Bezpieczne architektury, część 1: IAM, role, organizacje i SCP

Poziom: średnio

Dotyczy: SAA-C03 domena 1, zadanie 1.1 (bezpieczny dostęp do zasobów AWS), IAM, AWS STS, IAM Identity Center, AWS Organizations, IAM Access Analyzer, dni 3 do 5 planu

Czas: 3 dni po 1,5 godziny

Domena bezpiecznych architektur to 30 procent egzaminu, najwięcej ze wszystkich, a jej pierwsza część pyta o to, kto może co zrobić. Ta strona opisuje użytkowników, grupy, role, polityki i logikę, według której AWS rozstrzyga, czy żądanie przejdzie, a potem organizacje, polityki SCP i dostęp między kontami.

ZAŁOŻENIA SCENARIUSZA

ćwiczenia robimy na koncie `zielona-lab-aws` w organizacji ze strony Plan 28 dni i laboratorium AWS w Zielonej, zalogowani przez Identity Center jako `tomek`. Polityki SCP zakładamy z konta zarządzającego. Dostęp między kontami ćwiczymy między kontem laboratorium a kontem zarządzającym, a w opisie sklepu B2B jest to konto produkcyjne, którego w laboratorium nie mamy.

Skróty użyte na tej stronie (18)

Skrót	Co znaczy
ARN	Amazon Resource Name: jednoznaczna nazwa zasobu AWS, na przykład arn:aws:s3:::nazwa-kubelka
AWS	Amazon Web Services: chmura Amazonu
B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu

Skrót	Co znaczy
CSV	w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami
EC2	Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny
IAM	Identity and Access Management: zarządzanie tożsamościami i uprawnieniami (w AWS: użytkownicy, role, polityki)
JSON	JavaScript Object Notation: tekstowy format danych z klamrami i cudzysłowami
KMS	Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
OU	Organizational Unit: folder w Active Directory grupujący konta i komputery
RCP	Resource Control Policy: polityka organizacji AWS ograniczająca, co można zrobić z zasobami w kontach członkowskich, także z zewnątrz
S3	Simple Storage Service: magazyn plików w chmurze AWS
SAA-C03	kod wersji egzaminu AWS Solutions Architect Associate zdawanej od 30 sierpnia 2022, aktualnej w październiku 2026
SCP	Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym
STS	Security Token Service: usługa AWS wydająca tymczasowe poświadczenia, na przykład po przyjęciu roli
VPC	Virtual Private Cloud: prywatna sieć wirtualna klienta w chmurze AWS, w której stawiamy maszyny i zakładamy tablice tras
WWW	World Wide Web: strony i aplikacje otwierane w przeglądarce po HTTP albo HTTPS

Fiszka

Komendy wykonujemy w CloudShell albo w bash z profilem Identity Center. Pliki JSON z politykami stoją w Fiszce pod komendami, które ich używają. `IdKonta`, `NazwaRoli`, `NazwaPolityki`, `ArnPolityki`, `IdPolityki` i `IdJednostki` zastępujemy własnymi.

□□ ZMIENIA SYSTEM

Utworzenie polityki zarządzanej przez klienta: aws iam create-policy

```
aws iam create-policy --policy-name NazwaPolityki --policy-document file://odczyt-zdjec.json
```

Polityka zarządzana przez klienta to osobny obiekt z własnym ARN i wersjami, który podpinamy do wielu ról. Polityka wpisana bezpośrednio w jedną rolę (inline) znika razem z nią.

ARN = Amazon Resource Name: jednoznaczna nazwa zasobu AWS, na przykład arn:aws:s3:::nazwa-kubelka · **aws** = AWS CLI: narzędzie chmury Amazonu

PLIK KONFIGURACYJNY

Polityka odczytu jednego prefiksu kubełka: odczyt-zdjec.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListaTylkoPrefiksuZdjecia",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::NazwaKubelka",
      "Condition": { "StringLike": { "s3:prefix": ["zdjecia/*"] } }
    },
    {
      "Sid": "OdczytObiektowZdjecia",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::NazwaKubelka/zdjecia/*"
    }
  ]
}
```

`ListBucket` dotyczy kubełka, a `GetObject` obiektów, dlatego zasoby różnią się końcówką `/*`. To jedna z najczęstszych pomyłek w politykach S3.

S3 = Simple Storage Service: magazyn plików w chmurze AWS

ZMIENIA SYSTEM

Utworzenie roli dla instancji EC2: aws iam create-role

