Wheel Fudo PAM 3.7 - Dokumentacja Systemu

Wydanie niewspierane

Wheel Systems

09.09.2021

Spis treści

1 Informacje ogólne **1**
1.1 O dokumentacji . . . 1

2 Opis systemu **4**
2.1 PSM (Privileged Sessions Management) . . . 4
2.1.1 Citrix StoreFront (HTTP) . . . 4
2.1.2 HTTP . . . 5
2.1.3 ICA . . . 5
2.1.4 Modbus . . . 6
2.1.5 MS SQL (TDS) . . . 6
2.1.6 MySQL . . . 6
2.1.7 Oracle . . . 7
2.1.8 RDP . . . 7
2.1.9 SSH . . . 8
2.1.10 Telnet 3270 . . . 8
2.1.11 Telnet 5250 . . . 9
2.1.12 Telnet . . . 9
2.1.13 VNC . . . 9
2.1.14 X11 . . . 10
2.1.15 TCP . . . 11
2.2 AAPM (Application to Application Password Manager) . . . 11
2.3 Skarbiec haseł (Secret Manager) . . . 12
2.4 Efficiency Analyzer . . . 12
2.5 Portal użytkownika . . . 12
2.6 Model danych . . . 13
2.7 Scenariusze wdrożenia . . . 14
2.8 Tryby połączenia . . . 15
2.9 Metody i tryby uwierzytelniania użytkowników . . . 17
2.10 Mechanizmy bezpieczeństwa . . . 20
2.10.1 Szyfrowanie danych . . . 20
2.10.2 Kopie zapasowe . . . 20
2.10.3 Uprawnienia użytkowników . . . 20
2.10.4 Sandboxing . . . 21
2.10.5 Niezawodność . . . 21
2.10.6 Konfiguracja klastrowa . . . 21
2.11 Dashboard . . . 22

3 Instalacja i pierwsze uruchomienie **24**
3.1 Wymagania . . . 24
3.2 Urządzenie . . . 24
3.3 Pierwsze uruchomienie . . . 25

4 Szybki start **31**
4.1 SSH . . . 31
4.1.1 Założenia . . . 31
4.1.2 Konfiguracja . . . 31
4.1.3 Nawiązanie połączenia . . . 36
4.1.4 Podgląd sesji połączeniowej . . . 37
4.2 SSH w trybie bastionu . . . 37
4.2.1 Założenia . . . 38
4.2.2 Konfiguracja . . . 38
4.2.3 Nawiązanie połączenia . . . 42
4.2.4 Podgląd sesji połączeniowej . . . 44
4.3 RDP . . . 45
4.3.1 Broker połączeń RDP . . . 45
4.3.2 Założenia . . . 46
4.3.3 Konfiguracja . . . 46
4.3.4 Nawiązanie połączenia . . . 50
4.3.5 Podgląd sesji połączeniowej . . . 52
4.4 Telnet . . . 53
4.4.1 Założenia . . . 53
4.4.2 Konfiguracja . . . 53
4.4.3 Nawiązanie połączenia . . . 57
4.4.4 Podgląd sesji połączeniowej . . . 57
4.5 Telnet 5250 . . . 58
4.5.1 Założenia . . . 59
4.5.2 Konfiguracja . . . 59
4.5.3 Nawiązanie połączenia . . . 62
4.5.4 Podgląd sesji połączeniowej . . . 64
4.6 MySQL . . . 65
4.6.1 Założenia . . . 66
4.6.2 Konfiguracja . . . 66
4.6.3 Nawiązanie połączenia . . . 69
4.6.4 Podgląd sesji połączeniowej . . . 70
4.7 MS SQL . . . 71
4.7.1 Założenia . . . 71
4.7.2 Konfiguracja . . . 72
4.7.3 Nawiązanie połączenia . . . 76
4.7.4 Podgląd sesji połączeniowej . . . 77
4.8 HTTP . . . 78
4.8.1 Założenia . . . 79
4.8.2 Konfiguracja . . . 79
4.8.3 Nawiązanie połączenia . . . 82
4.8.4 Podgląd sesji połączeniowej . . . 83
4.9 Citrix . . . 83
4.9.1 ICA . . . 84
4.9.1.1 Plik konfiguracyjny połączenia ICA . . . 84
4.9.1.1.1 Plik ICA do połączeń bez TLS . . . 84

4.9.1.1.2 Plik ICA do połączeń TLS . . . 84
4.9.1.2 Założenia . . . 85
4.9.1.3 Konfiguracja . . . 85
4.9.1.4 Zdefiniowanie połączenia w pliku .ica . . . 89
4.9.1.5 Nawiązanie połączenia . . . 90
4.9.1.6 Podgląd sesji połączeniowej . . . 90
4.9.2 Citrix StoreFront . . . 90
4.9.2.1 Założenia . . . 90
4.9.2.2 Konfiguracja . . . 91
4.10 VNC . . . 98
4.10.1 Założenia . . . 98
4.10.2 Konfiguracja . . . 98
4.10.3 Nawiązanie połączenia . . . 102
4.10.4 Podgląd sesji połączeniowej . . . 104
4.11 Uwierzytelnienie użytkowników w katalogu LDAP . . . 105
4.11.1 Założenia . . . 105
4.11.2 Konfiguracja . . . 105

5 Użytkownicy **108**
5.1 Dodawanie użytkownika . . . 108
5.2 Modyfikowanie użytkownika . . . 114
5.3 Blokowanie użytkownika . . . 115
5.4 Odblokowanie użytkownika . . . 117
5.5 Usuwanie użytkownika . . . 117
5.6 Polityka czasowa dostępu do sejfów . . . 119
5.7 Role użytkownika . . . 120
5.8 Synchronizacja użytkowników z LDAP . . . 122
5.9 Dodawanie urządzenia mobilnego . . . 126
5.10 Usuwanie powiązanego urządzenia mobilnego . . . 129

6 Serwery **130**
6.1 Dodawanie serwera . . . 130
6.1.1 Serwery statyczne . . . 131
6.1.1.1 Dodawanie serwera Citrix . . . 131
6.1.1.2 Dodawanie serwera HTTP . . . 132
6.1.1.3 Dodawanie serwera ICA . . . 134
6.1.1.4 Dodawanie serwera Modbus . . . 136
6.1.1.5 Dodawanie serwera MS SQL . . . 138
6.1.1.6 Dodawanie serwera MySQL . . . 140
6.1.1.7 Dodawanie serwera Oracle . . . 142
6.1.1.8 Dodawanie serwera RDP . . . 144
6.1.1.9 Dodawanie serwera SSH . . . 146
6.1.1.10 Dodawanie serwera Telnet . . . 148
6.1.1.11 Dodawanie serwera Telnet 3270 . . . 150
6.1.1.12 Dodawanie serwera Telnet 5250 . . . 153
6.1.1.13 Dodawanie serwera VNC . . . 154
6.1.2 Serwery dynamiczne . . . 156
6.1.2.1 Definiowanie grupy serwerów . . . 156
6.1.2.2 Definiowanie pojedynczego hosta w ramach grupy serwerów . . . 156
6.2 Modyfikowanie serwera . . . 157
6.3 Blokowanie serwera . . . 158
6.4 Odblokowanie serwera . . . 159

6.5 Usuwanie serwera . . . 160
6.5.1 Usuwanie definicji serwera . . . 160
6.5.2 Usuwanie wybranego hosta z grupy serwerów dynamicznych . . . 161

7 Konta **162**
7.1 Dodawanie konta . . . 162
7.1.1 Dodawanie konta typu *anonymous* . . . 162
7.1.2 Dodawanie konta typu *forward* . . . 165
7.1.3 Dodawanie konta typu *regular* . . . 168
7.2 Edytowanie konta . . . 173
7.3 Blokowanie konta . . . 174
7.4 Odblokowanie konta . . . 175
7.5 Usuwanie konta . . . 175

8 Sejfy **177**
8.1 Dodawanie sejfu . . . 178
8.2 Modyfikowanie sejfu . . . 181
8.3 Blokowanie sejfu . . . 182
8.4 Odblokowanie sejfu . . . 183
8.5 Usuwanie sejfu . . . 184

9 Gniazda nasłuchiwania **186**
9.1 Dodawanie gniazda nasłuchiwania . . . 186
9.1.1 Dodawanie gniazda nasłuchiwania Citrix . . . 187
9.1.2 Dodawanie gniazda nasłuchiwania HTTP . . . 189
9.1.3 Dodawanie gniazda nasłuchiwania ICA . . . 191
9.1.4 Dodawanie gniazda nasłuchiwania Modbus . . . 193
9.1.5 Dodawanie gniazda MySQL . . . 195
9.1.6 Dodawanie gniazda Oracle . . . 197
9.1.7 Dodawanie gniazda RDP . . . 198
9.1.8 Dodawanie gniazda SSH . . . 201
9.1.9 Dodawanie gniazda MS SQL . . . 204
9.1.10 Dodawanie gniazda nasłuchiwania Telnet . . . 206
9.1.11 Dodawanie gniazda nasłuchiwania Telnet 3270 . . . 208
9.1.12 Dodawanie gniazda nasłuchiwania VNC . . . 210
9.2 Modyfikowanie gniazda nasłuchiwania . . . 212
9.3 Blokowanie gniazda nasłuchiwania . . . 213
9.4 Odblokowanie gniazda nasłuchiwania . . . 214
9.5 Usuwanie gniazda nasłuchiwania . . . 215

10 Modyfikatory haseł **217**
10.1 Polityki haseł . . . 217
10.1.1 Dodawanie polityki zmiany haseł . . . 217
10.1.2 Edytowanie polityki zmiany haseł . . . 218
10.1.3 Usuwanie polityki zmiany haseł . . . 218
10.2 Uniwersalne modyfikatory haseł . . . 219
10.2.1 Dodawanie uniwersalnego modyfikatora haseł . . . 219
10.2.2 Edytowanie uniwersalnego modyfikatora haseł . . . 220
10.2.3 Usuwanie modyfikatora haseł . . . 220
10.3 Konfigurowanie modyfikatora haseł Unix poprzez SSH . . . 221
10.4 Konfigurowanie modyfikatora haseł Windows WMI . . . 224

11 Polityki **227**

12 Sesje **235**
12.1 Filtrowanie sesji . . . 236
12.1.1 Definiowanie filtrów . . . 236
12.1.2 Przeszukiwanie pełnotekstowe . . . 238
12.1.3 Zarządzanie definicjami filtrowania . . . 239
12.2 Odtwarzanie sesji . . . 240
12.3 Podgląd trwających sesji . . . 242
12.4 Wstrzymywanie połączenia . . . 242
12.5 Przerywanie połączenia . . . 243
12.6 Dołączanie do sesji . . . 245
12.7 Udostępnianie sesji . . . 246
12.8 Komentowanie sesji . . . 247
12.9 Eksportowanie sesji . . . 250
12.10 Usuwanie sesji . . . 251
12.11 Przetwarzanie OCR sesji . . . 251
12.12 Znakowanie czasem wybranych sesji . . . 253
12.13 Akceptowanie połączeń oczekujących . . . 254
12.13.1 Interfejs administracyjny Fudo . . . 254
12.13.2 Fudo Mobile . . . 254
12.14 Odrzucanie połączeń oczekujących . . . 254
12.14.1 Interfejs administracyjny Fudo . . . 254
12.14.2 Fudo Mobile . . . 255

13 Raporty **257**
13.1 Subskrybowanie raportu cyklicznego . . . 257
13.2 Rezygnacja z subskrypcji raportu cyklicznego . . . 258
13.3 Generowanie raportu na żądanie . . . 258
13.4 Wyświetlanie i zapisywanie raportów . . . 259
13.5 Usuwanie raportów . . . 260

14 Analiza produktywności **261**
14.1 Zestawienie . . . 261
14.2 Analiza sesji . . . 262
14.3 Porównanie aktywności . . . 264

15 Administracja **265**
15.1 System . . . 265
15.1.1 Data i czas . . . 265
15.1.2 Certyfikat HTTPS . . . 268
15.1.3 Blokowanie nowych połączeń . . . 269
15.1.4 Dostęp SSH . . . 270
15.1.5 Domyślna domena . . . 271
15.1.6 Konto reset . . . 271
15.1.7 Funkcjonalności wrażliwe . . . 271
15.1.8 Aktualizacja systemu . . . 272
15.1.8.1 Aktualizowanie systemu . . . 273
15.1.8.2 Weryfikacja wykonalności aktualizacji . . . 273
15.1.8.3 Usuwanie migawki aktualizacji . . . 274
15.1.9 Licencja . . . 274
15.1.10 Diagnostyka . . . 275

15.2 Konfiguracja sieci . . . 277
15.2.1 Konfiguracja ustawień sieciowych . . . 277
15.2.1.1 Zarządzanie interfejsami fizycznymi . . . 277
15.2.1.2 Ustawianie adresu IP z konsoli . . . 281
15.2.1.3 Konfigurowanie mostu sieciowego . . . 285
15.2.1.4 Konfigurowanie sieci wirtualnych (VLAN) . . . 286
15.2.1.5 Konfigurowanie agregacji połączeń LACP . . . 286
15.2.2 Etykiety adresów IP . . . 288
15.2.3 Konfiguracja bajpasów . . . 288
15.2.4 Konfiguracja tras routingu . . . 289
15.2.5 Konfiguracja serwerów DNS . . . 290
15.2.6 Konfiguracja serwerów proxy . . . 292
15.2.7 Konfiguracja tablicy ARP . . . 294
15.3 Powiadomienia . . . 296
15.4 Znakowanie czasem . . . 298
15.5 Zewnętrzne serwery uwierzytelniania . . . 299
15.6 Zewnętrzne repozytoria haseł . . . 302
15.6.1 CyberArk Enterprise Password Vault . . . 302
15.6.2 Hitachi ID Privileged Access Manager . . . 303
15.6.3 Lieberman Enterprise Random Password Manager . . . 304
15.6.4 Thycotic Secret Server . . . 305
15.7 Zasoby . . . 306
15.8 Przywracanie poprzedniej wersji systemu . . . 308
15.9 Ponowne uruchomienie systemu . . . 309
15.10 SNMP . . . 310
15.10.1 Odczytywanie informacji SNMP poprzez `snmpwalk` . . . 311
15.10.2 Rozszerzenia SNMP Wheel Fudo PAM . . . 311
15.11 Kopie zapasowe i retencja . . . 319
15.12 Zewnętrzna macierz dyskowa . . . 321
15.12.1 Konfigurowanie zewnętrznej macierzy dyskowej . . . 322
15.12.2 Rozszerzanie zewnętrznej macierzy dyskowej . . . 322
15.13 Eksportowanie/importowanie konfiguracji systemu . . . 323
15.13.1 Eksportowanie konfiguracji . . . 323
15.13.2 Importowanie konfiguracji . . . 323
15.14 Konfiguracja klastrowa . . . 324
15.14.1 Inicjowanie klastra . . . 325
15.14.2 Zarządzanie węzłami klastra . . . 326
15.14.2.1 Dodawanie węzłów klastra . . . 326
15.14.2.2 Edytowanie węzłów klastra . . . 329
15.14.2.3 Usuwanie węzłów klastra . . . 330
15.14.3 Grupy redundancji . . . 330
15.15 Dziennik zdarzeń . . . 335
15.16 Integracja z serwerem CERB . . . 338
15.17 Czynności serwisowe . . . 348
15.17.1 Sporządzanie kopii zapasowej kluczy szyfrujących . . . 348
15.17.2 Monitorowanie stanu systemu . . . 352
15.17.3 Wymiana dysku macierzy . . . 353

16 Informacje uzupełniające **355**
16.1 Kody błędów . . . 355
16.2 Mapowanie parametrów Fudo 2.2 na Fudo 3.0 . . . 359

16.2.1 Połączenie . . . 360
16.2.2 Serwer . . . 362
16.3 Migracja modelu danych wersji 2.2 do 3.0 . . . 362
16.3.1 Serwer . . . 362
16.3.2 Sejf (dawniej *połączenie*) . . . 363
16.3.3 Konto (dawniej *dane logowania*) . . . 363
16.3.4 Gniazdo nasłuchiwania (dawniej *bastion* lub część serwera) . . . 363
16.3.5 Sesje . . . 364
16.4 Obsługa wspieranych protokołów . . . 364
16.4.1 Citrix StoreFront (HTTP) . . . 364
16.4.2 HTTP . . . 364
16.4.3 ICA . . . 365
16.4.4 Modbus . . . 365
16.4.5 MS SQL (TDS) . . . 365
16.4.6 MySQL . . . 365
16.4.7 Oracle . . . 366
16.4.8 RDP . . . 366
16.4.9 SSH . . . 367
16.4.10 Telnet . . . 367
16.4.11 Telnet 3270 . . . 367
16.4.12 Telnet 5250 . . . 368
16.4.13 VNC . . . 368
16.4.14 X11 . . . 368

17 AAPM (Application to Application Password Manager) 370
17.1 Informacje ogólne . . . 370
17.2 *fudopv* . . . 370
17.3 Interfejs API . . . 378

18 Service Now 379
18.1 Konfiguracja . . . 379
18.2 Wnioskowanie o dostęp do serwerów . . . 380
18.3 Przyznawanie dostępu . . . 382

19 Aplikacje klienckie 384
19.1 PuTTY . . . 384
19.2 Microsoft Remote Desktop . . . 386
19.3 VNC Viewer . . . 388
19.4 SQL Server Management Studio . . . 391

20 Usługa proxy dla uwierzytelnienia 4-Eyes 393
20.1 Instalacja usługi proxy . . . 393
20.2 Inicjalizacja konfiguracji za pomocą `whlproxyinit` . . . 393
20.3 Zarządzanie klastrami za pomocą `whlproxyctl` . . . 395
20.3.1 Dodawanie klastra . . . 395
20.3.2 Usuwanie klastra . . . 395
20.3.3 Wyświetlanie szczegółów klastra . . . 395
20.3.4 Wyświetlanie listy klastrów . . . 395
20.4 Zarządzanie węzłami za pomocą `whlproxyctl` . . . 396
20.4.1 Dodawanie węzła do klastra . . . 396
20.4.2 Usuwanie węzła klastra . . . 396
20.4.3 Wyświetlanie szczegółów węzła . . . 396

20.4.4 Wyświetlanie listy węzłów 396

21 Rozwiązywanie problemów **398**
21.1 Uruchamianie Wheel Fudo PAM 398
21.2 Połączenia z serwerami 399
21.3 Logowanie do panelu administracyjnego 404
21.4 Odtwarzanie sesji 405
21.5 Konfiguracja klastrowa 405
21.6 Znakowanie czasem 406

22 Często zadawane pytania **407**

23 Słownik pojęć **410**

Indeks **413**

ROZDZIAŁ 1

Informacje ogólne

1.1 O dokumentacji

Struktura dokumentacji

1. Informacje ogólne

Rozdział zawiera informacje na temat dokumentacji i różnicy w modelu danych pomiędzy wersją 2.x a 3.x.

2. Opis Systemu

Rozdział zawiera informacje na temat poszczególnych modułów Wheel Fudo PAM, opisuje scenariusze wdrożenia a także tryby połączenia oraz metody uwierzytelnienia użytkowników.

3. Instalacja i pierwsze uruchomienie

Rozdział opisuje procedurę wdrożenia Wheel Fudo PAM wraz z inicjalizacją systemu.

4. Szybki start

Rozdział zawiera przykłady konfiguracji typowych przypadków użycia.

5. Użytkownicy

Rozdział zawiera tematy związane z zarządzaniem użytkownikami.

6. Serwery

Rozdział zawiera tematy związane z zarządzaniem serwerami.

7. Konta

Rozdział zawiera tematy związane z zarządzaniem kontami.

8. Sejfy

Rozdział zawiera tematy związane z zarządzaniem sejfami.

9. Gniazda nasłuchiwania

Rozdział zawiera tematy związane z zarządzaniem gniazdami nasłuchiwania.

10. Modyfikatory haseł

Rozdział opisuje zagadnienia automatycznej zmiany haseł w systemach docelowych.

11. Polityki

Rozdział opisuje zagadnienia związane z proaktywnym monitoringiem.

12. Sesje

Rozdział zawiera informacje dotyczące rejestrowanych sesji dostępowych.

13. Raporty

Rozdział zawiera informacje na temat generowania raportów.

14. Analiza produktywności

Rozdział opisuje w szczegółach moduł analizy produktywności użytkowników w monitorowanych sesjach.

15. Administracja

Rozdział zawiera opisy procedur administracyjnych.

16. Informacje uzupełniające

Rozdział zawiera informacje uzupełniające bezpośrednio związane z procedurami zarządzania.

17. AAPM (Application to Application Password Manager)

Rozdział zawiera opis modułu zmiany haseł w aplikacjach trzecich.

18. Service Now

Rozdział zawiera opis integracji Wheel Fudo PAM z systemem zarządzania zgłoszeniami *Service Now*.

19. Rozwiązywanie problemów

Rozdział zawiera rozwiązania potencjalnych problemów jakie mogą pojawić się podczas korzystania z Wheel Fudo PAM.

