	<b>INSTRUKCJA</b>				<b>KS-AOW</b>
	<b>Zabezpieczenia w systemie KS-AOW</b>				
ISO 9001:2008	Dokument: 2018.05.08	Wydanie: 1		Waga: 90	

## Wstęp

Niniejszy dokument opisuje przykładowe działania zwiększające bezpieczeństwo przechowywania danych tworzonych w systemie KS-AOW na serwerze bazodanowym Firebird. Oprócz opisanych poniżej metod istnieje wiele innych, których ten dokument nie opisuje, jednak każda próba zwiększenia bezpieczeństwa danych zawartych w bazie danych jest wskazana, dlatego nie należy się ograniczać jedynie do opisanych w tym dokumencie przykładów. W przypadku korzystania z bazy danych Oracle zagadnienia związane z zabezpieczaniem dostępu do systemu KS-AOW od momentu zmiany poziomu bezpieczeństwa w samym systemie KS-AOW także mają zastosowanie. Dotyczy to również wątku zmiany domyślnych haseł do schematu apw\_user czy system.

## Zabezpieczenia infrastruktury

Opisana poniżej procedura zakłada, że zostały wykonane czynności mające na celu zabezpieczenie fizyczne serwera bazodanowego. Bez tego, żadna metoda zabezpieczania samych danych nie jest w 100% skuteczna. Zabezpieczenie infrastruktury powinno polegać na wydzieleniu komputera będącego serwerem bazodanowym i odseparowaniu go w taki sposób, aby osoby niepowołane nie mogły się do niego dostać. W tym celu można zastosować zabezpieczenia fizyczne w postaci zamków w drzwiach czy kontroli dostępu do pomieszczenia, w którym znajduje się komputer z zainstalowanym serwerem bazodanowym, a dostęp przez terminal powinien być zabezpieczony odpowiednimi mechanizmami uwierzytelniającymi.

Komputer, na którym znajduje się baza danych powinien być dobrany tak, aby w razie awarii sprzętowej nie utracić danych. Można to osiągnąć przez stosowanie mechanizmów macierzy RAID i regularne kopie zapasowe.

## Zabezpieczenia oprogramowania

### System operacyjny

Należy pamiętać, aby zainstalowany na serwerze bazodanowym system operacyjny był aktualizowany w kontekście poprawek bezpieczeństwa i wspierany przez swojego producenta. Należy reagować na ewentualne doniesienia o skutecznym złamaniu zabezpieczeń systemu operacyjnego i niezwłocznie instalować niezbędne poprawki. System operacyjny powinien być dobrany tak, aby możliwe było separowanie poszczególnych jego zasobów i procesów różnych użytkowników poprzez stosowanie mechanizmów uprawnień do plików.

### Oprogramowanie antywirusowe

Bezwzględnie na serwerze bazodanowym powinno być zainstalowane aktualne oprogramowanie antywirusowe z aktualną bazą sygnatur wirusów. Jeśli komputer, na którym zainstalowany jest serwer bazodanowy jest podłączony do Internetu bezwzględnie powinien posiadać włączoną zaporę systemową lub inne oprogramowanie monitorujące i blokujące niepotrzebny ruch sieciowy.

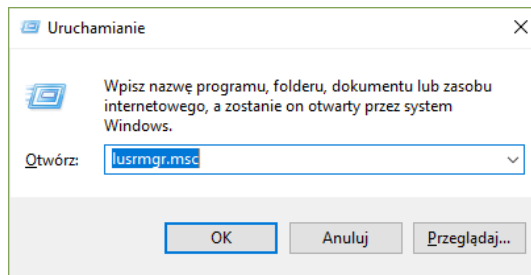
Tytuł: Zabezpieczenia w systemie KS-AOW	Wykonał: Łukasz Bek	Sprawdził: Joanna Stępiak - Piłśniak	Zatwierdził: Łukasz Bek	Strona 1
---	---------------------	---	-------------------------	----------

## Serwer bazodanowy

Serwer bazodanowy Firebird powinien być skonfigurowany tak, aby jego proces był uruchamiany na osobnym koncie użytkownika w szczególności, żeby nie było to konto SYSTEM. Poniżej przedstawiono sposób konfiguracji serwera bazodanowego i uruchomienie go na osobnym koncie użytkownika. Przykłady zostały opisane na systemie operacyjnym Windows w wersji 10.

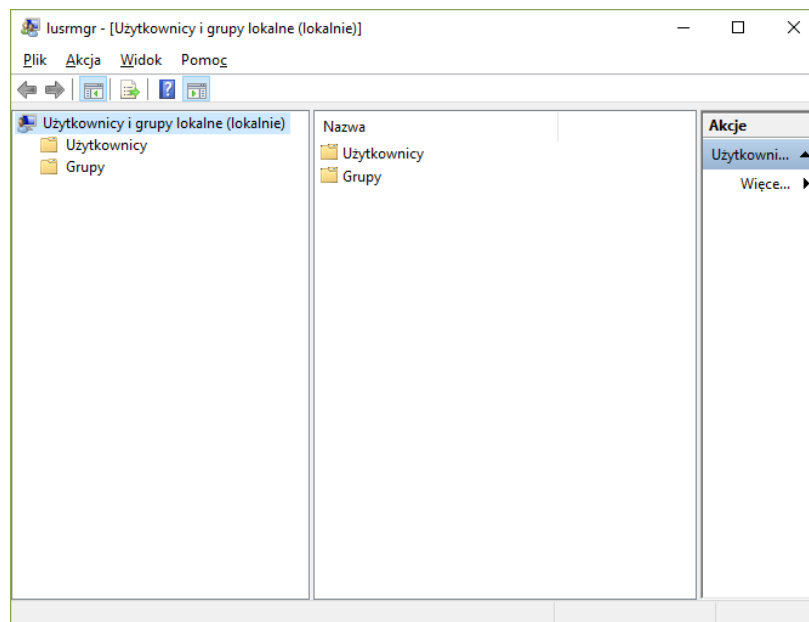
## Zakładanie nowego użytkownika OS

Pierwszym krokiem jest otwarcie konsoli zarządzania użytkownikami. Aby to zrobić używamy skrótu Windows + R (uruchom...). Powinno pojawić się okno jak poniżej.



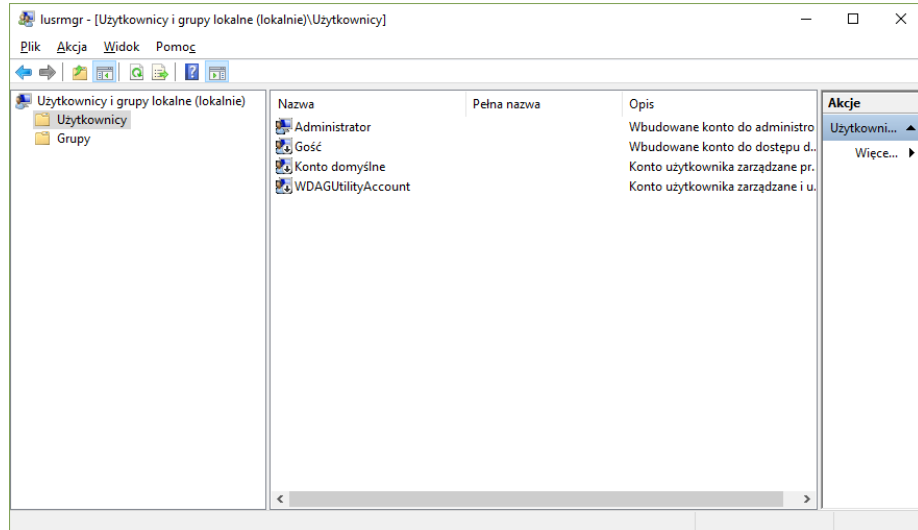
Rysunek 1 Uruchom

Po wpisaniu w pole edycyjne wyrażenia *lusrmgr.msc* i zatwierdzeniu przyciskiem OK powinna otworzyć się konsola zarządzania użytkownikami.



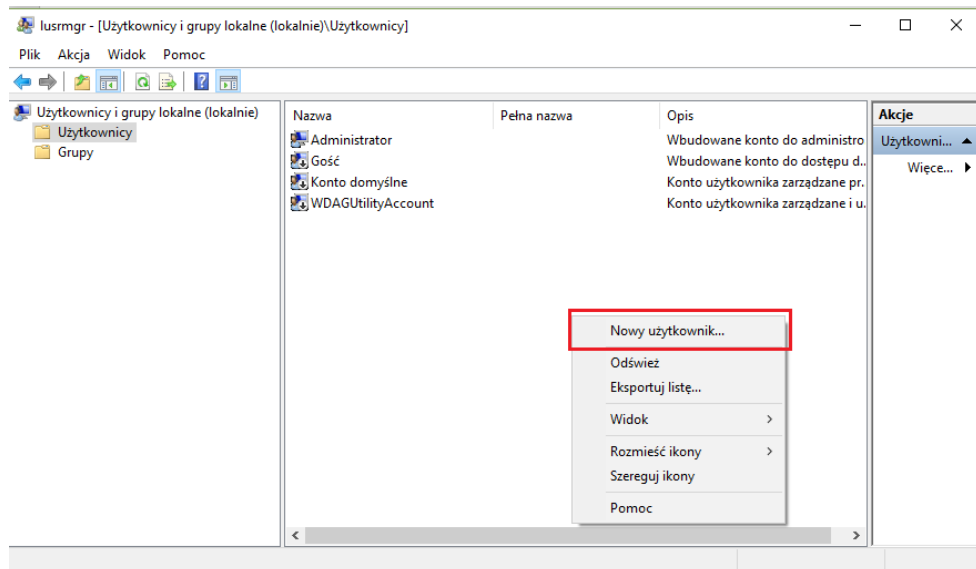
Rysunek 2 Konsola zarządzania użytkownikami

Klikamy w widoczny po lewej stronie folder Users. Pojawi się lista użytkowników w systemie.



