

# Bezpieczeństwo rozwiązań chmurowych

Dokumentacja wdrożenia aplikacji WWW

„Event Planner” (AWS, zakres do oceny 3.5)

Autorzy:

Grzegorz Latawiec 169576

Igor Guła 169784

Wiktoria Bzduń 169766

4 stycznia 2026

# Spis treści

<b>1 Cel i zakres</b>	<b>2</b>
<b>2 Założenia środowiska</b>	<b>2</b>
<b>3 Opis architektury rozwiązania</b>	<b>3</b>
3.1 Przepływy ruchu . . . . .	3
<b>4 Zarządzanie dostępem (IAM)</b>	<b>4</b>
<b>5 Bezpieczeństwo sieci (Security Groups oraz host firewall)</b>	<b>5</b>
<b>6 Segmentacja sieci (etap 3.5)</b>	<b>6</b>
6.1 Podsieci (Subnets) . . . . .	6
6.2 Routing: Internet Gateway oraz NAT Gateway . . . . .	7
<b>7 Warstwa dostępu: Bastion Host</b>	<b>8</b>
<b>8 Warstwa dostępu: Application Load Balancer</b>	<b>10</b>
8.1 Izolacja serwera aplikacyjnego . . . . .	11
<b>9 Konfiguracja usługi WWW na serwerze aplikacyjnym (Nginx)</b>	<b>12</b>
<b>10 Monitoring (Amazon CloudWatch)</b>	<b>13</b>
<b>11 Wnioski</b>	<b>13</b>

## 1 Cel i zakres

Celem pracy było przygotowanie środowiska chmurowego umożliwiającego uruchomienie prostej aplikacji WWW do planowania wydarzeń oraz wdrożenie podstawowych mechanizmów bezpieczeństwa. Zakres obejmuje:

- zarządzanie dostępem (konto nieuprzywilejowane, ograniczenie użycia konta root),
- ograniczenie ekspozycji usług poprzez reguły sieciowe,
- dokumentację wykonanych czynności wraz z dowodami w postaci zrzutów ekranu,
- segmentację sieci (podział na podsieć publiczną i prywatną) oraz pośrednie warstwy dostępu (Bastion Host, Application Load Balancer),
- podstawowy monitoring (CPU, ruch sieciowy) w CloudWatch.

## 2 Założenia środowiska

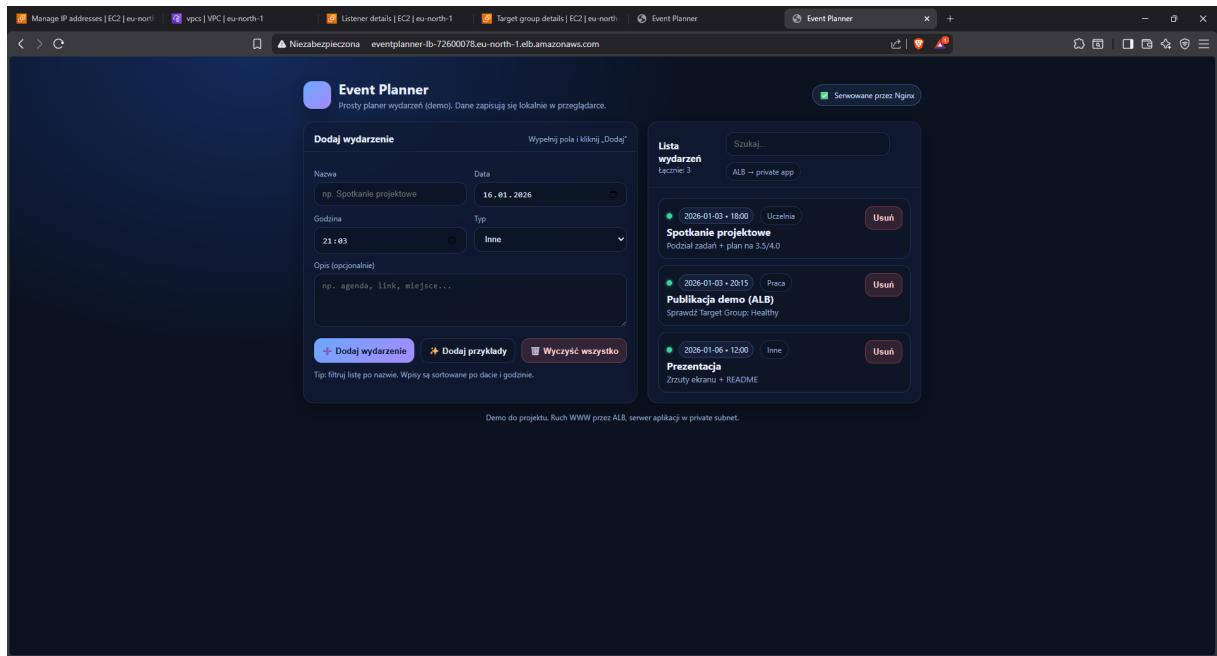
Wdrożenie zrealizowano w usługach Amazon Web Services. Aplikacja ma formę statycznej strony WWW serwowanej przez Nginx na instancji EC2. Dostęp publiczny do aplikacji realizowany jest przez Application Load Balancer, natomiast dostęp administracyjny (SSH) wyłącznie przez Bastion Host. Zastosowano zasadę minimalnych uprawnień w IAM oraz ograniczono otwarte porty do niezbędnych.