20. Często zadawane pytania

Rozdział zawiera odpowiedzi na często zadawane pytania.

21. Słownik pojęć

Rozdział zawiera listę pojęć technicznych występujących w dokumentacji.

Konwencje i symbole

Poniższa sekcja opisuje konwencje nazewnicze użyte w dokumentacji.

kursywa

Element interfejsu graficznego użytkownika.

`przykład`

Przykładowa wartość parametru konfiguracyjnego.

Informacja: Informacja uzupełniająca ściśle związana z opisywanym zagadnieniem, np. sugestia dotycząca postępowania; dodatkowe warunki, które należy spełnić.

Ostrzeżenie: Ostrzeżenie. Informacja istotna z punktu widzenia działania systemu. Nie zastosowanie się do zalecenia może mieć nieodwracalne skutki.

Nota prawna

ROZDZIAŁ 2

Opis systemu

Wheel Fudo PAM jest rozwiązaniem do zarządzania zdalnym dostępem uprzywilejowanym.

2.1 PSM (Privileged Sessions Management)

Moduł PSM służy do stałego monitorowania zdalnych sesji dostępu do infrastruktury IT. Wheel Fudo PAM pośredniczy w zestawianiu połączenia ze zdalnym zasobem i rejestruje wszelkie akcje użytkownika, włącznie z ruchem kursora myszy, danymi wprowadzanymi za pomocą klawiatury i przesyłanymi plikami.

Rejestrowany jest kompletny ruch sieciowy, włącznie z meta danymi, co pozwala na precyzyjne odtworzenie przebiegu sesji dostępowej oraz pełnotekstowe przeszukiwanie treści.

Wheel Fudo PAM pozwala również na podgląd aktualnie trwających połączeń i ingerencję administratora w monitorowaną sesję w przypadku stwierdzenia nadużycia praw dostępu.

2.1.1 Citrix StoreFront (HTTP)

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.

- Brak wsparcia dla trybu bastion wynika z ograniczeń protokołu. Citrix StoreFront sam w sobie daje dostęp do bastionu maszyn. Użytkownik logując się do Citrix StoreFront może wybrać w swoim panelu maszynę, z którą chce się połączyć za pomocą protokołu ICA.

2.1.2 HTTP

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak monitorowania ściąganych zasobów z zewnętrznych.
- Brak śledzenia przekierowań.

2.1.3 ICA

Wspierane tryby połączenia:

- *Bastion* (możliwość wpisania konta lub serwera docelowego w pliku ICA),
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- Citrix Receiver.

Wspierane algorytmy szyfrujące:

- Basic
- TLS

Uwagi:

- Połączenia ICA nie wspierają mechanizmu dołączania do sesji.
- Obsługa połączeń ICA poprzez interfejs *Citrix StoreFront* wymaga użycia kont typu *anonymous* lub *forward*.
- Nawiązanie bezpośredniego połączenia z serwerem (z pominięciem *Citrix StoreFront*) wymaga utworzyenia pliku konfiguracyjnego `.ica`. Więcej informacji znajdziesz w rozdziale *Plik konfiguracyjny połączenia ICA*.

2.1.4 Modbus

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

2.1.5 MS SQL (TDS)

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqsh.

2.1.6 MySQL

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- Oficjalny klient MySQL,
- Biblioteki PyMySQL dla Pythona.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.

2.1.7 Oracle

Ostrzeżenie: Wsparcie protokołu *Oracle* jest ograniczone z uwagi na jego zamknięty charakter. Firma Wheel Systems nie gwarantuje prawidłowej obsługi wszystkich funkcji tego protokołu.

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- SQLDeveloper 4.1.3.20.78,
- SQL*Plus: Release 11.2.0.4.0 Production.

Uwagi:

- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.
- Odtwarzacz uwzględnia tylko zapytania klientów (w podglądzie sesji nie wyświetlamy odpowiedzi serwera).
- Wspierane wersje 10 i 11.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

2.1.8 RDP

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- Wszystkie oficjalne Microsoft – Windows, macOS,
- FreeRDP 2.0 i nowsze.

Wspierane języki OCR:

- angielski,
- niemiecki,
- norweski,
- polski,
- rosyjski.

Uwagi:

- W przypadku uwierzytelnienia użytkowników Fudo przed AD (lub innym zewnętrznym źródłem) tryb bezpieczeństwa TLS+NLA (Network Level Authentication) nie jest obsługiwany; zamiast niego stosowany jest tryb TLS. Wsparcie dla trybu NLA po stronie serwera docelowego jest zapewnione.

RemoteApp

Wheel Fudo PAM natywnie wspiera mechnizm RemoteApp, nagrywając okna aplikacji tak samo jak połączenia RDP, z zachowaniem wszelkich restrykcji bezpieczeństwa.

Monitorowanie RemoteApp wymaga, aby połączenie było nawiązane poprzez odpowiednio przygotowany plik konfiguracyjny `*.rdp`, w którym zdefiniowany jest adres IP oraz numer portu Wheel Fudo PAM. Połączenia inicjowane poprzez *Remote Desktop Web Access* mogą być monitorowane jedynie w trybie transparentnym/bramy.

2.1.9 SSH

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wybrane wspierane funkcje:

- Multipleksowanie połączeń (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- SCP (surowy ruch, przerwanie sesji, możliwość wyodrębnienia poszczególnych plików),
- SFTP,
- Przekierowanie portów (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- SSH Agent forwarding (przeźroczysty, nie rejestrujemy),
- X11 - w ramach protokołu SSH (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Shell (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Terminal (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch).

Wspierane algorytmy szyfrujące: - Serwer: RSA, DSA - Gniazdo nasłuchiwania: RSA, DSA

Wspierane funkcje skrótu (algorytmy hashujące): - MD5 - SHA1

Uwagi: - Brak możliwości przekazywania (forwardowania) klucza SSH.

2.1.10 Telnet 3270

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,

- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- c3270.

2.1.11 Telnet 5250

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.
- Brak możliwości dołączenia do sesji.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- tn5250.

2.1.12 Telnet

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

2.1.13 VNC

Wspierane tryby połączenia:

- *Bastion*,
- *Brama*,

- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- TightVNC,
- RealVNC.

Wspierane języki OCR:

- angielski,
- niemiecki,
- norweski,
- polski,
- rosyjski.

Charakterystyka połączenia - serwer wymaga uwierzytelnienia

- Konto typu *anonymous*: wymaga podania hasła logowania do serwera VNC.
- Konto typu *regular*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo); ciąg znaków, na który podmieniana jest nazwa użytkownika jest ignorowany.
- Konto typu *forward*: hasło uwierzytelniające zgodne ze zdefiniowanym po stronie serwera VNC.

Charakterystyka połączenia - serwer nie wymaga uwierzytelnienia

- Konto typu *anonymous*: nie wymaga podawania jakichkolwiek danych na ekranie logowania.
- Konto typu *regular*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo); ciąg znaków określający hasło przekazywane do systemu docelowego może być pusty.
- Konto typu *forward*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo);

2.1.14 X11

Protokół X11 wspierany jest w ramach protokołu SSH.

Informacja: Funkcja *dołączania do sesji* nie jest dostępna dla połączeń realizowanych za pośrednictwem protokołu X11.

Wspierane serwery:

- Xorg,
- Xming,
- XQuartz.

2.1.15 TCP

TCP to generyczny typ protokołu, służący do monitorowania połączeń nieszyfrowanych.

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak możliwości dołączenia do sesji.

Wheel Fudo PAM wspiera następujące konfiguracje systemowe:

- Linux,
- FreeBSD,
- Mac OS X
- Microsoft Windows Server,
- Microsoft Windows,
- TightVNC,
- Solaris.

Tematy pokrewne:

- *Wymagania*
- *Model danych*
- *Mechanizmy bezpieczeństwa*

2.2 AAPM (Application to Application Password Manager)

Moduł *AAPM* umożliwia bezpieczną wymianę haseł pomiędzy aplikacjami.

Systemy operacyjne wspierane przez moduł AAPM:

- systemy operacyjne Microsoft Windows
- systemy operacyjne rodziny Linux
- systemy operacyjne rodziny BSD

Tematy pokrewne:

- *Wymagania*
- *Model danych*
- *Mechanizmy bezpieczeństwa*

2.3 Skarbiec haseł (Secret Manager)

Moduł *Secret Manager* umożliwia automatyczne zarządzanie danymi logowania na monitorowanych systemach i okresową zmianę haseł po upływie zdefiniowanego interwału czasowego.

Secret Manager potrafi zmieniać hasła na następujących systemach:

- Unix
- MySQL
- Cisco
- Cisco Enable Password
- MS Windows

Moduł *Secret Manager* umożliwia także zdefiniowanie własnych modyfikatorów haseł w postaci zestawu komend wykonywanych na zdalnej maszynie.

Wiecej informacji na temat modyfikatorów haseł znajdziesz w rozdziale Konfiguracja > *Modyfikatory haseł*.

2.4 Efficiency Analyzer

Moduł analizy wydajności śledzi akcje użytkowników i pozwala dostarczyć szczegółowych informacji o czasie aktywności i bezczynności.

2.5 Portal użytkownika

Portal użytkownika umożliwia przeglądanie listy zasobów, do których użytkownik posiada stosowne uprawnienia i inicjowanie połączenia z monitorowanym zasobem za pośrednictwem wybranego gniazda nasłuchiwania.

2.6 Model danych

Wheel Fudo PAM operuje na pięciu podstawowych typach obiektów: użytkownik, serwer, konto, sejf oraz gniazdo nasłuchiwania.

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

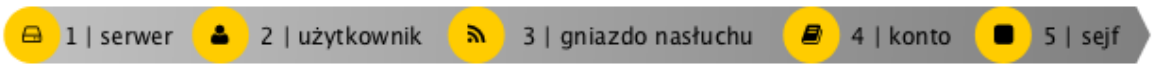
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

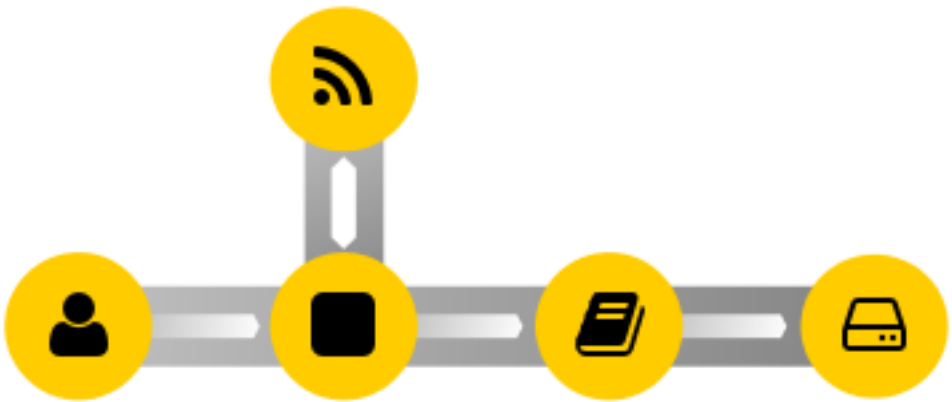
Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

Prawidłowe działanie systemu wymaga odpowiedniego skonfigurowania *serwerów*, *użytkowników*, *gniazd nasłuchiwania*, *kont uprzywilejowanych* oraz *sejfów*.



Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

Schemat relacji obiektów



Tematy pokrewne:

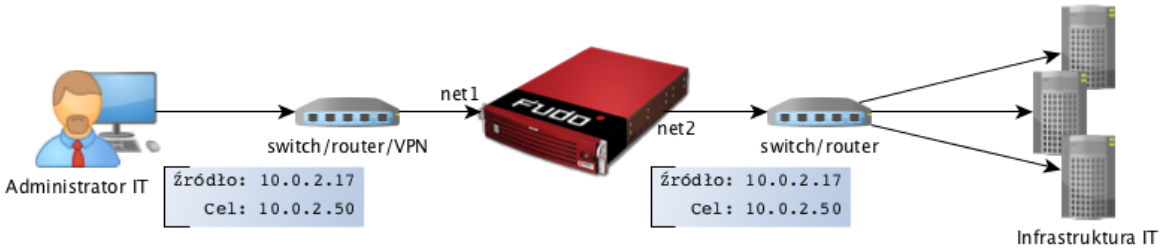
- *Opis systemu*
- *Metody i tryby uwierzytelniania użytkowników*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

2.7 Scenariusze wdrożenia

Informacja: Zaleca się umiejscowienie Wheel Fudo PAM w infrastrukturze IT tak, aby pośredniczyło jedynie w połączeniach administracyjnych. Pozwoli to na ograniczenie obciążenia systemu, optymalizację ruchu w sieci a także zachowanie ciągłości dostępu do usług w okoliczności awarii sprzętowej.

Most

W trybie mostu Wheel Fudo PAM pośredniczy w komunikacji pomiędzy użytkownikami i monitorowanymi serwerami bez względu na to czy ruch podlega monitorowaniu (tj. komunikacja przebiega z użyciem wspieranych protokołów) czy nie.



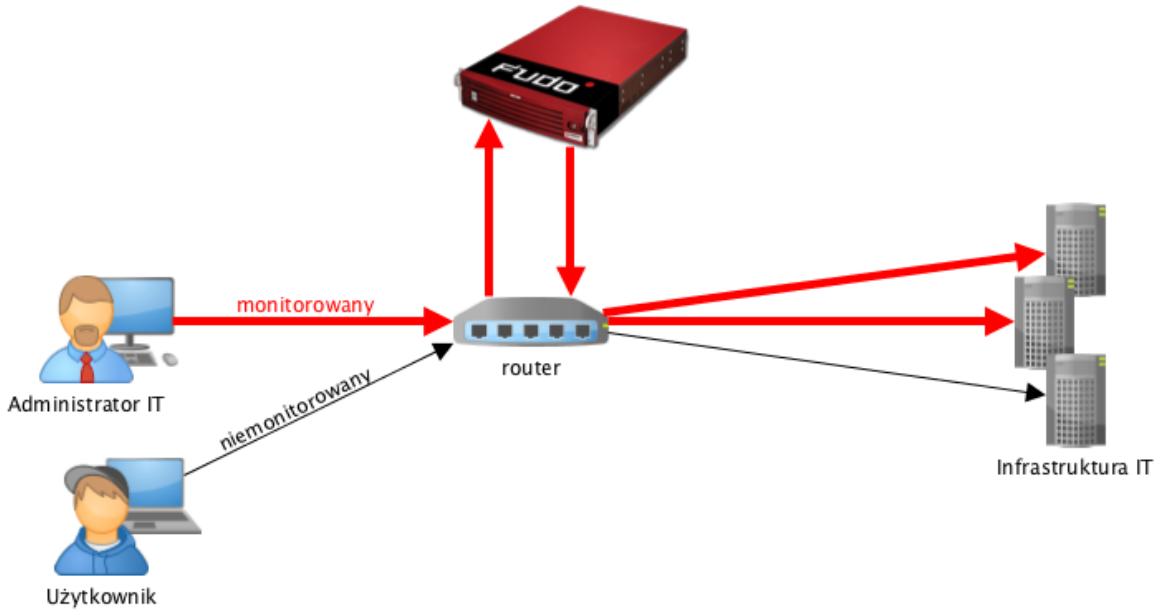
Wheel Fudo PAM pośrednicząc w przekazywaniu ruchu, zachowuje źródłowy adres IP klienta wysyłającego zapytania do serwerów.

Takie rozwiązanie pozwala na zachowanie dotychczasowych reguł na zaporach ogniowych regulujących dostęp do zasobów wewnętrznych.

Szczegóły na temat konfigurowania mostu znajdziesz w rozdziale *Konfiguracja sieci*.

Wymuszony routing

Tryb wymuszonego routingu wymaga użycia i odpowiedniego skonfigurowania routera. Taka topologia wdrożenia pozwala na sterowanie ruchem w sieci na poziomie trzeciej warstwy (sieci) modelu ISO/OSI, tak aby poprzez Wheel Fudo PAM kierowany był ruch administracyjny natomiast pozostałe zapytania były kierowane bezpośrednio do serwera docelowego.



Tryb ten nie wymaga zmian w topologii sieci i pozwala na optymalizację ruchu i obciążenia sprzętu poprzez rozdzielenie zapytań administracyjnych i produkcyjnych.

Tematy pokrewne:

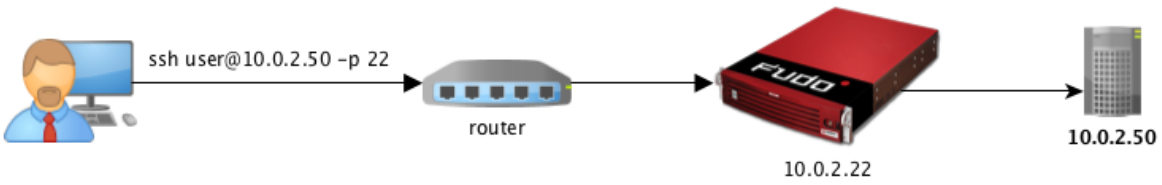
- *Tryby połączenia*
- *Zarządzanie serwerami*
- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Pierwsze uruchomienie*

2.8 Tryby połączenia

Niezależnie od zastosowanego scenariusza wdrożenia, Wheel Fudo PAM może pracować w trybie transparentnym, trybie bramy lub jako pośrednik (proxy).

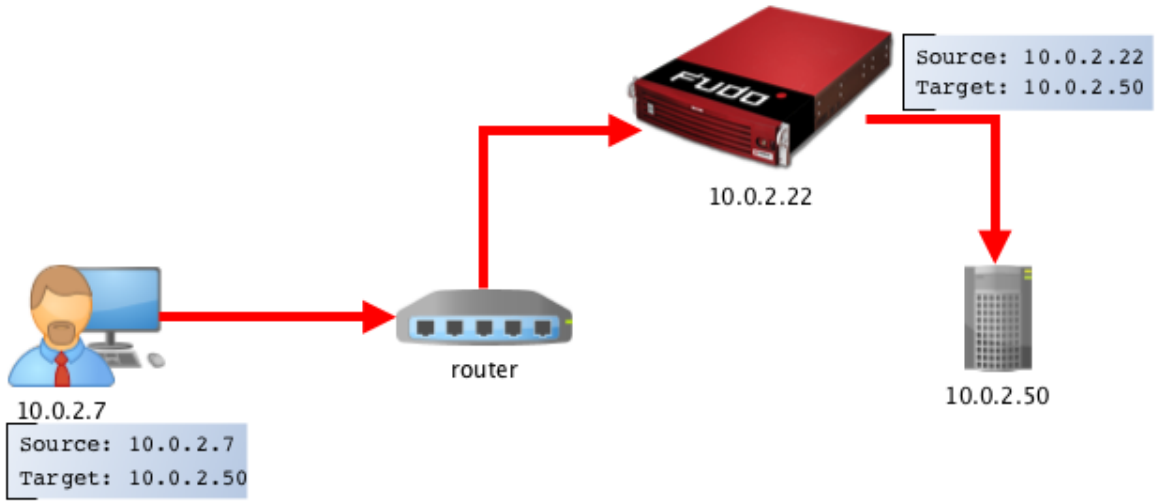
Przezroczysty

W trybie transparentnym, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Wheel Fudo PAM zestawiając połączenie z monitorowanym zasobem używa adresu IP klienta.



Brama

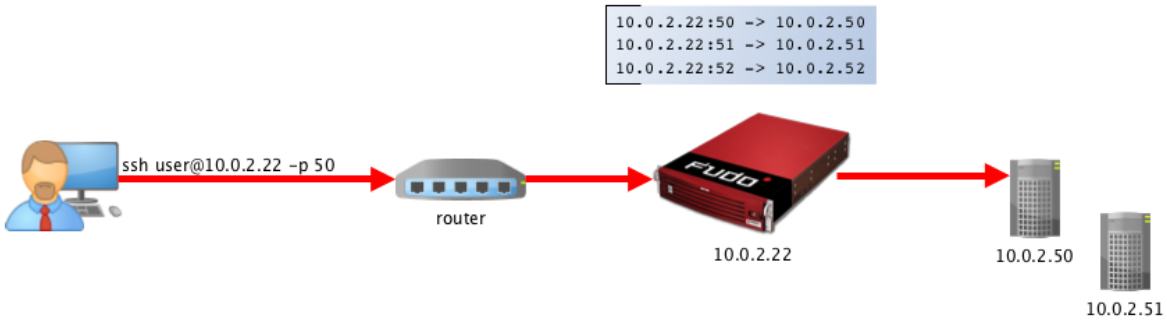
W trybie bramy, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Wheel Fudo PAM zestawiając połączenie z monitorowanym zasobem używa własnego adresu IP. Tryb pracy bramy pozwala na sterowanie ruchem sieciowym, by ten stale przechodził przez Wheel Fudo PAM, w przypadku gdy zastosowanie mają polityki kierowania ruchem.



Ustawienie adresu IP Wheel Fudo PAM jako adresu źródłowego pakietu sprawi, że odpowiedź z serwera trafi do Wheel Fudo PAM i dalej do klienta, a nie bezpośrednio do klienta.

