

Bezpieczeństwo, rozliczanie i monitorowanie w chmurach obliczeniowych

Michał Baliński
Senior IT Architect, AMG.net



” Bezpieczeństwo w chmurze

” Bezpieczeństwo teleinformatyczne

Zbiór zagadnień związany z szacowaniem i kontrolą ryzyka wynikającego z wykorzystania systemów informatycznych, rozpatrywany z perspektywy funkcji bezpieczeństwa. Do funkcji bezpieczeństwa zalicza się:

- Autentyczność
- Dostępność
- Niezaprzeczalność
- Rozliczalność
- Poufność
- Anonimowość
- Integralność



Funkcje bezpieczeństwa (1)

Autentyczność

(ang. authenticity) - zapewnienie że: dane, transakcje, komunikaty i dokumenty są prawdziwe. Przez autentyczność rozumie się także potwierdzenie tożsamości wszystkich zaangażowanych stron, czyli uwierzytelnienie (ang. authentication).

Niezaprzeczalność

(ang. non-repudiation) - brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie

Poufność

(ang. confidentiality) - funkcja bezpieczeństwa wskazująca obszar, w którym dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom.

Integralność

(ang. data integrity) - funkcja bezpieczeństwa polegająca na tym, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.

Funkcje bezpieczeństwa (2)

Dostępność

(ang. availability) - zapewnienie że: dane, transakcje, komunikaty i dokumenty są dostępne wtedy kiedy potrzeba.

Rozliczalność

(ang. accountability) - funkcja bezpieczeństwa zapewniająca, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi.

Anonimowość

(ang. anonymity) - określona cecha protokołu służąca do ochrony prywatności użytkownika systemu.

Authentication (uwierzytelnianie)

Weryfikacja tożsamości
użytkownika.

Authorization (autoryzacja)

Określenie, czy dany
użytkownik ma prawo dostępu
do danej akcji.

Accounting (rozliczanie)

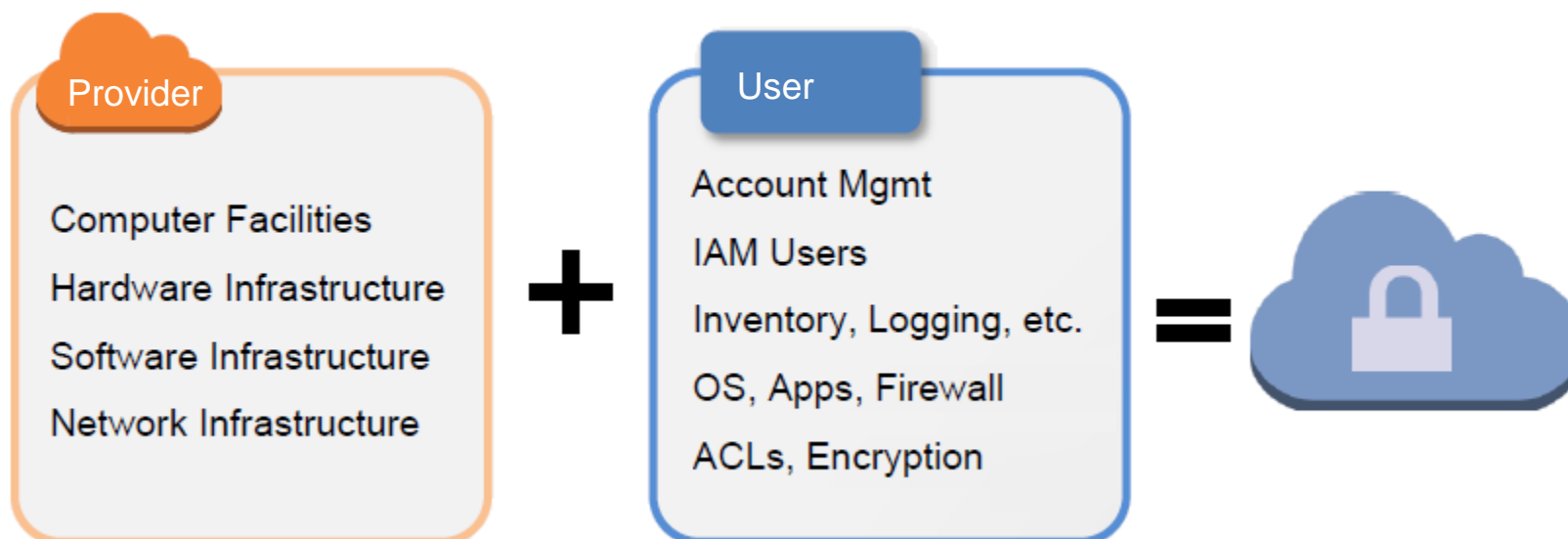
Zbieranie informacji o
wykorzystaniu zasobów na
potrzeby analizy zużycia
zasobów i trendów, alokacji
kosztów, audytu i rozliczania
finansowego

Trzy powiązane ze sobą aspekty dotyczące bezpieczeństwa i rozliczania w chmurach obliczeniowych.

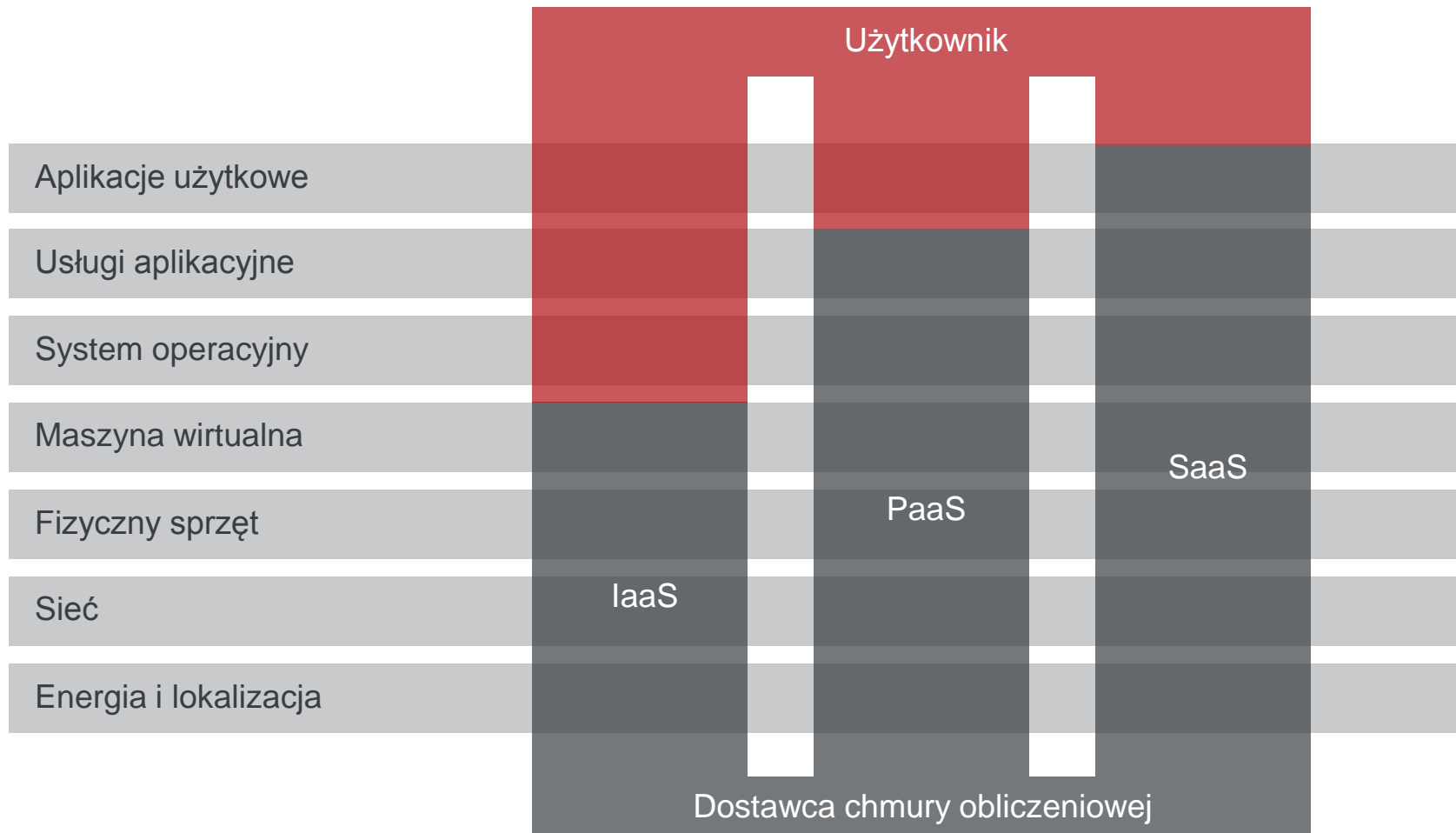
Pierwotnie pojęcie AAA pojawiło się w kontekście sieci telekomunikacyjnych (protokoły: Radius, Diameter). W pewnych aspektach chmury obliczeniowe mają cechy wspólne z sieciami telekomunikacyjnymi, dlatego w tej dziedzinie pojęcie AAA także znajduje zastosowanie. Chmury obliczeniowe - tak jak telekomunikacja - zapewniają pewne usługi, w których poszczególni użytkownicy powinni zostać uwierzytelnieni, zautoryzowani i rozliczeni za swoje działania.