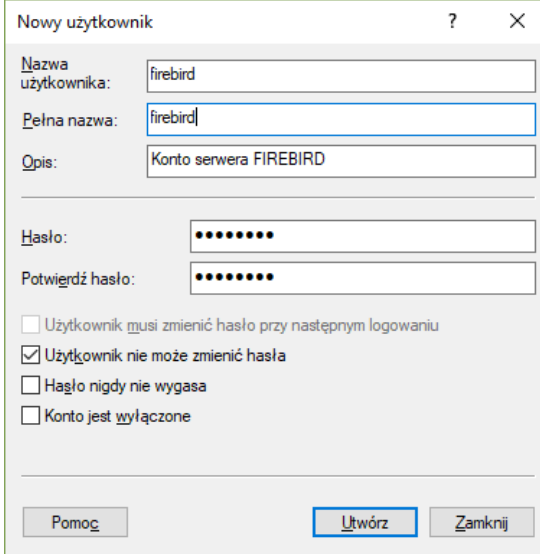
Rysunek 3 Lista użytkowników OS

Klikamy prawym przyciskiem myszy na puste pole na liście użytkowników i wybieramy Nowy użytkownik.



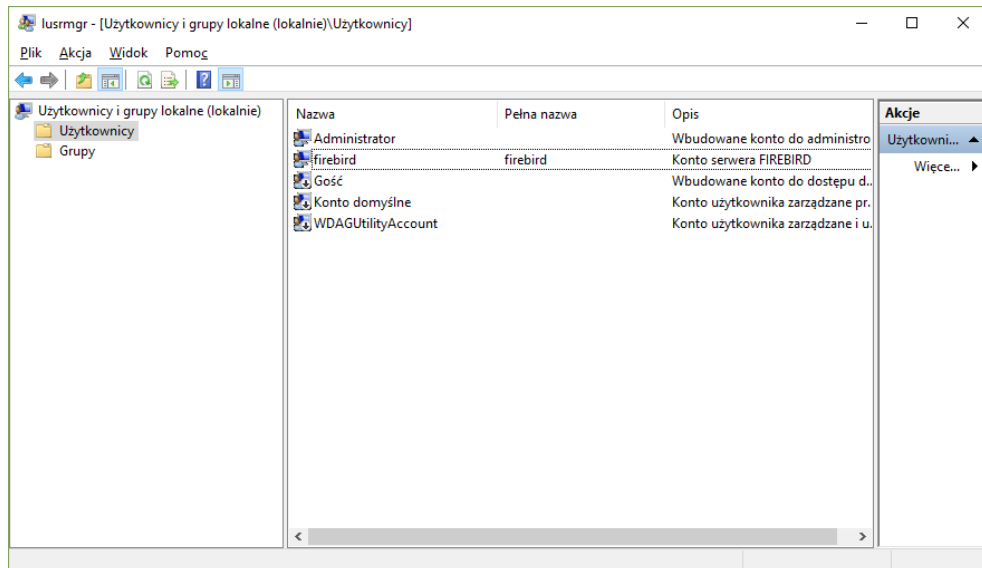
Rysunek 4 Nowy użytkownik

Uzupełniamy formularz jak poniżej. Użytkownik nie musi nazywać się firebird, może być to dowolna nazwa. Hasło powinno składać się przynajmniej z 8 znaków, zawierać małe i duże litery oraz znaki specjalne.



Rysunek 5 Nowe konto Firebird

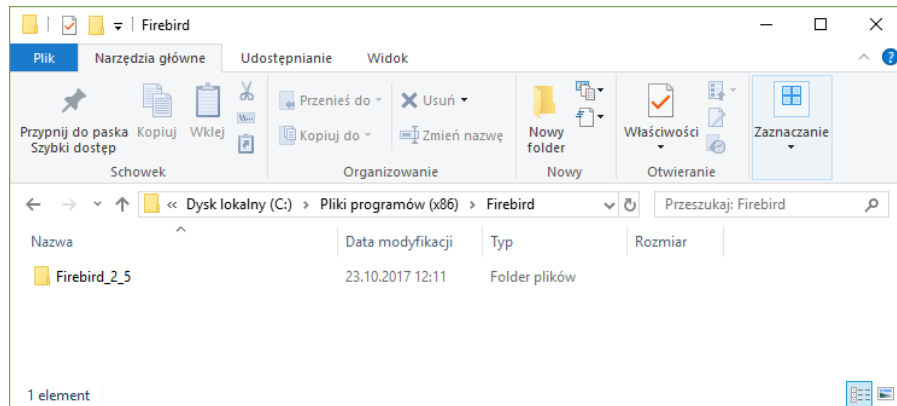
Po utworzeniu użytkownik będzie widoczny na liście użytkowników.



Rysunek 6 Konto serwera Firebird

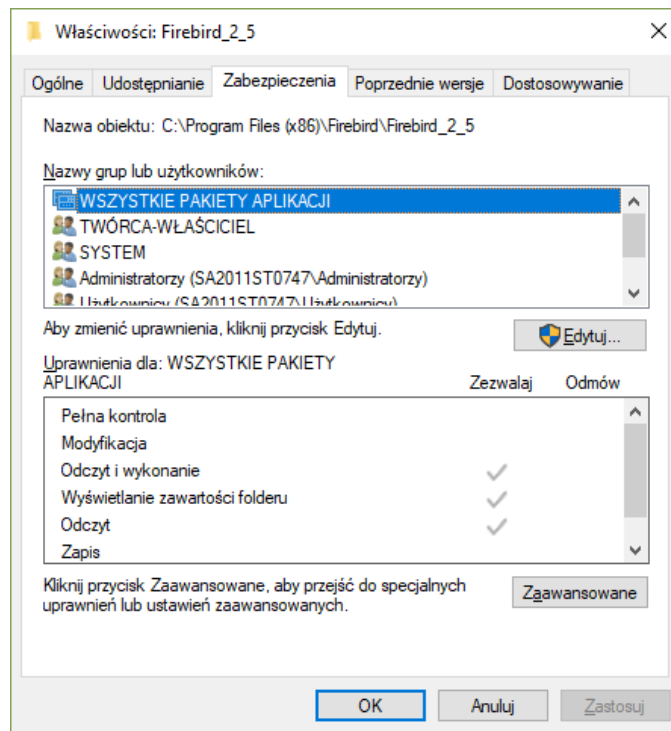
## Przydzielanie uprawnień użytkownikowi

Utworzony przed chwilą użytkownik powinien posiadać uprawnienia do folderu, w którym znajdują się pliki wykonywalne serwera Firebird. W tym celu przechodzimy w menadżerze folderów do folderu gdzie zainstalowany jest Firebird.



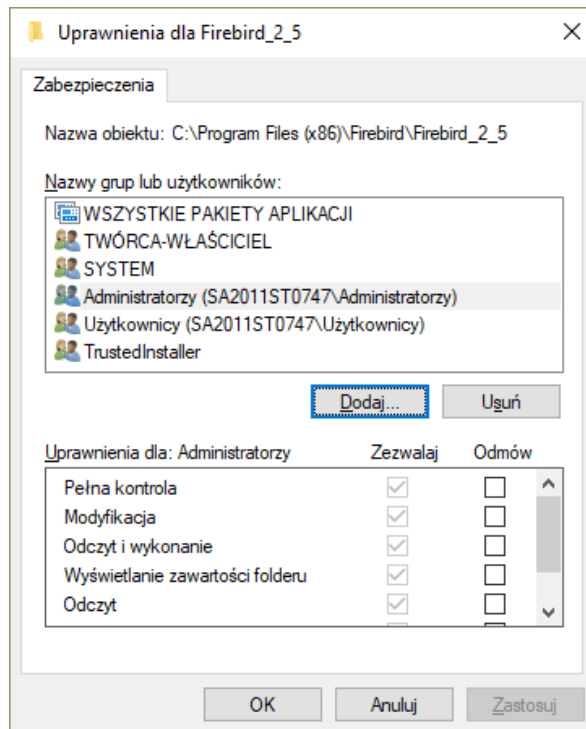
Rysunek 7 Ścieżka do folderu Firebird

Klikamy prawym przyciskiem myszy na folderze Firebird\_2\_5 (lub odpowiadającemu zainstalowanej wersji) i wybieramy właściwości.