Pośrednik

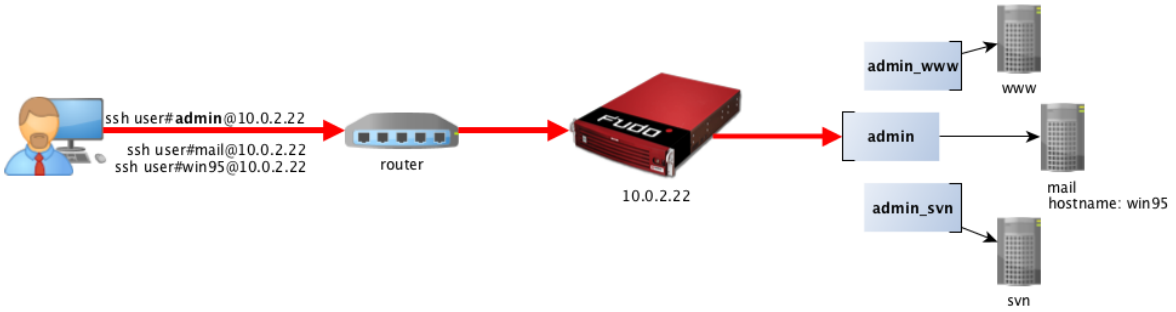
W trybie pośrednika, użytkownik nawiązuje połączenie z serwerem docelowym wskazując adres IP Wheel Fudo PAM i numer portu przypisany do danego serwera. Unikalność numeru portu pozwala na zestawienie połączenia z właściwym zasobem.



Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Wheel Fudo PAM.

Bastion

W trybie bastionu, konto na serwerze docelowym (lub sam serwer) zdefiniowane jest w ciągu identyfikującym użytkownika, np. `ssh user#mail@10.0.2.22`. Bastion pozwala na realizowanie dostępu do szeregu serwerów poprzez tę samą kombinację adresu IP i numeru portu, umożliwiając zachowanie domyślnych numerów portów dla poszczególnych protokołów.



Informacja:

- Tryb bastion wspierany jest w połączeniach realizowanych za pośrednictwem protokołów: SSH, RDP, VNC, Telnet, Telnet 3270, Telnet 5250, MS SQL, ICA.
- W przypadku gdy wskazane konto nie istnieje, Wheel Fudo PAM dokona próby dopasowania podanego ciągu znaków do nazwy serwera. Jeśli system nie stwierdzi istnienia obiektu serwera o takiej nazwie, spróbuje dokonać dopasowania na podstawie nazwy DNS hosta.
- Ciąg wskazujący obiekt docelowy, musi jednoznacznie identyfikować konto lub serwer.

Tematy pokrewne:

- *Scenariusze wdrożenia*
- *Zarządzanie serwerami*
- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Pierwsze uruchomienie*

2.9 Metody i tryby uwierzytelniania użytkowników

Metody uwierzytelniania użytkowników

Wheel Fudo PAM pośrednicząc w nawiązywaniu połączeń z serwerami dokonuje uwierzytelnienia użytkowników.

Wspierane metody uwierzytelnienia:

- *Hasło statyczne*,
- *Klucz publiczny*,
- *CERB*,
- *RADIUS*,
- *LDAP*,
- *Active Directory*.

Informacja: Zewnętrzne serwery uwierzytelniania CERB, RADIUS, LDAP oraz Active Directory, wymagają wcześniejszego skonfigurowania. Szczegółowe informacje na ten temat znajdziesz w rozdziale *Zarządzanie zewnętrznymi serwerami uwierzytelnienia*.

Tryby uwierzytelnienia

Po uwierzytelnieniu użytkownika, Wheel Fudo PAM zestawia połączenie ze zdalnym serwerem używając oryginalnych danych logowania, bądź dokonując ich podmiany.

Uwierzytelnianie z przekazywaniem loginu i hasła

W trybie uwierzytelniania z przekazywaniem loginu i hasła, Wheel Fudo PAM przekazuje wprowadzone przez użytkownika dane i wykorzystuje je w stanie niezmienionym do zestawienia połączenia z serwerem.

Informacja:

- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, wprowadzony przez użytkownika login jest ignorowany przy zestawianiu połączenia.

Uwierzytelnienie z podmianą loginu i hasła

W tym trybie uwierzytelniania, wprowadzone przez użytkownika login i hasło, przy zestawianiu połączenia z serwerem, są podmieniane na wcześniej zdefiniowane.

Uwierzytelnianie z podmianą loginu i hasła pozwala na jednoznaczne wskazanie podmiotu, który nawiązywał połączenie z serwerem, w sytuacji gdy wielu użytkowników korzysta z tego samego konta użytkownika na monitorowanym serwerze.

Takie rozwiązanie pozwala na uproszczenie zarządzania użytkownikami na monitorowanych serwerach.

Informacja:

- Hasło dostępu do serwera docelowego może być zdefiniowane w obiekcie *Konto*, lub każdorazowo pobierane z wewnętrznego lub zewnętrznego repozytorium haseł. Więcej informacji znajdziesz w rozdziałach *Modyfikatory haseł* i *Zewnętrzne repozytoria haseł*.
- W przypadku monitorowania dostępu do baz danych Oracle, hasło użytkownika i hasło do konta uprzywilejowanego, muszą być oba krótsze niż 16 znaków lub zawierać się w przedziale 16-32 znaków.
- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.

Podwójne uwierzytelnienie

W trybie podwójnego uwierzytelniania, użytkownik dwukrotnie podaje dane logowania. Pierwszy raz celem uwierzytelnienia przed Wheel Fudo PAM, drugi raz w celu zalogowania się do systemu docelowego.

Uwierzytelnianie z podmianą hasła

W tym trybie, podczas zestawiania połączenia, Wheel Fudo PAM przekazuje wprowadzony przez użytkownika login i podmienia podane hasło.

Informacja:

- Hasło dostępu do serwera docelowego może być zdefiniowane w obiekcie, lub każdorazowo pobierane z zewnętrznego repozytorium haseł. Więcej informacji znajdziesz w rozdziale *Zewnętrzne repozytoria haseł*.
- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login użytownika jest ignorowany przy zestawianiu połączenia.

Uwierzytelnienie przez serwer docelowy

W tym trybie, Wheel Fudo PAM przekazuje dane logowania do serwera docelowego, który weryfikuje ich poprawność i przekazuje status weryfikacji do Wheel Fudo PAM. Tryb uwierzytelnienia przez serwer docelowy dostępny jest dla połączeń *ssh* oraz *RDP* w trybie NLA.

Autoryzacja dostępu przez administratora (uwierzytelnienie w trybie 4-Eyes)

Wheel Fudo PAM umożliwia skonfigurowanie sejfu tak, aby każde żądanie połączenia realizowane za pośrednictwem danego obiektu, wymagało potwierdzenia przez administratora za pomocą aplikacji mobilnej *Fudo Mobile* lub z poziomu interfejsu administracyjnego.

- *Dodawanie urządzenia mobilnego*
- *Usuwanie powiązanego urządzenia mobilnego*

- *Konfiguracja serwerów proxy*
- *Dodawanie sejfu*
- *Akceptowanie połączeń oczekujących*
- *Odrzucanie połączeń oczekujących*

Tematy pokrewne:

- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

2.10 Mechanizmy bezpieczeństwa

2.10.1 Szyfrowanie danych

Dane przechowywane na Wheel Fudo PAM szyfrowane są za pomocą algorytmu AES-XTS, który wykorzystuje 256 bitowe klucze szyfrujące. Algorytm AES-XTS jest najefektywniejszym rozwiązaniem szyfrowania danych przechowywanych na napędach dyskowych.

Urządzenie fizyczne

Klucze szyfrujące przechowywane są na dwóch modułach pamięci USB (pendrive). Moduły te dostarczane są wraz z Wheel Fudo PAM w stanie niezainicjowanym. Ustalenie kluczy następuje przy pierwszym uruchomieniu urządzenia, podczas którego oba moduły pamięci USB muszą być podłączone (procedura pierwszego uruchomienia opisana jest w rozdziale *Pierwsze uruchomienie*).

Po zainicjowaniu kluczy i uruchomieniu Wheel Fudo PAM, oba moduły pamięci USB mogą zostać odłączone od urządzenia i umieszczone w bezpiecznym miejscu. W codziennej eksploatacji, klucz szyfrujący wymagany jest jedynie podczas uruchamiania systemu. Jeśli procedury bezpieczeństwa na to pozwalają, jeden z kluczy może być stale podłączony do Wheel Fudo PAM, dzięki czemu urządzenie będzie mogło uruchomić się samoczynnie w sytuacji np. zaniku zasilania, lub ponownego uruchomienia po aktualizacji systemu.

Środowisko wirtualne

W środowisku wirtualnym, system plików szyfrowany jest za pomocą frazy szyfrującej, definiowanej w procesie inicjalizacji obrazu systemu. Określony ciąg znaków musi być wprowadzony każdorazowo, podczas startu maszyny.

2.10.2 Kopie zapasowe

Wheel Fudo PAM posiada zaimplementowany mechanizm tworzenia kopii zapasowych danych na zewnętrznych serwerach, przy wykorzystaniu protokołu rsync.

2.10.3 Uprawnienia użytkowników

Każdy obiekt modelu danych posiada przypisanych użytkowników uprawnionych do zarządzania obiektem w zakresie określonym rolą użytkownika.

Więcej informacji na temat uprawnień użytkowników znajdziesz w rozdziale *Role użytkownika*.

2.10.4 Sandboxing

Wheel Fudo PAM wykorzystuje mechanizm sandboxowania CAPSICUM, który separuje poszczególne połączenia na poziomie systemu operacyjnego Wheel Fudo PAM. Ścisła kontrola przydzielonych zasobów systemowych i ograniczenie dostępu do informacji na temat systemu operacyjnego, zwiększają bezpieczeństwo oraz znacząco wpływają na stabilność systemu.

2.10.5 Niezawodność

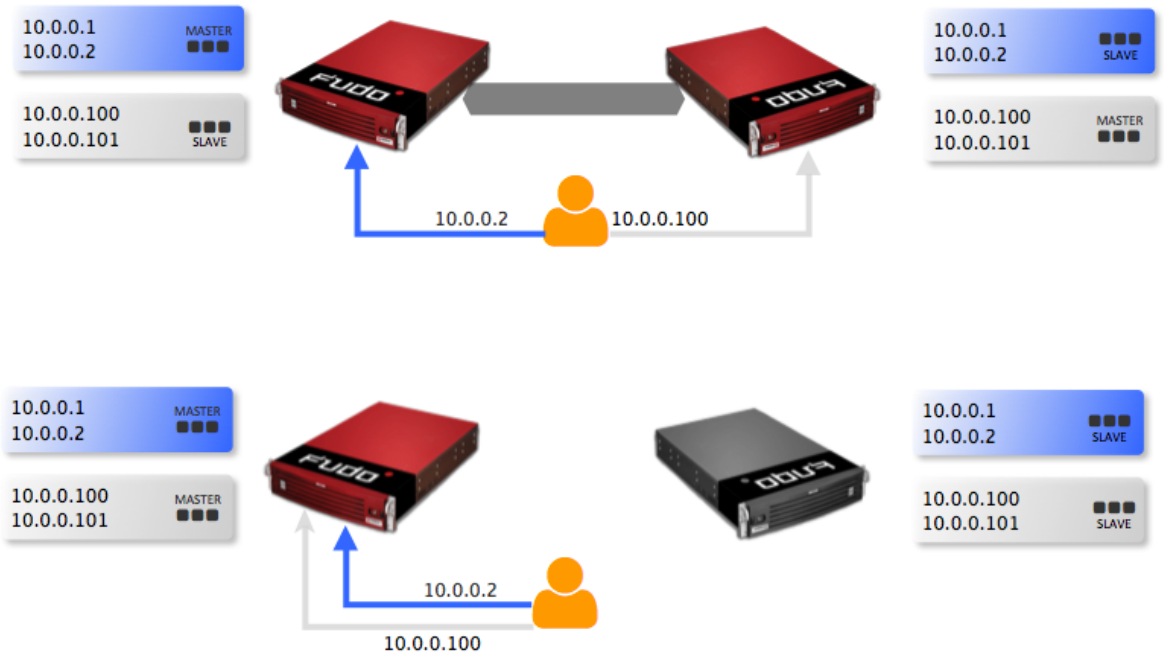
Wheel Fudo PAM dostarczane jest w konfiguracji sprzętowej zapewniającej optymalną wydajność i wysoką niezawodność systemu.

2.10.6 Konfiguracja klastrowa

Wheel Fudo PAM może pracować w konfiguracji klastrowej. Układ klastrowy pracuje w trybie multimaster, w którym konfiguracja systemu (połączenia, serwery, sesje, etc.) synchronizowana jest na każdym z węzłów klastra. W przypadku awarii węzła następuje automatyczne przełączenie na inny węzeł, co pozwala na zachowanie ciągłości świadczenia usług.

Ostrzeżenie: Konfiguracja klastrowa nie jest mechanizmem tworzenia kopii zapasowych danych. Dane sesji usunięte z jednego węzła, zostaną również usunięte z pozostałych węzłów klastra.

Adresy klastrowe agregowane są w grupy redundancji, które pozwalają na realizowanie statycznej dystrybucji żądań użytkowników na poszczególne węzły klastra, zachowując przy tym niezawodnościowy charakter klastra.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

- *Opis systemu*
- *Szybki start*
- *Pierwsze uruchomienie*

2.11 Dashboard

Widok startowy Wheel Fudo PAM umożliwia szybki dostęp do informacji o stanie urządzenia, a także pozwala na wykonanie procedury wyłączenia lub ponownego uruchomienia systemu.

Informacja: Informacja o zajętości przestrzeni dyskowej bierze pod uwagę obszar zarezerwowany przez mechanizm redundancji danych. Stąd wynika raportowana zajętość macierzy dyskowej po zainicjowaniu systemu.

Status dysków

●	Dysk pracuje prawidłowo.
●	Dysk w trakcie synchronizacji danych.
●	Błędy odczytu/zapisu danych - dysk nie działa prawidłowo i może wkrótce ulec awarii - skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.
●	Awaria dysku - dysk wymaga wymiany, skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.

Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

ROZDZIAŁ 3

Instalacja i pierwsze uruchomienie

Ten rozdział opisuje urządzenie fizyczne i procedurę pierwszego uruchomienia.

3.1 Wymagania

Panel zarządzający

Zarządzanie systemem odbywa się za pomocą panelu administracyjnego dostępnego z poziomu przeglądarki internetowej. Zalecanymi przeglądarkami są Google Chrome oraz Mozilla Firefox.

Wymagania sieciowe

Poprawne działanie Wheel Fudo PAM wymaga:

- Możliwości wykonywania połączeń dla sesji administracyjnych na port 443 urządzenia.
- Możliwości wykonywania połączeń do Wheel Fudo PAM przez klientów oraz z Wheel Fudo PAM do maszyn docelowych.
- Prawidłowo działającego *serwera czasu*.

Wymagania sprzętowe (*nie dotyczy maszyny wirtualnej*)

Wheel Fudo PAM jest całościowym rozwiązaniem sprzętowo-programowym. Zainstalowanie urządzenia wymaga fizycznej przestrzeni 2U (model F100x) lub 3U (model F300x) w szafie serwerowej oraz podłączenie do infrastruktury sieciowej.

Wymagania dla klienta VNC

Połączenia VNC muszą być realizowane w trybie odwzorowania kolorów 24-bit (true color).

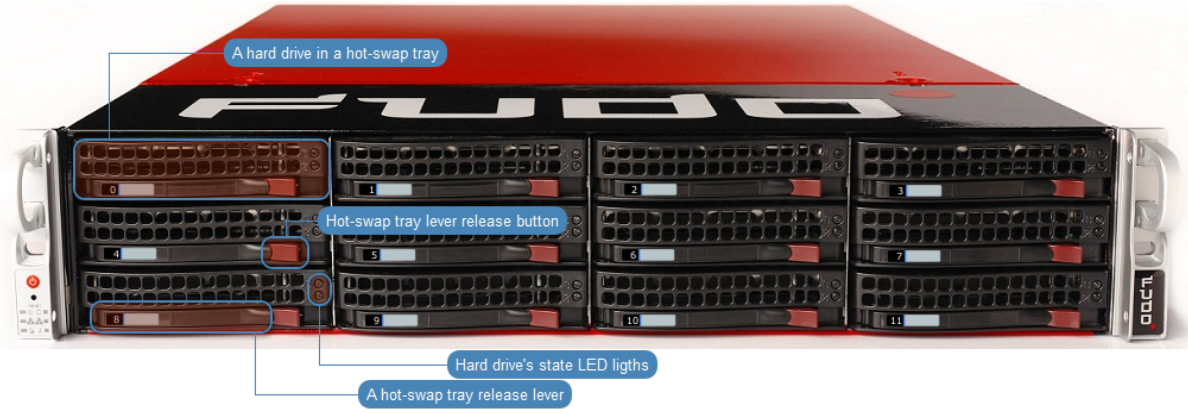
3.2 Urządzenie

Wheel Fudo PAM dostarczane jest w obudowie do montażu w standardowej szafie serwerowej 19".

Panel przedni

Zatoki dysków twardych

Pod przednim panelem obudowy, znajdują się zatoki dysków twardych, w kieszeniach umożliwiających wymianę dysku bez konieczności wyłączania urządzenia («hot-swap»).



Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

3.3 Pierwsze uruchomienie

Urządzenie fizyczne

Wheel Fudo PAM dostarczane jest z dwoma nośnikami pamięci USB, w stanie niezainicjowanym. Podczas pierwszego uruchomienia generowane są klucze szyfrujące, które zostają zapisane na dołączonych modułach pamięci USB. Więcej na temat kluczy szyfrujących znajdziesz w rozdziale *Mechanizmy bezpieczeństwa*.

Procedura pierwszego uruchomienia

1. Umieść urządzenie w szafie serwerowej 19".
2. Podłącz obydwa zasilacze do instalacji elektrycznej 230V.

Informacja: Podłączenie obydwu zasilaczy jest konieczne do uruchomienia systemu.

3. Podłącz kabel sieciowy do jednego z portów RJ-45.
4. Podłącz dostarczone wraz z urządzeniem nośniki pamięci flash do portów USB.

Informacja: Pierwsze uruchomienie wymaga podłączenia obu nośników pamięci. Więcej na temat inicjacji kluczy szyfrujących znajdziesz w rozdziale *Mechanizmy bezpieczeństwa*.

5. Wciśnij przycisk zasilania znajdujący się na przednim panelu obudowy.

6. Po zainicjowaniu kluczy szyfrujących, odłącz nośniki pamięci.

Ostrzeżenie:

- Bezwzględnie odłącz jeden z nośników i umieść w bezpiecznym miejscu, do którego dostęp mają tylko osoby upoważnione.
- Jeśli nośniki pamięci z zapisanymi kluczami zostaną utracone, urządzenie nie będzie mogło zostać uruchomione, a przechowywane tam dane nie będą dostępne. Producent nie przechowuje żadnych kluczy.