- Powierzenie poufnych danych zewnętrznemu dostawcy
- Korzystanie ze współdzielonej infrastruktury (*ang. multi-tenancy*)
- Ochrona danych osobowych (GIODO)
- Problemy prawodawstwa międzynarodowego
 - USA Patriot Act
 - EU / non-EU

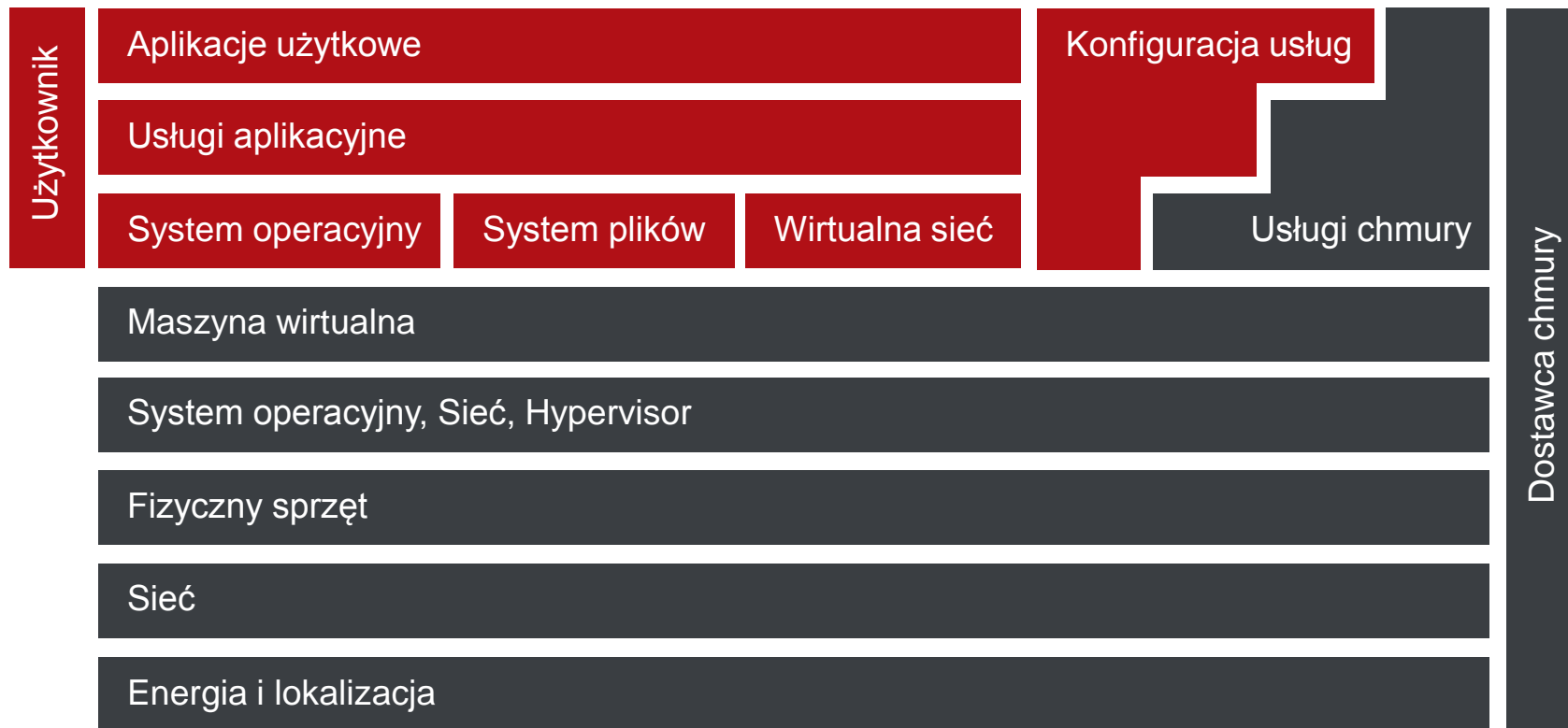
” Współdzielona odpowiedzialność



Współdzielona odpowiedzialność



Współdzielona odpowiedzialność



Użytkownik chmury

- Uprawnienia zarządzania infrastrukturą
- Reguły dostępu sieciowego, administracja
- Klucze i hasła SSH
- Klucze i hasła dostępu do aplikacji
- Klucze i hasła dostępu do chmury
- Szyfrowanie danych
- Audyt logów
- Aktualizacje systemu operacyjnego (guest)
- Kopie bezpieczeństwa
- Anty-wirus

Dostawca chmury

- Ochrona fizyczna serwerowni
- Ograniczenia dostępu do serwerowni
- Niszczenie nośników danych
- Monitoring
- Certyfikaty i audyty bezpieczeństwa
- Aktualizacje systemu operacyjnego (host)
- Bezpieczeństwo na poziomie hypervisora
- Zabezpieczenia sieci

Certyfikaty zgodności dostawcy chmury ze standardami:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 27001
- ITAR
- FIPS 140-2
- HIPAA
- CSA
- MPAA
- DoD 5220.22-M
- NIST 800-88



- Zabezpieczenia przed czynnikami zewnętrznymi:
 - Temperatura, pożar, powódź, zanik prądu, ...
- Ochrona serwerowni 24x7
- Kontrola dostępu do serwerowni (audyt, MFA)
- Rozdział obowiązków (*ang. Separation of Duties*)
- Ochrona sieciowa
 - Zabezpieczenia przed DoS / DDoS
 - Zabezpieczenie API
 - Zabezpieczenia na poziomie host OS i hypervisora
 - Blokada skanowania portów, snifferów i IP spoofingu
- Czyszczenie danych i fizyczne niszczenie nośników

Ochrona zapewniona przez dostawcę chmury



wydział
elektrotechniki
elektroniki
informatyki
i automatyki

AMG.net

A Bull Group Company

Dear AWS Customer,

The OpenSSL project has recently announced a security vulnerability in OpenSSL (which is used within ELB) affecting versions 1.0.1 and 1.0.2 (CVE-2014-0160). While we've mitigated the impact of this issue for the Elastic Load Balancing service, we are writing to you because you have used a custom SSL certificate with one or more of your load balancers. As a precaution, it is our recommendation that you rotate your SSL certificates as soon as possible.

If you're using the Amazon Linux AMI, you can simply run "sudo yum update openssl", and then restart any services using OpenSSL to protect any at-risk instances.

Thank you,

AWS Security



Your AWS account is compromised.

We recently became aware that your AWS Access Key (ending with 4AEQ) along with your Secret Key are publicly available on GitHub. This poses a security risk to you, could lead to excessive charges from unauthorized activity or abuse, and violates the AWS Customer Agreement.

...

Thank you,

AWS Security

” Dobre praktyki bezpieczeństwa

- Chronić dane podczas transportu
- Chronić przechowywane dane
- Zarządzać rolami i poziomami dostępu użytkowników
- Dbaj o bezpieczeństwo kluczy dostępowych
- Zabezpieczaj swoją aplikację na każdym poziomie

Chroń dane podczas transportu

- Używaj certyfikatów SSL podczas przesyłania danych wrażliwych/poufnych pomiędzy komponentami architektury, np. przeglądarką i serwerem webowym.
- Zasoby, do których dostęp powinien być ograniczony, umieszczaj w dedykowanej sieci prywatnej. Będą do nich miały dostęp jedynie wybrane komponenty korzystające z protokołu IPSec.

Chroń dane przechowywane w chmurze

- Szyfruj dane poufne/wrażliwe jeśli chcesz przechowywać je w chmurze (np. w S3). Szyfruj dane przed wysłaniem (np. GnuPG, OpenPGP).
- Rozważ opcje szyfrowanych systemów plików dla przechowywania danych wrażliwych.
- Pamiętaj by zabezpieczyć swoje dane przez awarią. Wykonuj regularne kopie zapasowe danych.

Zarządzaj danymi uwierzytelniającymi, rolami i uprawnieniami do usług w chmurze:

- Korzystaj z narzędzi klasy IAM (Identity and Access Management).
- Definiuj konta imienne dla użytkowników z przypisanymi unikalnymi danymi uwierzytelniającymi (*ang. credentials*).
- Przypisuj uprawnienia do konta. Nadawaj dostęp tylko do tych zasobów, których użytkownik potrzebuje.
- W szczególności nowy użytkownik nie ma dostępu do któregokolwiek z zasobu chmury.
- Korzystaj z narzędzi klasy HSM (Hardware Security Module, np. AWS Cloud HSM)

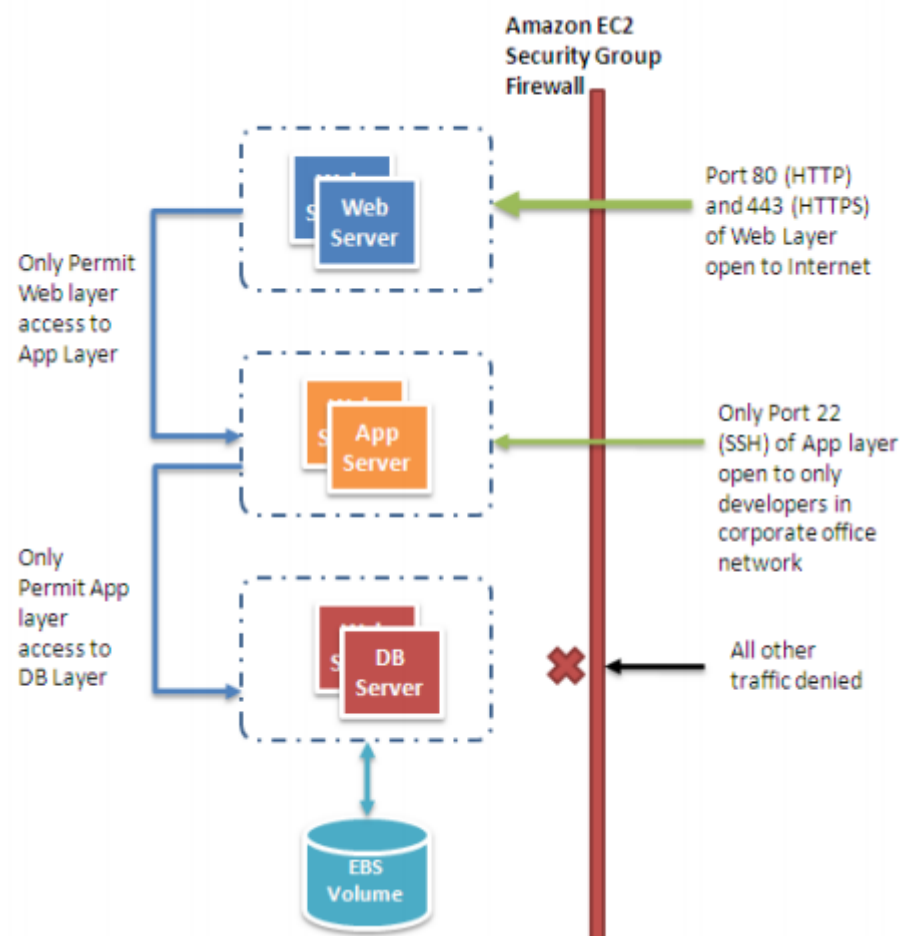
Dane uwierzytelniające do AWS:

- Typy danych uwierzytelniających:
 - hasło
 - klucz dostępowy
 - certyfikat X.509
- Klucz dostępowy (access key) składa się z dwóch części:
 - access key ID
 - secret access key
- Klucz dostępowy potrzebny jest do wyznaczenia podpisu żądania przy korzystaniu z REST lub Query API.
- Nie umieszczaj kluczy dostępowych w obrazie instancji (AMI). Ich zmiana będzie wymagała nowego obrazu AMI. Przekaż je jako parametr wywołania.
- Nie umieszczaj kluczy dostępowych w SCM (GIT, SVN, ...).



