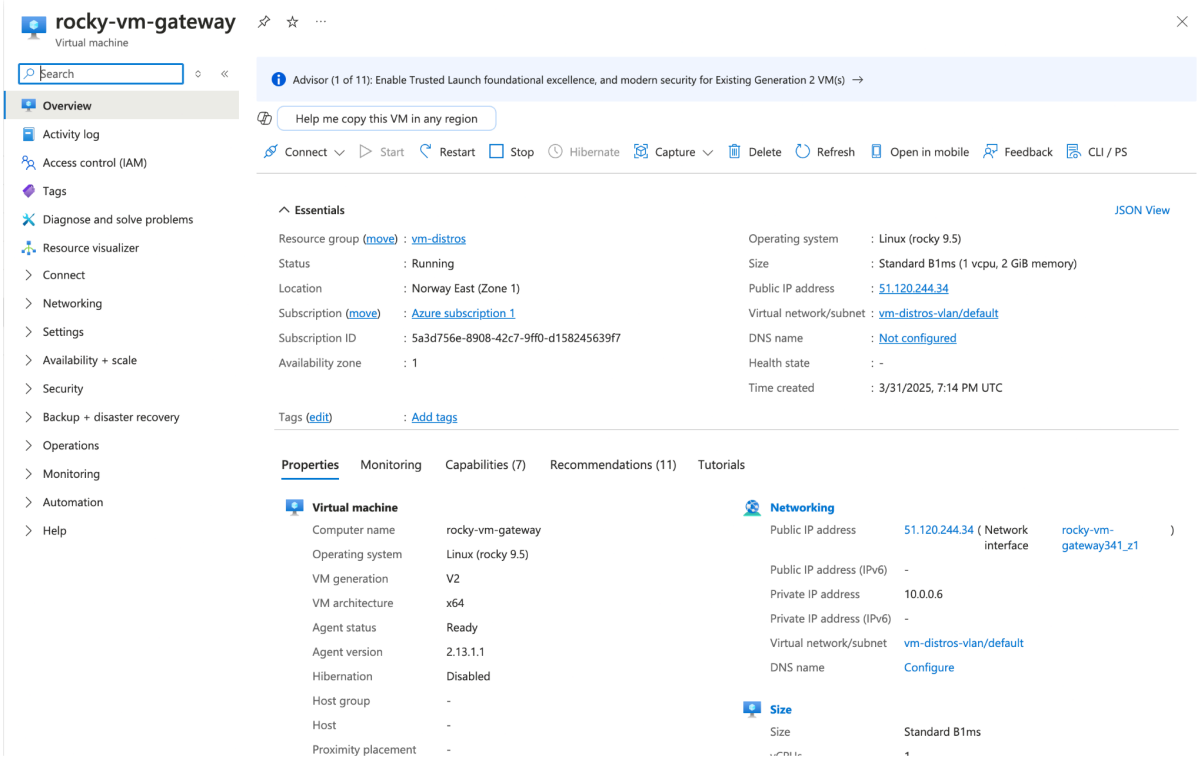
- **Microsoft Azure**

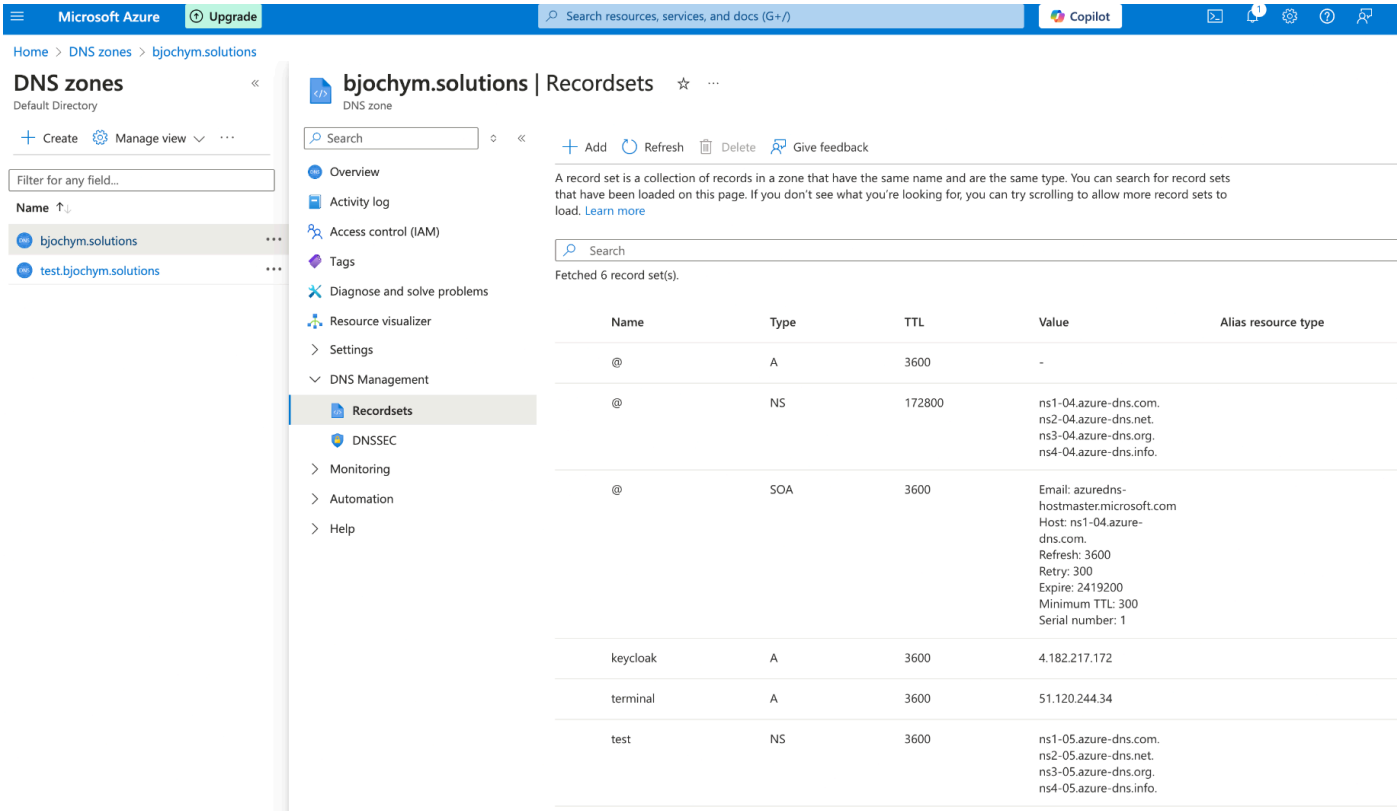
- **Maszyny Wirtualne:** Maszyny (Debian i Rocky Linux) są tworzone jako VM w ramach Azure.
- **Resource Groups:** Wszystkie zasoby (maszyny, sieci, adresy IP) są zarządzane w dedykowanych grupach zasobów.
- **Virtual Networks:** Maszyny wirtualne są połączone w prywatnej sieci (VNet) o podsieci 10.0.0.0/24.
- **Publiczny Adres IP i DNS:** Publiczny adres IP jest przypisany do gateway'a, a zarządzanie rekordami DNS odbywa się przy użyciu Azure. Domena została wykupiona u GoDaddy i skonfigurowana w Azure w celu zarządzania rekordami.