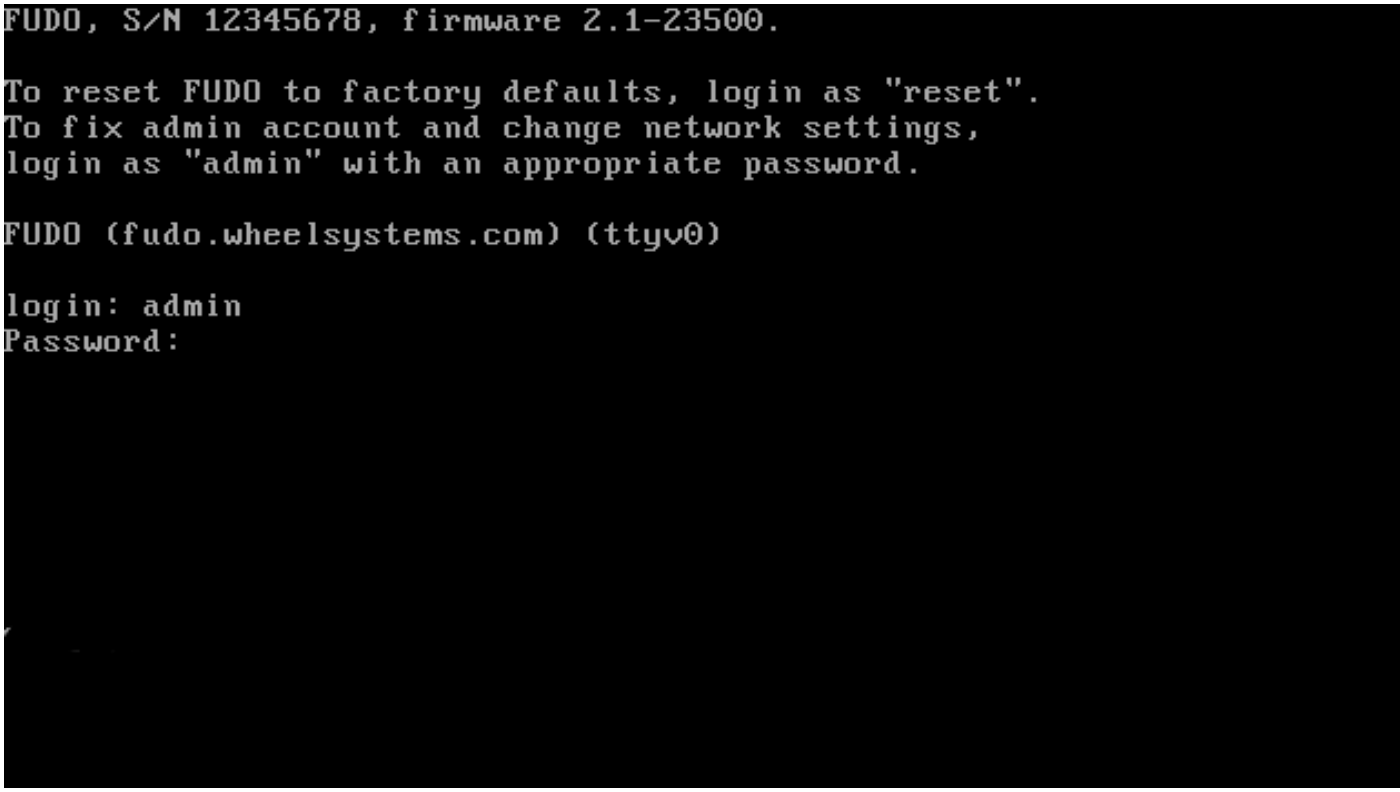
Informacja:

- W codziennej eksploatacji, jeden klucz szyfrujący potrzebny jest tylko do uruchomienia urządzenia, po czym może zostać odłączony.
- Zaleca się utworzenie dodatkowej kopii bezpieczeństwa klucza szyfrującego, zgodnie z procedurą opisaną w rozdziale *Sporządzanie kopii zapasowej kluczy szyfrujących*.

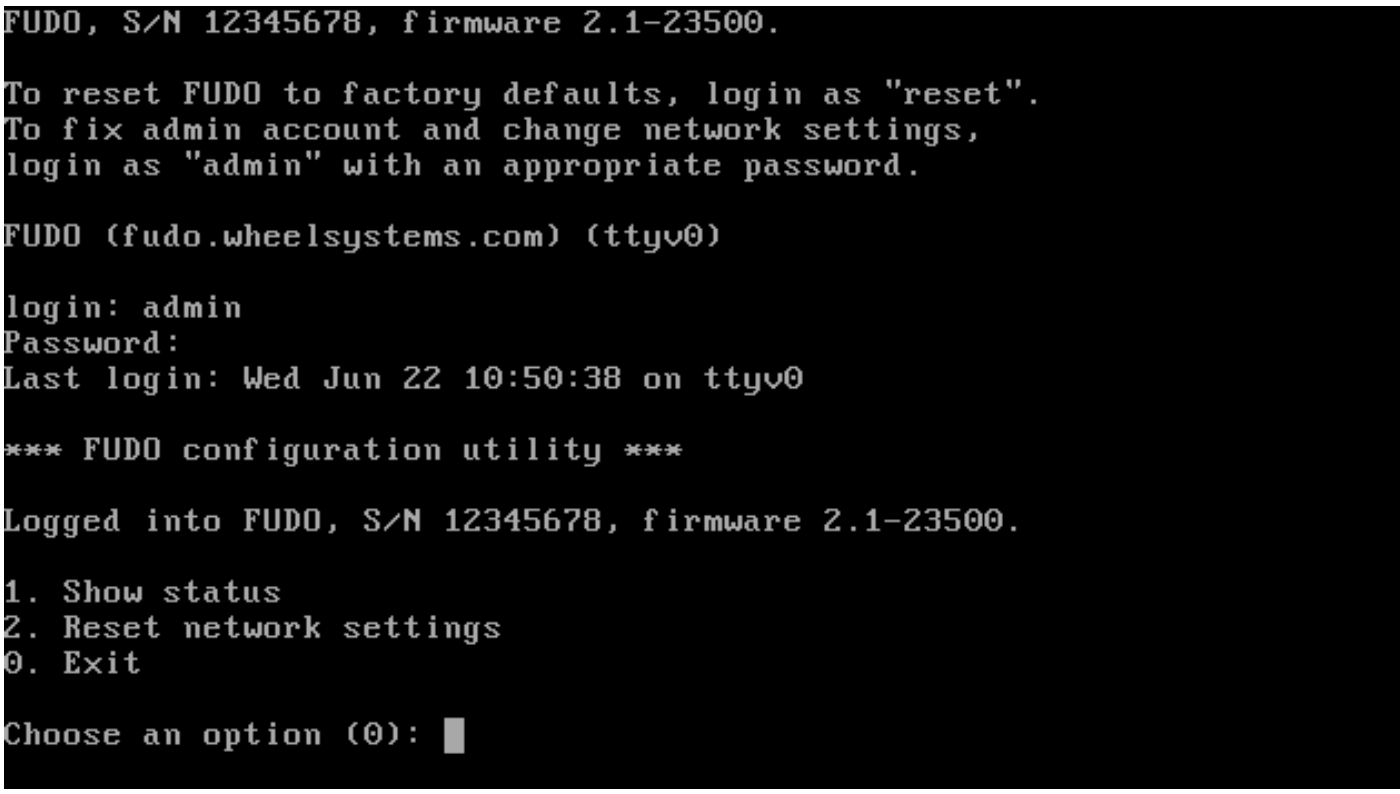
Ustawienie adresu IP z konsoli

1. Wprowadź login konta administratora.

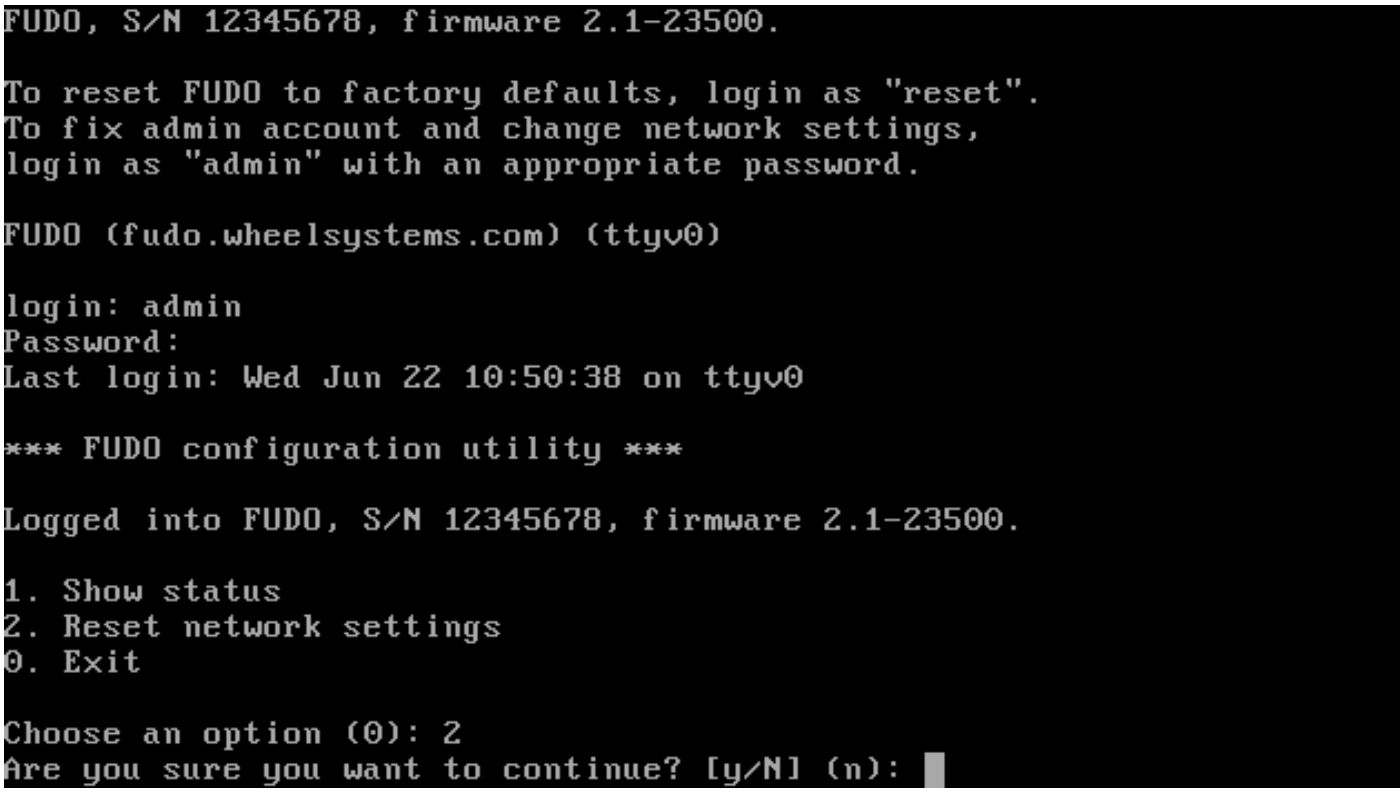
2. Wprowadź hasło do konta administratora.



3. Wpisz 2 i naciśnij klawisz *Enter*.



4. Wpisz y i naciśnij klawisz *Enter*, aby potwierdź chęć zmiany ustawień sieciowych.



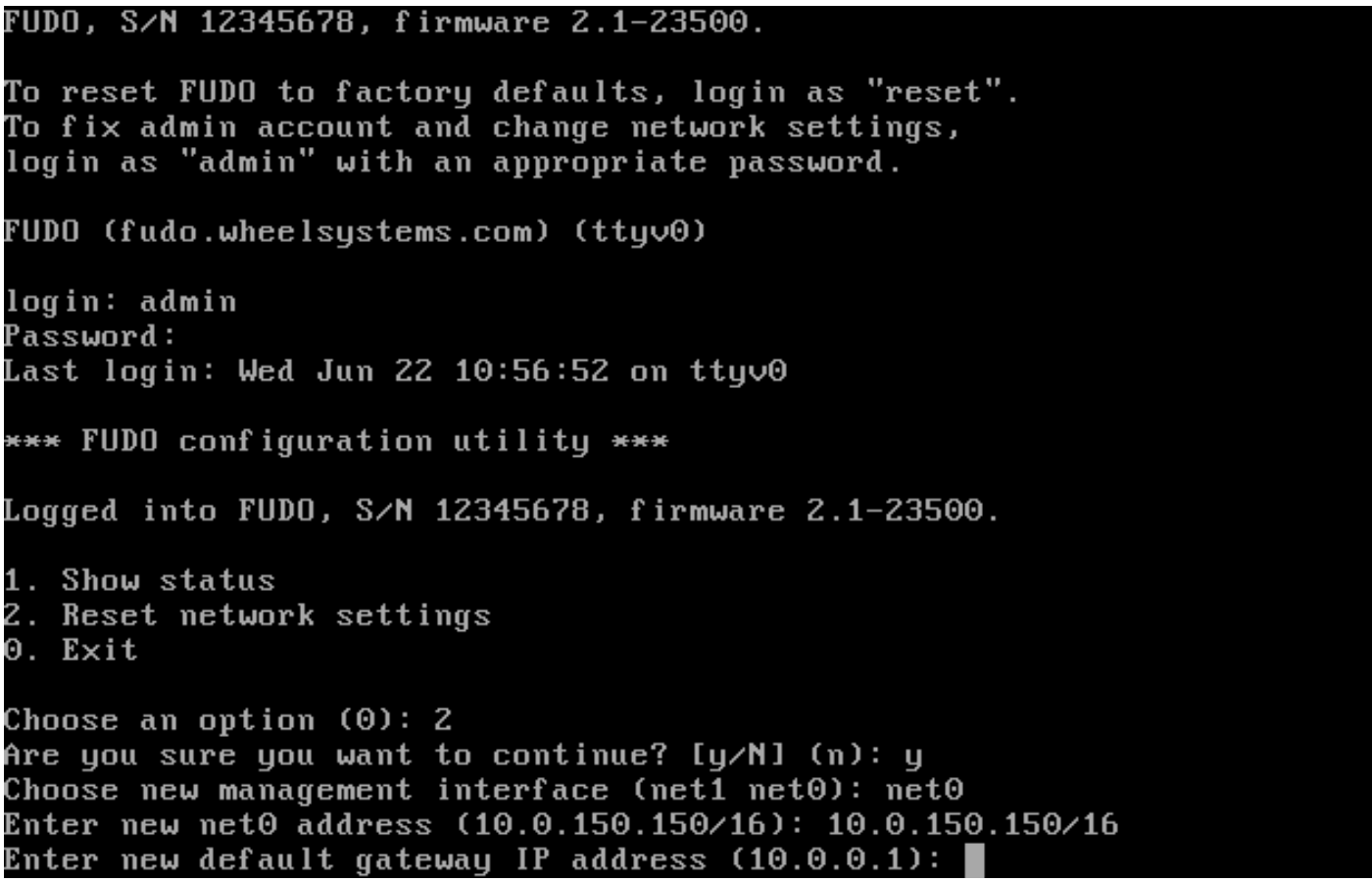
5. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Wheel Fudo PAM) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

6. Wprowadź adres IP urządzenia wraz z maską podsieci oddzieloną znakiem `/` (np. `10.0.0.8/24`) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

7. Wprowadź bramę sieci i naciśnij klawisz *Enter*.



Tematy pokrewne:

- *Wymagania*
- *Sporządzanie kopii zapasowej kluczy szyfrujących*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

ROZDZIAŁ 4

Szybki start

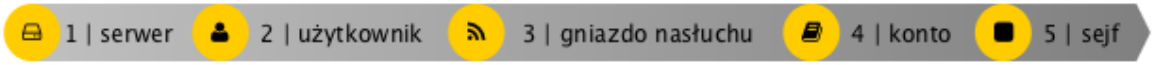
4.1 SSH

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się na Wheel Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Wheel Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

4.1.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.1.2 Konfiguracja



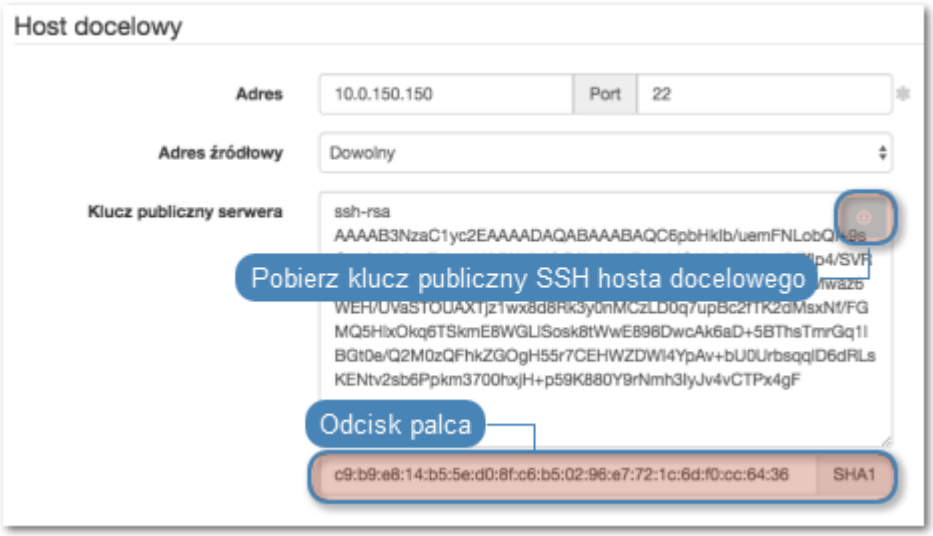
Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ssh_server
Zablokowane	✘
Protokół	`SSH`
Opis	✘
Uprawnienia	
Uprawnieni użytkownicy	✘
Host docelowy	
Adres	`10.0.150.150`
Port	22
Adres źródłowy	`Dowolny`

4. Pobierz lub wprowadź klucz publiczny SSH hosta docelowego.



5. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

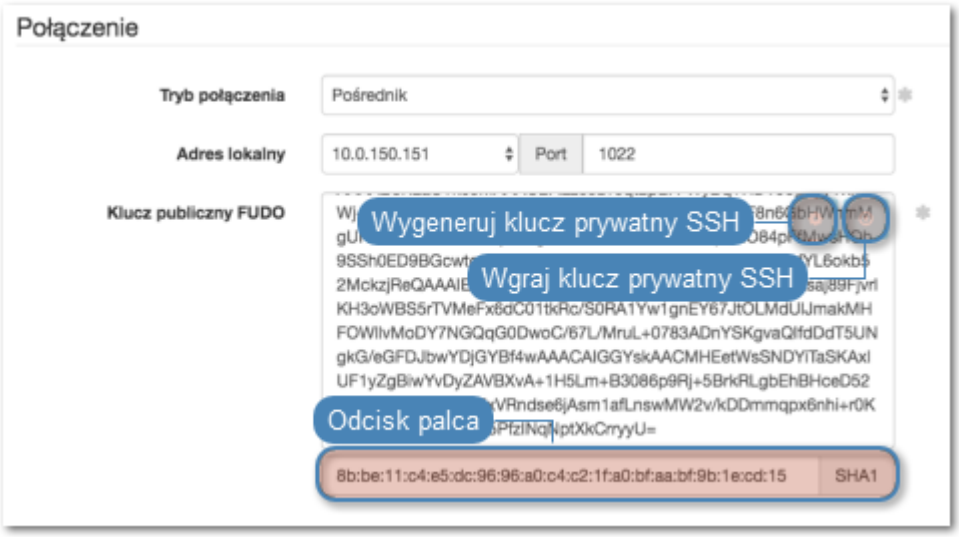
Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`ssh_listener`
Zablokowane	✗
Protokół	`SSH`
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`1022`

4. Kliknij ikonę wygenerowania klucza SSH lub wgraj klucz prywatny serwera.



Informacja: Ze względów bezpieczeństwa, formularz wyświetla klucz publiczny odpowiadający wgranemu lub wygenerowanemu kluczowi prywatnemu.

5. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_ssh_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ssh_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

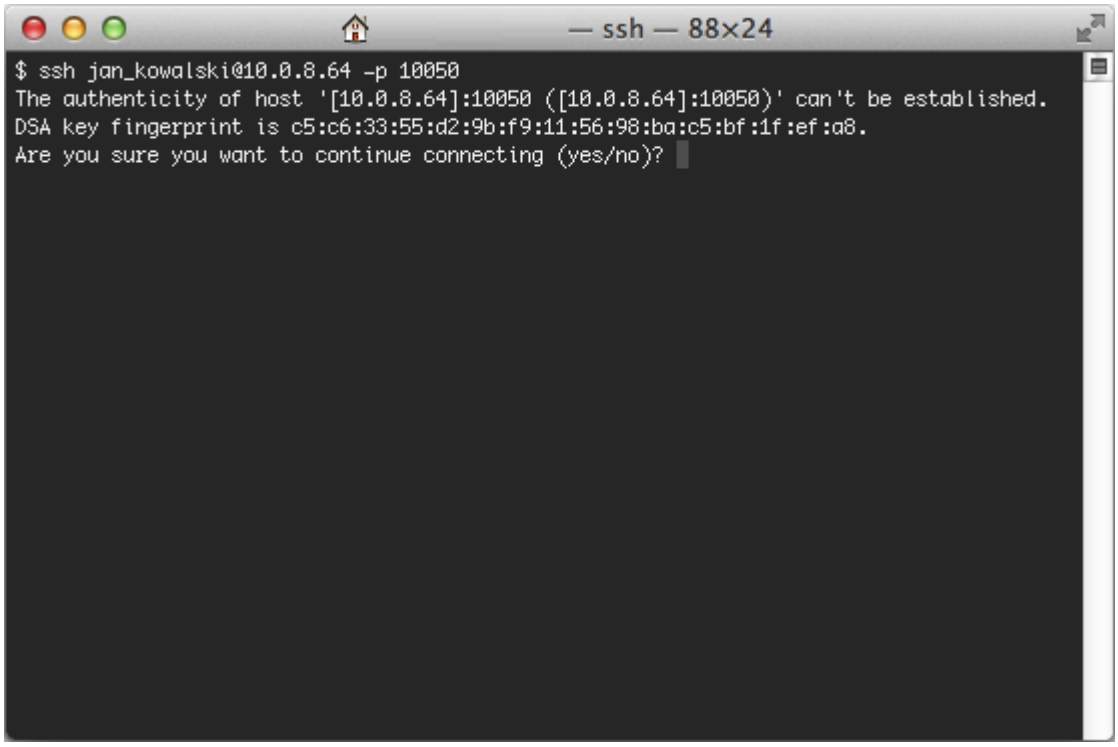
Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
`admin_ssh_server`	`ssh_listener`

4. Kliknij *Zapisz*.

4.1.3 Nawiązanie połączenia

W tym momencie użytkownik `jan_kowalski` może już podjąć próbę logowania.