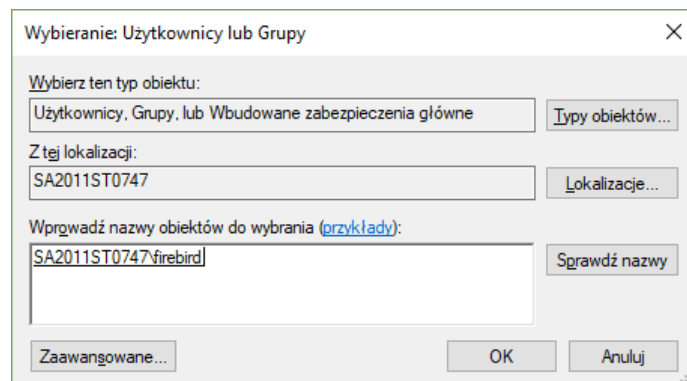
Rysunek 8 Właściwości folderu Firebird

Na zakładce Zabezpieczenia wybieramy przycisk Edytuj.



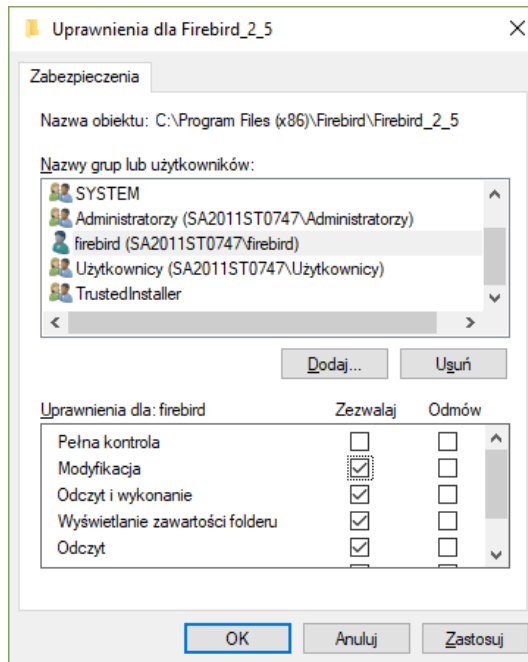
Rysunek 9 Edycja uprawnień

Klikamy przycisk Dodaj... i wprowadzamy nazwę utworzonego przed chwilą konta użytkownika. Poniższy zrzut ekranu odnosi się do komputera testowego. Jego treść będzie inna na komputerze, na którym wykonuje się tą operację.



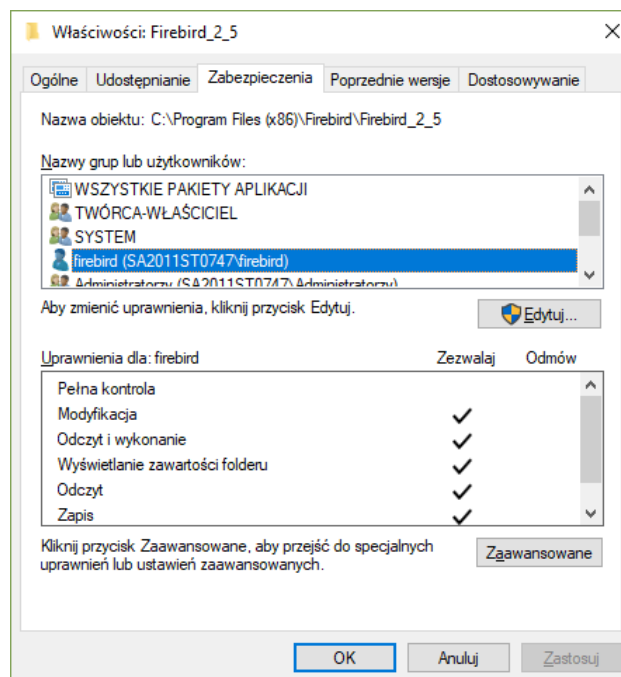
Rysunek 10 Uprawnienia użytkownika

Po potwierdzeniu w oknie uprawnień nadajemy użytkownikowi Firebird uprawnienie do modyfikacji plików i zatwierdzamy przyciskiem OK.



Rysunek 11 Uprawnienia do modyfikacji

Okno uprawnień powinno wyglądać podobnie jak to poniżej.

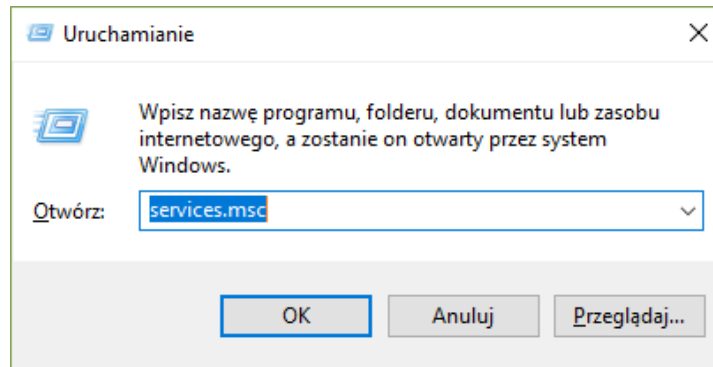


Rysunek 12 Okno uprawnień folderu firebird

## Uruchamianie serwera BD na koncie firebird

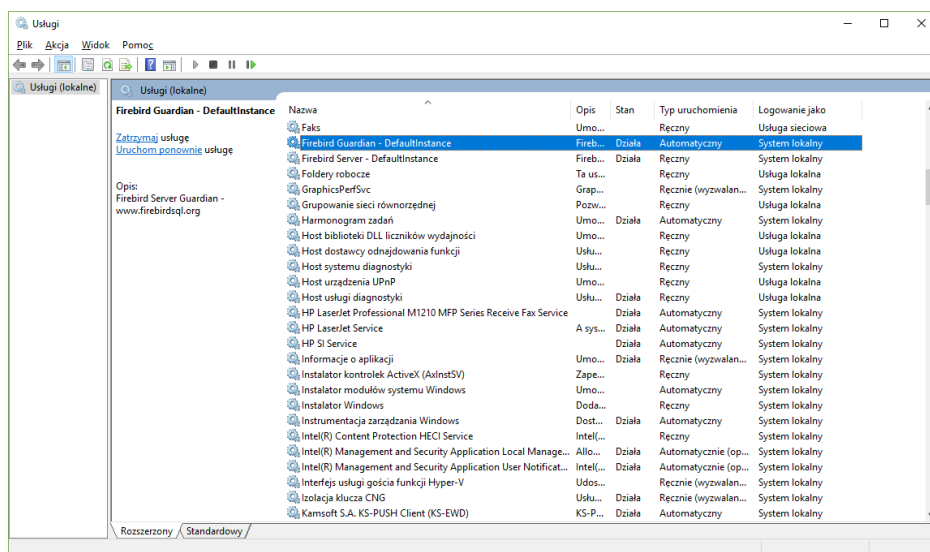
Kolejnym krokiem jest ustawienie usługi firebird tak, aby uruchamiała się na koncie Firebird.

W tym celu otwieramy usługi wpisując w okno uruchamiania (Windows + R) wartość services.msc



Rysunek 13 Uruchamianie przystawki usług

Po potwierdzeniu powinno pojawić się następujące okno:

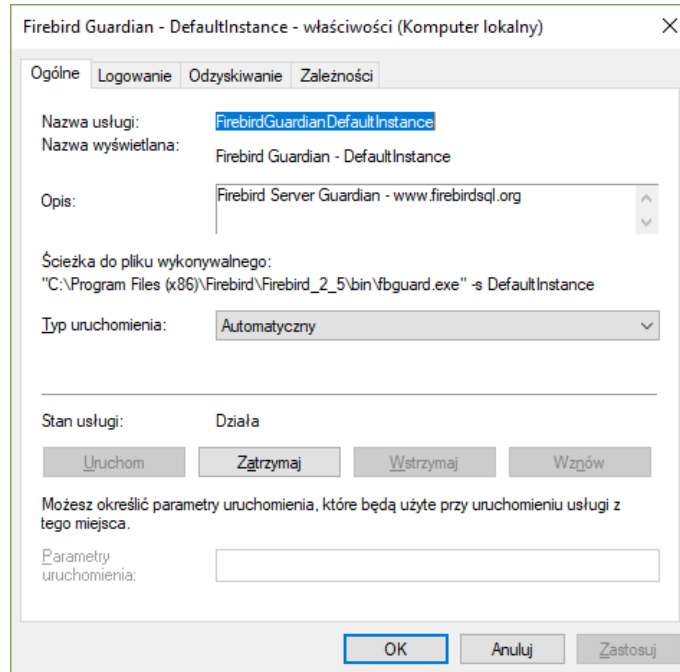


Rysunek 14 Usługi firebird

Wyszukujemy usługi Firebird Guardian - DefaultInstance oraz Firebird Server – DefaultInstance.