```
aws iam create-role --role-name NazwaRoli --assume-role-policy-document file://zaufanie-ec2.json
```

Rola ma dwie polityki: zaufania (kto może ją przyjąć) i uprawnień (co wolno po przyjęciu). Ten plik to polityka zaufania.

EC2 = Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny · **aws** = AWS CLI: narzędzie chmury Amazonu

PLIK KONFIGURACYJNY

Polityka zaufania roli dla EC2: zaufanie-ec2.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

EC2 = Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny

TYLKO ODCZYT

Podpięcie polityki uprawnień do roli: aws iam attach-role-policy

```
aws iam attach-role-policy --role-name NazwaRoli --policy-arn ArnPolityki
```

aws = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie profilu instancji z rolą: aws iam create-instance-profile

```
aws iam create-instance-profile --instance-profile-name NazwaRoli
aws iam add-role-to-instance-profile --instance-profile-name NazwaRoli --role-name
```

```
NazwaRoli
```

Instancja EC2 nie dostaje roli wprost, tylko profil instancji, który ją zawiera. Konsola robi to za nas, w CLI robimy to ręcznie.

EC2 = Elastic Compute Cloud: usługa AWS wynajmująca gotowe maszyny wirtualne na godziny · **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Symulacja uprawnień roli: aws iam simulate-principal-policy

```
aws iam simulate-principal-policy --policy-source-arn
arn:aws:iam::IdKonta:role/NazwaRoli --action-names s3:GetObject s3:PutObject --resource-
arns "arn:aws:s3:::NazwaKubelka/zdjecia/logo.png"
```

Przykład (kształt wyniku, skrócony):

```
{
    "EvaluationResults": [
        { "EvalActionName": "s3:GetObject", "EvalDecision": "allowed" },
        { "EvalActionName": "s3:PutObject", "EvalDecision": "implicitDeny" }
    ]
}
```

`implicitDeny` oznacza, że nic nie pozwala, a `explicitDeny`, że coś wprost zabrania. Symulator nie uwzględnia wszystkich rodzajów polityk (na przykład SCP przy symulacji z konta członkowskiego), więc wynik sprawdzamy też próbą.

SCP = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Ustawienie granicy uprawnień roli: aws iam put-role-permissions-boundary

```
aws iam put-role-permissions-boundary --role-name NazwaRoli --permissions-boundary
ArnPolityki
```

Granica uprawnień to sufit: rola może zrobić tylko to, na co pozwalają jednocześnie jej polityki i granica. Używamy jej, gdy pozwalamy programistom tworzyć role, ale nie silniejsze od ustalonego wzoru.

aws = AWS CLI: narzędzie chmury Amazonu

PLIK KONFIGURACYJNY

Polityka zaufania roli dla innego konta z identyfikatorem zewnętrznym: zaufanie-konto.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::IdKontaZaufanego:root" },
      "Action": "sts:AssumeRole",
      "Condition": { "StringEquals": { "sts:ExternalId": "zielona-audyt-2026" } }
    }
  ]
}
```

`root` w zasadzie oznacza całe konto, które potem samo decyduje, kto u niego może przyjąć rolę. Identyfikator zewnętrzny chroni przed problemem zdezorientowanego zastępcy, gdy rolę przyjmuje firma zewnętrzna obsługująca wielu klientów. Przyjęcie roli poleceniem `aws sts assume-role` opisuje strona AWS CLI: instalacja, profile, poświadczenia.

AWS = Amazon Web Services: chmura Amazonu · **CLI** = Command Line Interface: praca przez wpisywanie komend w terminalu

TYLKO ODCZYT

Raport poświadczeń konta: aws iam generate-credential-report

```
aws iam generate-credential-report
aws iam get-credential-report --query Content --output text | base64 -d | cut -d, -f1,4,8,9,11
```

Raport to plik CSV z każdym użytkownikiem IAM: czy ma hasło, MFA, klucze i kiedy były używane. Kolumny w `cut` to nazwa, hasło aktywne, MFA, klucz 1 aktywny i data ostatniego użycia klucza 1. Pan Wojtek pyta o to co roku.