Przykład:

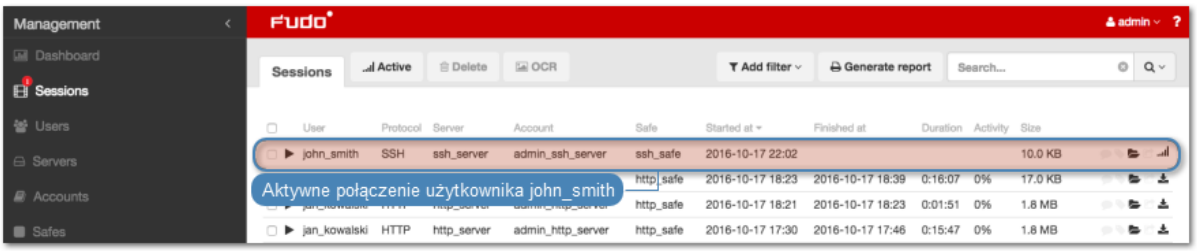


Informacja: Zwróć uwagę na *Odcisk Palca* (fingerprint), który wyświetla się przy pierwszym połączeniu. Jest to ten sam odcisk, który został wygenerowany w czasie dodawania serwera.

Po potwierdzeniu połączenia, użytkownik zostanie zapytany o hasło. Po uwierzytelnieniu sesja będzie podlegała monitorowaniu i rejestracji.

4.1.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.151`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *PuTTY*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*
- Konfiguracja

4.2 SSH w trybie bastionu

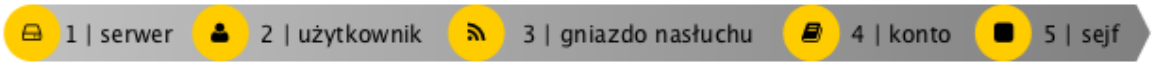
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się przed Wheel Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Nawiązując połączenie, użytkownik wskazuje konto `admin_ssh_server` i adres IP Wheel Fudo PAM. Połączenie realizowane jest za pośrednictwem portu numer 22, domyślnego dla protokołu SSH.

Wheel Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

4.2.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.2.2 Konfiguracja



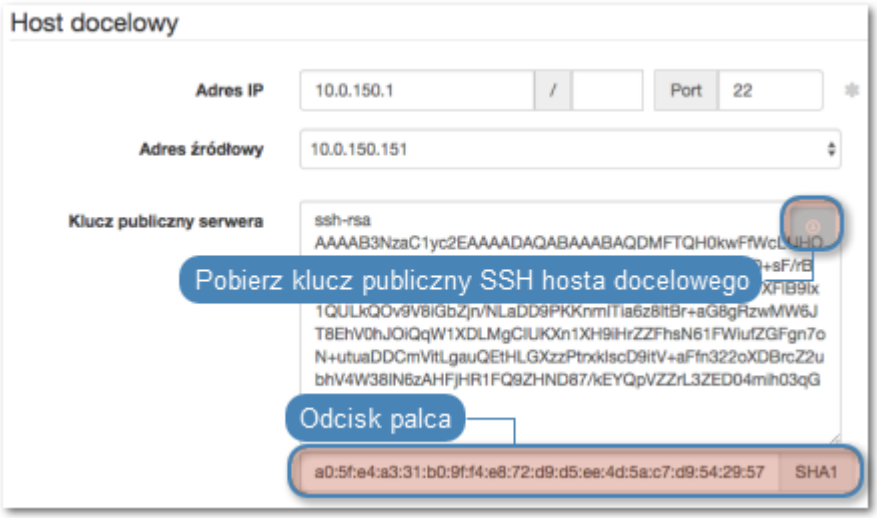
Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ssh_server
Zablokowane	✗
Protokół	`SSH`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.150.1`
Port	`22`
Adres źródłowy	`Dowolny`

4. Pobierz lub wprowadź klucz publiczny SSH hosta docelowego.



5. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✘
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✘
Organizacja	✘
Telefon	✘
Domena AD	✘
Baza LDAP	✘
Uprawnienia	
Uprawnieni użytkownicy	✘
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

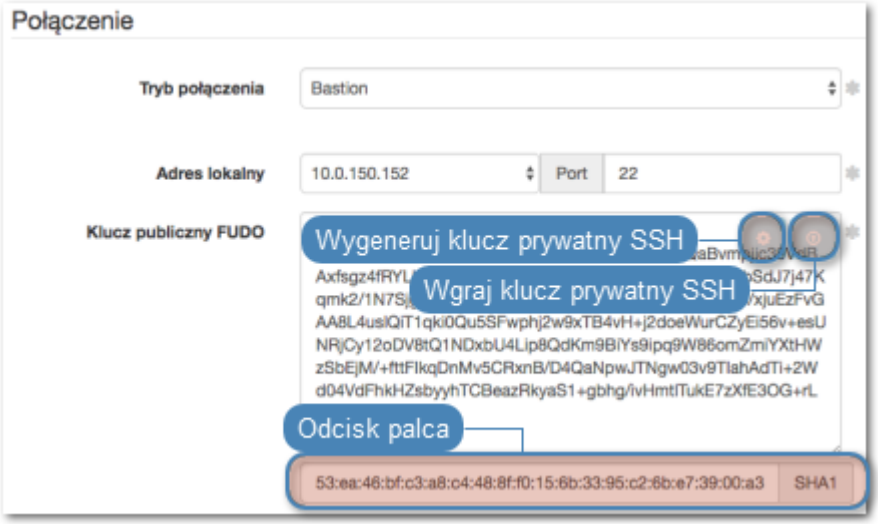
Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`ssh_listener`
Zablokowane	✘
Protokół	`SSH`
Uprawnienia	
Uprawnieni użytkownicy	✘
Tryb połączenia	`Bastion`
Adres lokalny	`10.0.150.151`
Port	22

4. Kliknij ikonę wygenerowania klucza SSH lub wgraj klucz prywatny serwera.



Informacja: Ze względów bezpieczeństwa, formularz wyświetla klucz publiczny odpowiadający wgranemu lub wygenerowanemu kluczowi prywatnemu.

5. Kliknij *Zapisz*.

Informacja: Upewnij się, że w ustawieniach sieciowych, na wskazanym adresie IP nie jest włączona opcja dostępu administracyjnego .

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_ssh_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ssh_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	`Statyczne, bez ograniczeń`
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

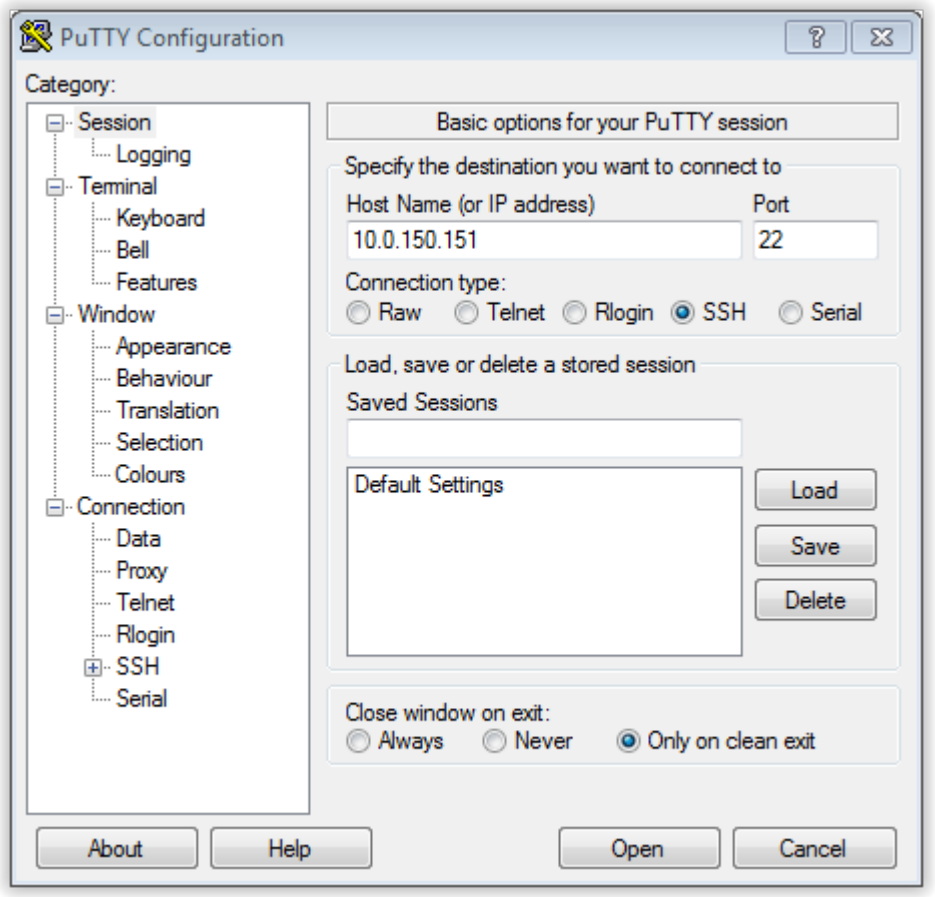
Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_ssh_server`	`ssh_listener`

4. Kliknij *Zapisz*.

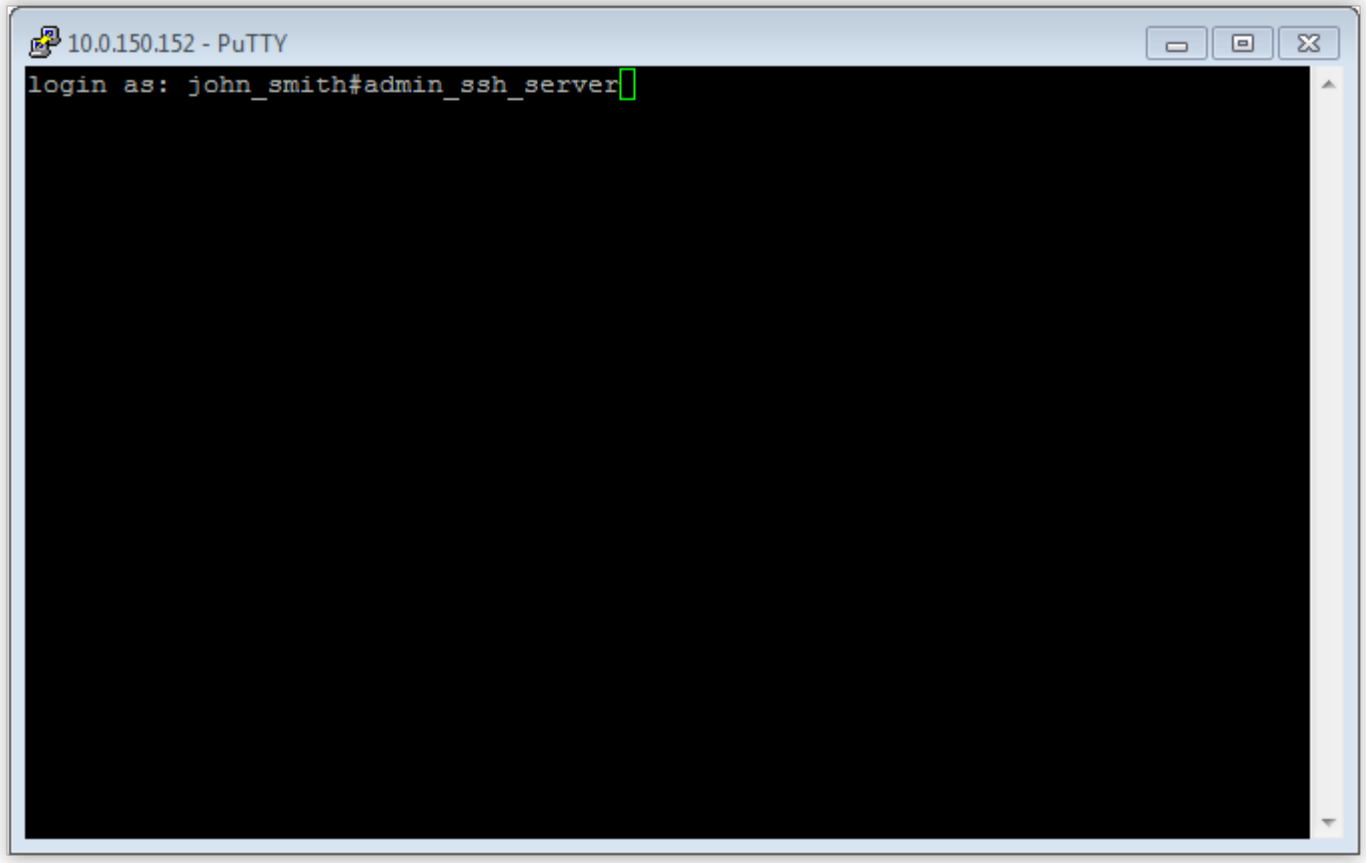
4.2.3 Nawiązanie połączenia

PuTTY - klient SSH dla systemu operacyjnego Microsoft Windows

1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres `10.0.150.151`.
3. Określ typ połączenia `SSH` i pozostaw domyślny numer portu.



4. Kliknij *Open*.
5. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



Informacja: Alternatywnie, zamiast nazwy konta, możesz wskazać nazwę obiektu serwera tj. `john_smith#ssh_server`.

6. Wprowadź hasło użytkownika.

4.2.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.150`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*

- Konfiguracja

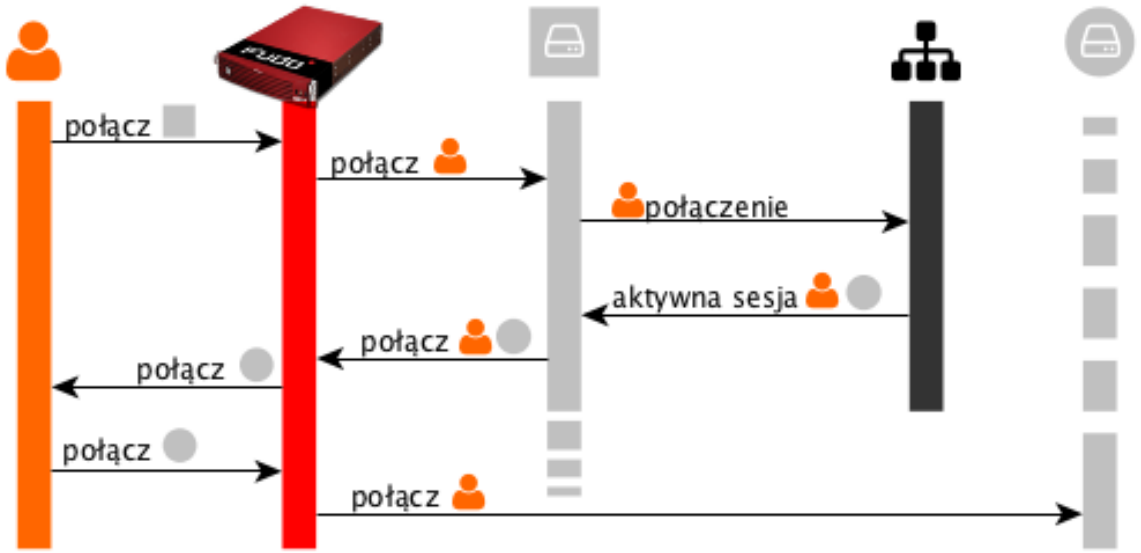
4.3 RDP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta *RDP* używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `admin`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

4.3.1 Broker połączeń RDP

Broker połączeń zdalnych umożliwia ponowne połączenie do istniejącej sesji w farmie serwerów z mechanizmem balansowania obciążeniem.

Jeśli broker stwierdzi aktywną sesję użytkownika na serwerze innym niż ten, z którym się połączył, połączenie zostanie przekierowane na serwer z istniejącą aktywną sesją a użytkownik zostanie poproszony o ponowne uwierzytelnienie.



Informacja: Aby proces przekierowania użytkownika się powiódł, wskazany przez broker

serwer, musi być zdefiniowany na Fudo i nasłuchiwać na domyślnym porcie RDP (3389) a użytkownik musi być uprawniony do łączenia się z tym zasobem.

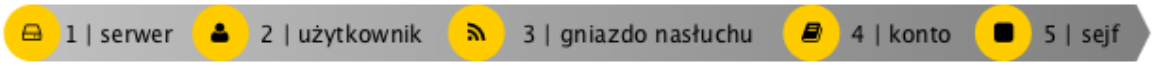
Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Konta*

4.3.2 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone a system został skonfigurowany do pracy w trybie mostu lub odpowiednio został skonfigurowany routing połączeń administracyjnych. Informacje na temat scenariuszy wdrożenia znajdziesz w rozdziale *Scenariusze wdrożenia*.

4.3.3 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	rdp_server
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Opis	`Serwer RDP`
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.35.10`
Port	`3389`
Adres źródłowy	`Dowolny`

4. Pobierz lub wprowadź certyfikat hosta docelowego.
5. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

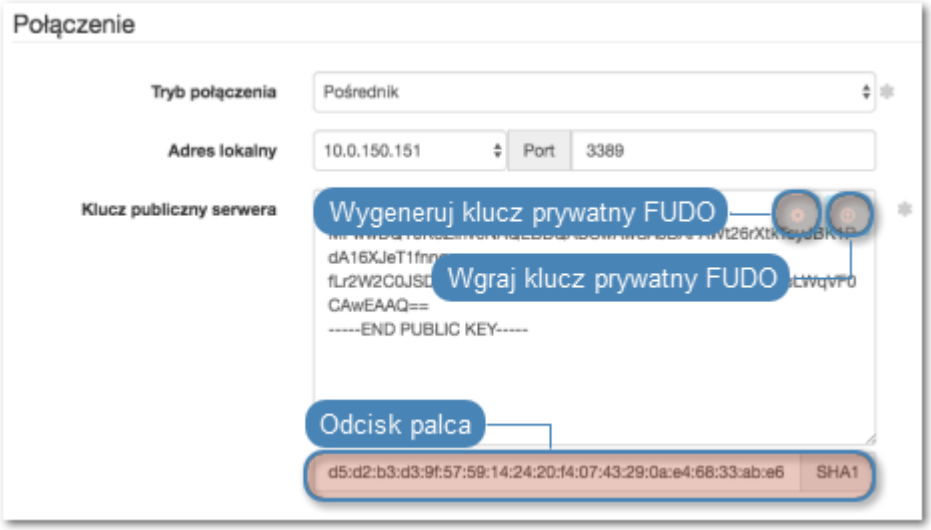
Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezro-

czysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`rdp_listener`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`3389`

4. Kliknij ikonę wygenerowania certyfikatu TLS lub wgraj klucz prywatny i publiczny w formacie PEM.



5. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_rdp_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`rdp_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

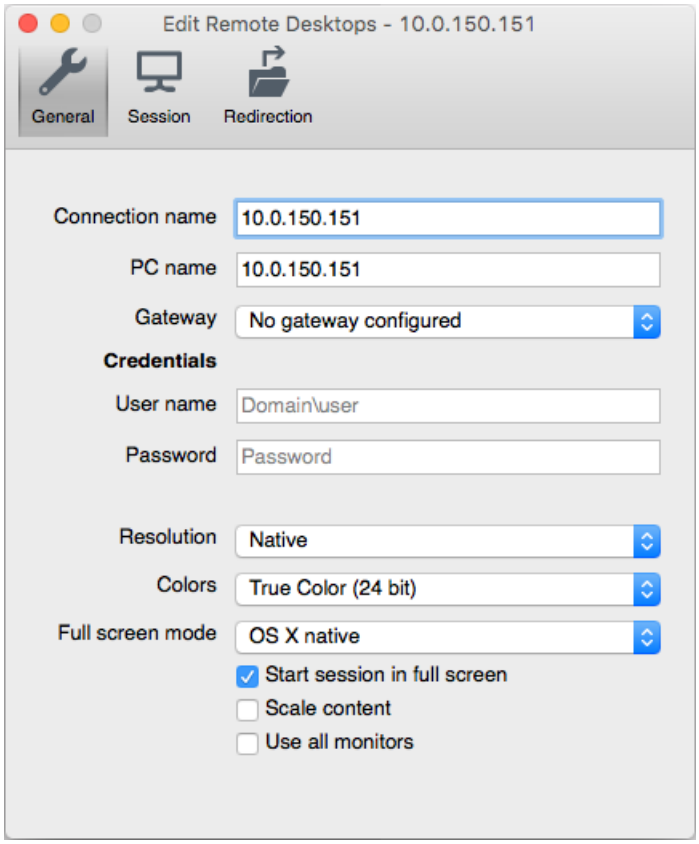
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`rdp_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_rdp_server`	`rdp_listener`

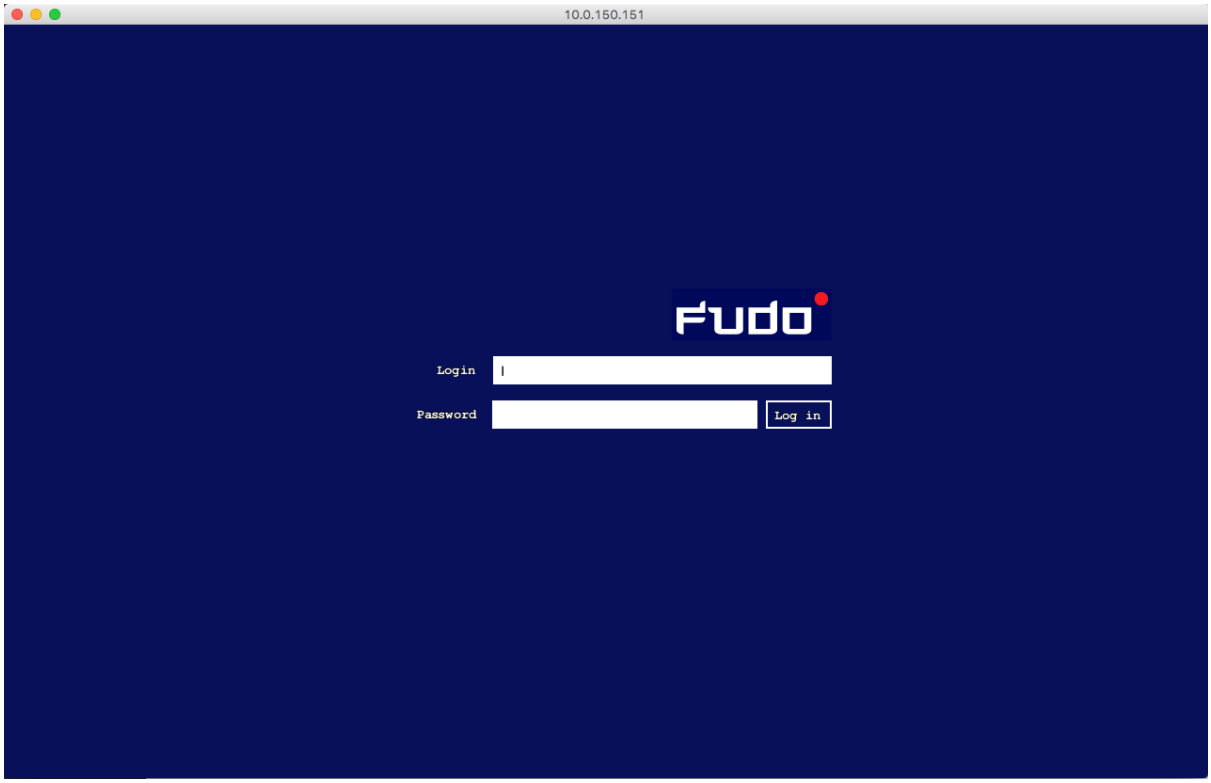
4. Kliknij *Zapisz*.