### 3 Opis architektury rozwiązania

Architektura została oparta o sieć VPC z podsiecią publiczną oraz prywatną. W podsieci prywatnej umieszczono serwer aplikacyjny EC2 bez publicznego adresu IP. W podsieci publicznej umieszczono Bastion Host (dla SSH) oraz Application Load Balancer (dla HTTP). Dostęp wychodzący z podsieci prywatnej do internetu został zapewniony poprzez NAT Gateway, co umożliwia wykonywanie połączeń wychodzących bez wystawiania instancji na ruch przychodzący [3].

#### 3.1 Przepływy ruchu

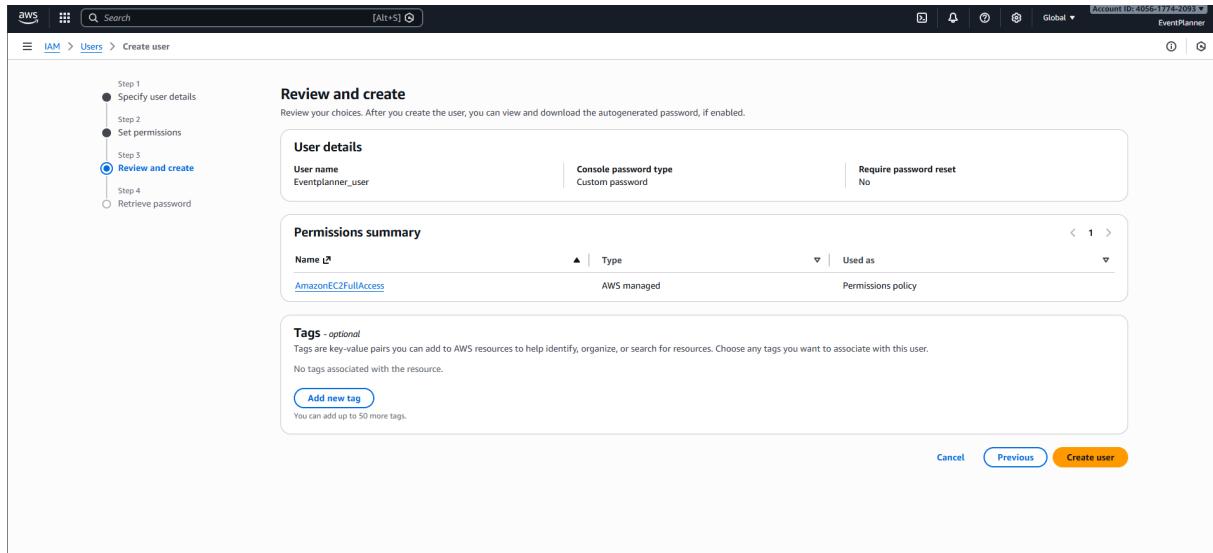
- **Ruch użytkowników (HTTP):** Internet → ALB → serwer aplikacyjny (EC2 w podsieci prywatnej).
- **Zarządzanie (SSH):** stacja robocza → Bastion Host (podsieć publiczna) → serwer aplikacyjny (podsieć prywatna).
- **Ruch wychodzący z podsieci prywatnej:** EC2 → NAT Gateway → Internet (np. aktualizacje systemu).



