FTC

Konfiguracja konta Google Cloud

10 kroków dla użytkowników chmury Google

Ta lista, składająca się z 10 kroków, pozwoli Ci skonfigurować konto Google Cloud tak, by zachować wysoki poziom bezpieczeństwa, kontrolę nad zasobami organizacji i dostępami oraz możliwości późniejszego bezproblemowego skalowania.

W dokumencie przedstawiliśmy najpopularniejszy, najbardziej uniwersalny sposób wykonywania danych kroków, ale możesz modyfikować zadania w zależności od potrzeb swojej organizacji. W wielu miejscach znajdują się odnośniki do oficjalnej dokumentacji Google, które dokładniej opisują dane zagadnienie.

Nawet jeśli już posiadasz obciążenia w chmurze Google, polecamy zapoznać się z krokami i zweryfikować, czy konfiguracja została przeprowadzona zgodnie z dobrymi praktykami Google.

> *Materiał został opracowany na podstawie oficjalnej dokumentacji Google Cloud.*

Spis treści

1. Zabezpieczenie konta Google

Do produktów chmurowych – zarówno do Google Workspace, Google Cloud Platform czy Google Identity – logujemy się za pomocą głównego konta Google. Odpowiednia konfiguracja zabezpieczeń jest podstawą dalszych działań. Jeśli gdziekolwiek zostawimy lukę, nieupoważniona osoba może uzyskać dostęp do zasobów. A jeśli konto ma wysokie uprawnienia w organizacji, włamanie może być naprawdę nieprzyjemne w skutkach.

W celu konfiguracji zabezpieczeń konta Google:

a) Przeprowadź kontrolę bezpieczeństwa pod adresem https://myaccount.google.com/security-checkup.

b) Zadbaj o silne hasło do swojego konta Google. Hasło powinno mieć inną treść niż na pozostałych portalach – w przypadku wycieku danych z innego serwisu, nieupoważniona osoba może skompletować dane logowania do Twojego konta Google. Do generowania i przechowywania danych dostępu możesz korzystać z managera haseł Google lub od zewnętrznego dostawcy, np. Bitwarden czy LastPass.

c) Upewnij się, że masz przypisane do konta zewnętrzny adres email i numer telefonu. Google będzie przesyłać Ci powiadomienia o podejrzanej aktywności na koncie, a Ty będziesz miał(-a) możliwość zdalnego zablokowania konta, jak też przywrócenia dostępu.

d) Upewnij się, że masz włączoną weryfikację dwuetapową (2FA). Łączy się to z potrzebą potwierdzenia logowania na zaufanym urządzeniu (np. smartfonie), do którego dostęp masz tylko Ty.

e) Aktualizuj używane oprogramowania do najnowszej oficjalnej wersji – przeglądarkę internetową, aplikację mobilną, system operacyjny na komputerze czy smartfonie. Wraz z nowymi wersjami, twórcy wprowadzają kolejne łatki bezpieczeństwa.

f) Zrób przegląd aplikacji, które mają dostęp do danych konta Google i wyłącz te, które wzbudzają Twoje podejrzenia. Dostępami aplikacji możesz zarządzać pod adresem https://myaccount.google.com/permissions. Unikaj instalowania aplikacji z nieoficjalnych źródeł.

g) Włącz blokadę ekranu, jako dane do odblokowania wskaż hasło lub kod pin (są skuteczniejsze niż metody biometryczne). Automatyczne wygaszanie urządzenia to dodatkowa warstwa zabezpieczenia.

2. Utworzenie konta superadministratora

Konto superadministratora to konto o najszerszym dostępie do usług ekosystemu Google. Konto superadmina **nie jest** polecane do codziennej pracy w środowisku chmurowym, a jedynie do wykonania pierwszych kroków konfiguracyjnych czy aktualizacji.

Powinno być dobrze zabezpieczone i odizolowane od środowiska GCP. W momencie gdy utworzymy grupę o dostępie administratorów w konsoli chmurowej, powinniśmy korzystać z niego zamiast z konta superadmina do codziennej pracy (z wyjątkiem sytuacji, gdy potrzebne będzie wprowadzenie zmian w, przykładowo, ustawieniach usługi zarządzania tożsamością Cloud Identity).