debian-vm
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Advisor (1 of 9): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s) →
Help me copy this VM in any region
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : debian-vm_group
Status : Running
Location : Norway East (Zone 1)
Subscription (move) : Azure subscription 1
Subscription ID : 5a3d756e-8908-42c7-9ff0-d158245639f7
Availability zone : 1
Operating system : Linux (debian 12)
Size : Standard B1ms (1 vcpu, 2 GiB memory)
Public IP address : -
Virtual network/subnet : vm-distros-vlan/default
DNS name : -
Health state : -
Time created : 3/31/2025, 6:55 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (7)
Recommendations (9)
Tutorials
Virtual machine
Computer name debian-vm
Operating system Linux (debian 12)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.7.3.0
Hibernation Disabled
Host group -
Host -
Proximity placement -
Networking
Public IP address -
Public IP address (IPv6) -
Private IP address 10.0.0.4
Private IP address (IPv6) -
Virtual network/subnet vm-distros-vlan/default
DNS name -
Size
Size Standard B1ms
vCPUs 1


rocky-vm
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Advisor (1 of 9): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s) →
Help me copy this VM in any region
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : vm-distros
Status : Running
Location : Norway East (Zone 1)
Subscription (move) : Azure subscription 1
Subscription ID : 5a3d756e-8908-42c7-9ff0-d158245639f7
Availability zone : 1
Operating system : Linux (rocky 9.3)
Size : Standard B1ms (1 vcpu, 2 GiB memory)
Public IP address : -
Virtual network/subnet : vm-distros-vlan/default
DNS name : -
Health state : -
Time created : 4/1/2025, 8:01 AM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (7)
Recommendations (9)
Tutorials
Virtual machine
Computer name rocky-vm
Operating system Linux (rocky 9.3)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.13.1.1
Hibernation Disabled
Host group -
Host -
Proximity placement -
Networking
Public IP address -
Public IP address (IPv6) -
Private IP address 10.0.0.5
Private IP address (IPv6) -
Virtual network/subnet vm-distros-vlan/default
DNS name -
Size
Size Standard B1ms
vCPUs 1


rocky-vm-gateway
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Monitoring
Automation
Help
Advisor (1 of 11): Enable Trusted Launch foundational excellence, and modern security for Existing Generation 2 VM(s)
Help me copy this VM in any region
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Refresh
Open in mobile
Feedback
CLI / PS
Essentials
JSON View
Resource group (move) : vm-distros
Status : Running
Location : Norway East (Zone 1)
Subscription (move) : Azure subscription 1
Subscription ID : 5a3d756e-8908-42c7-9ff0-d158245639f7
Availability zone : 1
Operating system : Linux (rocky 9.5)
Size : Standard B1ms (1 vcpu, 2 GiB memory)
Public IP address : 51.120.244.34
Virtual network/subnet : vm-distros-vlan/default
DNS name : Not configured
Health state : -
Time created : 3/31/2025, 7:14 PM UTC
Tags (edit) : Add tags
Properties
Monitoring
Capabilities (7)
Recommendations (11)
Tutorials
Virtual machine
Computer name rocky-vm-gateway
Operating system Linux (rocky 9.5)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.13.1.1
Hibernation Disabled
Host group -
Host -
Proximity placement -
Networking
Public IP address 51.120.244.34 (Network interface rocky-vm-gateway341_z1)
Public IP address (IPv6) -
Private IP address 10.0.0.6
Private IP address (IPv6) -
Virtual network/subnet vm-distros-vlan/default
DNS name Configure
Size
Size Standard B1ms


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
Home > DNS zones > bjochym.solutions
DNS zones
Default Directory
Create
Manage view
Filter for any field...
Name
bjochym.solutions
test.bjochym.solutions
bjochym.solutions | Recordsets
DNS zone
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
DNS Management
Recordsets
DNSSEC
Monitoring
Automation
Help
Add
Refresh
Delete
Give feedback
A record set is a collection of records in a zone that have the same name and are the same type. You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load. Learn more
Search
Fetched 6 record set(s).
Name
Type
TTL
Value
Alias resource type
@ A 3600 -
@ NS 172800 ns1-04.azure-dns.com. ns2-04.azure-dns.net. ns3-04.azure-dns.org. ns4-04.azure-dns.info.
@ SOA 3600 Email: azuredns-hostmaster.microsoft.com Host: ns1-04.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
keycloak A 3600 4.182.217.172
terminal A 3600 51.120.244.34
test NS 3600 ns1-05.azure-dns.com. ns2-05.azure-dns.net. ns3-05.azure-dns.org. ns4-05.azure-dns.info.