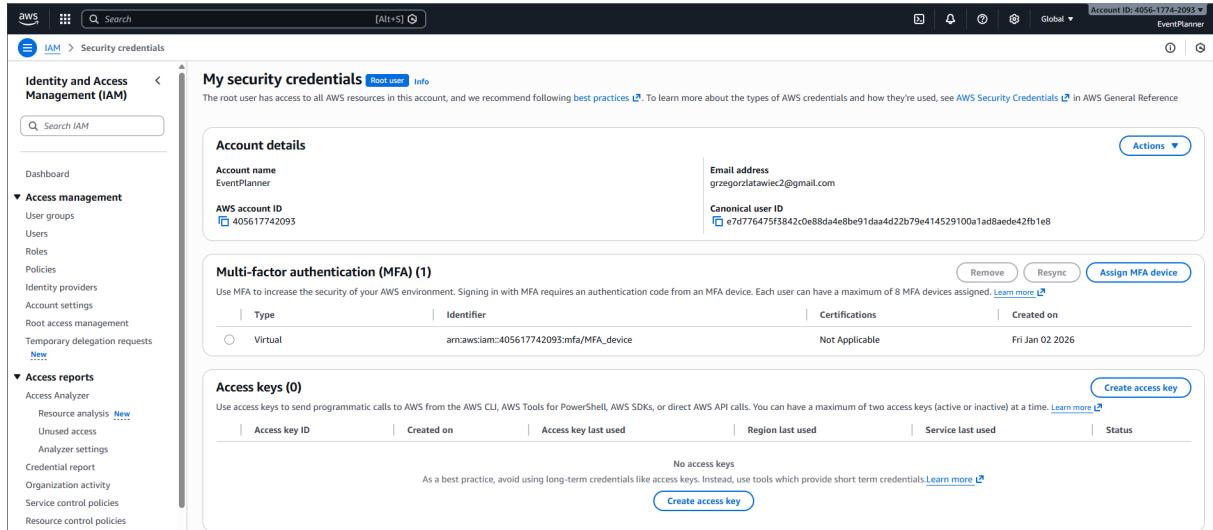
Rysunek 1: Dostęp do aplikacji „Event Planner” przez publiczny adres DNS Application Load Balancer.

## 4 Zarządzanie dostępem (IAM)

W ramach etapu bazowego utworzono dedykowanego użytkownika IAM wykorzystywanego do prac konfiguracyjnych, zgodnie z zasadą *least privilege* [1]. Ograniczono stosowanie konta root do czynności administracyjnych wymagających jego użycia, a dodatkowo włączono mechanizm uwierzytelniania wieloskładnikowego (MFA), co stanowi zalecaną praktykę dla zabezpieczenia konta [2].



Rysunek 2: Utworzenie dedykowanego użytkownika IAM do prac operacyjnych.



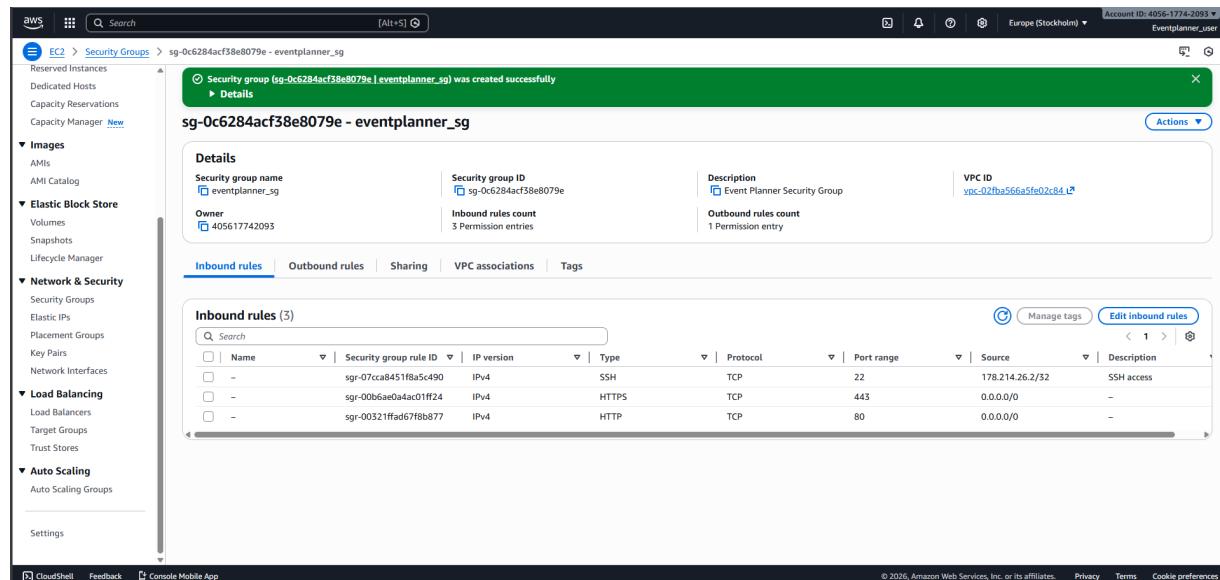
Rysunek 3: Konfiguracja MFA dla użytkownika root (widoczne potwierdzenie przypisanego urządzenia MFA).