Zanim zaczniesz konfigurację konta superadministratora:

a) Zapoznaj się z dobrymi praktykami zabezpieczenia konta superadministratora.

b) Przygotuj adres email, który będzie używany jako adres do logowania do konta superadministratora, np. adam@nazwa-firmy.com. Adres będzie potrzeby w procesie tworzenia konta.

c) Przygotuj inny adres email, który będzie połączony z kontem superadmina. Dodatkowy adres będzie potrzebny do rejestracji w usłudze Cloud Identity oraz do odzyskiwania dostępu do głównego konta. Powinien być to adres spoza domeny organizacji.

d) Przygotuj dostęp administratora do strefy DNS.

Do wykonania kolejnych kroków potrzebna będzie aplikacja Cloud Identity w konsoli administracyjnej Google Workspace. Cloud Identity pozwala w jednolity sposób zarządzać tożsamością, dostępami i endpointami w wielu usługach Google. W ramach Cloud Identity otrzymujesz 50 bezpłatnych licencji. W razie potrzeby możesz rozszerzyć pakiet o kolejne bezpłatne licencje lub przejść na wersję premium.

Jeśli jesteś nowym użytkownikiem Cloud Identity:

a) Wejdź pod adres https://workspace.google.com/signup/gcpidentity/welcome, gdzie utworzysz konto Cloud Identity. Możesz również zlecić wykonanie tego kroku inżynierom chmurowym FOTC.

b) Przeprowadź weryfikację domeny. Konfiguracja może zająć do kilku godzin.

c) Gdy zostaniesz poproszony o dodanie użytkowników, pomiń ten krok (wybierz **I have finished adding users for now**), ponieważ grupy użytkowników będziemy tworzyć na dalszym etapie konfiguracji.

Jeśli jesteś użytkownikiem Google Workspace:

a) Dodaj licencje Cloud Identity do konta Google Workspace. Możesz to zrobić z konta superadministratora w zakładce **Billing > Get more services > Cloud Identity** lub z pomocą partnera Google Cloud.

b) Wyłącz automatyczne przyznawanie licencji. W innym przypadku wszyscy nowi użytkownicy Google Identity będą otrzymywali również płatne konto Google Workspace, co może niepotrzebnie generować koszty.

3. Utworzenie grup i dodanie użytkowników

W tym kroku dodajemy użytkowników i tworzymy grupy (na razie nie nadajemy uprawnień – tym zajmiemy się w następnym kroku). Zadanie będziemy realizować w konsoli administracyjnej Google Workspace oraz konsoli Google Cloud Platform.

WAŻNE:

- Niektórzy użytkownicy w Twojej domenie mogą już mieć konta Google. Może się tak zdarzyć, gdy pracownik użyje adresu e-mail w domenie firmy, aby zarejestrować się w usłudze konsumenckiej Google, np. YouTube czy na Dysk Google. Musisz namierzyć te konta i zaplanować ich migrację oddzielnie od kont pozostałych użytkowników. Jeśli nie znajdziesz i nie przeniesiesz tych kont, w konsoli administracyjnej Google Workspace wystąpią konflikty kont.

Zanim zaczniesz:

a) Upewnij się, że w oknie przeglądarki jesteś zalogowany do konsoli administracyjnej Google Workspace oraz konsoli Google Cloud Platform na koncie superadministratora utworzonym w poprzednim kroku.

b) Przejdź do panelu konfiguracji: https://console.cloud.google.com/cloud-setup/.

- Jeśli organizacja już używa narzędzi do zarządzania tożsamością (np. Active Directory, Azure AD, Okta czy Ping Identity), możesz przeprowadzić integrację, by użytkownicy logowali się do Google Cloud z pomocą dotychczasowego narzędzia. Więcej informacji znajdziesz tutaj.

- Połącz Google Cloud Identity z usługą Active Directory, by zapewnić użytkownikom wygodne i bezpieczne logowanie jednokrotne (SSO).
- Lub utwórz własne rozwiązanie, korzystając z Google Workspace Admin SDK.

Dodawanie użytkowników w konsoli administracyjnej Google Workspace:

a) Zaloguj się do konsoli administracyjnej Google Workspace, używając konta superadministratora.

b) Dodaj użytkowników pojedynczo (tworząc konto dla każdego z osobna), grupowo (importując arkusz kalkulacyjny z danymi użytkowników) lub poprzez API (zalecane dla dużych organizacji, liczących tysiące pracowników).