Zabezpieczaj aplikację na każdym poziomie:

- Sieć prywatna (VPC)
 - Security group (zapora stanowa)
 - Network ACL (zapora bezstanowa)
- Instancja
 - OS firewall
 - Aktualizacje oprogramowania
 - Dobre praktyki OS (np. nie używaj root'a)
- Object storage (S3)
 - IAM policies
 - S3 ACL's
- Infrastruktura
 - Zabezpieczaj dostęp do interfejsów zarządzania infrastrukturą w chmurze



- Regularnie pobieraj poprawki ze stron dostawcy oprogramowania i aktualizuj oprogramowanie obrazów instancji
- Testuj instancje po aktualizacji oprogramowania
- Przygotuj automatyczne skrypty umożliwiające okresowe wykonywanie testów bezpieczeństwa
- Upewnij się, że oprogramowanie dostarczane przez firmy trzecie jest bezpieczne i skonfigurowane zgodnie z rekomendacjami producenta
- Nie uruchamiaj procesów z poziomu użytkowników: root / Administrator.

” Identity and Access Management

IAM Identity and Access Management

Zagadnienie zarządzania tożsamością oraz prawami dostępu. Dotyczy:

- Zarządzania tożsamościami (wiedzą o tożsamościach)
- Zarządzania uprawnieniami
- Usług informacji o tożsamości
- Usług uwierzytelniania oraz autoryzacji

- Typy komponentów
 - Service Provider (SP), Service Consumer (SC), Identity Provider (IdP), Identity Store (IS)
 - Policy Administration Point (PAP)
 - Policy Decision Point (PDP)
 - Policy Enforcement Point (PEP)
 - Policy Information Point (PIP)
 - Policy Retrieval Point (PRP)
- Usługi katalogowe (LDAP, AD, NIS, ...)
- Federacja tożsamości (*ang. identity federation*), SSO (*ang. Single Sign-On*)
- Protokół OAuth2
- SAML (*ang. Security Assertion Markup Language*)
- OpenID
- RBAC (*ang. Role Based Access Control*), ACL (*ang. Access Control List*)
- XACML (*ang. eXtensible Access Control Markup Language*)
- MFA (*ang. Multi Factor Authentication*), OTP (*ang. one-time password*)
- Fine-grained vs Coarse-grained privileges



Przykładowe (typowe) domeny logowania (*ang. realms*)

Logowanie do aplikacji webowej

- Zarządzane przez aplikację

Aplikacja

Logowanie do instancji EC2, logowanie do bazy danych

- Dane uwierzytelniające na poziomie systemu operacyjnego, bazy danych itp.
- Częściowo zarządzane przez usługę w chmurze (np. klucz SSH w AWS EC2 lub OpenStack Keystone)

Usługa

Logowanie do interfejsu zarządzania infrastrukturą w chmurze

- Cloud IAM (AWS IAM, OpenStack Keystone, ...)

Infrastruktura

Dobłą praktyką jest pozostawić te domeny rozdzielnymi.



IAM

- Zarządzanie
 - Użytkownikami
 - Grupami
 - Rolami (instancji)
 - Uprawnieniami
 - Danymi uwierzytelniającymi
 - Federacją
 - Polityka haseł
 - MFA, OTP
- Encje
 - Konto AWS
 - Grupy
 - Użytkownicy
 - Role



Keystone

- Zarządzanie
 - Użytkownikami
 - Projektami (*ang. tenant*)
 - Rolami (użytkowników)
 - Politykami dostępu
 - Danymi uwierzytelniającymi
 - Katalogiem usług
 - Federacją i bazą tożsamości
- Encje
 - Domena OpenStack
 - Projekt (*ang. tenant*)
 - Użytkownicy
 - Role

Authorization Policy Document

- JSON Format
- Action (API)
 - Specific API(s) that you can call, such as:
 - S3::GetObject
 - S3::GetObjectVersion
 - S3::Get*
- Resource identifier (some services)
 - Applies to specific resources, such as:
 - arn:aws:s3:::bucketname/keyname
 - arn:aws:s3:::my_website/images/header.jpg
 - arn:aws:s3:::my_website/images/*
- Condition (optional)
 - Applies to specific conditions, such as:
 - SSL required
 - Request must originate from specific IP range (CIDR)
 - Request requires MFA
 - Request valid until (or after) some date/time

Authorization Policy Document

```
{ "Statement" : [  
  {  
    "Effect" : "Allow",  
    "Action" : "s3:Get*",  
    "Resource" : "arn:aws:s3:::my-bucket/secure/*",  
    "Condition" : {  
      "IpAddress" : {  
        "aws:SourceIp" : [ "174.128.53.0/24" ]  
      }  
    },  
    { ANOTHER STATEMENT... }  
  ]  
}
```

Fine-grained

Manage User Permissions Cancel X

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [Overview of Policies](#) in Using AWS Identity and Access Management.

Effect Allow ☒ Deny ☐

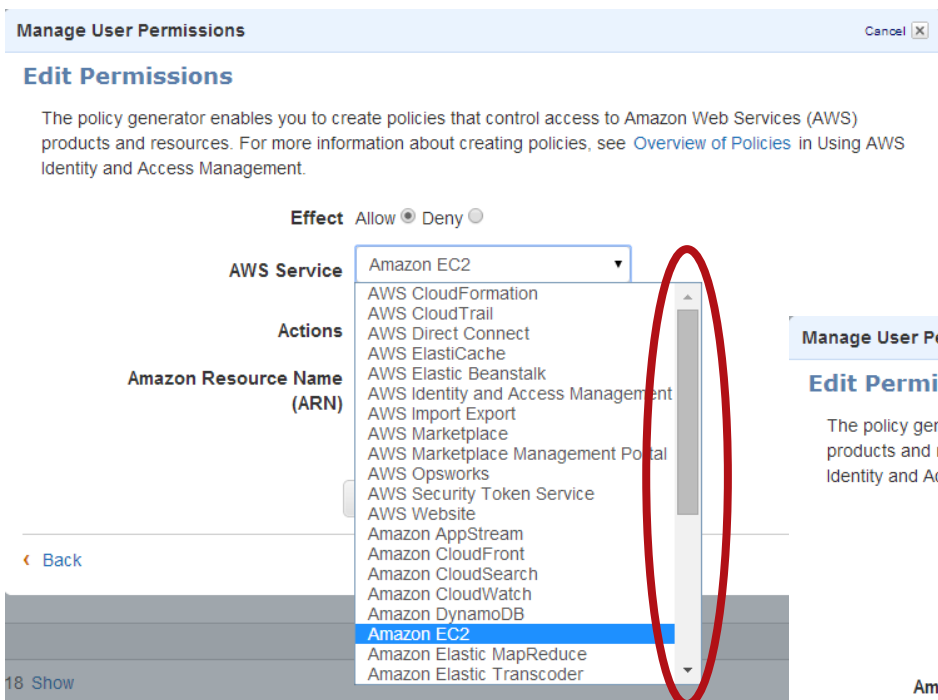
AWS Service Amazon EC2

Actions

Amazon Resource Name (ARN)

[Back](#)

18 Show



Manage User Permissions Cancel X

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see [Overview of Policies](#) in Using AWS Identity and Access Management.

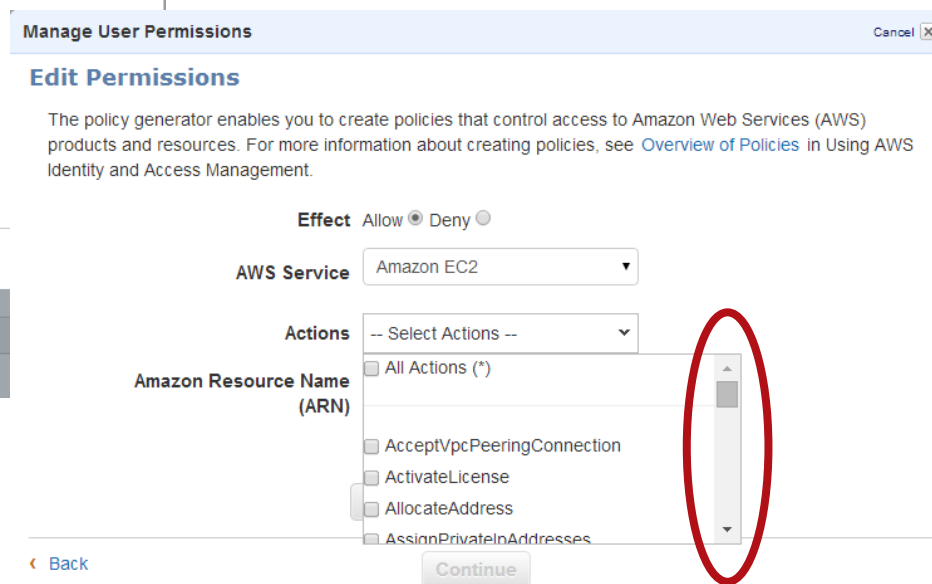
Effect Allow ☒ Deny ☐

AWS Service Amazon EC2

Actions -- Select Actions --

Amazon Resource Name (ARN)

[Back](#) Continue



```
{"Statement": [{  
  "Sid": "AddCannedAcl",  
  "Effect": "Allow",  
  "Principal": {  
    "AWS": [  
      "arn:aws:iam::111122223333:root",  
      "arn:aws:iam::444455556666:root"]  
    },  
  "Action": ["s3:PutObject", "s3:PutObjectAcl"],  
  "Resource": ["arn:aws:s3:::bucket/*"],  
  "Condition": {  
    "StringEquals": {"s3:x-amz-acl": ["public-read"]}  
  }  
}]}
```

STS (*ang. Security Token Service*)

- Umożliwia pozyskanie tokenu

Tymczasowy token

- Wygasa po konfigurowalnym czasie (15 min. – 36 h.)

