Użytkownicy i hasła

Poziom: średni **Dotyczy: SAP HANA 2.0 SPS ≥ 04** **Czas: ~25 min**

Konto `SYSTEM` w HANA jest odpowiednikiem `postgres` czy `root@localhost` — jedyne, którego zablokowanie albo utrata hasła bez trybu awaryjnego oznacza brak jakiegokolwiek sposobu na zalogowanie się do bazy przez SQL.

Skróty użyte na tej stronie (4)

Skrót	Co znaczy
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
HANA	SAP HANA: baza danych w pamięci firmy SAP, używana do dużych systemów księgowych i magazynowych
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung: niemiecki producent oprogramowania klasy ERP, właściciel silnika HANA i przejętego wcześniej Sybase ASE
SQL	Structured Query Language: język zapytań do relacyjnych baz danych

Fiszka

ZMIENIA SYSTEM

Utworzenie użytkownika: CREATE USER

```
CREATE USER NazwaUsera PASSWORD "TrudneHaslo1!";
```

ZMIENIA SYSTEM

Utworzenie konta technicznego bez wymuszenia zmiany hasła: CREATE USER ... NO FORCE_FIRST_PASSWORD_CHANGE

```
CREATE USER NazwaUsera PASSWORD "TrudneHaslo1!" NO FORCE_FIRST_PASSWORD_CHANGE;
```

HANA domyślnie wymusza zmianę hasła przy pierwszym logowaniu nowo utworzonego konta — dopisanie `NO FORCE_FIRST_PASSWORD_CHANGE` do `CREATE USER` wyłącza ten wymóg, przydatne dla kont technicznych, za którymi nie stoi żaden człowiek logujący się interaktywnie.

HANA = SAP HANA: baza danych w pamięci firmy SAP, używana do dużych systemów księgowych i magazynowych

ZMIENIA SYSTEM

Zmiana hasła konta: ALTER USER ... PASSWORD

```
ALTER USER NazwaUsera PASSWORD "NoweTrudneHaslo1!";
```

ZMIENIA SYSTEM

Odblokowanie zablokowanego konta: ALTER USER ... ACCOUNT UNLOCK

```
ALTER USER NazwaUsera ACCOUNT UNLOCK;
```

Odblokowanie nie zmienia hasła — jeśli powodem blokady było zapomniane hasło, a nie literówka, odblokowanie samo w sobie nie rozwiąże problemu logowania.

OSTROŻNIE · NIEODWRACALNE

Reset hasła konta SYSTEM w trybie awaryjnym: hdbnameserver -resetUserSystem

```
./hdbenv.sh
./exe/hdbnameserver -resetUserSystem
```

Wykonujemy z poziomu CLI Bash/SH, zalogowani na odpowiedniego użytkownika administracyjnego instancji (`sidadm`). Ta procedura jest zarazem najważniejszym argumentem za tym, żeby dostęp do konta systemowego `sidadm` traktować z taką samą powagą jak dostęp do konta `SYSTEM` w samej bazie — każdy, kto potrafi zalogować się jako `sidadm` na serwer, potrafi zresetować hasło `SYSTEM` bez znajomości poprzedniego hasła.

CLI = Command Line Interface: praca przez wpisywanie komend w terminalu

□□ TYLKO ODCZYT

Uruchomienie instancji po resecie hasła: HDB start

```
HDB start
```

Po zresetowaniu hasła uruchamiamy instancję normalnie, i logujemy się kontem `SYSTEM` z nowym hasłem, żeby jak najszybciej nadać właściwe uprawnienia docelowemu kontu administracyjnemu i przestać używać `SYSTEM` na co dzień.

□□ ZMIENIA SYSTEM

Nadanie przywileju systemowego: GRANT USER ADMIN

```
GRANT USER ADMIN TO NazwaUsera;
```

□□ ZMIENIA SYSTEM

Nadanie przywileju obiektowego: GRANT SELECT ON SCHEMA

```
GRANT SELECT ON SCHEMA NazwaSchematu TO NazwaUsera;
```

□□ ZMIENIA SYSTEM

Utworzenie roli i nadanie jej użytkownikowi: CREATE ROLE

```
CREATE ROLE NazwaRoli;
GRANT SELECT ON SCHEMA NazwaSchematu TO NazwaRoli;
GRANT NazwaRoli TO NazwaUsera;
```

Role katalogowe (`CREATE ROLE`) różnią się od ról repozytoryjnych (`.hdbrole`) definiowanych jako obiekty projektu HANA XS/HDI i wdrażanych razem z kodem aplikacji — te drugie są wersjonowane razem z resztą modelu danych, pierwsze zarządzane są ręcznie przez administratora bazy.