Tworzenie grup

Korzystając z opcji Grupy w konsoli GCP możesz przypisać użytkowników do grup o różnym poziomie dostępu. Każda grupa w panelu IAM będzie miała przypisany unikalny adres email, np. gcp-organization-admins@nazwa-firmy.com.

Google zaleca, żeby utworzyć następujące grupy:

a) **gcp-organization-admins** – grupa użytkowników, którzy mogą administrować dowolnymi zasobami należącymi do organizacji. Osoby z tej grupy mają dostęp do wszystkich zasobów, dlatego należy być raczej powściągliwym w kwestii przyznawania uprawnień administratora;

b) **gcp-network-admins** – użytkownicy w tej grupie mogą tworzyć sieci, VPNy, firewalle, zarządzać urządzeniami sieciowymi czy load balancerami;

c) **gcp-billing-admins** – grupa mogąca zarządzać kontami rozliczeniowymi i kontrolować budżet;

d) **gcp-devops** – użytkownicy, którzy mają możliwość tworzenia i zarządzania pipelinami CI/CD oraz monitorowania działania systemu;

e) **gcp-developers** – osoby tworzące kod źródłowy i testujące aplikacje;

f) **gcp-security-admins** – grupa tworząca i zarządzająca zabezpieczeniami i politykami bezpieczeństwa dla całej organizacji.

Aby utworzyć grupy i dodać użytkowników w konsoli GCP:

a) Zaloguj się do konsoli GCP na konto superadministratora.

b) Przejdź do zakładki Groups (IAM & Admin > Groups).

c) Wciśnij **Create**.

d) Uzupełnij informacje o grupie – nazwę, adres email, opis.

e) Dodaj użytkowników do grupy. Wciśnij **Add member**, wprowadź adres email i wskaż rolę. Pamiętaj, że nawet jeśli przyznasz użytkownikowi indywidualnie niższy poziom dostępu, będzie miał on poziom dostępu przypisany grupie, w której się znajduje.

f) Wciśnij **Submit**, by utworzyć grupę składającą się ze wskazanych użytkowników.

WAŻNE:

- Google zaleca przyznawanie poziomów dostępu grupom, nie poszczególnym użytkownikom. Prowadź kontrolę dostępu opartą o role (role-based access control, RBAC). Przypisuj uprawnienia do grup użytkowników, posługując się funkcjonalnością Grup Google.

4. Przypisanie dostępu grupom

W tym kroku przyznajemy poziom dostępu nowo utworzonym grupom.

Upewnij się, czy organizacja została utworzona:

a) Zaloguj się do konsoli GCP używając konta superadministratora.

b) Przejdź do panelu Identity & Organization (IAM & Admin > Identity & Organization), by dokończyć tworzenie organizacji w konsoli GCP. Konfiguracja może zająć kilka minut.

c) Sprawdź, czy nazwa pojawia się na liście organizacji. Wejdź w listę projektów w niebieskim menu górnym, a następnie kliknij pasek **Select from** u góry okna pop-up. Nazwa może pojawić się dopiero po kilku minutach lub po odświeżeniu okna.

Ustawienie poziomu dostępu dla grupy

W tym kroku ustawiamy poziom dostępu dla grupy administratorów gcp-organization-admins@nazwa-firmy.com. Ten krok możesz wykonać następnie dla pozostałych grup, wskazując określony przez siebie zakres dostępu.

a) Upewnij się, że w konsoli GCP znajdujesz się w panelu organizacji, w obszarze której chcesz ustawić dostępy.

b) Kiedy zostaniesz poproszony o adres email, wpis adres grupy, np. gcp-organization-admins@nazwa-firmy.com.

c) Kiedy zostaniesz poproszony o wskazanie roli, wybierz **Resource Manager > Organization Administrator.**

d) Żeby dodać kolejne uprawnienia, kliknij **Add another role**. By administratorzy mieli niezbędne dostępy, poleca się przypisać grupie role:

- Resource Manager > Folder Admin
- Resource Manager > Project Creator
- Billing > Billing Account User
- Roles > Organization Role Administrator
- Organization Policy > Organization Policy Administrator
- Security Center > Security Center Admin
- Support > Support Account Administrator

e) Kiedy skończysz, kliknij **Save**.

Powtórz kroki dla kolejnych grup, wskazując niezbędne poziomy dostępów.