Federacja tożsamości

- STS umożliwia SSO z innymi aplikacjami (np. korporacyjnym uwierzytelnianiem)

Role

- Uwierzytelniona i zaufana jednostka może pozyskać token
- Jednostka to instancja EC2 lub np. użytkownik z innego konta

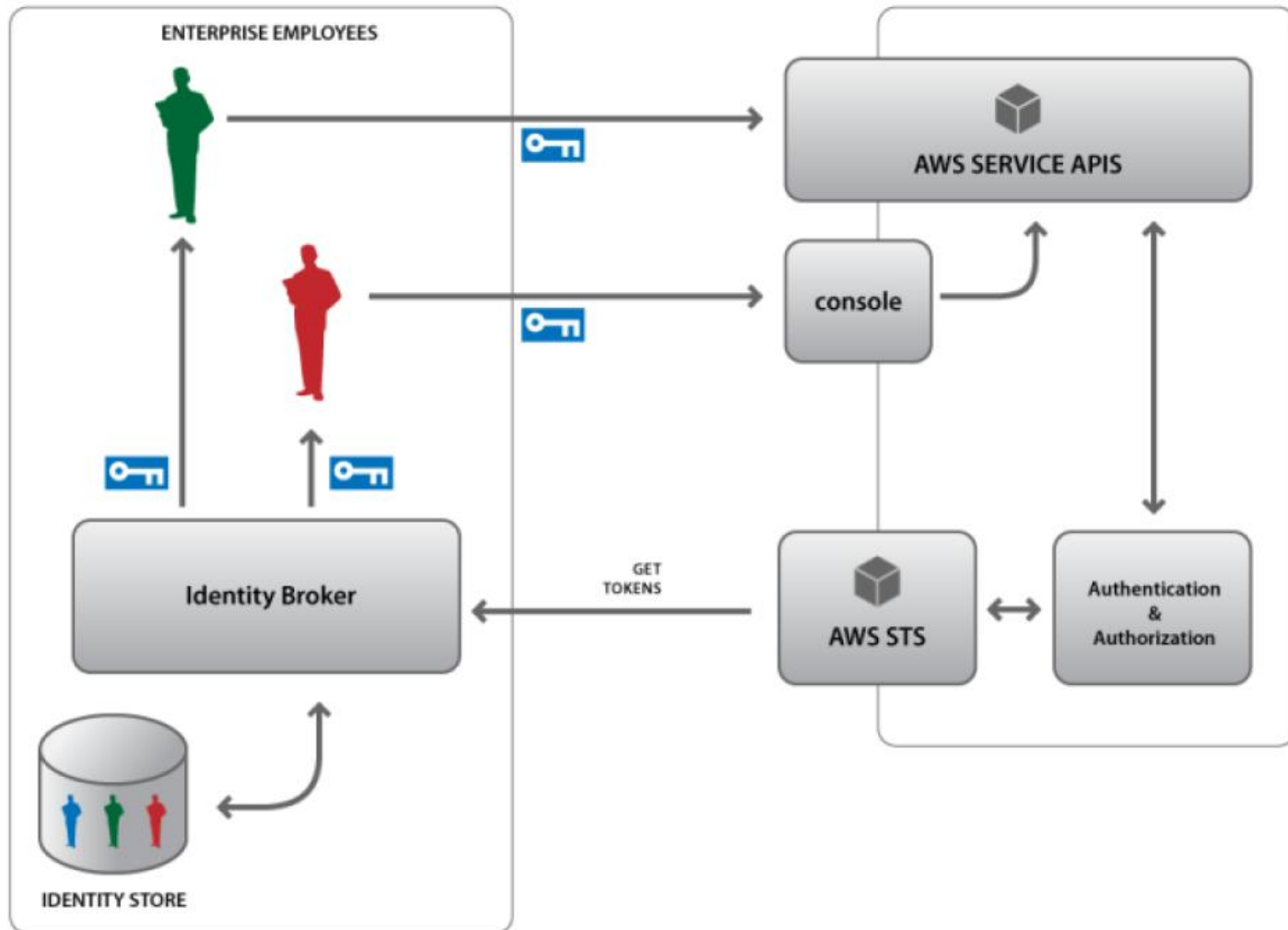
Role EC2 w IAM

- W IAM można utworzyć rolę
- Do roli można przypisać uprawnienia
- Startując instancję EC2 można jej przypisać rolę
- Z wewnątrz instancji EC2 można odpytać się o jej metadane (w tym rolę)
- Z wewnątrz instancji EC2 można pobrać **token** do AWS API, który będzie miał uprawnienia takie jak rola instancji
- Powyższe pozwala na dostęp do API AWS bez przechowywania w kodzie źródłowym kluczy dostępowych

Metadata service

- 169.254.x.x – link-local addresses, nierutowalny adres
- <http://169.254.169.254/latest/meta-data/> - pobranie aktualnych metadanych
- http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name