CSV = w Windowsie: Cluster Shared Volume, dysk widoczny naraz dla wszystkich węzłów klastra; w danych: Comma-Separated Values, plik z wartościami oddzielonymi przecinkami · **IAM** = Identity and Access Management: zarządzanie tożsamościami i uprawnieniami (w AWS: użytkownicy, role, polityki) · **MFA** = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu · **aws** = AWS CLI: narzędzie chmury Amazonu

TYLKO ODCZYT

Sprawdzenie MFA użytkownika głównego: aws iam get-account-summary

```
aws iam get-account-summary --query "SummaryMap.AccountMFAEnabled"
```

Wynik `1` oznacza włączone MFA na użytkowniku głównym konta.

MFA = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Utworzenie analizatora dostępu z zewnątrz: aws accessanalyzer create-analyzer

```
aws accessanalyzer create-analyzer --analyzer-name NazwaAnalizatora --type ACCOUNT
```

IAM Access Analyzer przegląda polityki zasobów (kubełki, klucze KMS, role, kolejki) i zgłasza te, które dają dostęp spoza konta. Z `--type ORGANIZATION` granicą zaufania jest cała organizacja.

IAM = Identity and Access Management: zarządzanie tożsamościami i uprawnieniami (w AWS: użytkownicy, role, polityki) · **KMS** = Key Management Service: usługa chmurowa przechowująca i zarządzająca kluczami szyfrującymi · **aws** = AWS CLI: narzędzie chmury Amazonu

ZMIENIA SYSTEM

Włączenie typu polityk SCP w organizacji: aws organizations enable-policy-type

```
aws organizations enable-policy-type --root-id IdKorzenia --policy-type
SERVICE_CONTROL_POLICY
```

Wykonujemy raz, na koncie zarządzającym.

□□ **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **aws** = AWS CLI: narzędzie chmury Amazonu

□□ **ZMIENIA SYSTEM**

Utworzenie polityki SCP: aws organizations create-policy

```
aws organizations create-policy --name tylko-frankfurt --type SERVICE_CONTROL_POLICY --
description "Laboratorium tylko w eu-central-1" --content file://scp-tylko-
frankfurt.json
```

□□ **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **aws** = AWS CLI: narzędzie chmury Amazonu

□□ **TYLKO ODCZYT**

Podpięcie SCP do jednostki organizacyjnej: aws organizations attach-policy

```
aws organizations attach-policy --policy-id IdPolityki --target-id IdJednostki
```

SCP działa na wszystkie konta w jednostce, ale nie na konto zarządzające. Lista polityk podpiętych do celu: `aws organizations list-policies-for-target --target-id IdJednostki --filter SERVICE_CONTROL_POLICY`.

□□ **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **aws** = AWS CLI: narzędzie chmury Amazonu