4.3.4 Nawiązanie połączenia

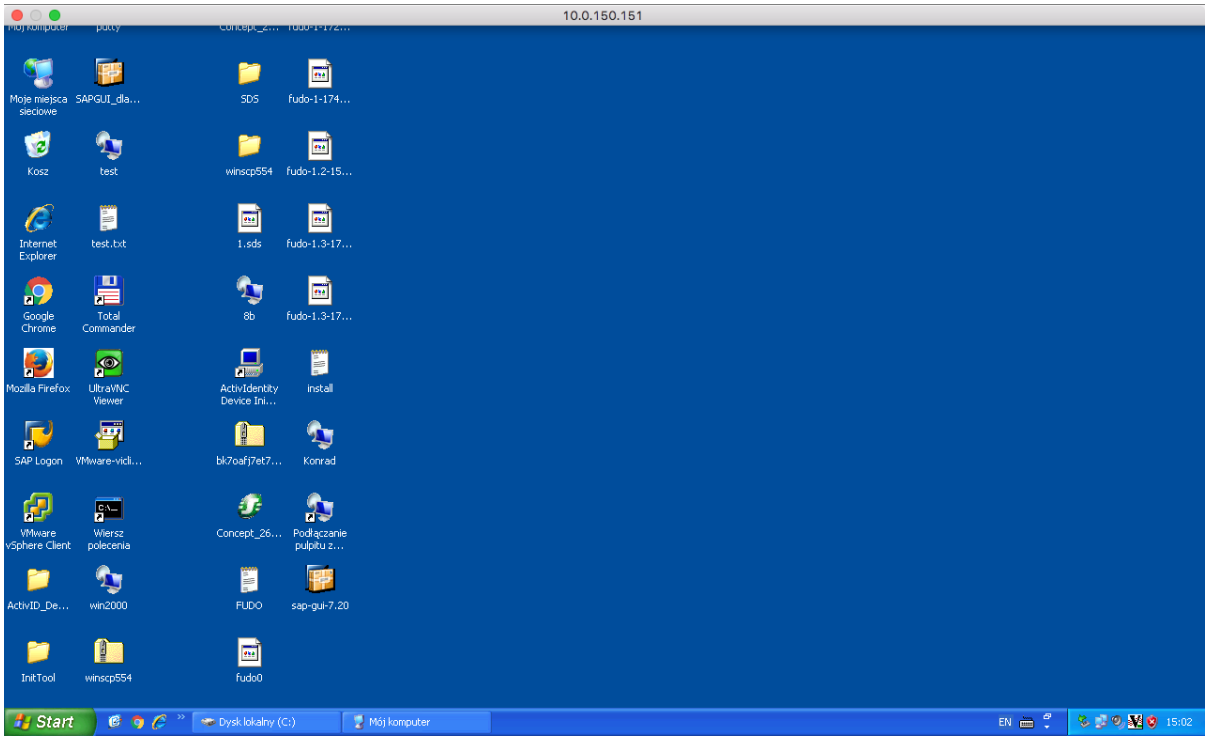
1. Uruchom klienta połączeń RDP.
2. Skonfiguruj połączenie zdalnego pulpitu.



3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: Wheel Fudo PAM pozwala na zastosowanie własnych ekranów logowania, braku dostępu i zakończenia sesji dla połączeń RDP i VNC. Więcej informacji na temat konfigurowania własnych ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.



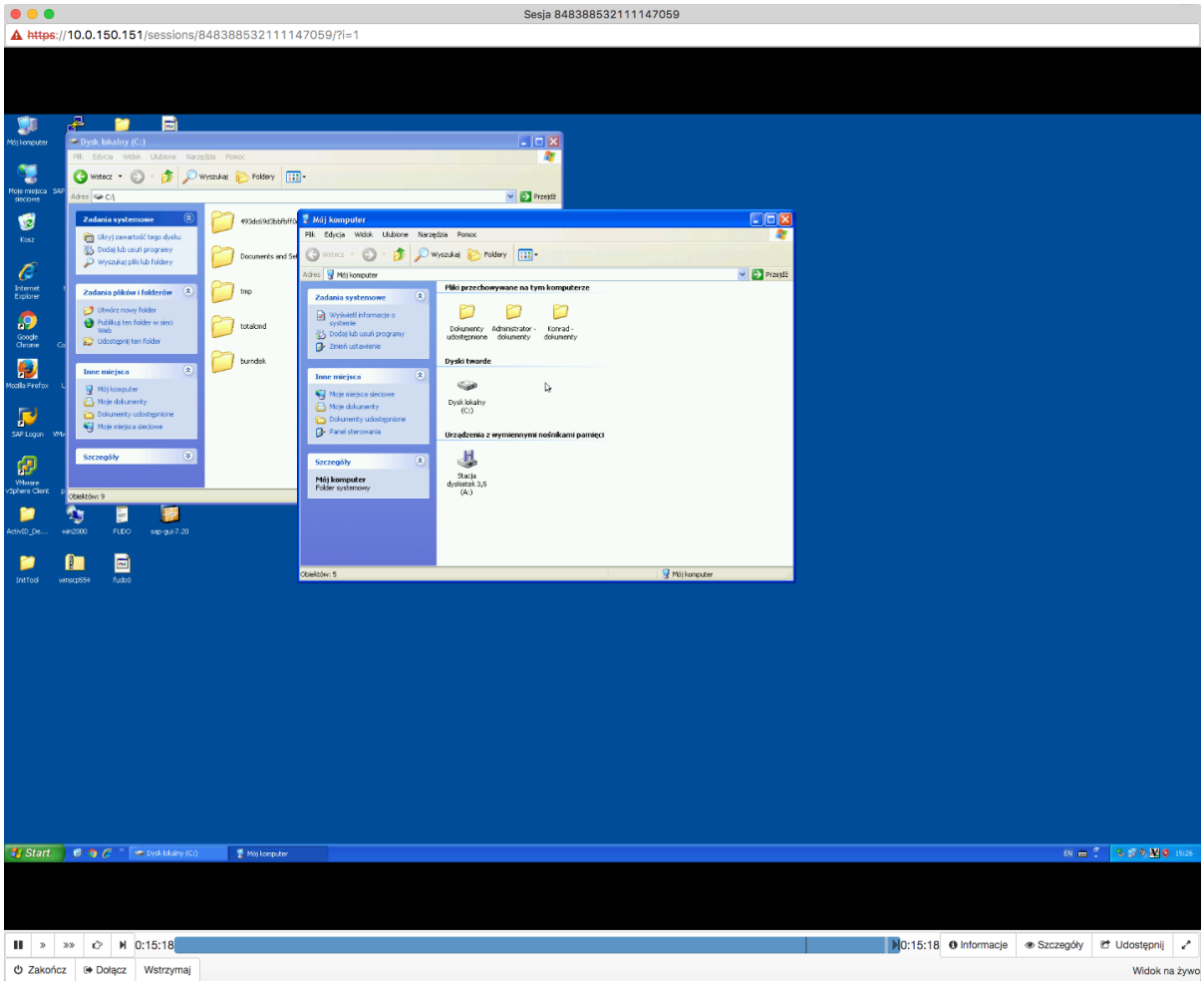
4.3.5 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Microsoft Remote Desktop*
- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Telnet*
- *Zasoby*
- *Model danych*
- Konfiguracja

4.4 Telnet

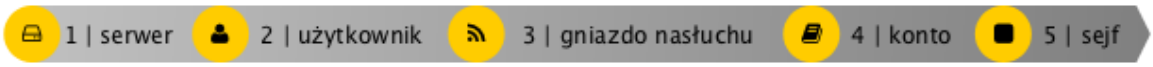
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń Telnet ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta protokołu Telnet używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

Informacja: Połączenia telnet realizowane za pośrednictwem Wheel Fudo PAM nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Wheel Fudo PAM musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.

4.4.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia opisana jest w rozdziale *Pierwsze uruchomienie*.

4.4.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	telnet_server
Zablokowane	✗
Protokół	`Telnet`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.35.137`
Port	`23`
Adres źródłowy	`Dowolny`
Użyj bezpiecznych połączeń TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`telnet_listener`
Zablokowane	✗
Protokół	`Telnet`
Włącz obsługę SSLv2	✗
Włącz obsługę SSLv3	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj bezpiecznych połączeń TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą

loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_telnet_server`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`telnet_server`
Dane uwierzytelniające	
Zastąp sekret	`hasłem`
Hasło	✗
Powtórz hasło	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`telnet_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_telnet_server`	`telnet_listener`

4. Kliknij *Zapisz*.

4.4.3 Nawiązanie połączenia

1. Uruchom klienta połączeń Telnet.
2. Nawiąż połączenie z serwerem:

```
telnet> open 10.0.150.151
Trying 10.0.150.151...
Connected to 10.0.150.151.
Escape character is '^]'.
```

3. Wprowadź dane uwierzytelniające użytkownika na Wheel Fudo PAM:

```
FUDO Authentication.
FUDO Login: john_smith
FUDO Password: john
```

4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

```
FreeBSD/amd64 (fbsd83-cerb.whl) (pts/0)
login:
password:
```

Informacja: Połączenia telnet nie wspierają mechanizmów podmiany danych logowania.

4.4.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia RDP*
- *Zasoby*
- *Model danych*
- Konfiguracja

4.5 Telnet 5250

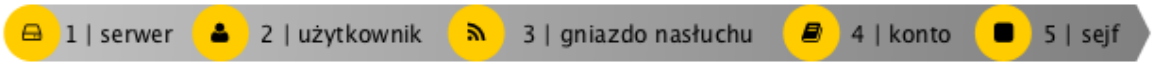
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń Telnet 5250 ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta protokołu Telnet używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

Informacja: Połączenia telnet realizowane za pośrednictwem Wheel Fudo PAM nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Wheel Fudo PAM musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.

4.5.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia opisana jest w rozdziale *Pierwsze uruchomienie*.

4.5.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	telnet_server
Zablokowane	✗
Protokół	`Telnet 5250`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.35.137`
Port	`23`
Adres źródłowy	`Dowolny`
Użyj bezpiecznych połączeń TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.

2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie > Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`telnet_listener`
Zablokowane	✗
Protokół	`Telnet 5250`
Włącz obsługę SSLv2	✗
Włącz obsługę SSLv3	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj bezpiecznych połączeń TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_telnet_server`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`telnet_server`
Dane uwierzytelniające	
Zastąp sekret	`hasłem`
Hasło	✗
Powtórz hasło	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`telnet_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_telnet_server`	`telnet_listener`

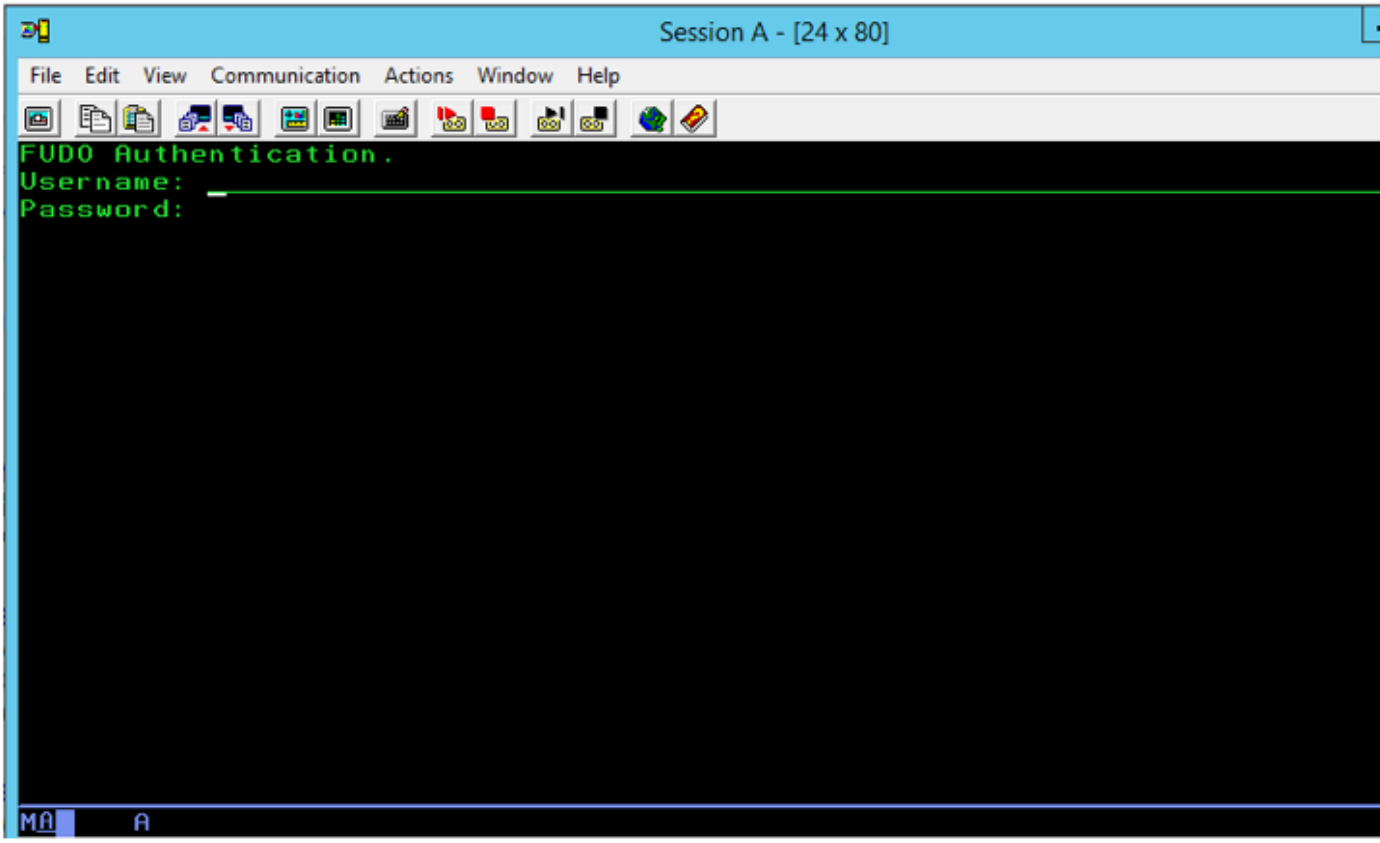
4. Kliknij *Zapisz*.

4.5.3 Nawiązanie połączenia

1. Uruchom klienta połączeń Telnet.
2. Nawiąż połączenie z serwerem:

```
telnet> open 10.0.150.151
Trying 10.0.150.151...
Connected to 10.0.150.151.
Escape character is '^]'.
```

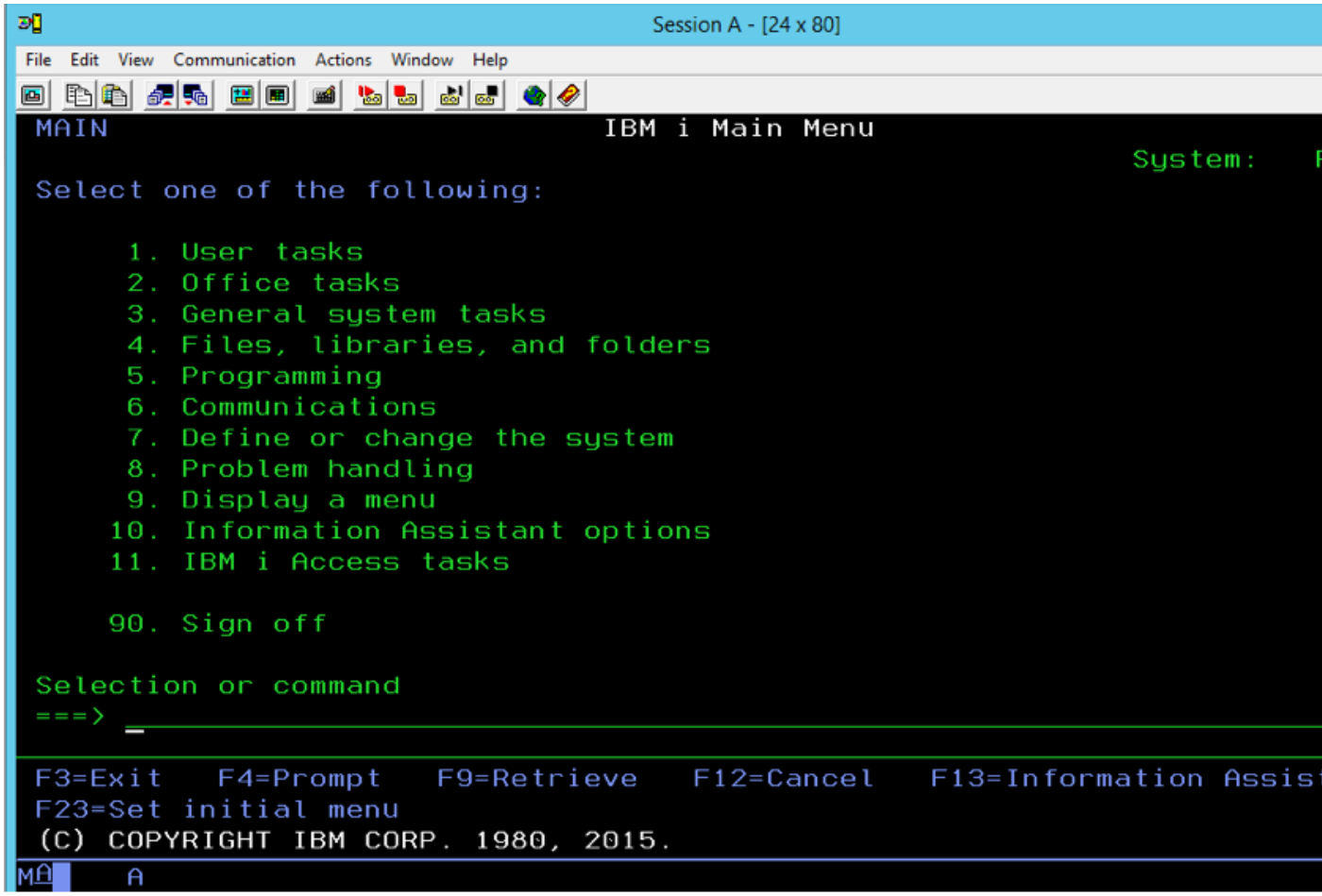
3. Wprowadź dane uwierzytelniające użytkownika na Wheel Fudo PAM.