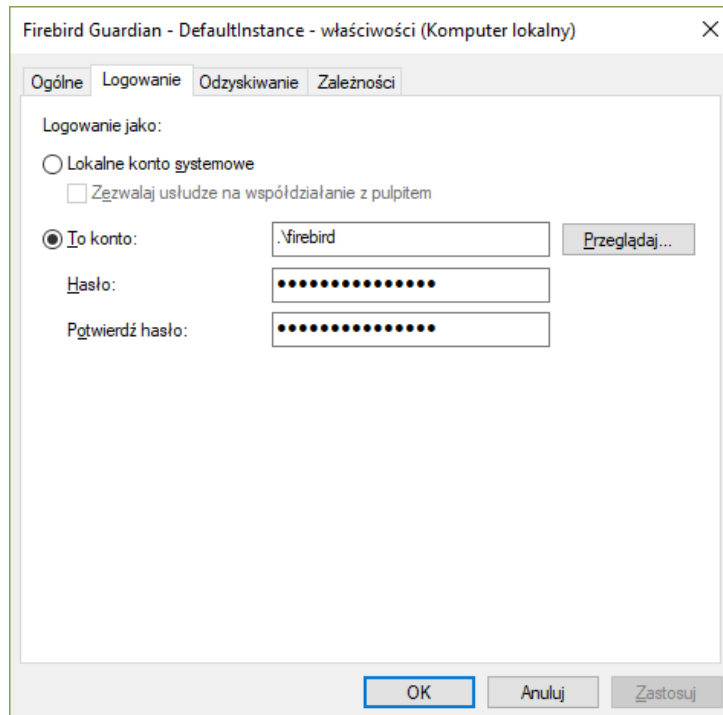
Klikamy dwukrotnie lewym przyciskiem myszy na usługę Firebird Guardian – DefaultInstance. Na ekranie pojawi się poniższe okno konfiguracyjne.





Rysunek 15 Konfiguracja usługi Guardian

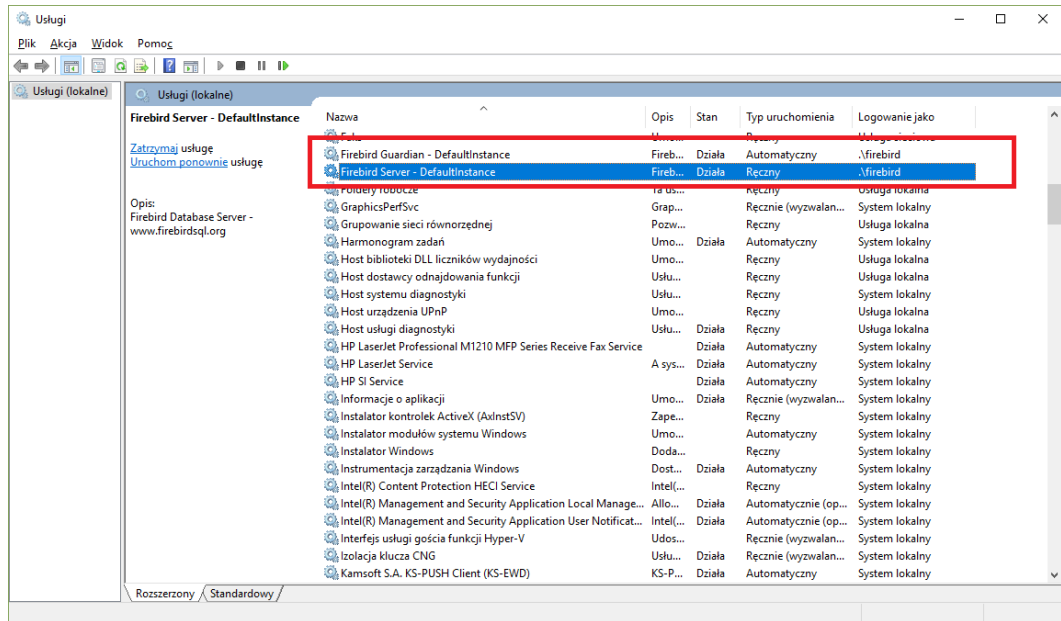
Przechodzimy na zakładkę Logowanie i ustawiamy usługę tak, aby uruchamiała się na koncie wcześniej założonego użytkownika firebird.



Rysunek 16 Uruchamianie na koncie firebird.

Po potwierdzeniu należy zrestartować usługę Firebird Guardian. Jeśli wszystko poszło dobrze usługa powinna uruchomić się pomyślnie. W innym przypadku należy zweryfikować wpisaną nazwę użytkownika oraz hasło. Te same kroki należy wykonać dla usługi Firebird Server.

Po wykonaniu powyższych czynności okno powinno wyglądać tak jak poniżej.



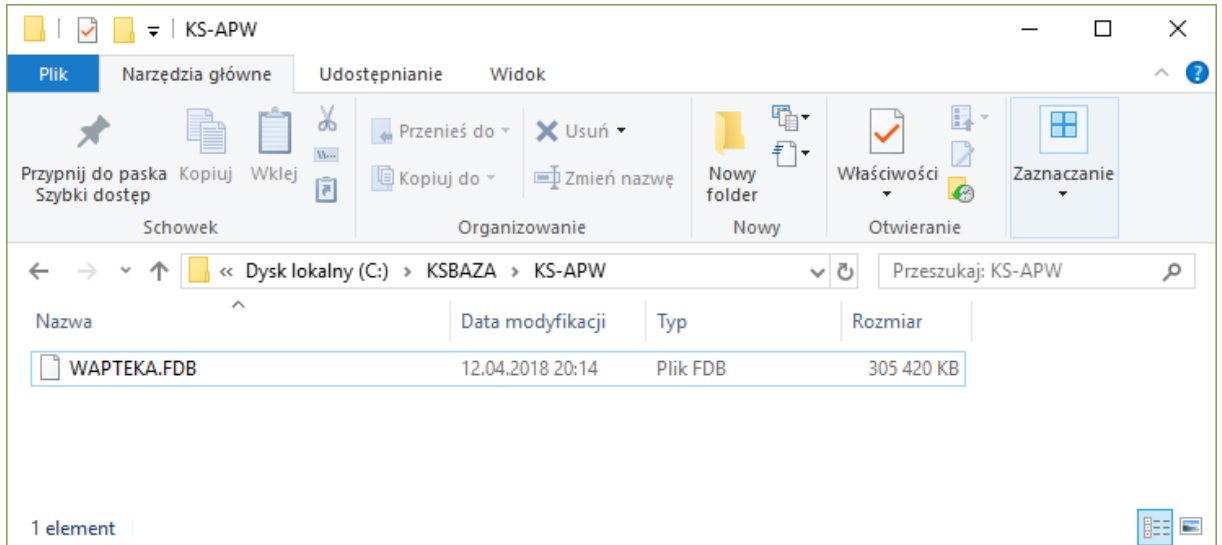
Rysunek 17 Firebird uruchamiany na osobnym koncie

Jeśli wszystko wykonało się pomyślnie, użytkownicy nadal mogą pracować z systemem KS-AOW. Jeśli uruchomienie KS-AOW zakończy się błędem należy zweryfikować czy wykonano wszystkie kroki opisane powyżej. Ewentualnie wrócić do poprzedniej konfiguracji zmieniając uruchamianie serwera Firebird na lokalne konto systemowe.

## Nadawanie uprawnień do pliku bazodanowego

Kolejnym krokiem jest odebranie uprawnień innym użytkownikom niż firebird dostępu do pliku bazy danych systemu KS-AOW. Spowoduje to, że inny użytkownik niż firebird nie będzie mógł usunąć i skopiować pliku bazy danych. Tym samym zabezpieczy to nas przed skopiowaniem bazy danych przez osoby niepowołane.

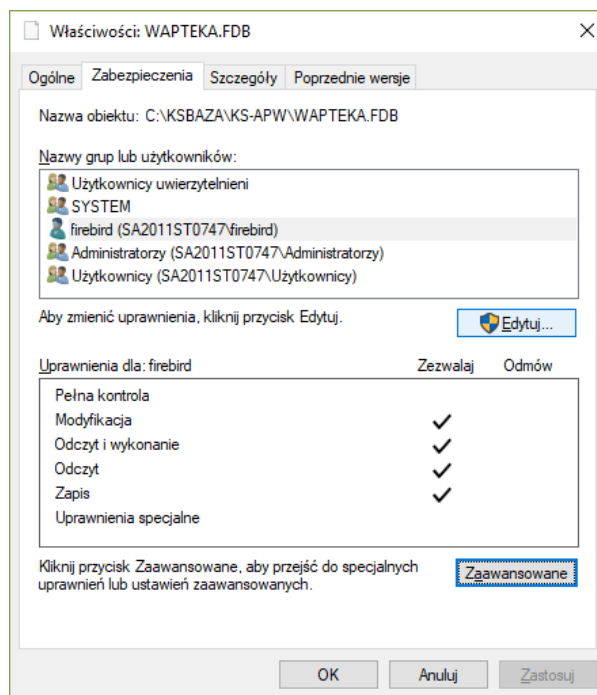
W tym celu należy na dysku twardym zlokalizować plik bazodanowy wapteka.fdb (zazwyczaj w lokalizacji c:\ksbaza\ks-apw\wapteka.fdb).