□□ **PLIK KONFIGURACYJNY**

Polityka SCP blokująca regiony poza Frankfurtem: scp-tylko-frankfurt.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ZakazPozaFrankfurtem",
      "Effect": "Deny",
      "NotAction": [
        "a4b:*", "acm:*", "aws-marketplace-management:*", "aws-marketplace:*", "aws-
portal:*",
        "budgets:*", "ce:*", "chime:*", "cloudfront:*", "config:*", "cur:*",
"directconnect:*",
        "ec2:DescribeRegions", "ec2:DescribeTransitGateways", "ec2:DescribeVpnGateways",
        "fms:*", "globalaccelerator:*", "health:*", "iam:*", "importexport:*", "kms:*",
        "mobileanalytics:*", "networkmanager:*", "organizations:*", "pricing:*",
        "route53:*", "route53domains:*", "route53-recovery-cluster:*",
        "route53-recovery-control-config:*", "route53-recovery-readiness:*",
        "s3:GetAccountPublic*", "s3:ListAllMyBuckets", "s3:ListMultiRegionAccessPoints",
        "s3:PutAccountPublic*", "shield:*", "sts:*", "support:*", "trustedadvisor:*",
        "waf-regional:*", "waf:*", "wafv2:*", "wellarchitected:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": { "aws:RequestedRegion": ["eu-central-1"] },
        "ArnNotLike": { "aws:PrincipalARN":
["arn:aws:iam::*:role/OrganizationAccountAccessRole"] }
      }
    }
  ]
}
```

To przykład z dokumentacji AWS Organizations z naszym regionem. Lista `NotAction` wyłącza usługi globalne, których punkty końcowe są w `us-east-1`, a AWS ostrzega, że może nie obejmować najnowszych usług. Rola `OrganizationAccountAccessRole`, którą `create-account` zakłada w każdym nowym koncie, zostaje wyłączona spod zakazu jako awaryjne wejście.

□□ **SCP** = Service Connection Point: obiekt w Active Directory, po którym komputery domenowe znajdują swój tenant Entra ID przy dołączaniu hybrydowym · **AWS** = Amazon Web Services: chmura Amazonu

Z życia wzięte

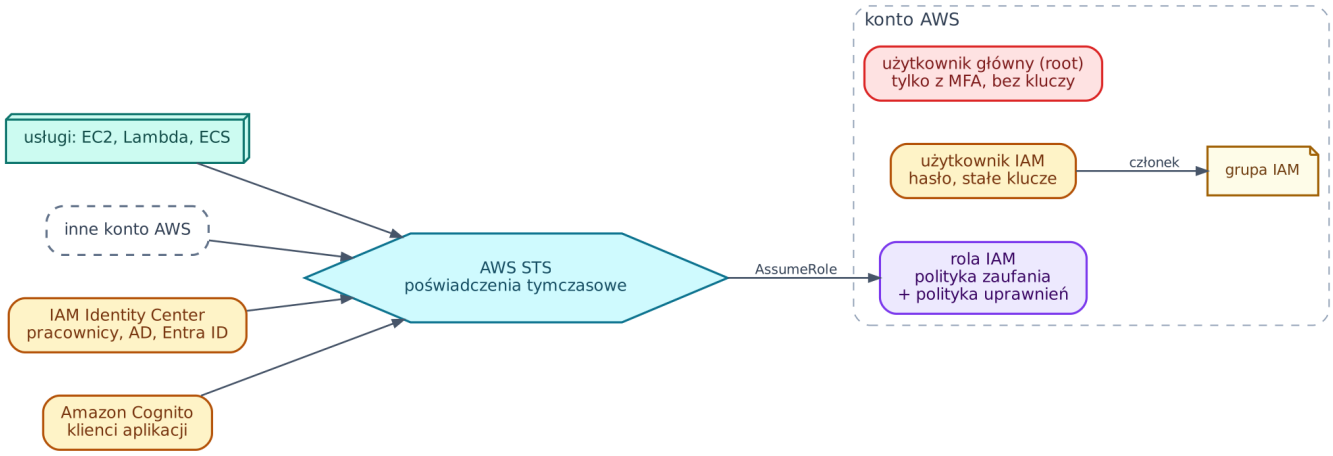
Z ŻYCIA WZIĘTE

Poniedziałek, 13:30. Ola prosi, żeby aplikacja sklepu w laboratorium czytała zdjęcia produktów z kubełka, i przysyła Tomkowi klucz dostępu, który „i tak już ma”. Tomek pyta, skąd go ma, i słyszy, że z pliku na `app01` sprzed dwóch lat. Zamiast wpisywać klucz do konfiguracji, Tomek zakłada rolę z polityką `odczyt-zdjec.json` i profil instancji, a stary klucz trafia na listę do wyłączenia po sprawdzeniu raportu poświadczeń. Ola przyznaje, że nie wiedziała, kto jeszcze używa tego klucza, i to jest najlepszy argument za rolą.

Jak to działa

Rozwiń: jak to działa pod spodem

Tożsamości w AWS



Rysunek 1. Tożsamości w AWS: użytkownik główny, użytkownicy IAM i grupy, role przyjmowane przez ludzi, usługi i inne konta, oraz użytkownicy Identity Center, którzy dostają role w kontach (kliknięcie otwiera pełny rozmiar)

Tożsamość	Poświadczenia	Kiedy jest odpowiedzią na egzaminie

Użytkownik główny (root)	e-mail i hasło konta	tylko zadania, które go wymagają (zmiana planu wsparcia, zamknięcie konta); zawsze z MFA, bez kluczy