Pamiętaj o dobrych praktykach bezpieczeństwa

Przyznawaj dostępy zgodnie z zasadą najmniejszego uprzywilejowania (principle of least privilege). Przyzwanie użytkownikom najniższego niezbędnego poziomu dostępu pozwoli uniknąć powstawaniu awarii na skutek błędu ludzkiego czy zminimalizuje skutki ataku hakerskiego.

Po nadaniu uprawnień grupom powinieneś zrezygnować z używania konta superadministratora do dalszej konfiguracji środowiska GCP, a kolejne zadania delegować członkom poszczególnych grup. Odizolowanie konta superadministratora i ról administratorów w organizacji jest jedną z dobrych praktyk bezpieczeństwa zalecanych przez Google. Rola superadmina powinna zostać ograniczona do zarządzania tożsamościami w Cloud Identity i Google Workspace, rola administratora GCP do zarządzania zasobami w infrastrukturze chmurowej, a pozostałe role odpowiednio

przypisanym obszarom (np. zarządzaniu kontem rozliczeniowym, sieciami czy bezpieczeństwem).

5. Utworzenie hierarchii zasobów

W tym kroku tworzymy strukturę składającą się z folderów i projektów w odpowiedniej hierarchii.

a) **Foldery** pozwalają grupować i izolować zasoby wewnątrz projektu. Mogą wprowadzać podziały na zasoby pomiędzy, przykładowo, zespołami czy między środowiskami (developerskie, testowe, produkcyjne, itd.).

b) **Projekty** zawierają zasoby w chmurze, takie jak maszyny wirtualne, bazy danych, dyski pamięci.

Wprowadzenie podziału jest potrzebne, by móc w dalszej kolejności kontrolować, który członek organizacji ma dostęp do jakiego obszaru.

Ten krok może wykonać osoba o uprawnieniach administratora z grupy gcp-organization-admins@nazwa-firmy.com.

Przykładowy diagram hierarchii

W przykładzie podanym poniżej hierarchia zasobów w organizacji Example.com obejmuje cztery poziomy:

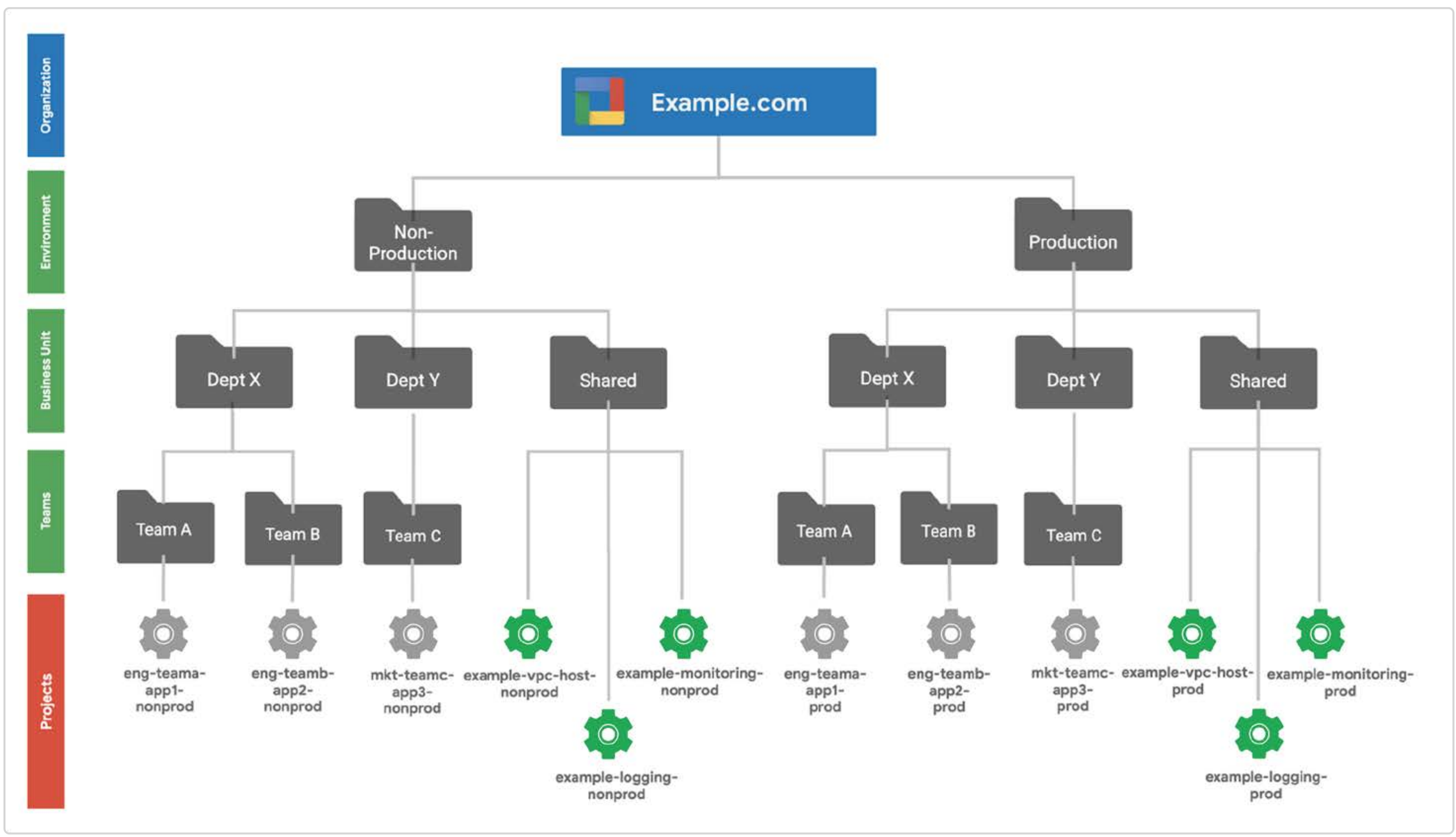
a) **Podział na zasoby produkcyjne i nieprodukcyjne.** Izolacja środowisk pozwala lepiej kontrolować zasoby i uniknąć błędów w aplikacji wynikających z wprowadzenia zmian w innym obszarze.