## 5 Bezpieczeństwo sieci (Security Groups oraz host firewall)

Konfiguracja bezpieczeństwa sieciowego została zrealizowana w oparciu o *Security Groups*, które stanowią stanowe listy kontroli dostępu na poziomie instancji. Otworzono wyłącznie porty wymagane do działania systemu:

- port 80/tcp dla HTTP (dostęp do aplikacji przez ALB),
- port 22/tcp dla SSH (dostęp administracyjny ograniczony do źródła).

Dodatkowo na poziomie systemu operacyjnego wykorzystano `ufw` w celu wzmacniania ochrony hosta (zasada obrony w głębi, *defense in depth*). Przykładowy stan regułu `ufw` przedstawiono na rys. 5.



Rysunek 4: Reguły przychodzące w Security Group (SSH ograniczony do wskazanego adresu IP; ruch WWW na portach 80/443).

```
ubuntu@ip-172-31-47-160:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         --          --
22/tcp (OpenSSH)           ALLOW IN   Anywhere
80,443/tcp (Nginx Full)   ALLOW IN   Anywhere
22/tcp (OpenSSH (v6))      ALLOW IN   Anywhere (v6)
80,443/tcp (Nginx Full (v6)) ALLOW IN   Anywhere (v6)

ubuntu@ip-172-31-47-160:~$
```

Rysunek 5: Status zapory `ufw` na hoście (dodatkowa warstwa kontroli ruchu).

# 6 Segmentacja sieci (etap 3.5)

W etapie 3.5 wykonano segmentację sieci poprzez umieszczenie serwera aplikacyjnego w podsieci prywatnej bez bezpośredniego dostępu przychodzącego z internetu. Podejście to ogranicza powierzchnię ataku i jest zgodne z zaleceniami projektowania sieci w chmurze.

## 6.1 Podsieci (Subnets)

W obrębie VPC utworzono podsieci:

- **Public subnet(y)** – przeznaczone dla zasobów wymagających ekspozycji (ALB, Bastion Host),
- **Private subnet** – przeznaczony dla serwera aplikacyjnego EC2 bez publicznego IP.

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	IPv6 CIDR	IPv6 C
eventplanner-subnet-public2-eu-north...	subnet-0a4227ff136e845a	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.16.0/20	—	—
public-subnet	subnet-0d8b686ef1fbf3055	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.100.0/24	—	—
eventplanner-subnet-private2-eu-north...	subnet-02de30e7884a740f3	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.144.0/20	—	—
eventplanner-subnet-public1-eu-north...	subnet-07f0d91abefbf0512d	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.0.0/20	—	—
eventplanner-subnet-private1-eu-north...	subnet-00b45488ed35e7037	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.128.0/20	—	—
private-subnet	subnet-08cf9711765ad120	Available	vpc-067dc97b52c2b6907   eve...	Off	10.0.200.0/24	—	—

Rysunek 6: Lista podsieci w VPC, w tym podsieć prywatna dla serwera aplikacyjnego oraz podsieć publiczna dla warstwy dostępowej.

## 6.2 Routing: Internet Gateway oraz NAT Gateway

Tablice routingu skonfigurowano w sposób rozdzielający ruch publiczny i prywatny:

- tablica routingu dla podsieci publicznej zawiera trasę domyślną do Internet Gateway [4],
- tablica routingu dla podsieci prywatnej zapewnia ruch wewnętrz VPC; dostęp do internetu dla połączeń wychodzących realizowany jest poprzez NAT Gateway [3].

The screenshot shows the AWS VPC Route Tables page for a specific route table. The main header indicates a successful update of subnet associations. The route table ID is rtb-036c253ea08b65af7 and it is named /public-rt.

**Details Info:**

- Route table ID: rtb-036c253ea08b65af7
- Main: No
- VPC: vpc-067dc97b52c2b6907 | eventplanner-vpc
- Owner ID: 405617742093
- Explicit subnet associations: subnet-0d8b68e6f1fbf3055 / public-subnet
- Edge associations: -

**Routes (2):**

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-055fd475e4e7c26a	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Rysunek 7: Tablica routingu dla podsieci publicznej (trasa 0.0.0.0/0 do Internet Gateway).

The screenshot shows the AWS VPC Route Tables page for a different route table. The main header indicates a successful update of subnet associations. The route table ID is rtb-0ddd61a3c863a3375 and it is named /private-rt.