Rysunek 18 Zmiana uprawnień pliku wapteka.fdb

Klikamy prawym przyciskiem myszy na plik wapteka.fdb i wywołujemy okno właściwości a na nim zakładkę zabezpieczenia.

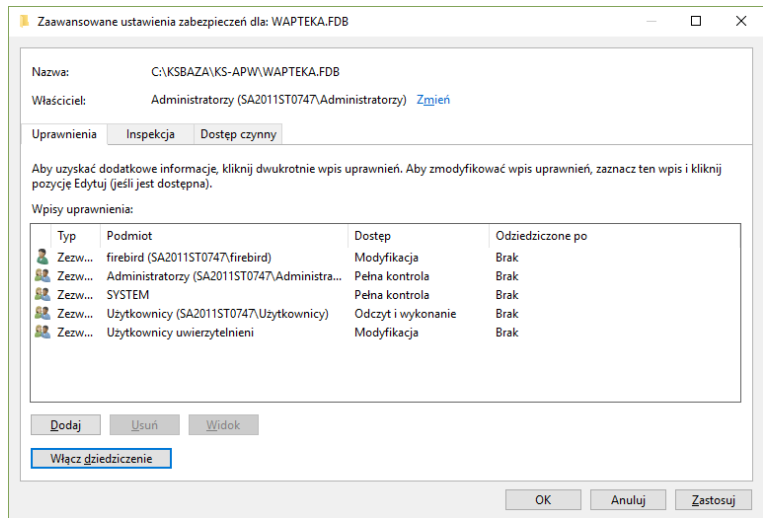
Najpierw dodajemy uprawnienia do użytkownika Firebird (podobnie jak do folderu samego serwera firebird opisanego wcześniej). Użytkownik firebird powinien posiadać przynajmniej takie uprawnienia jak przedstawia poniższy rysunek.



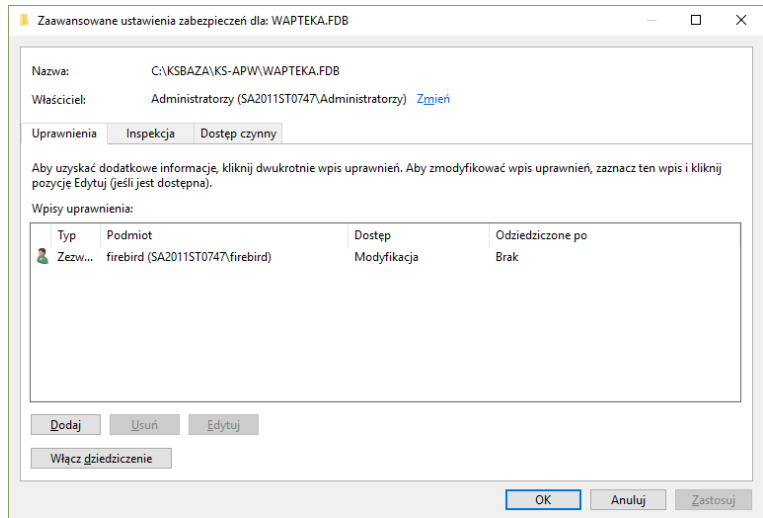
Rysunek 19 Uprawnienia użytkownika firebird

Następnym krokiem jest usunięcie z listy innych użytkowników niż firebird. Spowoduje to, że do tego pliku dostęp będzie miał tylko i wyłącznie serwer bazodanowy firebird. W tym celu używamy przycisku Zaawansowane. Pojawi się okno jak poniżej. Przed usunięciem upewnij się, że dziedziczenie jest wyłączone (tak jak na poniższym rysunku).

Tytuł: Zabezpieczenia w systemie KS-AOW	Wykonał: Łukasz Bek	Sprawił: Joanna Stępiak - Piłśniak	Zatwierdził: Łukasz Bek	Strona 11
---	---------------------	------------------------------------	-------------------------	-----------

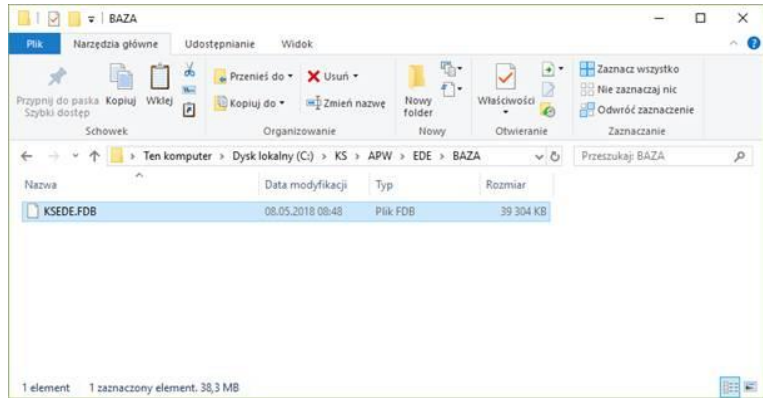


Rysunek 20 Uprawnienia użytkownika firebird



Rysunek 21 Uprawnienia użytkownika Firebird

Te same kroki należy wykonać dla bazy danych KS-EDE (KSEDE.FDB) znajdującej się w katalogu c:\ks\apw\ede\baza.



Rysunek 22 Baza danych KS-EDE

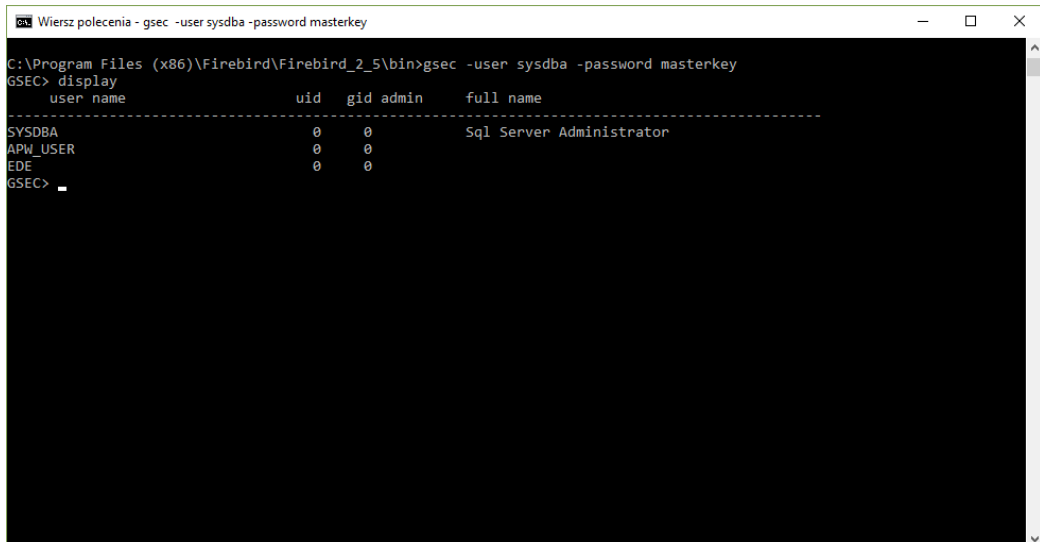
Upewnij się że po zatwierdzeniu system KS-AOW uruchamia się pomyślnie. Jeśli nie, musisz zalogować się do systemu Windows na użytkownika firebird i z tego poziomu zmienić (dodać) uprawnienia do pliku bazodanowego innym użytkownikom lub jako administrator wywłaszczyć plik bazy danych (zmienić właściciela) i zmienić uprawnienia.

Jeśli system KS-AOW uruchamia się poprawnie konfiguracja dostępu do pliku bazy danych jest zakończona. Sprawdź czy z poziomu innego użytkownika niż firebird możesz skopiować plik bazodanowy. Oczywiście użytkownik z uprawnieniami administracyjnymi nadal może wywłaszczyć plik bazy danych i nadać mu dowolne uprawnienia jednak inni użytkownicy nie mają już takich uprawnień.

## Zmiana domyślnych haseł serwera bazodanowego (dot. FIREBIRD)

Zaleca się zmianę domyślnego hasła można to wykonać np. za pomocą narzędzia GSEC.