b) **Działy w firmie.** Na wykresie są zaprezentowane są jako Dept X oraz Dept Y, gdzie, przykładowo, jeden folder może zawierać zasoby działu marketingu, drugie

zespołu inżynieryjnego. Folder Shared zawiera zasoby współdzielone, np. sieci, logi i monitoring.

c) **Zespoły.** Na schemacie są one pokazane jako Team A, Team B i Team C. Mogą być to mniejsze zespoły w działach, zajmujące się, przykładowo, developmentem produktu, analityką danych czy obsługą witryny internetowej firmy.

d) **Projekty.** Najniżej w hierarchii, przypisane do folderu, znajdują się projekty.



By utworzyć folder:

a) Zaloguj się do konsoli GCP na koncie administratora.

b) Upewnij się, że znajdujesz się w panelu organizacji, w której chcesz utworzyć hierarchię. Sprawdzisz to na górnym niebieskim pasku menu.

c) Przejdź do sekcji Manage Projects and Folders (IAM & Admin > Manage resources).

d) Kliknij **Create folder**.

e) Podaj nazwę folderu.

f) W panelu **Destination** kliknij **Browse** i wskaż, pod którym węzłem lub innym folderem ma znaleźć się nowy folder.

g) Wciśnij **Create**.

h) Powtórz kroki w celu utworzenia kolejnych folderów.

By utworzyć projekt:

a) Zaloguj się do konsoli GCP na koncie administratora.

b) Upewnij się, że znajdujesz się w panelu organizacji, w której chcesz utworzyć hierarchię. Sprawdzisz to na górnym niebieskim pasku menu.

c) Przejdź do sekcji Manage Projects and Folders (IAM & Admin > Manage resources).

d) Kliknij **Create project**.

e) Wpisz nazwę projektu. Limit nazwy wynosi 30 znaków; żeby sprawnie poruszać się wśród projektów, Google proponuje przyjąć formę nazewnictwa `<dział>-<zespół>-<nazwa aplikacji>-<środowisko>`, na przykład `mkt-team1-companywebsite-prod` dla projektu zawierającego wersję produkcyjną strony internetowej.

f) Jeśli zostaniesz poproszony, wskaż konto rozliczeniowe, pod którym ma się znajdować projekt.

g) Wskaż, jaka ma być lokalizacja projektu. Kliknij w tym celu **Browse** i wybierz nazwę docelowego folderu.

h) Kliknij **Create**.

i) Powtórz kroki w celu utworzenia kolejnych projektów.