**Details Info:**

- Route table ID: rtb-0ddd61a3c863a3375
- Main: No
- VPC: vpc-067dc97b52c2b6907 | eventplanner-vpc
- Owner ID: 405617742093
- Explicit subnet associations: subnet-08cfca9711765ad120 / private-subnet
- Edge associations: -

**Routes (1):**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

Rysunek 8: Tablica routingu dla podsieci prywatnej (asocjacja z private subnet).

## 7 Warstwa dostępu: Bastion Host

Zarządzanie serwerem aplikacyjnym zrealizowano poprzez Bastion Host umieszczony w podsieci publicznej. Połączenie SSH do serwera aplikacyjnego jest nawiązywane dopiero z Bastiona, co eliminuje konieczność wystawiania portu 22 w podsieci prywatnej na internet.

The screenshot shows the AWS EC2 Instances page. In the left sidebar, under the 'Instances' section, the 'bastion-host' instance is selected. The main pane displays the 'Instances (1/4) Info' table with one row for the selected instance. The instance details page for 'bastion-host' is shown below, with the 'Details' tab selected. Key information includes:

- Public IPv4 address:** 13.48.42.209
- Instance state:** Running
- Private IP DNS name (IPv4 only):** ip-10-0-100-228.eu-north-1.compute.internal
- Instance type:** t3.micro
- VPC ID:** vpc-067dc97b52c2b6907 (eventplanner-vpc)

Rysunek 9: Szczegóły instancji Bastion Host (publiczny adres IPv4).

The screenshot shows a terminal window with the following content:

```
ubuntu@ip-10-0-100-210:~$ ssh -i eventplanner_key.pem ubuntu@10.0.200.210
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1015-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Jan  2 20:09:13 UTC 2026

  System load: 0.0          Temperature:      -273.1 C
  Usage of /: 30.0% of 6.71GB Processes:           113
  Memory usage: 25%          Users logged in:     0
  Swap usage:  0%          IPv4 address for ens5: 10.0.200.210

Expanded Security Maintenance for Applications is not enabled.

74 updates can be applied immediately.
28 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Jan  2 19:38:02 2026 from 10.0.100.228
ubuntu@ip-10-0-200-210:~$
```

Rysunek 10: Połączenie SSH z Bastion Host do serwera aplikacyjnego w podsieci prywatnej.

```
ubuntu@ip-172-31-47-160: ~

No containers need to be restarted.

User sessions running outdated binaries:
  ubuntu @ session #2: sshd[1060]
  ubuntu @ user manager service: systemd[1065]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-47-160:~$ sudo systemctl enable nginx
Synchronizing state of nginx.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable nginx
ubuntu@ip-172-31-47-160:~$ sudo systemctl start nginx
ubuntu@ip-172-31-47-160:~$ sudo systemctl status nginx --no-pager
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
  Active: active (running) since Fri 2026-01-02 18:33:22 UTC; 32s ago
    Docs: man:nginx(8)
 Main PID: 13003 (nginx)
   Tasks: 3 (limit: 1008)
  Memory: 2.4M (peak: 5.3M)
    CPU: 24ms
   CGroup: /system.slice/nginx.service
           ├─13003 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
           ├─13005 "nginx: worker process"
           └─13006 "nginx: worker process"

Jan 02 18:33:22 ip-172-31-47-160 systemd[1]: Starting nginx.service - A high performance web server and a revers...rver...
Jan 02 18:33:22 ip-172-31-47-160 systemd[1]: Started nginx.service - A high performance web server and a reverse...server.
Hint: Some lines were ellipsized, use -l to show in full.
ubuntu@ip-172-31-47-160:~$
```

Rysunek 11: Potwierdzenie poprawnego zalogowania do instancji (sesja SSH).

## 8 Warstwa dostępu: Application Load Balancer

Dostęp użytkowników końcowych do aplikacji realizowany jest przez Application Load Balancer (ALB) w trybie *internet-facing*. ALB przekazuje ruch HTTP do zarejestrowanego Target Group, która wskazuje instancję aplikacyjną jako cel ruchu. Mechanizm zdrowia Target Group umożliwia weryfikację dostępności backendu; status *Healthy* oznacza, że instancja pomyślnie przechodzi testy [6, 5].

The screenshot shows the AWS EC2 Load balancers console. On the left, there is a navigation sidebar with various services like Savings Plans, Reserved Instances, and Auto Scaling. The main area displays a table titled 'Load balancers (1)'. The table has columns for Name, State, Type, Scheme, IP address type, VPC ID, Availability Zones, Security groups, and DNS name. One row is listed: 'eventplanner-lb' (Active, application, Internet-facing, IPv4, vpc-067dc97b52c2b6907, 2 Availability Zones, sg-06f65fb45a2ed86f1, eventplanner-lb). Below the table, a message says '0 load balancers selected'.