Użytkownik IAM	hasło i klucze, stałe	rzadko: stary system, który nie umie przyjąć roli
Grupa IAM	brak, to zbiór użytkowników	nadanie tych samych uprawnień wielu użytkownikom IAM; grupa nie może być zasadą w polityce
Rola IAM	tymczasowe, z AWS STS	usługi (EC2, Lambda, ECS), dostęp między kontami, federacja
Użytkownik Identity Center	logowanie przez portal, tymczasowe	ludzie w organizacji z wieloma kontami

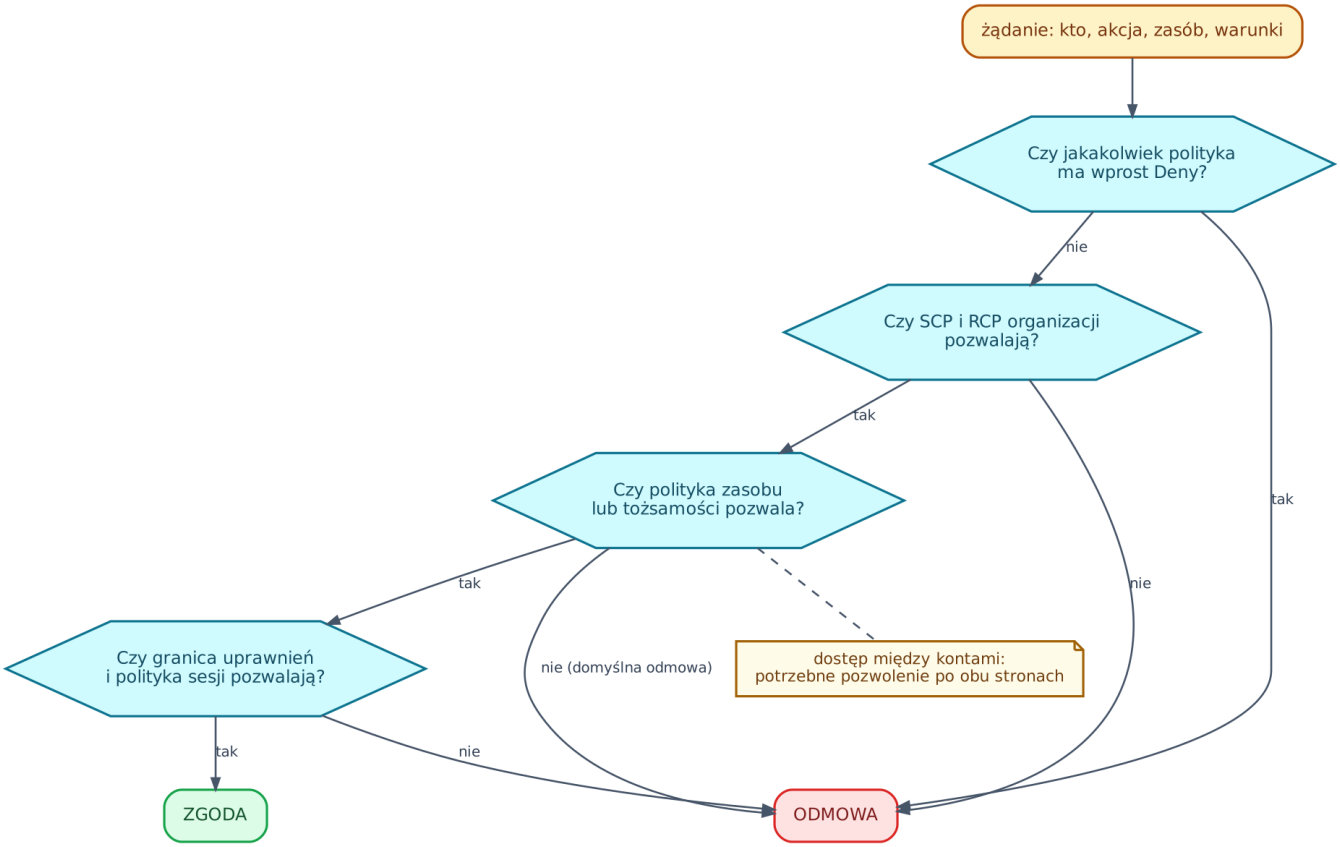
> **Pojęcie: AWS STS (Security Token Service).** Usługa, która wydaje tymczasowe poświadczenia: klucz, sekret i token sesji z datą wygaśnięcia. Każde przyjęcie roli, logowanie przez Identity Center i federacja kończy się wywołaniem STS.

> **Pojęcie: federacja.** Logowanie do AWS kontem z zewnętrznego katalogu (Active Directory, Entra ID, Google) bez zakładania użytkowników IAM. Dostawca tożsamości potwierdza, kim jest człowiek, a AWS daje mu rolę. Dla pracowników odpowiedzią jest Identity Center, dla klientów aplikacji mobilnej albo WWW Amazon Cognito.

Polityki i logika oceny

> **Pojęcie: polityka.** Dokument JSON z listą instrukcji. Każda instrukcja ma efekt (`Allow` albo `Deny`), akcje, zasoby i opcjonalne warunki. Polityka tożsamości jest podpięta do użytkownika, grupy albo roli, a polityka zasobu do samego zasobu (kubełka, klucza KMS, kolejki) i ma dodatkowo pole `Principal`.

AWS zaczyna od odmowy i szuka pozwolenia. Wprost zapisane `Deny` wygrywa zawsze, niezależnie od tego, gdzie stoi. W jednym koncie wystarczy pozwolenie w polityce tożsamości albo w polityce zasobu, ale SCP, granica uprawnień i polityka sesji muszą pozwalać jednocześnie, bo działają jak filtry. Przy dostępie między kontami potrzebne są obie strony: polityka zasobu w koncie docelowym i polityka tożsamości w koncie źródłowym.



Rysunek 2. Kolejność oceny żądania: wprost zapisana odmowa, SCP i RCP organizacji, polityka zasobu, polityka tożsamości, granica uprawnień i polityka sesji; brak pozwolenia oznacza odmowę (kliknięcie otwiera pełny rozmiar)

Rodzaj polityki	Daje uprawnienia	Ogranicza uprawnienia	Gdzie
polityka tożsamości	tak	tak (przez `Deny`)	użytkownik, grupa, rola
polityka zasobu	tak	tak	kubełek S3, klucz KMS, kolejka SQS, rola (polityka zaufania)
SCP (Service Control Policy)	nie	tak, dla tożsamości w kontach członkowskich	organizacja, jednostka, konto
RCP (Resource Control Policy)	nie	tak, dla zasobów w kontach członkowskich	organizacja, jednostka, konto
granica uprawnień	nie	tak	użytkownik albo rola
polityka sesji	nie	tak	przy `assume-role`

> □□ RCP, czyli polityki kontroli zasobów, AWS dodał do Organizations pod koniec 2024 roku, po wydaniu przewodnika SAA-C03. Na egzaminie spodziewamy się głównie SCP. Gdy pytanie mówi o ograniczeniu, kto spoza organizacji może sięgnąć do zasobów, RCP jest poprawną odpowiedzią w dzisiejszym AWS, ale sprawdzamy, czy w ogóle pada jako opcja.