□□ **HANA** = SAP HANA: baza danych w pamięci firmy SAP, używana do dużych systemów księgowych i magazynowych

Z życia wzięte

Z ŻYCIA WZIĘTE

Tomek trzy razy z rzędu wpisuje złe hasło do konta technicznego pilotażu ZHP, testując nowy skrypt integracyjny Oli, i konto blokuje się po szóstej nieudanej próbie. Odblokowanie przez ALTER USER ... ACCOUNT UNLOCK nie pomaga, bo hasło w skrypcie wciąż jest nieaktualne po zmianie miesiąc wcześniej. Dopiero ustawienie nowego hasła przez ALTER USER ... PASSWORD i poprawienie skryptu Oli kończy serię blokad.

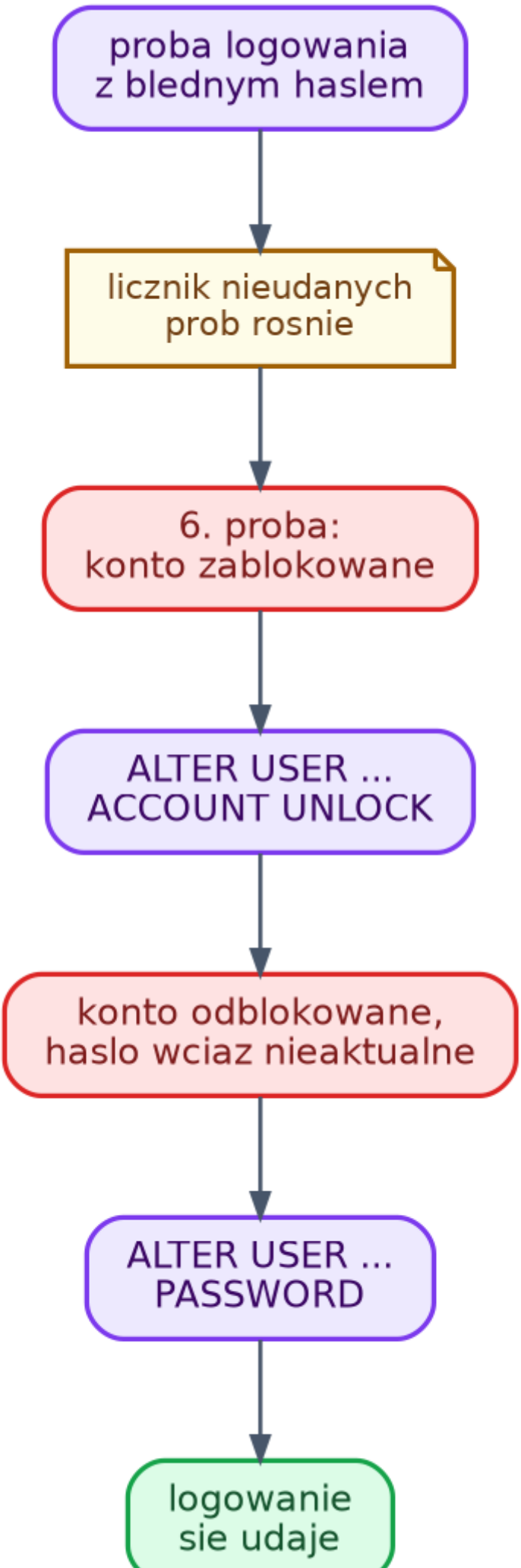
CREATE USER i polityka haseł

Pojęcie: użytkownik bazodanowy HANA. Konto istniejące osobno w każdej bazie tenant oraz osobno w System DB, opisanych na stronie Architektura SAP HANA: instancja, numer, nazwa SID, procesy — konto istniejące w jednym tenancie jest niewidoczne w drugim, nawet w ramach tej samej instalacji.

Pojęcie: polityka haseł. Zestaw parametrów systemowych (`password_layout`, `minimal_password_length`, `password_expire_warning_time`, `maximum_invalid_connect_attempts`) kontrolujących wymogi wobec haseł i zachowanie po nieudanych próbach logowania — konfigurowana globalnie w `nameserver.ini`, sekcja `[password policy]`, wspólna dla wszystkich kont danej instalacji.