Rysunek 12: Application Load Balancer w stanie *Active*.

The screenshot shows the AWS EC2 Target groups console. On the left, there is a navigation sidebar with various services like Instances, Images, and Auto Scaling. The main area displays a table titled 'eventplanner-tg'. The table has columns for Target type (Instance), Protocol (HTTP: 80), Protocol version (HTTP1), and VPC (vpc-067dc97b52c2b6907). It shows 1 total target, all healthy. Below the table, a section titled 'Registered targets (1)' shows a single entry: 'i-0036a286ad1adb754' (eventplanner..., 80, eu-north-1a (e...), Healthy). At the bottom, there are tabs for Targets, Monitoring, Health checks, Attributes, and Tags.

Rysunek 13: Target Group zinstancją backendową w stanie *Healthy*.

## 8.1 Izolacja serwera aplikacyjnego

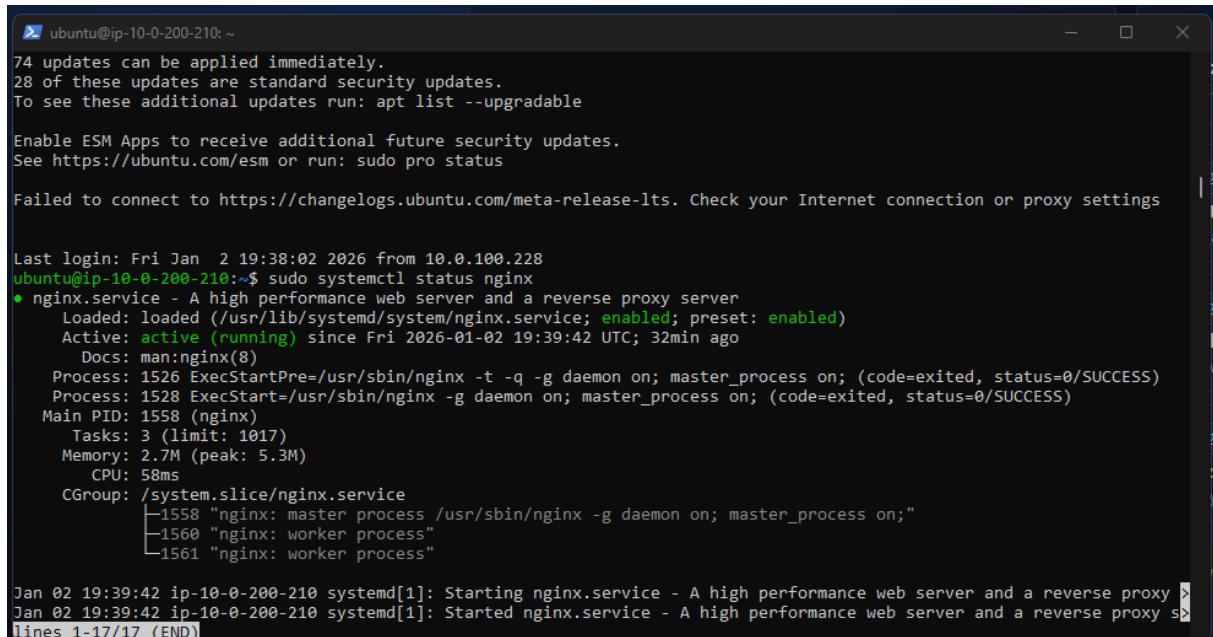
Serwer aplikacyjny nie posiada publicznego adresu IPv4, a ruch HTTP jest dopuszczany wyłącznie z warstwy ALB (co wynika z zastosowania reguł Security Group i separacji podsieci). Potwierdzenie braku publicznego adresu na instancji aplikacyjnej przedstawiono na rys. 14.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, AWS Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, IAM Roles, CloudShell, Feedback, and Console Mobile App. The main area displays a table titled 'Instances (1/4) info' with one row selected: 'eventplanner-app' (Instance ID: i-0036a286ad1adb754). The instance is running, t3.micro, in eu-north-1a, with a Private IP DNS of ip-10-0-200-210.eu-north-1.compute.internal. Below the table, the detailed view for 'i-0036a286ad1adb754 (eventplanner-app)' is shown under the 'Details' tab. It includes sections for Instance summary, Images, IPv6 address, Hostname type, Auto-assigned IP address, Public IPv4 address, Instance state, Private IP DNS name, Instance type, VPC ID, and Subnet ID. The Public IPv4 address section is empty, indicating no public IP is assigned.