Uruchomienie narzędzia pokazano na rysunku poniżej.



```

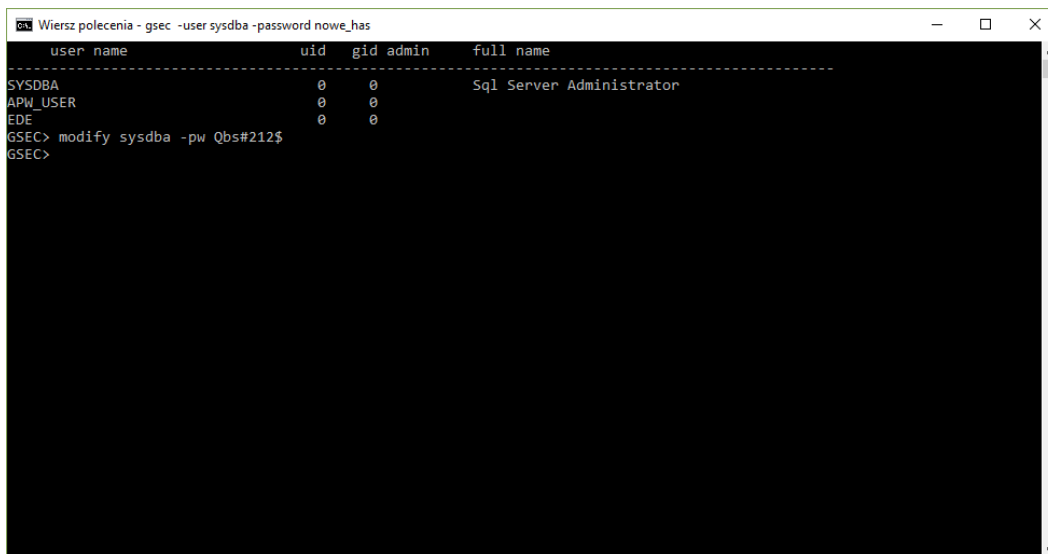
C:\Program Files (x86)\Firebird\Firebird_2_5\bin>gsec -user sysdba -password masterkey
GSEC> display
  user name      uid  gid admin  full name
-----
SYSDBA          0    0      0      Sql Server Administrator
APW_USER        0    0      0
EDE             0    0      0
GSEC>

```

Rysunek 223 Narzędzie GSEC

Poleceniem *display* możemy wyświetlić listę użytkowników Firebird. Zaleca się zmianę haseł zarówno dla użytkownika SYSDBA jak i użytkownika APW\_USER.

Aby zmienić hasło należy użyć polecenia *modify* jak na rysunku poniżej.



```

Wiersz polecenia - gsec -user sysdba -password nowe_has
-----
user name          uid  gid admin  full name
-----
SYSDBA             0    0         Sql Server Administrator
APW_USER           0    0
EDE                0    0
GSEC> modify sysdba -pw Qbs#212$
GSEC>

```

Rysunek 24 Zmiana hasła użytkownika sysdba

UWAGA!! Przedstawione powyżej hasło jest jedynie przykładem. Użytkownik powinien zastosować inne losowe maksymalnie 8 znakowe hasło. Firebird używa zawsze tylko 8 pierwszych bajtów hasła, dlatego stosowanie hasła dłuższego niż 8 znaków jest bezcelowe.

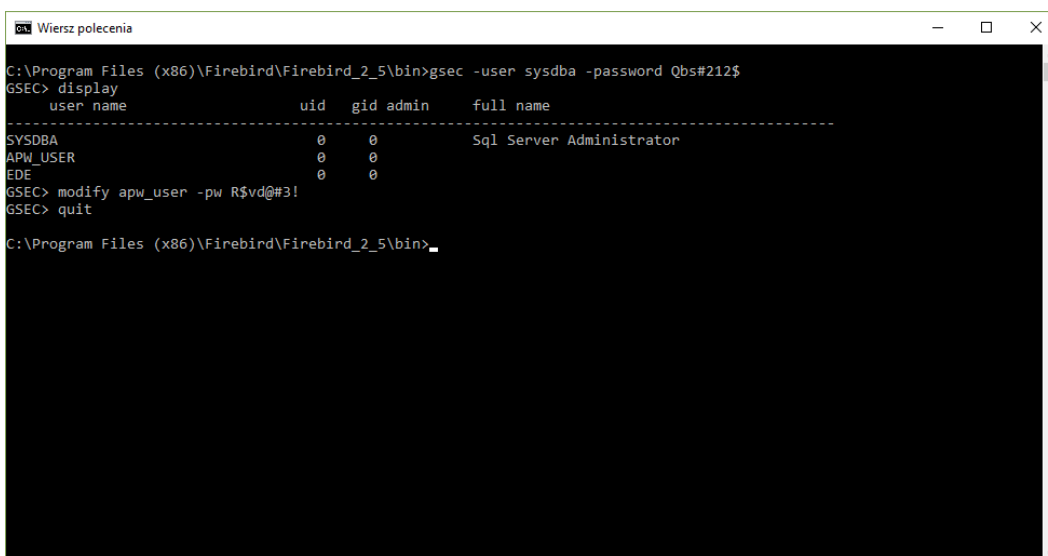
Następnie tak wprowadzone hasło należy wpisać w plik APMAN.INI na serwerze oraz wszystkich stacjach końcowych:

```

[KS-APW]
DB_TYPE=FB
DB_USER=apw_user
DB_PASSWD=#B6A7C7A517A637460
DB_PATH=C:\KS\APW\AP\WAPTEKA.FDB
DB_SERVER=localhost
SYSDBA_PWD=Qbs#212$

```

Podobnie zmieniamy hasło dla użytkownika apw\_user



```

Wiersz polecenia
C:\Program Files (x86)\Firebird\Firebird_2_5\bin>gsec -user sysdba -password Qbs#212$
GSEC> display
-----
user name          uid  gid admin  full name
-----
SYSDBA             0    0         Sql Server Administrator
APW_USER           0    0
EDE                0    0
GSEC> modify apw_user -pw R$vd@#3!
GSEC> quit

C:\Program Files (x86)\Firebird\Firebird_2_5\bin>_

```

Rysunek 25 Zmiana hasła użytkownika apw\_user

<b>KS</b>	<b>INSTRUKCJA</b>				<b>KS-AOW</b>
	<b>Zabezpieczenia w systemie KS-AOW</b>				
ISO 9001:2008	Dokument: 2018.05.08	Wydanie: 1		Waga: 90	

UWAGA!! Przedstawione powyżej hasło jest jedynie przykładem. Użytkownik powinien zastosować inne losowe maksymalnie 8 znakowe hasło. Firebird używa zawsze tylko 8 pierwszych bajtów hasła, dlatego stosowanie hasła dłuższego niż 8 znaków jest bezcelowe.

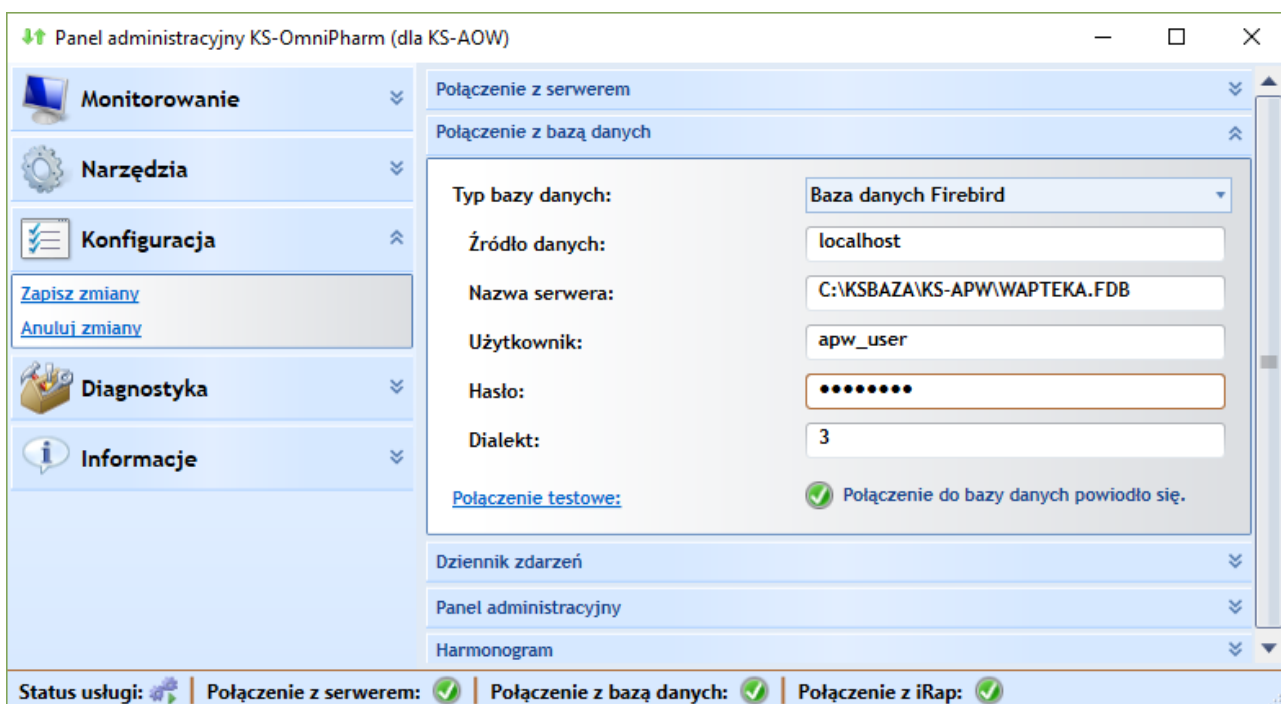
Następnie tak wprowadzone hasło należy wpisać w plik APMAN.INI na serwerze oraz wszystkich stacjach końcowych:

```
[KS-APW]
DB_TYPE=FB
DB_USER=apw_user
DB_PASSWD=R$vd@#3!
DB_PATH=C:\KS\APW\AP\WAPTEKA.FDB
DB_SERVER=localhost
SYSDBA_PWD=Qbs#212$
```

Hasło zostanie zaszyfrowane przy następnym logowaniu do systemu. Zaleca się zalogowanie do systemu KS-AOW po wpisaniu hasła w apman.ini

Przed przejściem do konfiguracji kolejnego stanowiska należy upewnić się, czy system KS-AOW działa prawidłowo uruchamiając podstawowe moduły na stanowisku.