Organizacje, SCP i Control Tower

> **Pojęcie: AWS Organizations.** Usługa łącząca wiele kont AWS w drzewo: korzeń, jednostki organizacyjne (OU) i konta. Daje jeden rachunek za wszystkie konta, wspólne rabaty ilościowe i polityki działające z góry na całe gałęzie.

> **Pojęcie: SCP.** Polityka organizacji, która wyznacza maksimum tego, co wolno zrobić tożsamościom w kontach członkowskich, łącznie z ich użytkownikiem głównym. SCP sama niczego nie daje, a nie działa na konto zarządzające ani na role powiązane z usługami.

> **Pojęcie: AWS Control Tower.** Usługa, która zakłada gotową strefę lądowania (landing zone): organizację z kontami logów i audytu, IAM Identity Center i zestawem kontrolek, czyli gotowych SCP i reguł AWS Config. Na egzaminie jest odpowiedzią, gdy firma chce szybko i według dobrych praktyk uruchomić wiele kont z centralnym nadzorem.

Pułapki egzaminacyjne

- „Najmniejsze uprawnienia” (least privilege) oznacza politykę z konkretnymi akcjami i zasobami, a nie zarządzaną politykę `PowerUserAccess`.
- Aplikacja na EC2 albo w Lambdzie potrzebuje dostępu do S3: rola. Klucz w kodzie, w zmiennej środowiskowej albo w pliku jest zawsze złą odpowiedzią.
- Firma zewnętrzna potrzebuje dostępu do naszego konta: rola z zaufaniem do jej konta i `sts:ExternalId`, a nie użytkownik IAM z kluczem.
- Trzeba zabronić czegoś wszystkim kontom, także administratorom: SCP. Polityka IAM tego nie zrobi, bo administrator konta może ją zmienić.
- SCP z samym `Allow` niczego nie daje. Gdy użytkownik ma `AdministratorAccess`, a SCP pozwala tylko na S3, użytkownik może tylko S3.

- Dostęp do kubełka dla innego konta: polityka kubełka wskazująca konto plus polityka tożsamości w tamtym koncie.
- Grupa IAM nie może być wskazana w polu `Principal` polityki zasobu.

Częste błędy

Objaw	Przyczyna	Co robimy
`AccessDenied` mimo `Allow` w polityce tożsamości	`Deny` w SCP, w polityce zasobu albo granica uprawnień	`simulate-principal-policy`, a potem SCP na jednostce i polityka kubełka
`aws s3 ls s3://NazwaKubelka` działa, a pobranie pliku nie	polityka daje `ListBucket`, ale `GetObject` ma zły zasób	zasób z końcówką `/*` dla obiektów
Instancja nie widzi roli	rola bez profilu instancji albo profil nie podpięty	`create-instance-profile`, `add-role-to-instance-profile`, podpięcie w EC2
`assume-role` z innego konta odmawia	brak polityki tożsamości w koncie źródłowym albo zły `ExternalId`	obie strony zaufania i warunek
Po podpięciu SCP nie działa konsola w innym regionie	to zamierzone, SCP blokuje regiony	praca w `eu-central-1`
Po SCP przestało działać coś globalnego	usługa globalna spoza listy `NotAction`	dopisujemy usługę do listy wyjątków

□□ Ćwiczenia

1. Dzień 3. Tworzymy politykę `odczyt-zdjec.json` dla kubełka laboratorium, rolę `lab-ec2-zdjecia` z zaufaniem do EC2 i symulujemy `GetObject` na prefiksie `zdjecia/` i `faktury/`. Jakie dwie decyzje dostaniemy?

Odpowiedź