6. Przyznanie dostępów do poszczególnych poziomów

W tym kroku przyznajemy użytkownikom chmury role w oparciu o utworzoną hierarchię zasobów. Pozwoli to kontrolować i wygodnie skalować w przyszłości poziom dostępu do poszczególnych obszarów.

Ten krok może zrealizować osoba z grupy administratorów – gcp-organization-admins@nazwa-firmy.com.

Dostęp będziemy przyznawać na trzech poziomach:

a) **Organizacji** – użytkownik będzie miał dostęp do wszystkich folderów i projektów w danej organizacji;

b) **Folderu** – użytkownik będzie miał dostęp do podfolderów i projektów we wskazanym folderze;

c) **Projektu** – użytkownik będzie miał dostęp do zasobów we wskazanym projekcie.

WAŻNE

Pamiętaj o zasadzie principle of least privilege. Polecamy też przyznawać dostępy nie indywidualnym użytkownikom, a grupom. Tworzenie grup zostało opisane w punkcie 3.

Przyznawanie uprawnień na poziomie organizacji

a) Upewnij się, że jesteś zalogowany na koncie administratora z grupy gcp-organization-admins.

b) Przejdź do panelu Manage resources (IAM & Admin > Manage resources).

c) Na liście zaznacz okienko obok nazwy swojej organizacji.

d) Jeśli pasek **Info panel** jest ukryty, w prawym górnym rogu kliknij **Show info panel.**

e) W panelu Info panel przejdź do karty Permissions i wybierz **Add member**.

f) W formularzu wskaż adres mailowy grupy, które chcej przyznać dostęp.

g) W polu **Select a role** wskaż poziom dostępu.

h) Jeśli chcesz dodać kolejną rolę, kliknij **Add another role**.

i) Kiedy wszystko jest gotowe, kliknij **Save**.

j) W razie potrzeby powtórz kroki dla kolejnych grup użytkowników.

Przyznawanie uprawnień na poziomie folderu

a) W panelu Manage resources (IAM & Admin > Manage resources) odznacz pole przy organizacji i **zaznacz pole przy wybranym folderze.**

b) W panelu **Info panel**, w karcie **Permissions**, kliknij **Add member**.

c) W polu **New members** wpisz adres mailowy grupy, której chcesz przyznać dostęp.

d) W polu **Select a role** wskaż poziom dostępu.

e) Jeśli chcesz dodać kolejną rolę, kliknij **Add another role**.

f) Kiedy wszystko jest gotowe, kliknij **Save**.

g) W razie potrzeby powtórz krok dla kolejnych grup użytkowników oraz dla kolejnych folderów.

Przyznawanie uprawnień na poziomie projektu

a) W panelu Manage resources (IAM & Admin > Manage resources) odznacz pole przy folderze i **zaznacz pole przy wybranym projekcie lub projektach.**

b) W panelu **Info panel**, w karcie **Permissions**, kliknij **Add member**.

c) W polu **New members** wpisz adres mailowy grupy, której chcesz przyznać dostęp.

d) W polu **Select a role** wskaż poziom dostępu.

e) Jeśli chcesz dodać kolejną rolę, kliknij **Add another role**.

f) Kiedy wszystko jest gotowe, kliknij **Save**.

g) W razie potrzeby powtórz krok dla kolejnych grup użytkowników oraz dla kolejnych folderów.

7. Utworzenie i konfiguracja sieci wewnętrznej

W tym kroku konfigurujemy Virtual Private Cloud (VPC), czyli bezpieczne, prywatne środowisko dla zasobów znajdujących się w chmurze publicznej, również pomiędzy różnymi projektami. Za pośrednictwem VPC można utworzyć też środowisko hybrydowe łączące usługi Google Cloud z usługami innych dostawców czy wygodnie przeprowadzić migrację aplikacji do usług GCP z zachowaniem zależności poprzedniego środowiska.

Ten krok może wykonać administrator sieci z grupy dostępu gcp-network-admins@nazwa-firmy.com

Konfiguracja może przebiegać różnie w zależności od specyfiki posiadanego środowiska. Niżej podajemy listę czynności powtarzanych często wśród różnych środowisk, ale wskazujemy też źródła, które pomogą zgłębić dany obszar.