Federacja za pomocą STS



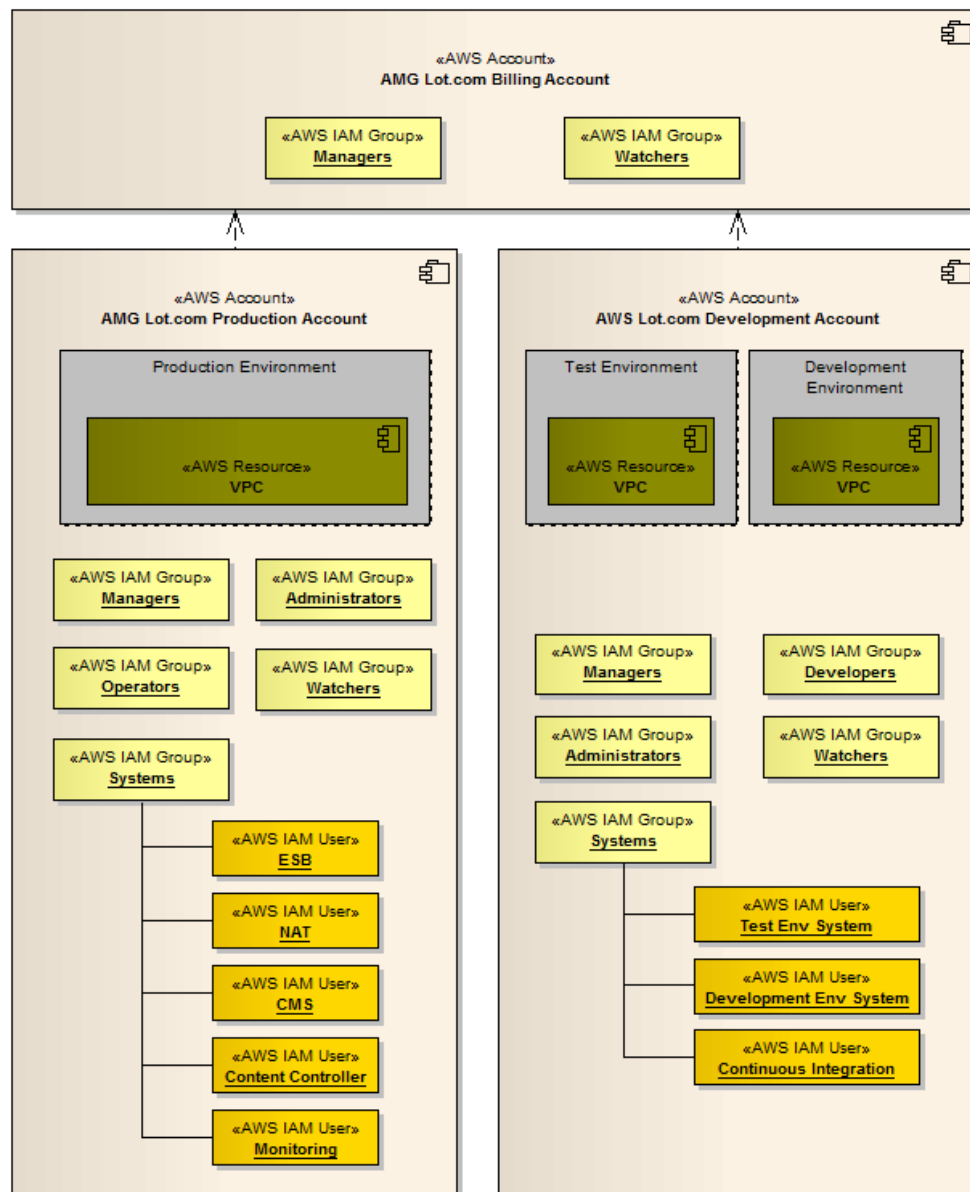
AWS IAM

Separacja kont per środowisko

- Inne uprawnienia
- Inni użytkownicy
- Osobne rachunki
- Inne klucze dostępowe

Consolidated billing

- Wspólne konto rozliczeniowe

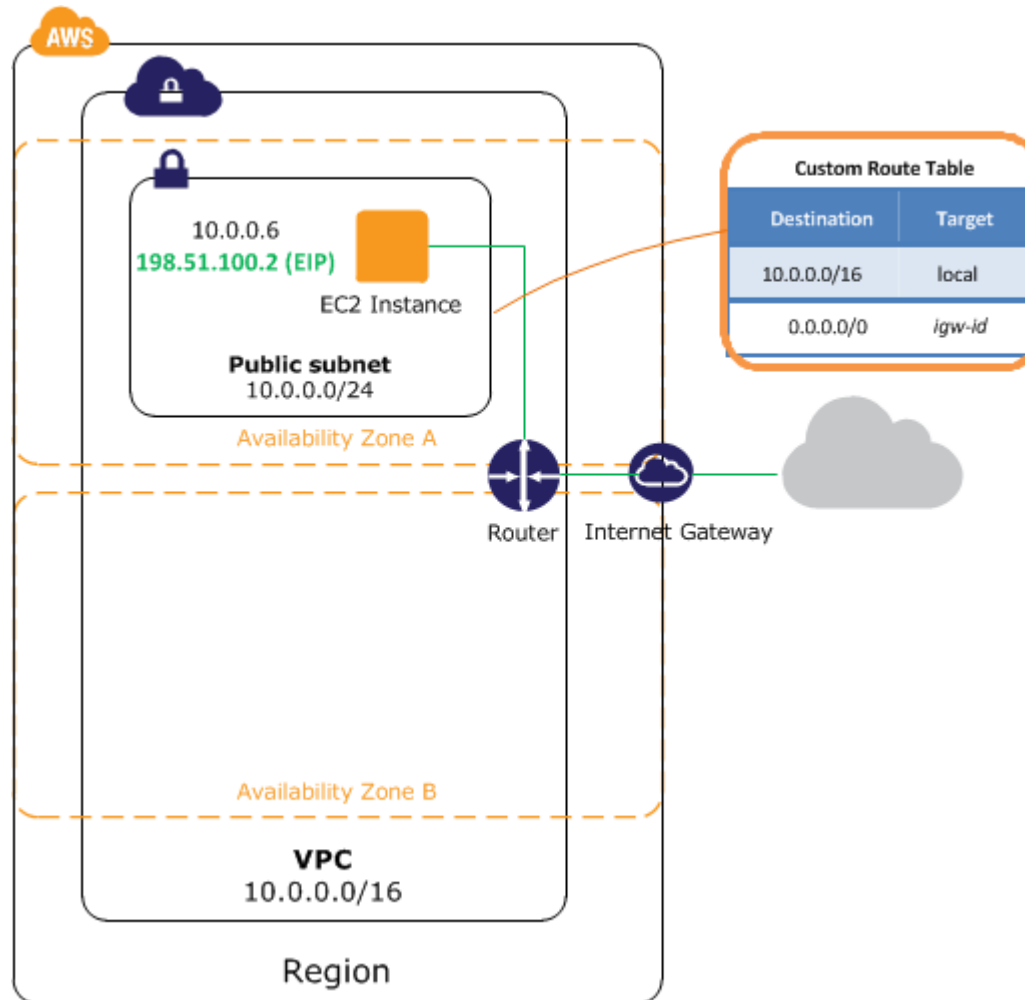


Wirtualna sieć

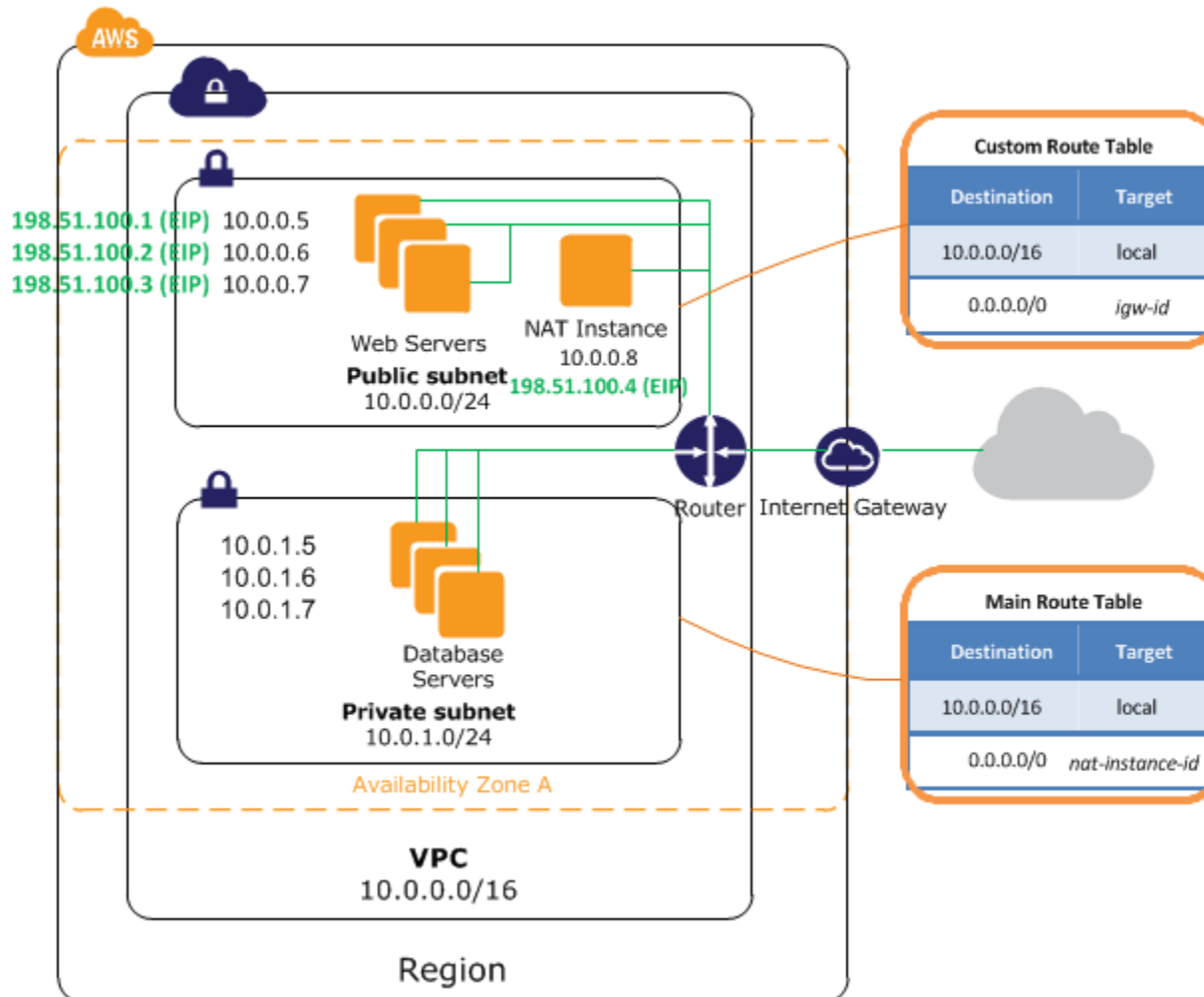
Na przykładzie AWS VPC

- Wirtualna sieć (VPC) - adresacja
- Router – tablica ruchu
- Podsieć (subnet)
- Floating IP (Public IP)
- Elastic Network Interface – wirtualny interfejs sieciowy
- Internet Gateway
- Virtual Private Gateway
- Security Group (stanowy firewall)
- Network ACL (bezstanowy firewall)
- Network Address Translation (NAT)
- Bastion host