```
aws iam create-policy --policy-name lab-odczyt-zdjec --policy-document file://odczyt-zdjec.json
aws iam create-role --role-name lab-ec2-zdjecia --assume-role-policy-document file://zaufanie-ec2.json
aws iam attach-role-policy --role-name lab-ec2-zdjecia --policy-arn arn:aws:iam::IdKonta:policy/lab-odczyt-zdjec
aws iam simulate-principal-policy --policy-source-arn arn:aws:iam::IdKonta:role/lab-ec2-
```

```
zdjecia --action-names s3:GetObject --resource-arns
"arn:aws:s3:::NazwaKubelka/zdjecia/a.png" "arn:aws:s3:::NazwaKubelka/faktury/f.pdf"
```

Dla `zdjecia/a.png` decyzja `allowed`, dla `faktury/f.pdf` decyzja `implicitDeny`, bo żadna instrukcja nie obejmuje tego zasobu. Na koniec dnia usuwamy rolę i politykę (`detach-role-policy`, `delete-role`, `delete-policy`).

1. Dzień 4. Firma audytorska pana Wojtka ma własne konto AWS i ma czytać konfigurację naszego konta przez rok. Opisujemy rozwiązanie w trzech zdaniach i podajemy dwie rzeczy, które ustawiamy w polityce zaufania.

Odpowiedź

Tworzymy rolę z polityką uprawnień `SecurityAudit` (polityka zarządzana przez AWS do odczytu konfiguracji) i z polityką zaufania wskazującą konto firmy audytorskiej. Firma przyjmuje rolę przez `sts:AssumeRole` ze swojego konta i dostaje poświadczenia tymczasowe. Po roku usuwamy rolę albo zmieniamy zaufanie. W polityce zaufania ustawiamy `Principal` z ARN konta audytora i warunek `sts:ExternalId` z wartością uzgodnioną z audytorem.

1. Dzień 5. Podpinamy SCP `tylko-frankfurt` do jednostki `Laboratorium` i sprawdzamy, że w Irlandii nie da się utworzyć VPC. Jakie polecenie i jaki błąd spodziewamy się zobaczyć?

Odpowiedź