Rysunek 14: Instancja aplikacyjna w podsieci prywatnej (brak publicznego IPv4).

## 9 Konfiguracja usługi WWW na serwerze aplikacyjnym (Nginx)

Na instancji aplikacyjnej uruchomiono serwer WWW Nginx, który dostarcza stronę „Event Planner”. Z punktu widzenia wymagań projektu istotne było wykazanie, że usługa działa oraz jest uruchomiona jako usługa systemowa. Stan usługi przedstawiono na rys. 15. Dodatkowo zweryfikowano dostępność aplikacji przez przeglądarkę (rys. 1 oraz rys. 16).



```
ubuntu@ip-10-0-200-210: ~
74 updates can be applied immediately.
28 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

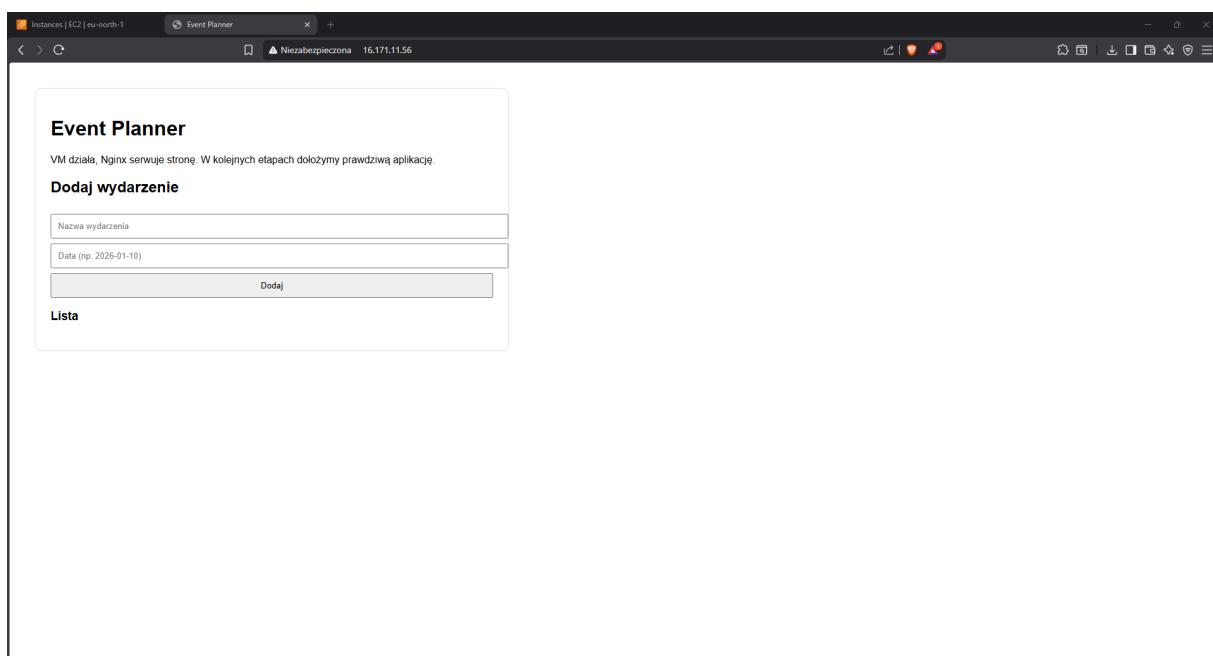
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Jan  2 19:38:02 2026 from 10.0.100.228
ubuntu@ip-10-0-200-210:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
  Active: active (running) since Fri 2026-01-02 19:39:42 UTC; 32min ago
    Docs: man:nginx(8)
 Process: 1526 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Process: 1528 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
 Main PID: 1558 (nginx)
   Tasks: 3 (limit: 1017)
  Memory: 2.7M (peak: 5.3M)
    CPU: 58ms
   CGroup: /system.slice/nginx.service
           ├─1558 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
           ├─1560 "nginx: worker process"
           └─1561 "nginx: worker process"

Jan 02 19:39:42 ip-10-0-200-210 systemd[1]: Starting nginx.service - A high performance web server and a reverse proxy
Jan 02 19:39:42 ip-10-0-200-210 systemd[1]: Started nginx.service - A high performance web server and a reverse proxy
lines 1-17/17 (END)
```