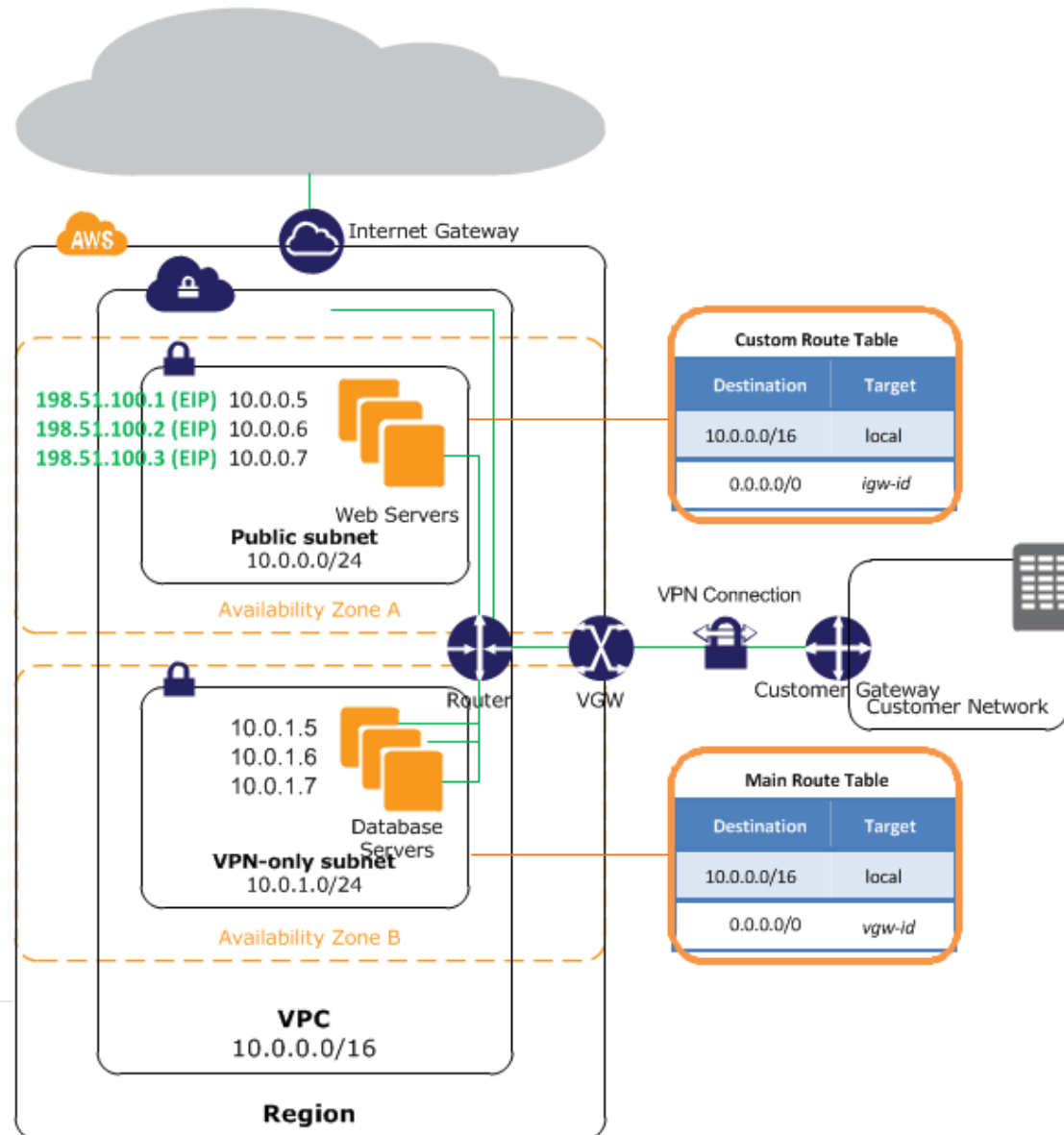
VPC z siecią publiczną



VPC z siecią publiczną i prywatną



VPC – public, private, VPN



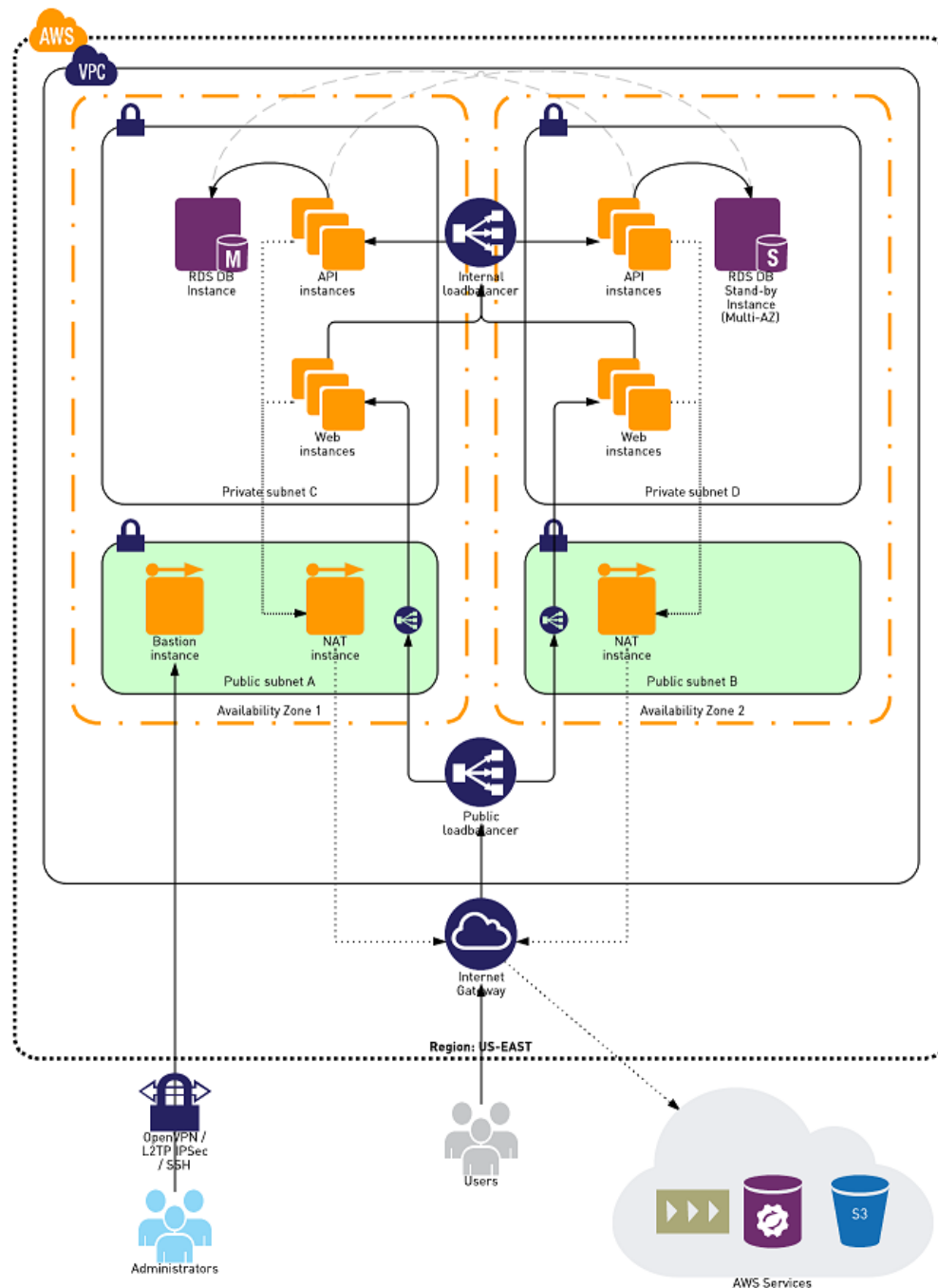
VPC – Bastion host, NAT

Bastion host

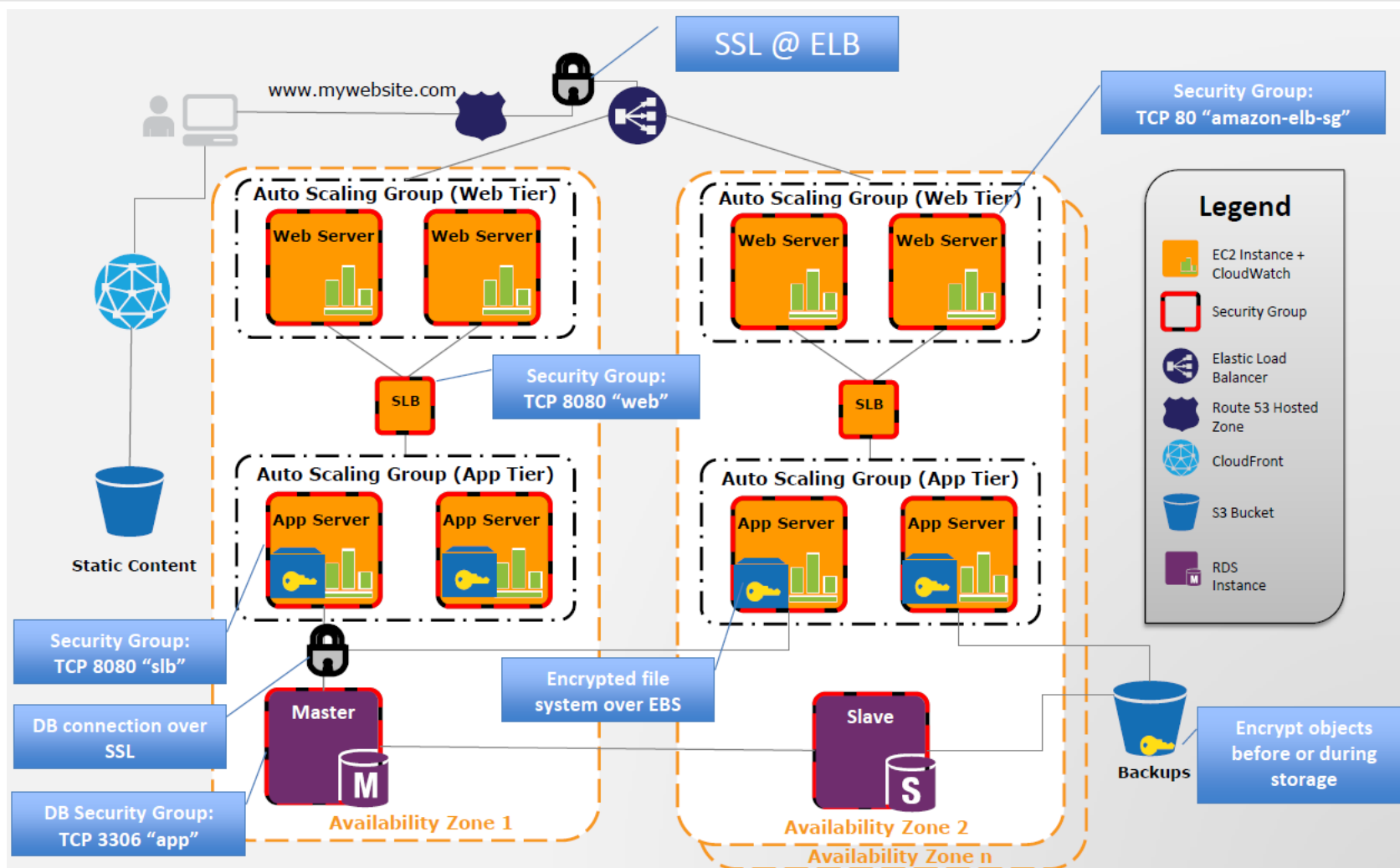
- Posiada publiczne IP
- Wpuszcza ruch administracyjny z internetu (np. SSH)
- Może być wykorzystany zamiast VPG (VPN)

NAT instance

- Posiada publiczne IP
- Wypuszcza ruch do internetu z instancji bez publicznego IP



Punkty zabezpieczeń



” Rozliczanie i monitoring

Zbieranie informacji o wykorzystaniu zasobów na potrzeby analizy zużycia zasobów i trendów, alokacji kosztów, audytu i rozliczania finansowego

- AWS CloudWatch

- Monitoring
- Alarmy

- AWS CloudTrail

- Dane audytowe
- Historia żądań API

- AWS Billing Console

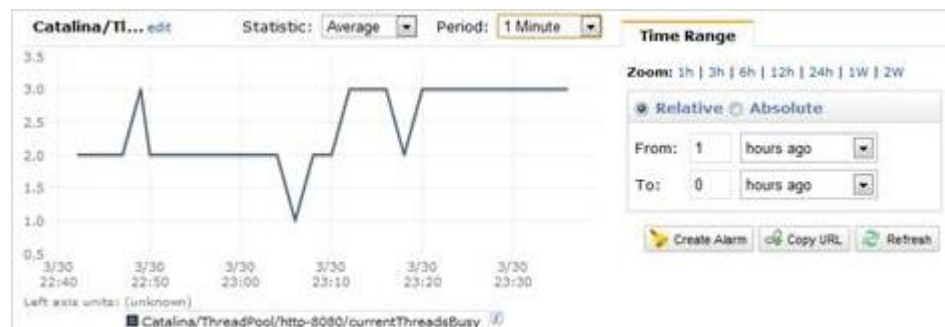
- Raporty finansowe

- AWS Cost Calculator

- Szacowanie kosztów

- OpenStack Ceilometer

- Metryki, dane audytowe, rozliczanie



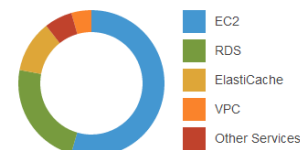
Current month-to-date balance for April 2014