```
aws ec2 create-vpc --cidr-block 10.60.0.0/16 --region eu-west-1
```

Spodziewamy się błędu `UnauthorizedOperation` z informacją, że żądanie zostało odrzucone wprost przez politykę kontroli usług (treść komunikatu sprawdzamy w laboratorium). Ten sam test w `eu-central-1` działa. Testowe VPC usuwamy, a SCP zostawiamy do końca kursu.

1. Pytanie w stylu egzaminu: zespół programistów ma tworzyć role dla swoich funkcji Lambda, ale żadna z tych ról nie może mieć uprawnień do IAM ani do usuwania kopii zapasowych. Co jest najprostszym rozwiązaniem w jednym koncie?

Odpowiedź

Granica uprawnień (permissions boundary) bez akcji `iam:*` i `backup:Delete*`, plus polityka programistów, która pozwala na `iam:CreateRole` tylko z warunkiem `iam:PermissionsBoundary` równym ARN tej granicy. SCP też by zadziałała, ale dotyczy całego konta, także administratorów, a w jednym koncie bez organizacji nie istnieje.

1. Pytanie w stylu egzaminu: firma ma 40 kont i chce, żeby żadne z nich nie mogło wyłączyć CloudTrail, nawet przez administratora konta. Która usługa?

Odpowiedź

SCP w AWS Organizations z `Deny` dla `cloudtrail:StopLogging` i `cloudtrail:DeleteTrail`, podpięta do korzenia albo jednostek. Alternatywnie Control Tower, który zakłada taką kontrolkę sam. Polityki IAM w każdym koncie są złą odpowiedzią, bo administrator może je zmienić.

Krok projektu: sklep B2B

W projekcie sklepu zakładamy trzy konta w jednostce `Sklep`: `sklep-prod`, `sklep-test` i wspólne `logi`, wszystkie pod SCP, która różni się od laboratoryjnej tylko listą regionów: `eu-central-1` i region zapasowy `eu-west-1` dla odtwarzania po katastrofie, oraz z zakazem wyłączania CloudTrail. Kasia dostaje w Identity Center zestaw tylko do odczytu na `sklep-prod`, zespół Oli `PowerUserAccess` na `sklep-test`, a aplikacja na EC2 rolę z odczytem zdjęć i sekretu bazy. Żaden człowiek nie ma klucza dostępu.

Powiązane: Bezpieczne architektury, część 2: VPC, szyfrowanie KMS, sekrety i ochrona aplikacji · Konto i uprawnienia do pobierania plików z S3 · AWS CLI: instalacja, profile, poświadczenia

Źródła: przewodnik SAA-C03, domena 1, zadanie 1.1; dokumentacja IAM (logika oceny polityk, granice uprawnień, profile instancji, raport poświadczeń, problem zdezorientowanego zastępcy); dokumentacja AWS Organizations (SCP, przykład blokady regionów, RCP); dokumentacja IAM Access Analyzer; dokumentacja AWS Control Tower. Parametry poleceń sprawdzone z modelem usług AWS CLI (botocore 1.43) 19 października 2026.

Revision #3
Created 2026-10-18 23:00:33 UTC by Tomasz Konieczny
Updated 2026-10-26 14:27:30 UTC by Tomasz Konieczny