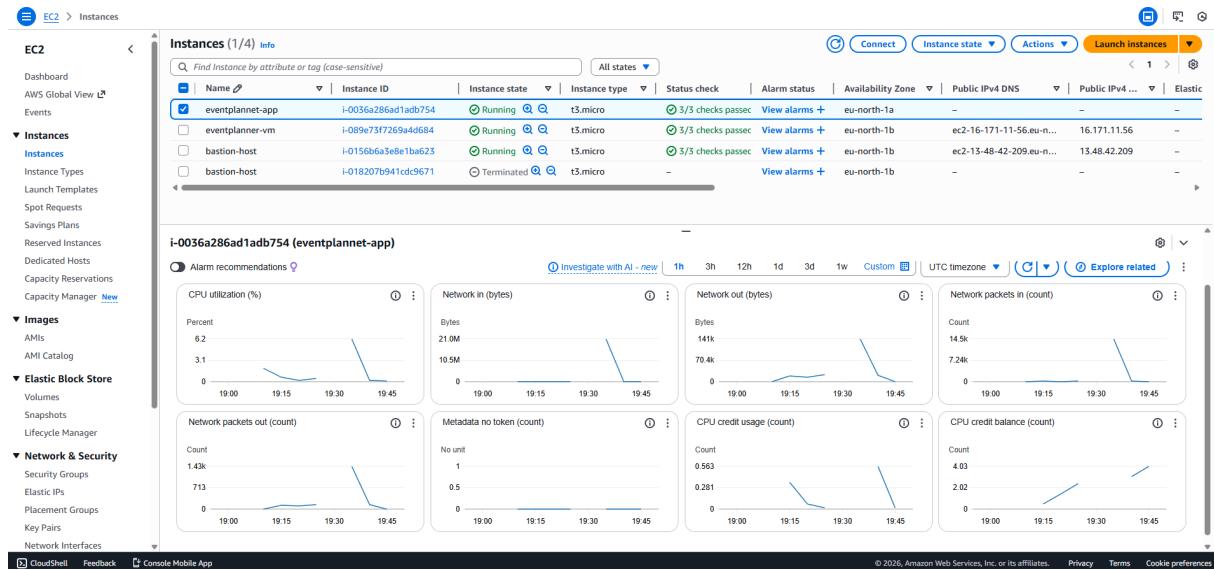
Rysunek 15: Stan usługi Nginx na serwerze (aktywna jednostka systemd).



Rysunek 16: Weryfikacja działania strony serwowanej przez Nginx (widok w przeglądarce).

## 10 Monitoring (Amazon CloudWatch)

Włączono podstawowy monitoring zasobów w Amazon CloudWatch. Monitorowane są metryki instancji EC2, w szczególności CPUUtilization oraz metryki ruchu sieciowego (NetworkIn, NetworkOut) [7]. Przykładowy widok metryk w konsoli przedstawiono na rys. 17.



Rysunek 17: Podstawowe metryki instancji EC2 w CloudWatch (CPU oraz ruch sieciowy).

## 11 Wnioski

Zrealizowane wdrożenie spełnia wymagania do oceny 3.5 poprzez zastosowanie:

- dedykowanego użytkownika IAM i ograniczenie użycia konta root (MFA),
- minimalizacji ekspozycji usług poprzez reguły Security Group oraz dodatkowo ufw,
- segmentacji sieci (public/private subnet),
- pośredniej warstwy dostępu do aplikacji przez ALB oraz do administracji przez Bastion Host,
- podstawowego monitoringu zasobów w CloudWatch.

Przyjęta architektura ogranicza bezpośredni dostęp do zasobów w podsieci prywatnej, utrzymując jednocześnie funkcjonalność systemu. W praktyce stanowi to typowy wzorzec wdrożeniowy dla prostych usług WWW w środowisku chmurowym.

## Literatura

- [1] AWS, *Security best practices in IAM*. Dostęp: <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>.
- [2] AWS, *Root user best practices for your AWS account*. Dostęp: <https://docs.aws.amazon.com/IAM/latest/UserGuide/root-user-best-practices.html>.
- [3] AWS, *NAT gateways – Amazon VPC User Guide*. Dostęp: <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>.
- [4] AWS, *Internet gateways – Amazon VPC User Guide*. Dostęp: [https://docs.aws.amazon.com/vpc/latest/userguide/VPC\\_Internet\\_Gateway.html](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html).
- [5] AWS, *Target groups for your Application Load Balancers*. Dostęp: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html>.
- [6] AWS, *Health checks for Application Load Balancer target groups*. Dostęp: <https://docs.aws.amazon.com/elasticloadbalancing/latest/application/target-group-health-checks.html>.
- [7] AWS, *CloudWatch metrics for Amazon EC2 instances*. Dostęp: [https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing\\_metrics\\_with\\_cloudwatch.html](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/viewing_metrics_with_cloudwatch.html).