4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

```
FreeBSD/amd64 (fbsd83-cerb.whl) (pts/0)
login:
password:
```

Informacja: Połączenia telnet nie wspierają mechanizmów podmiany danych logowania.



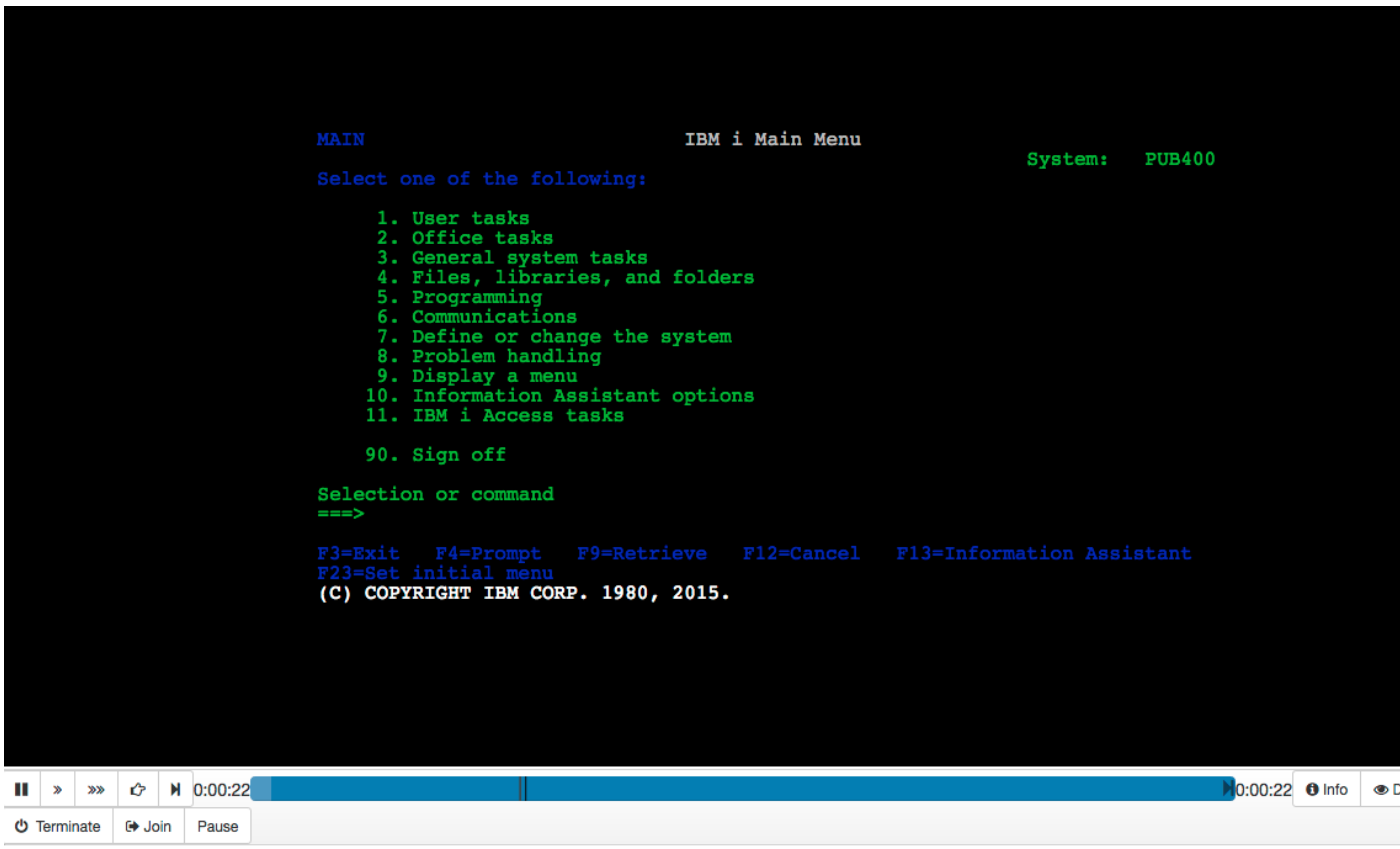
4.5.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia RDP*
- *Zasoby*
- *Model danych*
- Konfiguracja

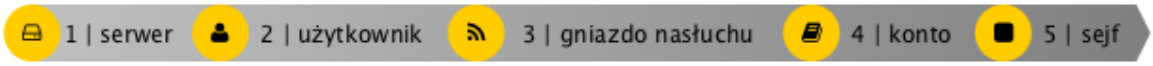
4.6 MySQL

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń ze zdalnym serwerem baz danych MySQL. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta MySQL używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `admin`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

4.6.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.6.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	mysql_server
Zablokowane	✗
Protokół	`MySQL`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.1.35`
Port	`3306`
Adres źródłowy	`Dowolny`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.

2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`mysql_listener`
Zablokowane	✗
Protokół	`MySQL`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.40.50`
Port	`3306`

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą

loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_mysql_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`mysql_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

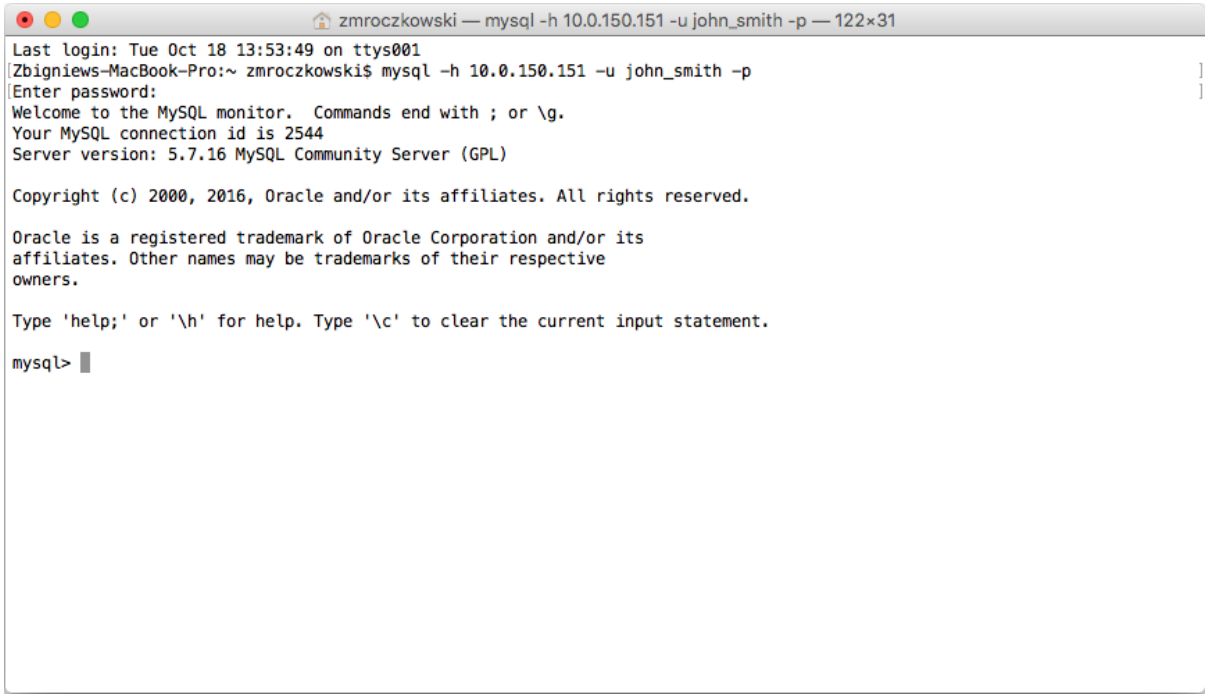
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`msyql_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_mysql_server`	`mysql_listener`

4. Kliknij *Zapisz*.

4.6.3 Nawiązanie połączenia

1. Uruchom terminal tekstowy.
2. Wprowadź komendę `mysql -h 10.0.150.151 -u john_smith -p`, aby nawiązać połączenie z serwerem baz danych.
3. Wprowadź hasło użytkownika.



4. Kontynuuj przeglądanie zawartości serwera poprzez zapytania sql.

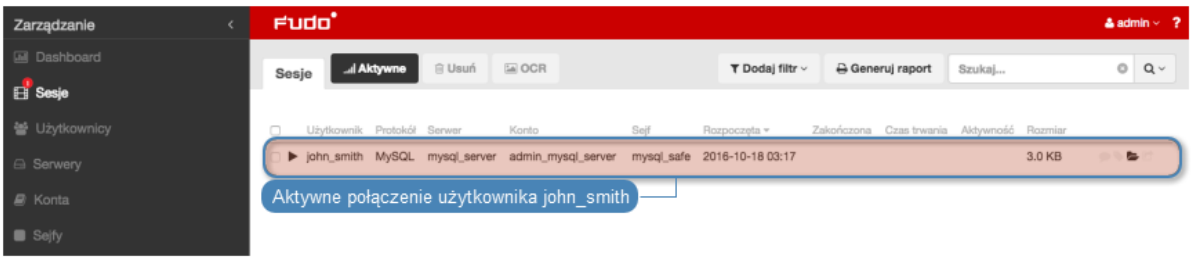
4.6.4 Podgląd sesji połączeniowej

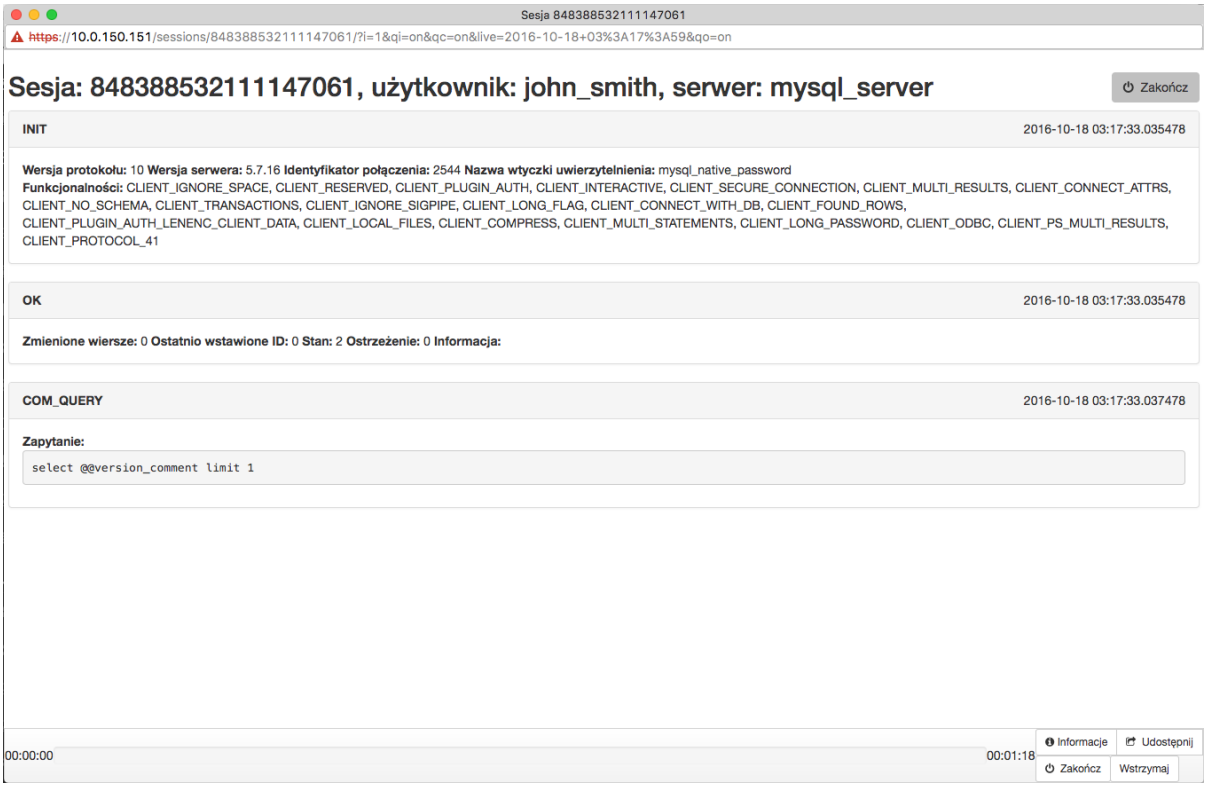
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.





Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*

- *Szybki start - konfigurowanie połączenia Telnet*
- *Telnet*
- *Wymagania*
- *Model danych*
- Konfiguracja

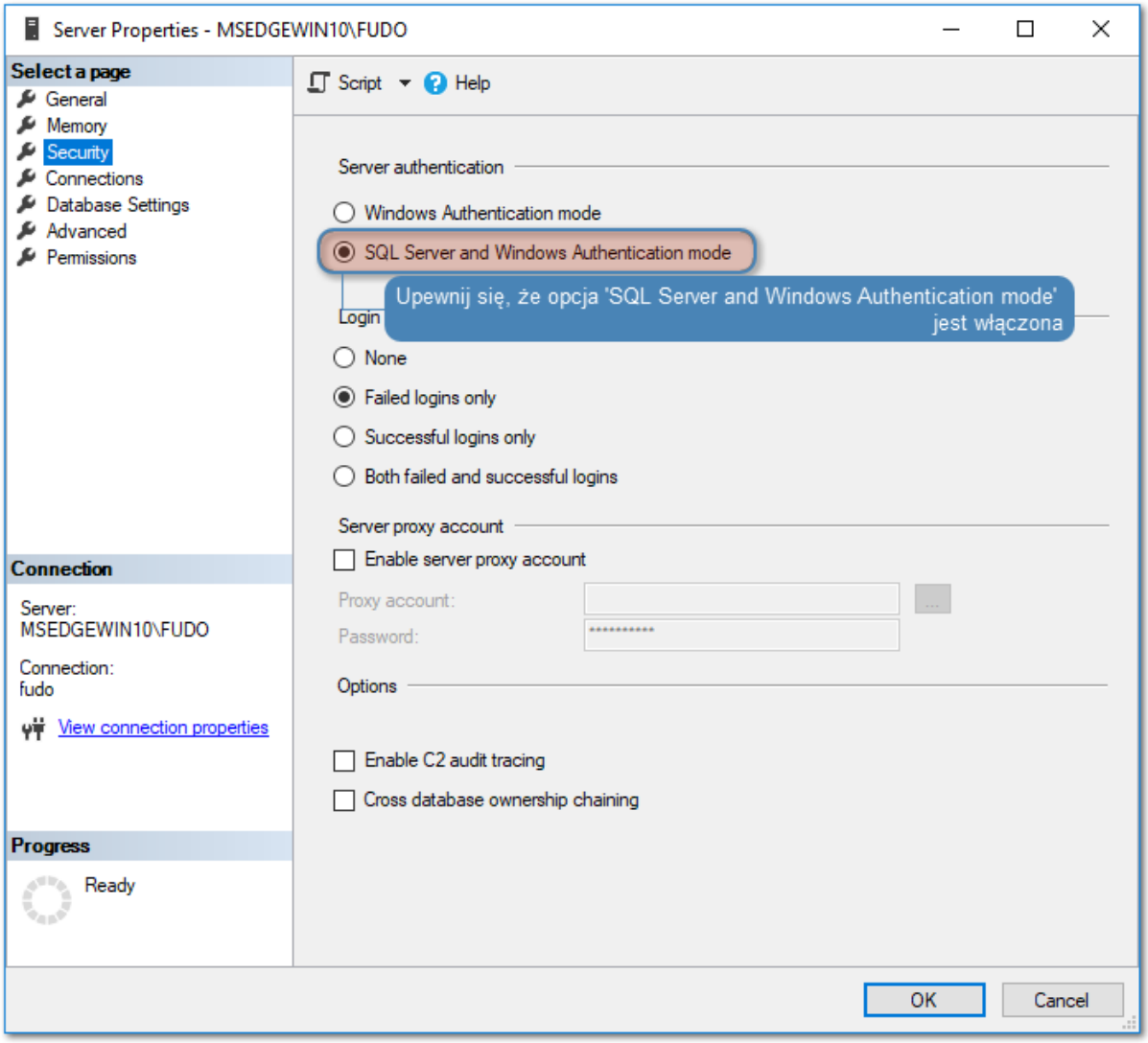
4.7 MS SQL

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń ze zdalnym serwerem baz danych MS SQL. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta *SQL Server Management Studio*, używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `fudo`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

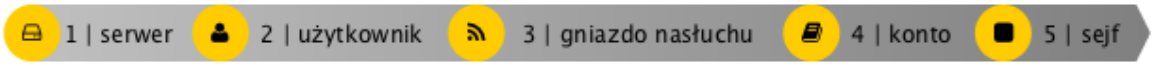
4.7.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

Informacja: Upewnij się, że serwer SQL ma włączony tryb uwierzytelnienia *SQL Server and Windows Authentication*.



4.7.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	mssql_server
Zablokowane	✗
Protokół	`MS SQL (TDS)`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.150.154`
Port	`1433`
Adres źródłowy	`Dowolny`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.

2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`MSSQL_proxy`
Zablokowane	✗
Protokół	`MS SQL (TDS)`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.150`
Port	`1433`

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie > Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_mssql_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`mssql_server`
Dane uwierzytelniające	
Domena	✗
Login	`fudo`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfikator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

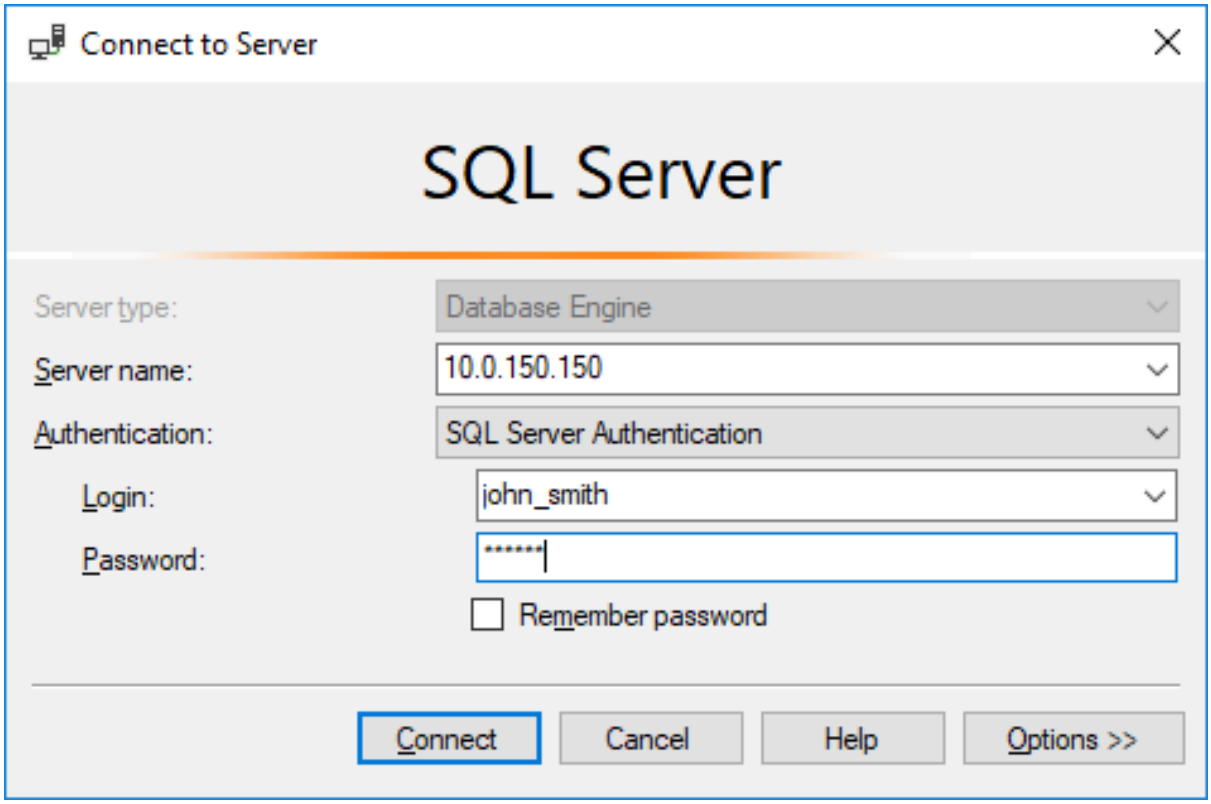
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

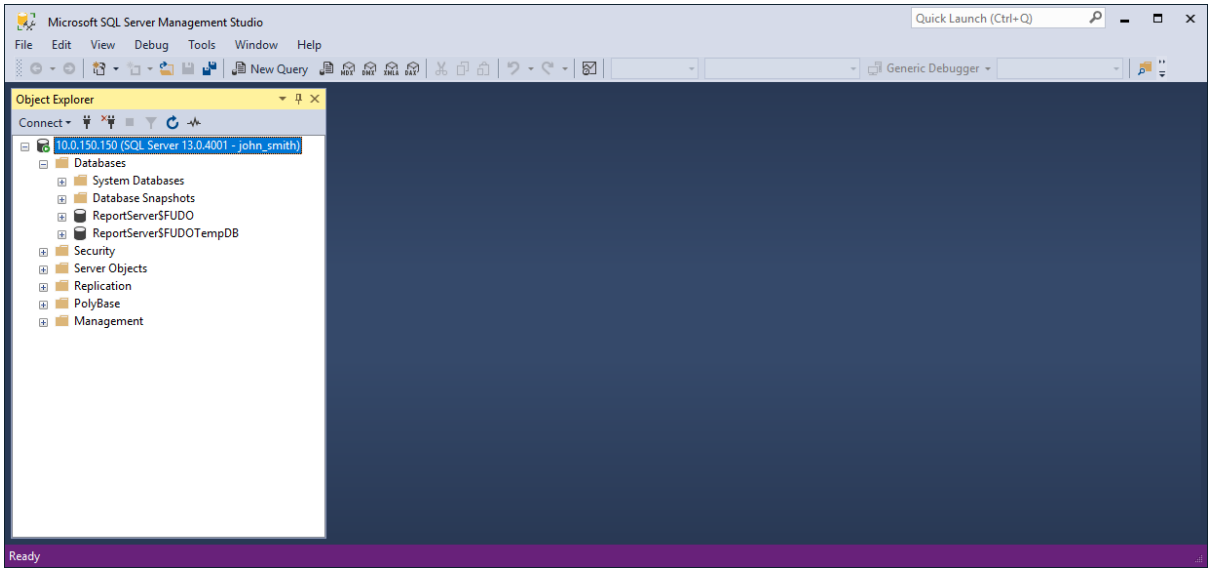
Parametr	Wartość
Ogólne	
Nazwa	`mssql_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_mssql_server`	`MSSQL_proxy`

4. Kliknij *Zapisz*.

4.7.3 Nawiązanie połączenia

1. Uruchom *SQL Server Management Studio*.
2. Wprowadź wcześniej skonfigurowany adres proxy, na którym Fudo oczekuje na połączenia z serwerem MS SQL (10.0.150.150).
3. Z listy rozwijalnej *Authentication*, wybierz *SQL Server Authentication*.
4. Wprowadź nazwę użytkownika oraz hasło.
5. Kliknij *Connect*.