Jeśli apteka korzysta z KS-OmniPharm nowe hasło należy wpisać w konfiguracji dostępnej w panelu administracyjnym.



Rysunek 23 Panel sterowania KS-OmniPharm

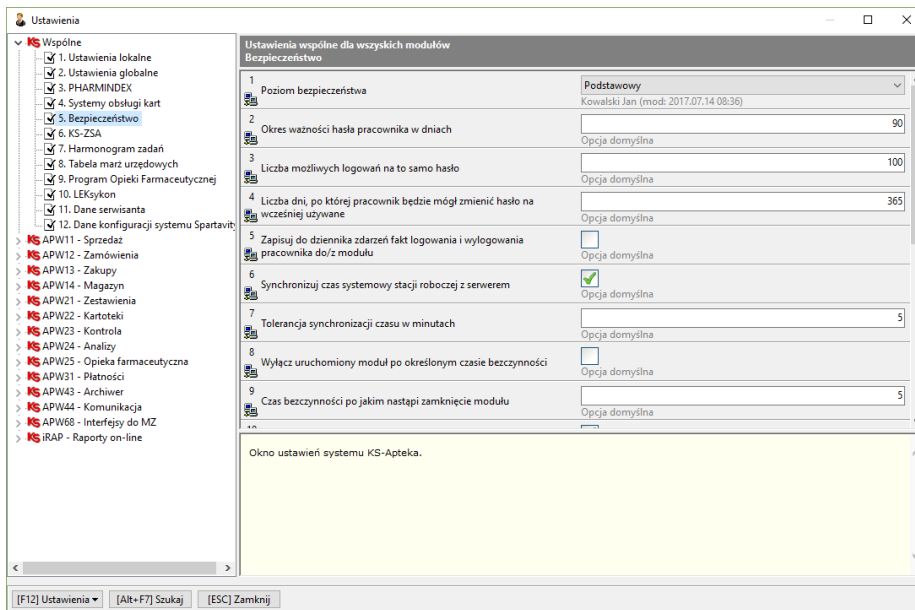
## System KS-AOW

### Polityka haseł

Zaloguj się do systemu KS-AOW do modułu APW41 – Administrator.

Tytuł: Zabezpieczenia w systemie KS-AOW	Wykonał: Łukasz Bek	Sprawdził: Joanna Stępiak - Piłśniak	Zatwierdził: Łukasz Bek	Strona 15
---	---------------------	--------------------------------------	-------------------------	-----------

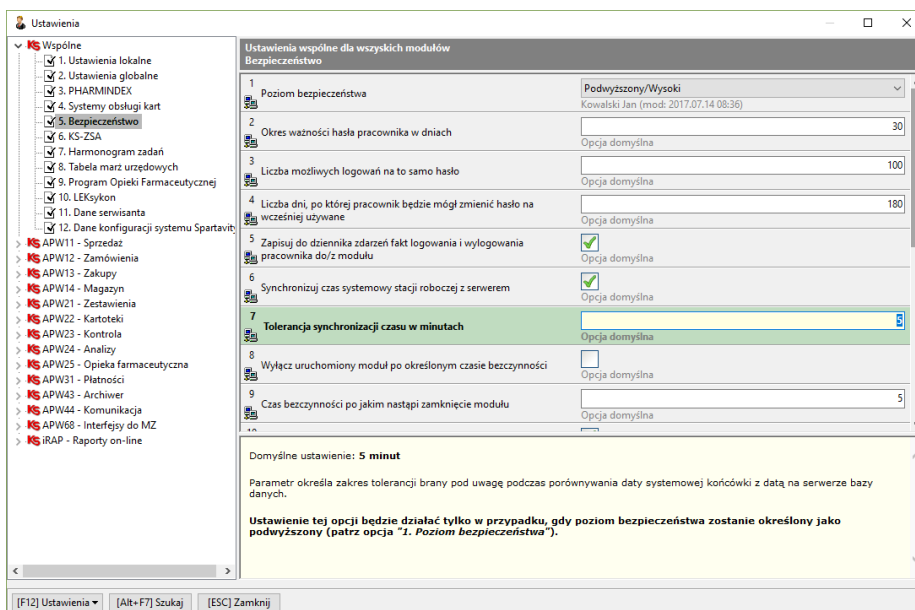
Przejdź do funkcjonalności Opcje modułów i wyszukaj opcje związane z bezpieczeństwem.



Rysunek 246 Bezpieczeństwo

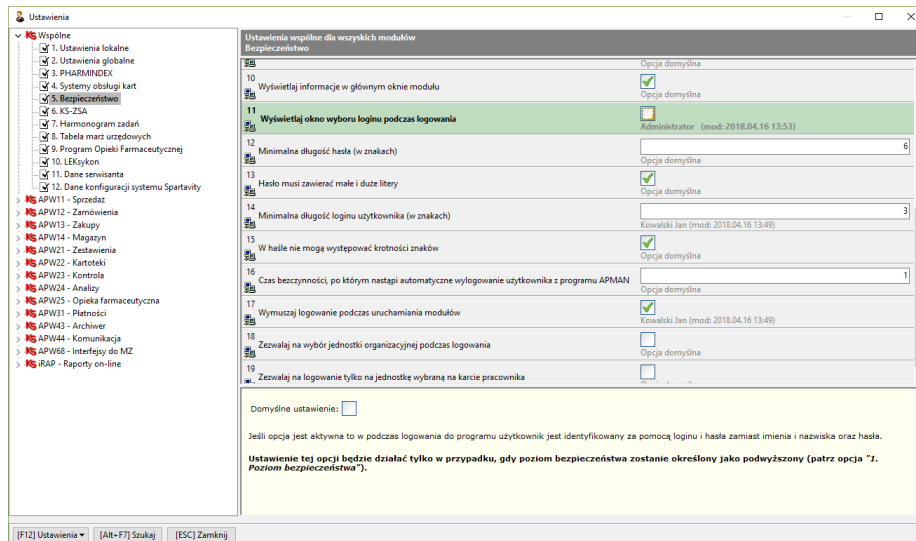
Ustaw opcję Wspolne.5.1 na „Podwyższony”.

Dostosuj ustawienia kolejnych opcji do potrzeb. Poniżej przedstawiono zalecaną konfigurację.



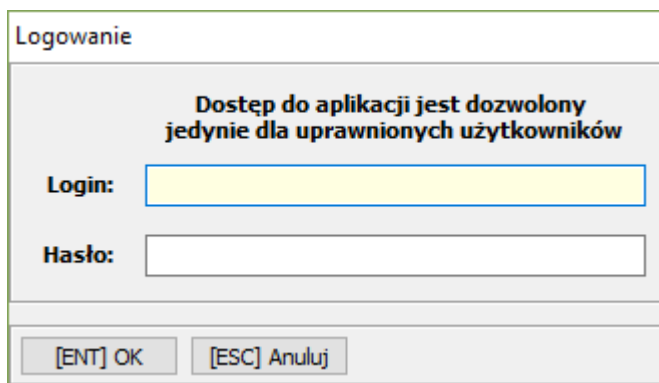
Rysunek 27 Ustawianie bezpieczeństwa





Rysunek 28 Ustawianie bezpieczeństwa c.d.

Ustaw odpowiednie loginy i hasła na kartach pracowników. Jeśli nie chcesz aby administrator znał hasła Użytkowników, na karcie pracownika możesz zaznaczyć opcję aby użytkownik zmienił hasło przy kolejnym logowaniu. Przy próbie ponownego logowania do systemu Użytkownicy powinni zobaczyć okno logowania przedstawione poniżej.