\$2,169.02



By Service

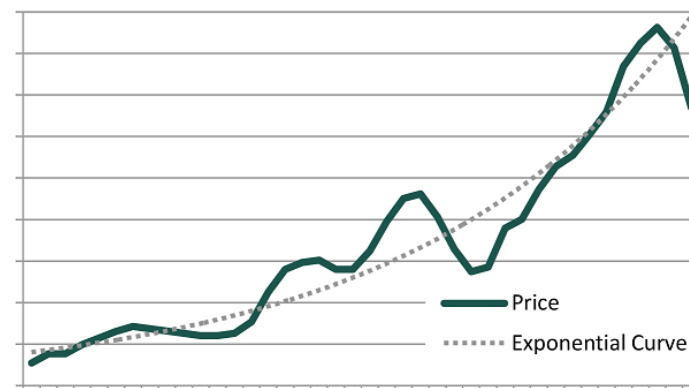
[Bill Details](#)



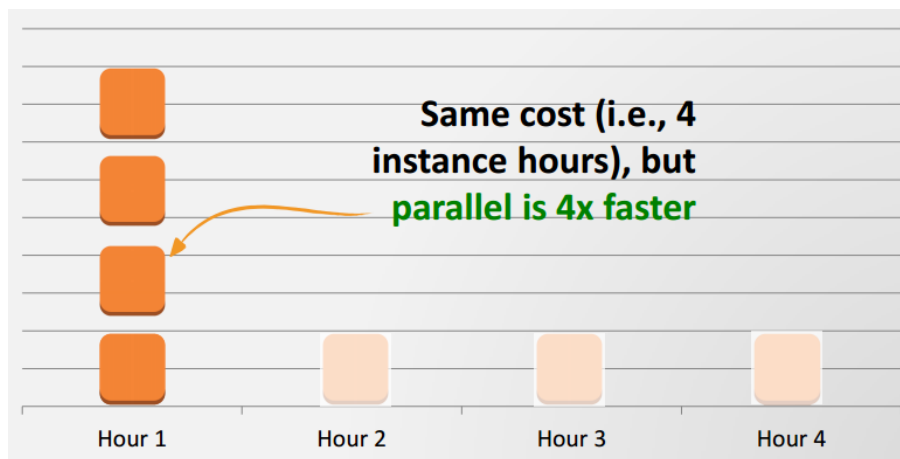
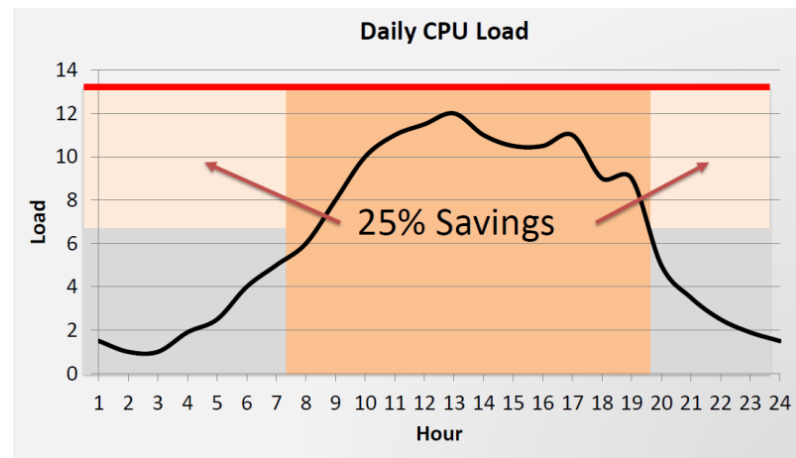
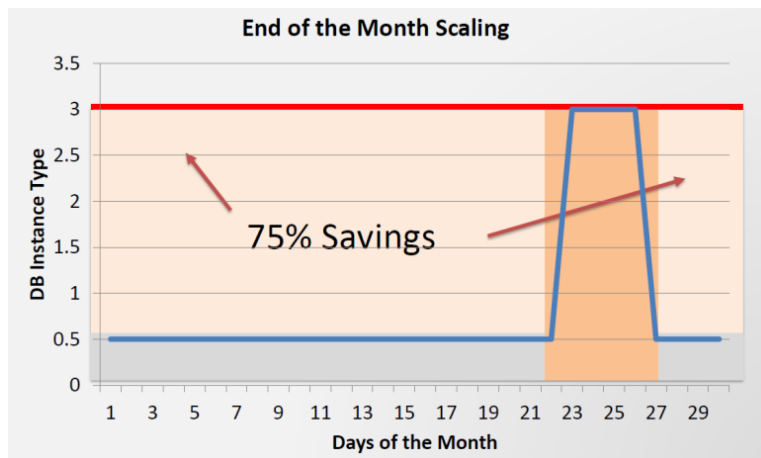
| Top Services | Amount |
|----------------|-------------------|
| EC2 | \$1,181.76 |
| RDS | \$508.53 |
| ElastiCache | \$248.48 |
| VPC | \$96.30 |
| Other Services | \$133.95 |
| Tax | \$0.00 |
| Total | \$2,169.02 |

Model kosztów

- pay per use – opłata za rzeczywiste zużycie
 - pre-paid
 - post-paid
- mierzalność zużycia usług
- przykładowe cenniki
 - Used Elastic IP – free
 - Unused Elastic IP – \$.005 / h
 - ELB - \$.025 / h + \$.0008 / GB
 - EBS - \$.10 GB/month + \$.10 per 1M I/O
 - S3 - \$.076 GB/month + \$.005 per 1K req.



Optymalizacja kosztów



Model kosztów EC2

- Różne ceny dla różnych typów instancji
- Inne ceny w różnych regionach
- Różne modele rozliczania
 - On-demand
 - Reserved
 - Light
 - Medium
 - Heavy
 - Spot
- Powyższe modele dotyczą jedynie rozliczania – godziny per typ instancji są przeliczane na koniec miesiąca. Można gasić i uruchamiać różne instancje w obrębie jednego abonamentu reserved.

Reserved Instance Cost Savings Over On-Demand

(m1.large - Linux - One Year RI)

| Annual Utilization | On Demand | Light Utilization RI | Medium Utilization RI | Heavy Utilization RI |
|--------------------|------------|----------------------|-----------------------|----------------------|
| 10% | \$234.00 | -77.95% | -210.43% | -479.49% |
| 20% | \$468.00 | -18.97% | -73.68% | -189.74% |
| 30% | \$702.00 | 0.68% | -28.09% | -93.16% |
| 40% | \$936.00 | 10.51% | -5.30% | -44.87% |
| 50% | \$1,170.00 | 16.41% | 8.38% | -15.90% |
| 60% | \$1,404.00 | 20.34% | 17.49% | 3.42% |
| 70% | \$1,638.00 | 23.15% | 24.00% | 17.22% |
| 80% | \$1,872.00 | 25.26% | 28.89% | 27.56% |
| 90% | \$2,106.00 | 26.89% | 32.69% | 35.61% |
| 100% | \$2,340.00 | 28.21% | 35.73% | 42.05% |