Konfiguracja wewnętrznej sieci w chmurze

a) **Utworzenie VPC.** Najwygodniej będzie Ci posłużyć się listą zadań w konsoli GCP.

b) **Ustawienie połączenia pomiędzy siecią zewnętrznego dostawcy a Google Cloud.** Jeśli korzystasz z infrastruktury on-premise lub usług innego dostawcy chmurowego, możesz włączyć usługę Cloud VPN, która pozwoli bezpiecznie połączyć sieci za pośrednictwem IPSec VPN. Cloud VPN jest odpowiednie dla połączeń o prędkości do 3.0 Gbps. Jeśli potrzebujesz szybszego połączenia aby połączyć sieci, zapoznaj się z Partner Interconnect i Dedicated Interconnect. By utworzyć połączenie VPN, postępuj zgodnie z instrukcjami zawartymi tutaj.

c) **Utworzenie ścieżki dla ruchu wychodzącego (egress).** Aby umożliwić maszynom wirtualnym połączenie z internetem bez angażowania zewnętrznego adresu IP, możesz posłużyć się usługą Cloud NAT. Możesz skonfigurować Cloud NAT w taki sposób, by umożliwiał ruch ze wszystkich adresów IP w danym regionie lub tylko określonego zakresu. Żeby utworzyć ścieżkę ruchu wychodzącego, postępuj zgodnie z instrukcjami zawartymi na tej podstronie.

d) **Implementacja mechanizmów zabezpieczeń sieci.** Zapory sieciowe umożliwiają filtrowanie ruchu, blokując ruch lub umożliwiając dostęp do instancji, zgodnie z ustaloną konfiguracją. Żeby utworzyć zapory firewall, postępuj zgodnie z tymi instrukcjami.

e) **Wskazanie opcji ruchu przychodzącego (ingress).** Cloud Load Balancing umożliwia kontrolę nad dystrybucją zasobów obliczeniowych w obrębie regionu. Load balancing pozwala spełnić wymagania dostępności dla ruchu przychodzącego i wychodzącego w sieci VPC. Tutaj zapoznasz się z rodzajami load balancerów i wybierzesz ten, który będzie odpowiadał potrzebom Twojej organizacji.

8. Konfiguracja monitoringu i eksportu logów

W tym kroku ustawiamy wskaźniki i powiadomienia, korzystając z usług dziennika logów Cloud Logging oraz panelu monitorowania zasobów Cloud Monitoring. Nadzorowanie zasobów w chmurze, poziomu wydajności i dostępności usług oraz aplikacji pozwala szybko namierzać i reagować na anomalie.

Ten krok może zostać zrealizowany przez specjalistę DevOps z grupy dostępów gcp-devops@nazwa-firmy.com

Cloud Monitoring

To narzędzie, które kolekcjonuje metryki, eventy i metadane z usług Google Cloud oraz z komponentów aplikacji. Aby uruchomić monitoring dla poszczególnych projektów:

a) Upewnij się, że jesteś zalogowany w konsoli chmurowej na koncie z poziomem dostępu gcp-devops w obszarze projektu, dla którego chcesz uruchomić usługę.

b) Z menu po lewej stronie wybierz usługę **Monitoring**.

c) Po kliknięciu zostanie automatycznie utworzony panel z podsumowaniem danego projektu. W panelu znajdą się informacje m.in. o monitorowanych zasobach, regułach dostępności czy incydentach.

d) Panel możesz dostosować tak, by po wejściu w usługę widzieć najważniejsze informacje. Możesz również ustawić reguły kontroli dostępu uptime checks czy polityki alertów, generujące powiadomienie w przypadku wystąpienia anomalii. Więcej informacji o opcjach konfiguracji usługi Cloud Monitoring znajdziesz w artykule na blogu FOTC.

Cloud Logging

Cloud Logging umożliwia przechowywanie, analizowanie, monitorowanie i powiadamianie o logach i eventach z usług Google Cloud Platform oraz połączonych usług Amazon Web Services. Pozwala też pobieranie określonego zakresu logów i eksportowania ich do zewnętrznych narzędzi analitycznych. Aby prowadzić eksport danych z usługi:

a) Upewnij się, że jesteś zalogowany w konsoli chmurowej na koncie z poziomem dostępu gcp-devops.

b) Włącz możliwość eksportowania logów do usługi BigQuery, posługując się następującymi wartościami:

- wskaż projekt, np. przykladowy-projekt-logi,
- utwórz zbiór danych BigQuery; jako **Dataset ID** podaj nazwę zbioru danych, np. `przykladowy_projekt_logi_eksport`,
- po wprowadzeniu nazwy, kliknij **Create dataset.**

c) Powtórz kroki dla kolejnych projektów.

d) Przejrzyj ustawienia okresowej retencji logów i zweryfikuj, czy spełniają wymagania Twojej organizacji. Jeśli nie, ustaw reguły eksportu logów do Cloud Storage.