ALTER USER ... PASSWORD i odblokowanie konta

Pojęcie: konto zablokowane. Po przekroczeniu limitu nieudanych prób logowania (`maximum_invalid_connect_attempts`, domyślnie 6 prób) HANA blokuje konto automatycznie — kolejne próby logowania, nawet z prawidłowym hasłem, kończą się błędem blokady, dopóki konto nie zostanie odblokowane ręcznie przez administratora.


proba logowania
z blednym haslem
licznik nieudanych
prob rosnie
6. proba:
konto zablokowane
ALTER USER ...
ACCOUNT UNLOCK
konto odblokowane,
haslo wciaz nieaktualne
ALTER USER ...
PASSWORD
logowanie
sie udaje

 *Blokada konta po nieudanych próbach logowania i dwa niezależne kroki naprawy: odblokowanie i zmiana hasła (kliknięcie otwiera pełny rozmiar)*

Reset hasła dla usera SYSTEM danej instancji

Pojęcie: konto SYSTEM. Wbudowane konto administracyjne istniejące w każdej bazie (System DB i każdym tenancie osobno) od momentu instalacji, z pełnymi uprawnieniami do zarządzania tą bazą — odpowiednik `root@localhost` w MySQL. Utrata hasła do `SYSTEM` przy braku innego konta z uprawnieniami `USER ADMIN` oznacza, że żadne polecenie SQL nie odblokuje sytuacji — jedynym wyjściem zostaje tryb awaryjny wykonywany z poziomu systemu operacyjnego, nie z poziomu SQL.

Pojęcie: tryb awaryjny hdbnameserver -resetUserSystem. Uruchamia proces `nameserver` w specjalnym, ograniczonym trybie jednego użytkownika, poza normalnym procesem startowym instancji — narzędzie interaktywnie prosi o wpisanie nowego hasła dla konta `SYSTEM` (dwukrotnie, do potwierdzenia), po czym zapisuje je bezpośrednio, z pominięciem zwykłego uwierzytelniania SQL. Instancja przed uruchomieniem tej procedury musi być zatrzymana (`HDB stop`, opisane na stronie sapcontrol i zarządzanie instancją) — polecenie startuje własny, tymczasowy proces `nameserver` tylko na czas resetu, nie działa równolegle z normalnie uruchomioną instancją.

Role i przywileje w HANA

Pojęcie: przywilej systemowy (system privilege). Uprawnienie dotyczące całej instalacji albo całej bazy, niezwiązane z konkretnym obiektem — na przykład `USER ADMIN` (zarządzanie kontami), `CATALOG READ` (odczyt metadanych każdego schematu), `BACKUP ADMIN`.

Pojęcie: przywilej obiektowy (object privilege). Uprawnienie do konkretnego obiektu — schematu, tabeli, widoku — analogiczne do `GRANT SELECT ON tabela` w innych silnikach.

> **Pojęcie: rola w HANA.** Nazwany zestaw przywilejów (systemowych, obiektowych i innych), nadawany kontom zbiorczo — mechanizm analogiczny do ról opisanych na stronie Użytkownicy i uprawnienia w kontekście MySQL, tyle że w HANA role istnieją od samego początku, nie jako dodatek wersji.

Częste błędy

Codzienna praca na koncie SYSTEM. Konto `SYSTEM` nie powinno być używane do bieżącej administracji — każde nietypowe zachowanie aplikacji uruchomionej przypadkiem na tym koncie ma wtedy pełne uprawnienia do całej bazy. Właściwą praktyką jest nadanie `USER ADMIN` osobnemu, nazwanemu kontu administracyjnemu i pozostawienie `SYSTEM` wyłącznie na sytuacje awaryjne.

Zapominanie, że konto istnieje osobno w każdej bazie. Utworzenie użytkownika w jednym tenancie nie tworzy go w System DB ani w innym tenancie tej samej instalacji — próba połączenia tym samym kontem do innej bazy kończy się błędem uwierzytelnienia, mimo że konto „przecież istnieje" w sensie ogólnym.

Powiązane: Architektura SAP HANA: instancja, numer, nazwa SID, procesy · sapcontrol i zarządzanie instancją · hdbsql: klient wiersza poleceń

Źródła: dokumentacja SAP HANA, „SAP HANA Security Guide", rozdział „User Management" i „Password Policy" · SAP Note 2371112 „Reset SYSTEM user password" · procedura autora

---

Revision #42
Created 2025-03-09 17:37:15 UTC by Tomasz Konieczny
Updated 2026-10-26 14:08:35 UTC by Tomasz Konieczny