3. Architektura i Przepływ Danych

Logowanie i Uwierzytelnianie

1. **Wejście na stronę:**
   Użytkownik wchodzi na adres `https://terminal.bjochym.solutions`. Strona główna wyświetla statyczną stronę logowania (login.html).

2. **Proces logowania:**
   Po kliknięciu przycisku „Zaloguj się” użytkownik trafia do skryptu PHP (`login.php`), który inicjuje przepływ OIDC. Użytkownik zostaje przekierowany do serwera Keycloak, gdzie podaje dane logowania. Po udanym uwierzytelnieniu Keycloak przekierowuje użytkownika z powrotem do witryny, a PHP zapisuje dane sesji.

3. **Strona wyboru:**
   Użytkownik trafia na stronę `choose.php`, gdzie ma do wyboru dwa przyciski:

   - **Debian TTYD:** Kliknięcie przekierowuje do `/debian/`, a Nginx proxy’uje ruch do ttyd na maszynie Debian (IP: 10.0.0.4, port: 7681).

   - **Rocky Linux TTYD:** Kliknięcie przekierowuje do `/rocky/`, a Nginx kieruje ruch do ttyd na maszynie Rocky Linux (IP: 10.0.0.10, port: 7681).

Przekierowanie Ruchu przez Nginx

- **Reverse Proxy:**
  Nginx przekierowuje żądania na ścieżkach `/debian/` oraz `/rocky/` do odpowiednich maszyn w sieci LAN.

- **WebSocket:**
  Dzięki odpowiednim nagłówkom (Upgrade i Connection) ttyd komunikuje się z przeglądarką w czasie rzeczywistym.

- **Auth_request:**
  Mechanizm auth_request sprawdza za pomocą skryptu PHP (`auth_check.php`), czy użytkownik posiada aktywną sesję. W przypadku braku autoryzacji następuje przekierowanie do strony logowania.

Wylogowanie

- **Wylogowanie:**
  Na stronie `choose.php` znajduje się przycisk „Wyloguj się”, który kieruje do skryptu

`logout.php`.

- **Skrypt logout.php:**
  Skrypt usuwa dane sesji PHP (oraz opcjonalnie przekierowuje do Keycloak, aby zakończyć sesję na poziomie uwierzytelniania). W wyniku tego użytkownik traci dostęp do zabezpieczonych zasobów i przy kolejnym wejściu musi ponownie się zalogować, co zwiększa bezpieczeństwo.

---

4. Podsumowanie

Projekt łączy technologie webowe (HTML, CSS, PHP, OIDC), narzędzia terminalowe (ttyd) oraz infrastrukturę chmurową Azure. Kluczowe elementy rozwiązania obejmują:

- **Bezpieczne uwierzytelnianie** przy użyciu serwera Keycloak oraz PHP OIDC.

- **Reverse Proxy Nginx** z obsługą WebSocket i mechanizmem auth_request, które kierują ruch do ttyd na maszynach w prywatnej sieci.

- **Infrastrukturę Azure**: maszyny wirtualne, Virtual Networks, publiczny adres IP oraz zarządzanie rekordami DNS (domena wykupiona u GoDaddy i skonfigurowana w Azure).

- **Udostępnienie terminali** za pomocą ttyd działających na prywatnych adresach IP (10.0.0.4 dla Debiana i 10.0.0.10 dla Rocky Linux), które dzięki Nginx stają się dostępne z Internetu.

- **Proces wylogowania**, który usuwa sesję użytkownika, zabezpieczając system poprzez wymuszenie ponownego logowania.