9. Ustawienie alertów na koncie rozliczeniowym

Aktywne konto rozliczeniowe jest niezbędne, by korzystać z usług chmurowych. Konto billingowe jest połączone z przynajmniej jednym projektem w GCP i służy do płacenia za zasoby takie jak moc maszyn obliczeniowych, sieć czy pamięć. Na koncie rozliczeniowym można ustawić alerty, kiedy poziom zużycia osiągnie określony pułap.

Konfigurację powiadomień na koncie rozliczeniowym może wykonać osoba o poziomie dostępu administratora konta rozliczeniowego (gcp-billing-admins@nazwa-domeny.com).

Ustawienie powiadomień o zużyciu

a) W zakładce **Billing > Budgets & alerts** kliknij **Create budget.**

b) Podaj nazwę budżetu. Możesz wyznaczyć, które projekty lub usługi ma obejmować; jeśli tego nie zrobisz, ustawienie będzie monitorować całe zużycie dla wszystkich elementów.

c) Wskaż rodzaj budżetu – **Specified amount**, obejmujący dokładną kwotę lub **Last month's spend**, aktualizujący się automatycznie w oparciu o wydatki z poprzedniego miesiąca

d) Uzupełnij kwotę. Jeśli chcesz, by w budżecie były uwzględnione kredyty pochodzące z rabatów, promocji lub vouchera, zaznacz opcję **Include credits in cost.**

e) Wyznacz pułapy, na których chcesz otrzymywać notyfikacje. To może być powiadomienie otrzymywane w momencie osiągnięcia dokładnie określonej kwoty (**Trigger on: Actual**) lub powiadomienie o zbliżaniu się do pułapu (**Trigger on: Forecast**).

f) Po zapisaniu budżetu będzie on widoczny w zakładce **Billing > Budgets & alerts,** a notyfikacje będą przychodziły na adres mailowy.

Możesz ustawić wiele budżetów, np. budżet generalny (na całe zużycie GCP), osobny dla konkretnego projektu czy budżet obejmujący zestaw kilku lub kilkunastu usług.

10. Ustawienia zabezpieczeń organizacji

Żeby podnieść poziom zabezpieczeń organizacji w chmurze, zalecane jest wdrożenie usługi Security Command Center. To platforma do kompleksowego zarządzania bezpieczeństwem i ryzykiem związanym z przechowywaniem oraz przetwarzaniem danych, umożliwiająca monitorowanie zasobów w chmurze, skanowanie dysków w celu namierzenia wrażliwych danych, wykrywanie luk bezpieczeństwa czy przeglądania zakresu dostępu do krytycznych zasobów.

Ten krok może wykonać administrator z grupy dostępów gcp-organization-admins.

Uruchomienie usługi:

a) Upewnij się, że jesteś zalogowany na koncie administratora w konsoli GCP.

b) Włącz pulpit nawigacyjny Security Command Center.

c) Ustaw polityki organizacji postępując zgodnie z instrukcjami, uwzględniając:

- oznaczenie swojej organizacji, gdy zostaniesz poproszony o wskazanie projektu, folderu lub organizacji,
- wybór opcji **Skip default network creation** po wyświetleniu monitu o wybór ograniczenia z listy **Organization policies**,
- włączenie opcji wymuszania (**enforcement option: On**);

d) Skonfiguruj ograniczenia udostępniania w domenie.

e) Wyłącz dostęp zewnętrznych adresów IP do maszyn wirtualnych.

Chcesz nawiązać współpracę z FOTC? Skontaktuj się z Bartoszem

Bartosz Szymański

Google Cloud Platform Customer Guide

+48 532 519 008

bs@fotc.com

Jesteś naszym klientem i masz pytanie? Zgłoś się do Karola

Karol Mucha

Customer Success Specialist

+48 880 525 542

kmu@fotc.com

Polub nas na Facebooku

Zostań członkiem grupy Google Cloud Platform Polska

Dołącz do naszej sieci Linkedin