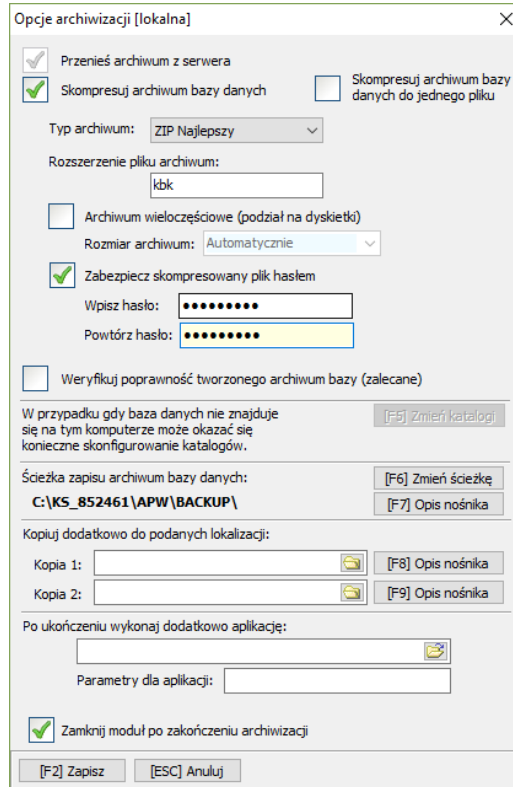


Rysunek 259 Logowanie do systemu

## Archiwum bazy danych KS-AOW

Zaleca się, aby wykonywane archiwum bazy danych KS-AOW było archiwizowane z hasłem. Aby to zrobić uruchamiamy moduł APW43 – Archiwer.

W opcjach archiwizacji wybieramy opcję „Skompresuj archiwum bazy danych”, „ZIP najlepszy” w polu Typ archiwum. Zaleca się również zmianę domyślnego rozszerzenia pliku kopii zapasowej na mniej znaną np. .kbk. Wybieramy opcję „Zabezpiecz skompresowany plik hasłem” i wpisujemy hasło do archiwum. Zaleca się zmianę tego hasła nie rzadziej niż raz na 30 dni.

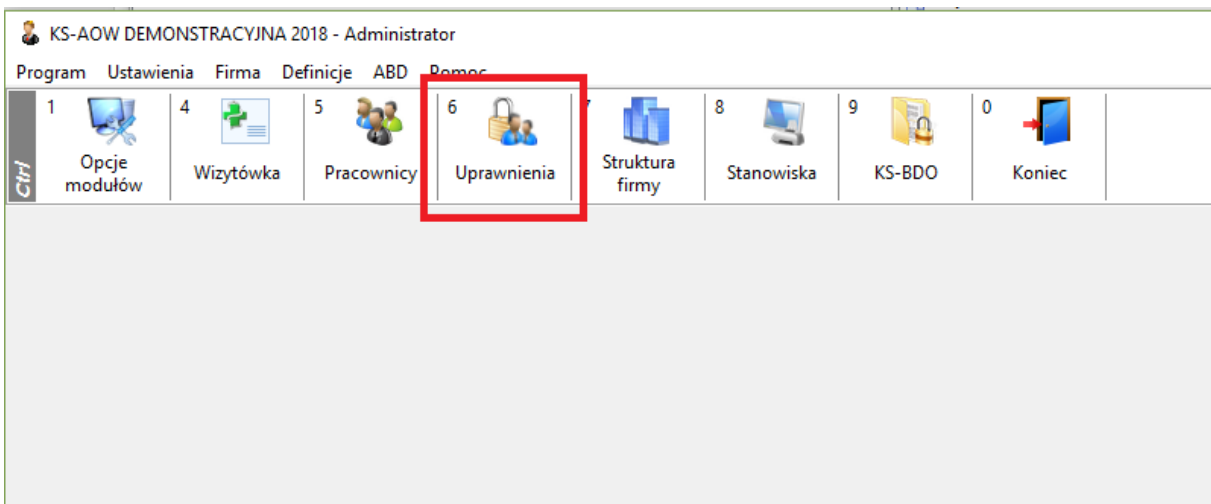


Rysunek 3026 Archiwum bazy danych

## Uprawnienia

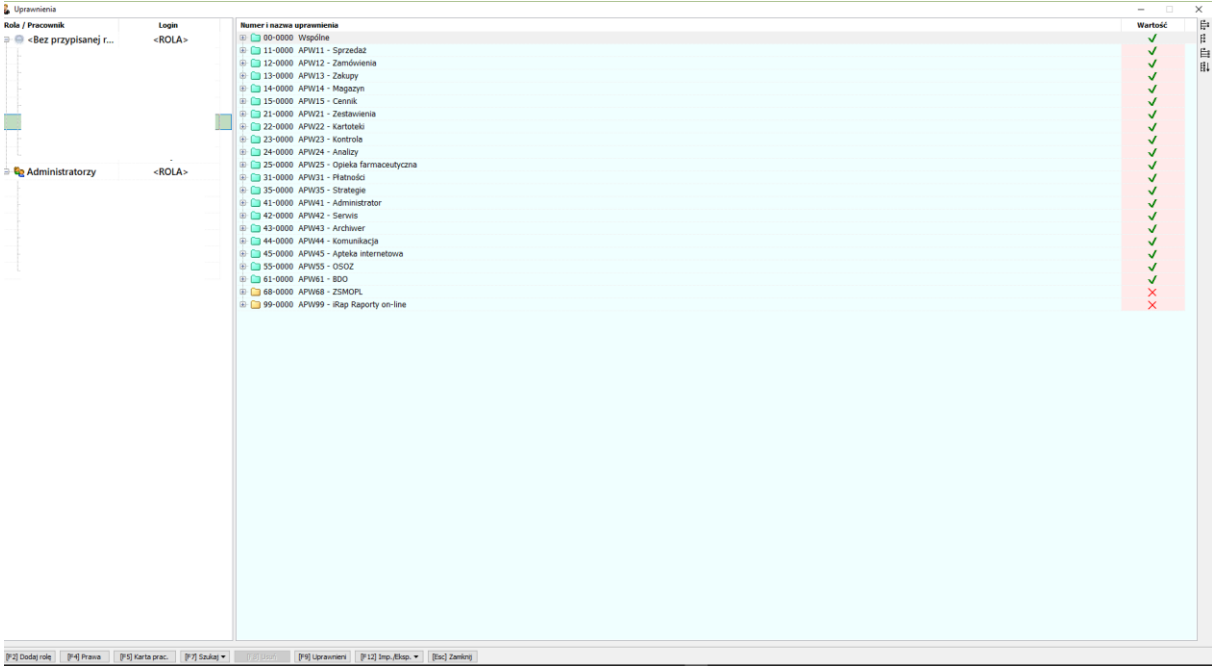
Upewnij się, że pracownicy logujący się do systemu mają tylko te uprawnienia, które powinni mieć.

Uprawnienia możemy konfigurować w module APW41 – Administrator. Wybierz „Uprawnienia”.



Rysunek 31 Uprawnienia

W oknie uprawnień zweryfikuj uprawnienia użytkowników i odbierz im te, które nie są im potrzebne.



Role / Pracownik	Logon	Numer i nazwa uprawnienia	Wartość
<Bez przypisanej r...>	<ROLA>	00-0000 Wspólne	✓
		11-0000 APW11 - Sprzedaż	✓
		12-0000 APW12 - Zamówienia	✓
		13-0000 APW13 - Zakupy	✓
		14-0000 APW14 - Magazyn	✓
		15-0000 APW15 - Cenik	✓
		21-0000 APW21 - Zestawienia	✓
		22-0000 APW22 - Kartoteki	✓
		23-0000 APW23 - Kontrola	✓
		24-0000 APW24 - Analiza	✓
		25-0000 APW25 - Opieka farmaceutyczna	✓
		31-0000 APW31 - Płatności	✓
		35-0000 APW35 - Strategie	✓
		41-0000 APW41 - Administrator	✓
		42-0000 APW42 - Serwis	✓
		43-0000 APW43 - Archiwizacja	✓
		44-0000 APW44 - Komunikacja	✓
		45-0000 APW45 - Apteka internetowa	✓
		55-0000 APW55 - DOSZ	✓
		61-0000 APW61 - BDO	✓
		68-0000 APW68 - ZSMOPL	✗
		99-0000 APW99 - iRap Raporty on-line	✗

Rysunek 32 Uprawnienia użytkowników

## Zakończenie

Przedstawione powyżej rozwiązania mają na celu podwyższenie poziomu bezpieczeństwa systemu KS-AOW i systemów bazodanowych. Wszystkie zaprezentowane możliwości istnieją w systemie KS-AOW i w systemach operacyjnych od wielu lat, jednak nie zawsze są stosowane przez Użytkowników. Należy jednak pamiętać, że niektóre dane przechowywane w systemie KS-AOW są danymi osobowymi i zgodnie z RODO należy zapewnić należyte środki, aby je zabezpieczyć. Wprowadzenie wszystkich wyżej wymienionych metod nie zwalnia Administratora danych osobowych z wprowadzenia wszystkich niezbędnych procedur wynikających z RODO.