Optimal Savings



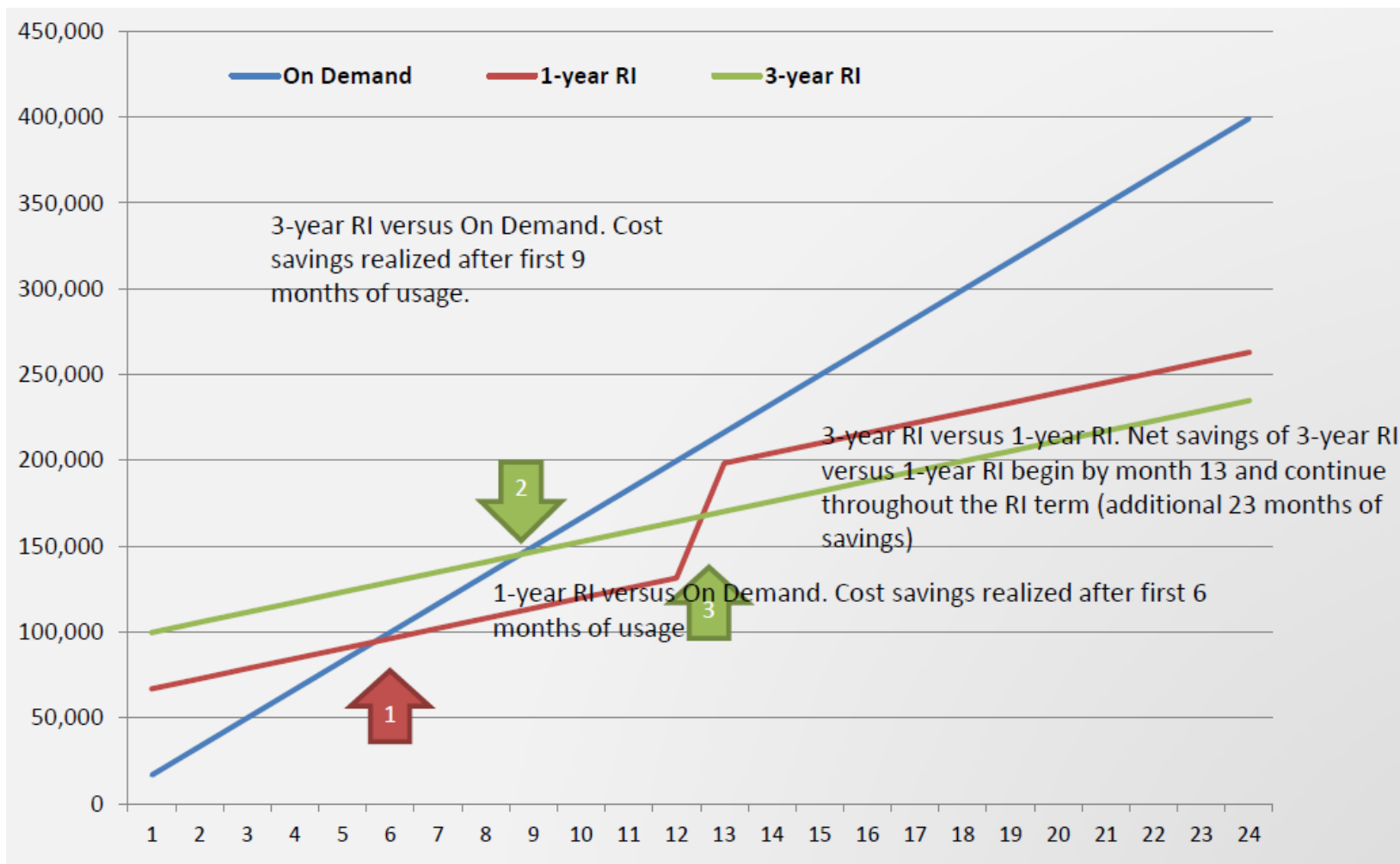
Sub-Optimal Savings



Least Savings



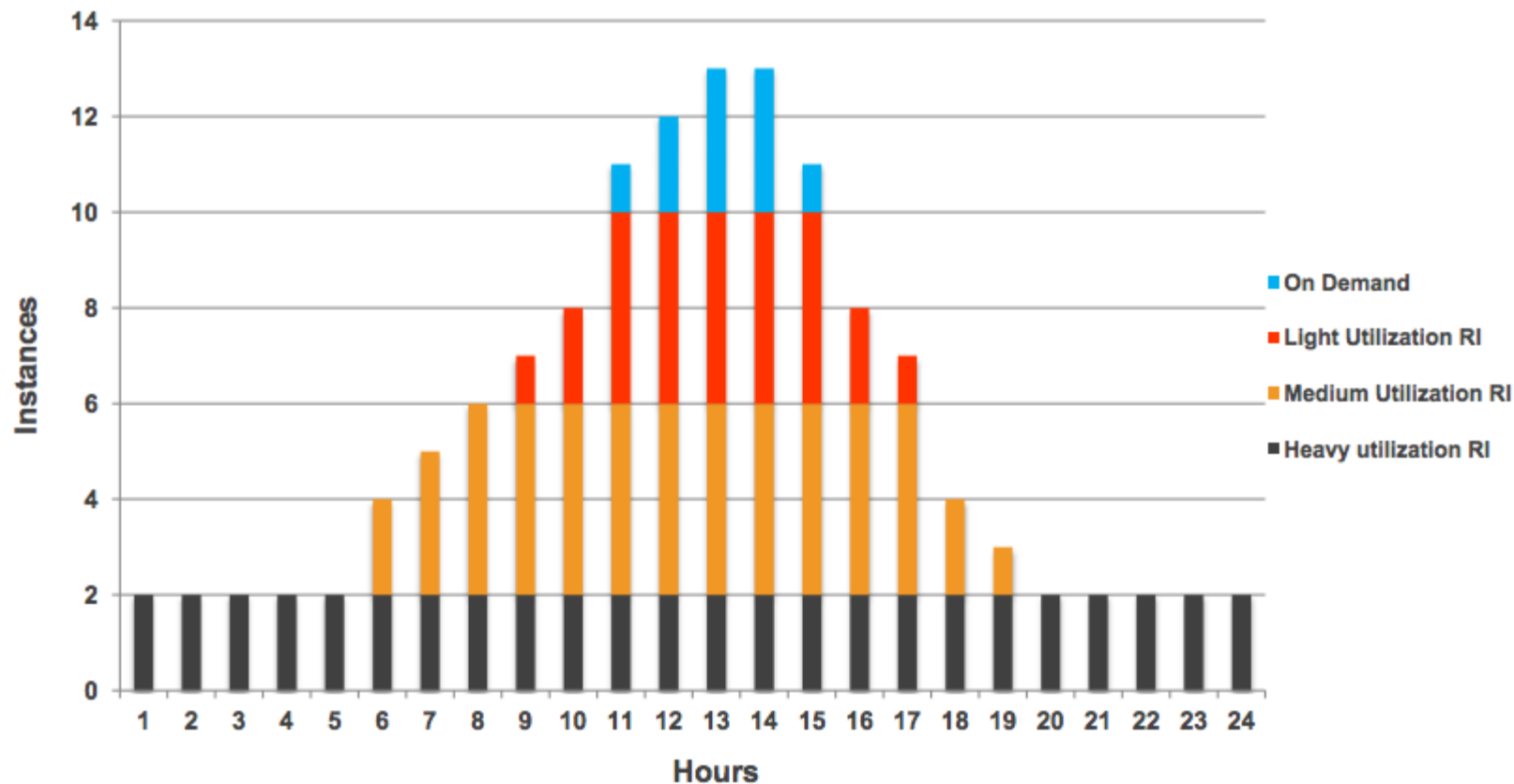
Koszty EC2 – on-demand vs reserved



<http://whichinstance.com/>

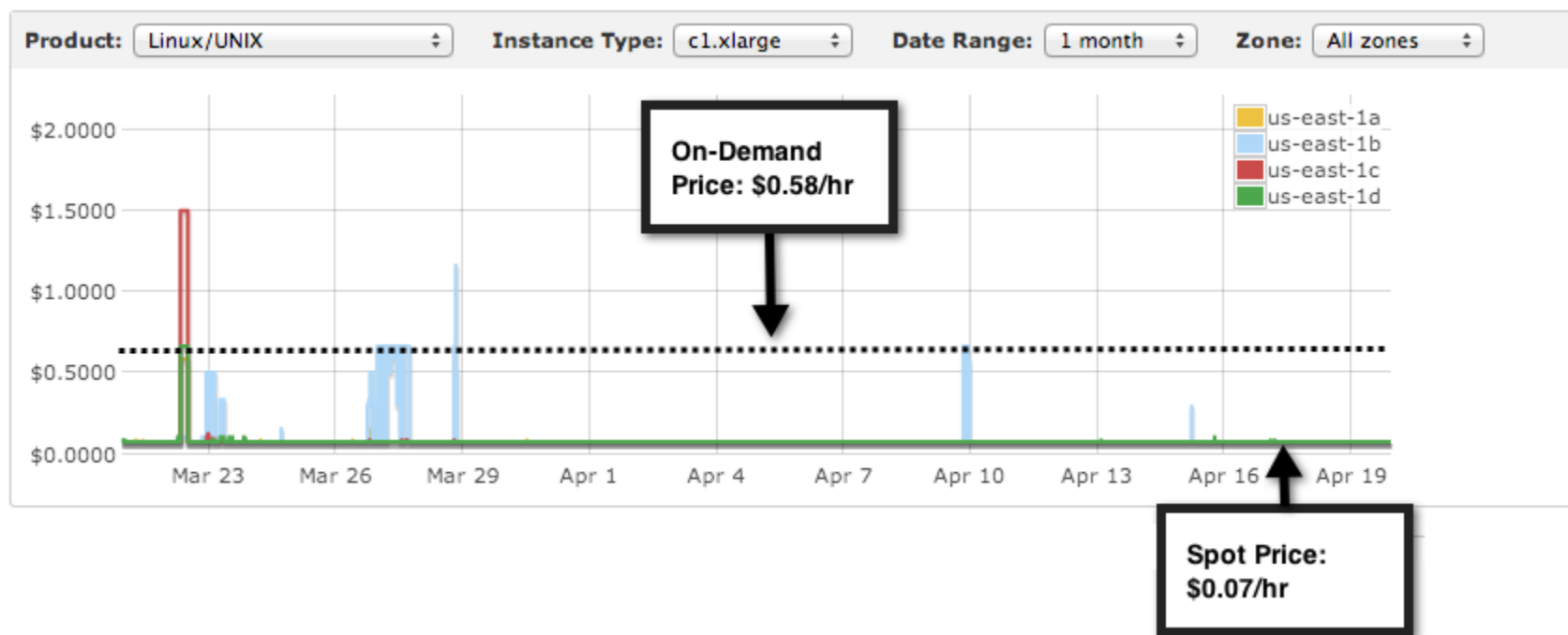


Wykorzystanie różnych instancji EC2



Instancje Spot

- Cena zależna od podaży i popytu, zmienna w czasie
- Dobrze nadaje się do przetwarzania wsadowego, asynchronicznego itp.
- Można próbować instancji spot, a jeśli się nie uda uruchomić on-demand
- Można łączyć: np. master-node on-demand i worker node'y spot



- Jinesh Varia
Architecting for the Cloud: Best Practices
- Amazon Web Services
Architecting on AWS – Designing for Cost
- Amazon Web Services
Architecting on AWS – IAM
- Amazon Web Services
Architecting on AWS – VPC
- Amazon Web Services
AWS Overview of security processes
- AWS Architecture Center
<http://aws.amazon.com/architecture/>
- US National Institute of Standards and Technology
NIST Cloud Computing Reference Architecture

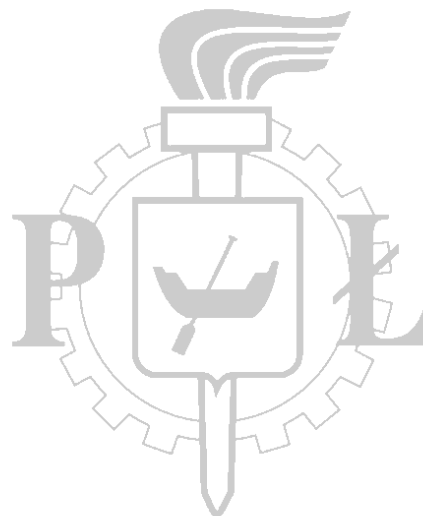




wydział
elektrotechniki
elektroniki
informatyki
i automatyki

AMG.net

A Bull Group Company



Dziękujemy za uwagę