4.7.4 Podgląd sesji połączeniowej

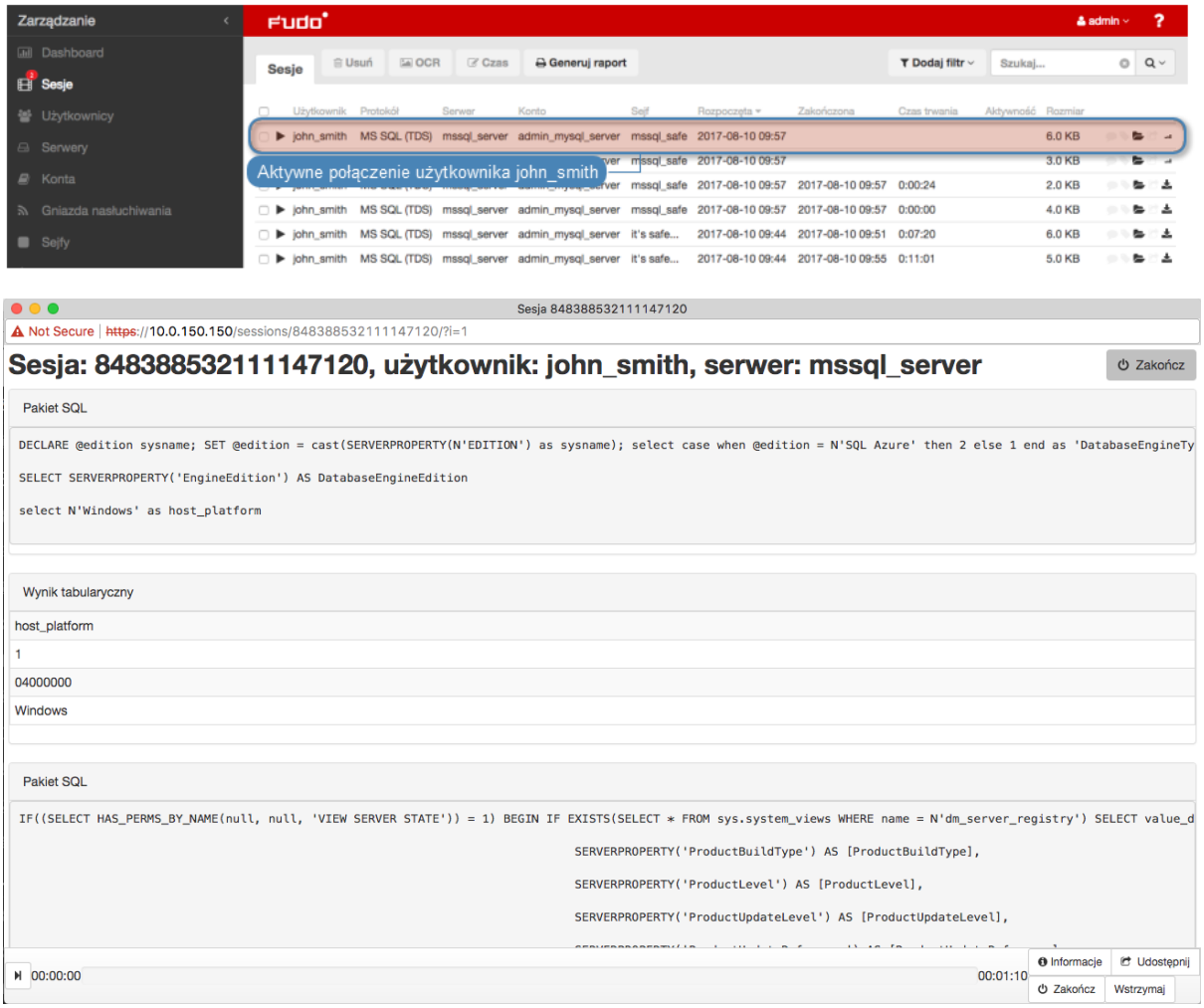
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.

3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ▶.



Tematy pokrewne:

- *SQL Server Management Studio*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia SSH*
- *Telnet*
- *Wymagania*
- *Model danych*
- Konfiguracja

4.8 HTTP

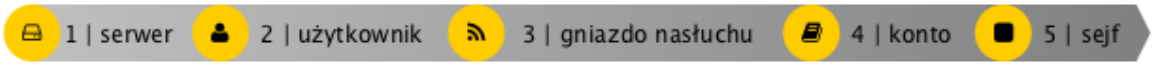
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń HTTP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik przegląda zasoby monitorowanego serwera korzystając z przeglądarki internetowej. Użytkownik uwierzytelniany jest przez Wheel Fudo PAM na podstawie danych zapisanych w

lokalnej bazie użytkowników. Sesja połączeniowa będzie wymagała ponownego uwierzytelnienia po 15 minutach (900 sekund) braku aktywności.

4.8.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.8.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	http_server
Zablokowane	✗
Protokół	`HTTP`
Czas oczekiwania HTTP	900
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`www.wheelsystems.com`
Port	80
Host HTTP	✗
Użyj TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie > Użytkownicy.*
2. Kliknij *+ Dodaj.*
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij Zapisz.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie > Gniazda nasłuchiwania.*
2. Kliknij *+ Dodaj.*
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`http_listener`
Zablokowane	✗
Protokół	`HTTP`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`8080`
Użyj bezpiecznych połączeń (TLS)	✗

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_http_server`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`http_server`
Dane uwierzytelniające	
Zastąp sekret	`hasłem`
Hasło	✗
Powtórz hasło	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i

szczegóły relacji użytkownik-serwer.

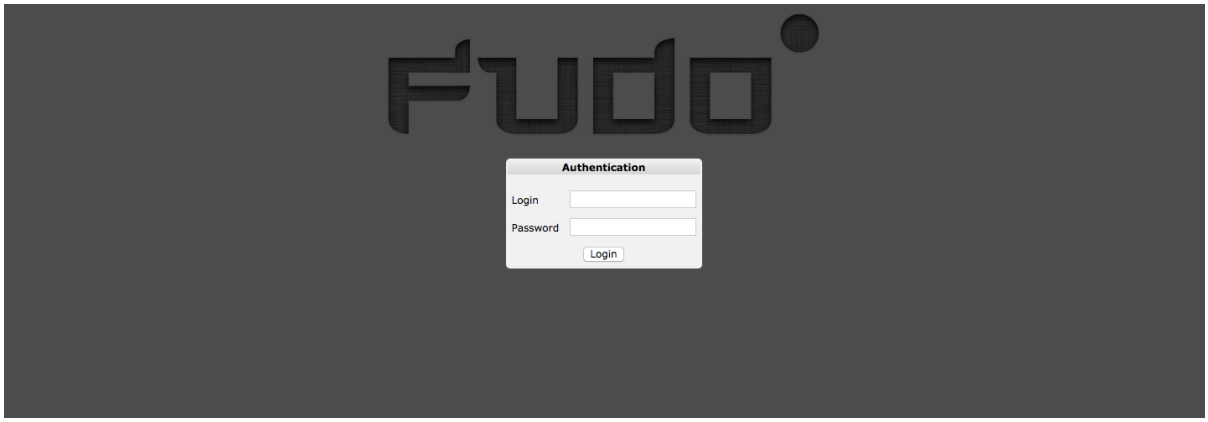
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`http_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_http_server`	`http_listener`

4. Kliknij *Zapisz*.

4.8.3 Nawiązanie połączenia

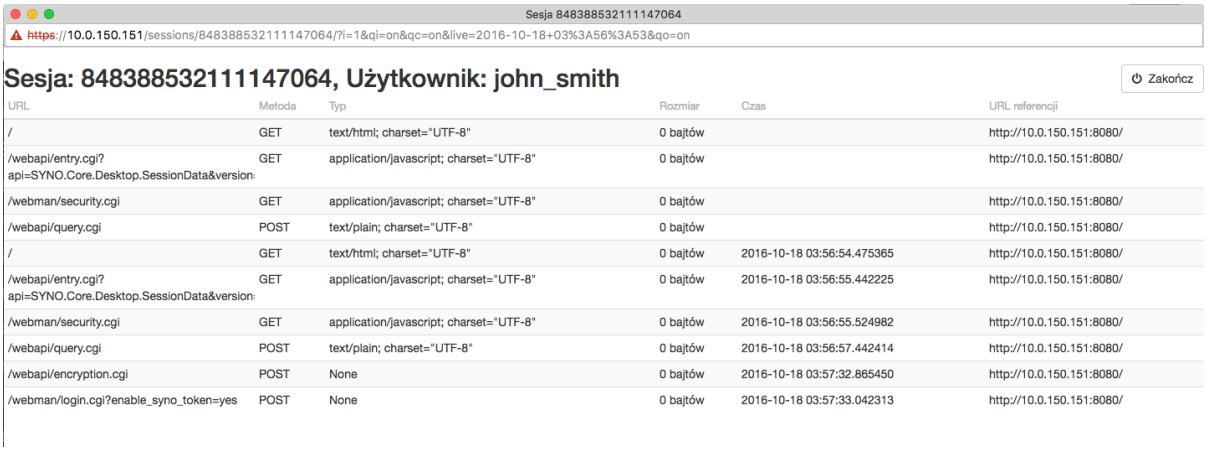
1. Uruchom przeglądarkę internetową.
2. W pasku adresu wprowadź 10.0.150.151:8080.
3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter] lub klikając przycisk *Login*.



4. Kontynuuj przeglądanie serwisu.

4.8.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Wymagania*
- *Model danych*
- Konfiguracja

4.9 Citrix

Połączenia administracyjne realizowane z wykorzystniem protokołu ICA mogą być nawiązywane bezpośrednio za pomocą aplikacji klienckiej lub za pośrednictwem intefejsu Citrix StoreFront.

4.9.1 ICA

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń ICA ze zdalnym serwerem, z wykorzystaniem aplikacji klienckiej protokołu ICA. Klient nawiązuje połączenie używając indywidualnej nazwy użytkownika i hasła (john_smith/john), które zostają zamienione na parametry konta uprzywilejowanego (citrixuser/password) w momencie zestawiania połączenia z serwerem docelowym.

4.9.1.1 Plik konfiguracyjny połączenia ICA

Plik konfiguracyjny `.ica` definiuje parametry konfiguracyjne umożliwiające nawiązanie połączenia z monitorowanym serwerem za pomocą klienta protokołu ICA.

4.9.1.1.1 Plik ICA do połączeń bez TLS

```
[ApplicationServers]
<nazwa połączenia>=

[<nazwa połączenia>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Informacja: `<nazwa połączenia>` służy do celów informacyjnych i może być dowolnym ciągiem znaków.

4.9.1.1.2 Plik ICA do połączeń TLS

```
[ApplicationServers]
<nazwa połączenia>=

[<nazwa połączenia>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Informacja: `<nazwa połączenia>` służy do celów informacyjnych i może być dowolnym ciągiem znaków.

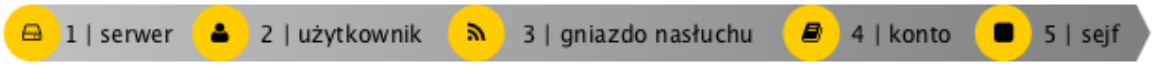
Tematy pokrewne:

- *ICA*
- *ICA*
- *Model danych*

4.9.1.2 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.9.1.3 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ica_server
Zablokowane	✗
Protokół	`ICA`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.0.21`
Port	`1494`
Użyj TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij Zapisz.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.

2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`http_listener`
Zablokowane	✗
Protokół	`ICA`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`2494`
Użyj bezpiecznych połączeń (TLS)	✗

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

Informacja: Połączenia bezpośrednie z serwerami ICA wspierają wszystkie typy kont.

---

1. Wybierz z lewego menu *Zarządzanie > Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_ica_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ica_server`
Dane uwierzytelniające	
Domena	✗
Login	`citrixuser`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora hasła	Statyczne, bez ograniczeń
Modyfikator hasła	
Modyfikator hasła	`Brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`ica_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
`admin_ica_server`	`ica_listener`

4. Kliknij *Zapisz*.

Informacja: W przypadku połączeń szyfrowanych protokołem TLS, Fudo zwraca klientowi Citrix *plik konfiguracyjny .ica*, w którym adresem serwera (*Address*) jest nazwa zwyczajowa (*Common Name*) z certyfikatu TLS.

4.9.1.4 Zdefiniowanie połączenia w pliku .ica

Bezpośrednie połączenie ze zdalnym serwerem za pośrednictwem protokołu ICA wymaga utworzenia pliku konfiguracyjnego, zawierającego parametry połączenia. Plik konfiguracyjny powinien wskazywać gniazdo nasłuchiwania za pomocą którego nawiązane zostanie połączenie z monitorowanym serwerem.

Informacja: Szczegółowe informacje na temat pliku konfiguracyjnego znajdziesz w rozdziale *Plik konfiguracyjny połączenia ICA*.

---

1. Utwórz plik tekstowy o następującej treści:

```
[ApplicationServers]
ica_connection_example=

[ica_connection_example]
ProxyType=SOCKSV5
ProxyHost=10.0.150.151:2494
ProxyUsername=*
ProxyPassword=*
Address=john_smith
Username=john_smith
ClearPassword=john
TransportDriver=TCP/IP
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
EncryptionLevelSession=Basic
Compress=Off
```

2. Zapisz plik z dowolną nazwą, nadając mu rozszerzenie `.ica`.

4.9.1.5 Nawiązanie połączenia

1. Kliknij dwukrotnie plik z parametrami połączenia, aby uruchomić klienta protokołu ICA.
2. Kontynuuj korzystanie z usługi.

4.9.1.6 Podgląd sesji połączeniowej

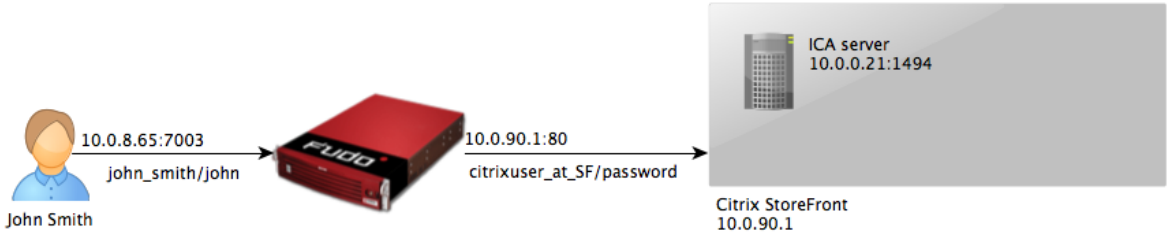
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Model danych*
- *Dodawanie serwera ICA*
- *Dodawanie gniazda nasłuchiwania ICA*
- *ICA*

4.9.2 Citrix StoreFront

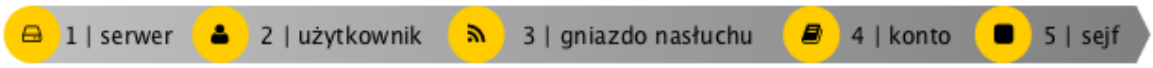
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń ICA ze zdalnym serwerem, w przypadku której inicjowanie połączenia następuje za pośrednictwem Citrix StoreFront.



4.9.2.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.9.2.2 Konfiguracja



Dodanie serwera ICA

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Ogólne	
Nazwa	`ica_server`
Zablokowane	✗
Protokół	`ICA`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.0.21`
Port	`1494`
Użyj TLS	✗

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania dla serwera ICA

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`ica_listener`
Zablokowane	✗
Protokół	`ICA`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`2494`
Użyj bezpiecznych połączeń (TLS)	✗

4. Kliknij *Zapisz*.

Dodanie konta dla serwera ICA

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

Informacja: Połączenia z serwerami ICA za pośrednictwem Citrix StoreFront wymagają konta skonfigurowanego w trybie *anonymous* lub *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`ICA_forward`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ica_server`
Dane uwierzytelniające	
Zastąp sekret	✗
Przekazuj domenę	✓

4. Kliknij *Zapisz*.

Dodanie serwera Citrix StoreFront

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	`citrix_storefront`
Zablokowane	✗
Protokół	`Citrix StoreFront (HTTP)`
Czas oczekiwania HTTP	`900`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.90.1`
Port	`80`
Adres źródłowy	`Dowolny`
URL	`http://10.0.90.1/Citrix/StoreWeb/`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania dla serwera Citrix StoreFront

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`citrix_storefront_listener`
Zablokowane	✗
Protokół	`Citrix StoreFront (HTTP)`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.8.65`
Port	`7003`
Użyj szyfrowania TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta dla Citrix StoreFront

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą

loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`citrixuser_at_SF`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`citrix_storefront`
Dane uwierzytelniające	
Domena	`tech.whl`
Login	`citrixuser`
Zastąp sekret	`hasłem`
Hasło	password
Powtórz hasło	password
Polityka modyfikatora hasła	`Statyczne, bez ograniczeń`
Modyfikator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij Zapisz.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

Informacja: Przy wybieraniu listenera ICA, którego adres ma być zwrócony do klienta przeszukiwane są jedynie sejfy, w których znajduje się listener Citrix StoreFront, z którego użytkownik aktualnie korzysta.

---

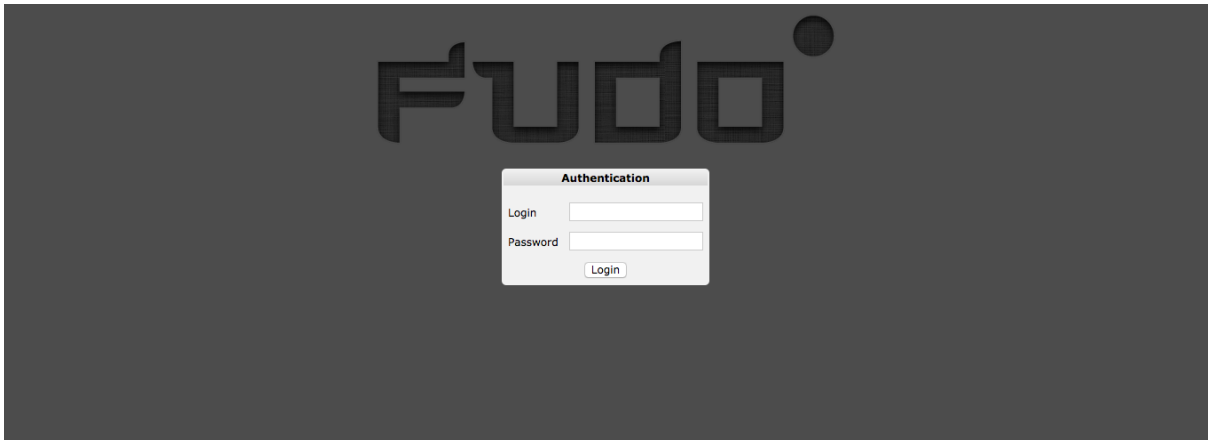
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`ica_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`citrixuser_at_SF`	`citrix_storefront_listener`
`ICA_forward`	`ica_listener`

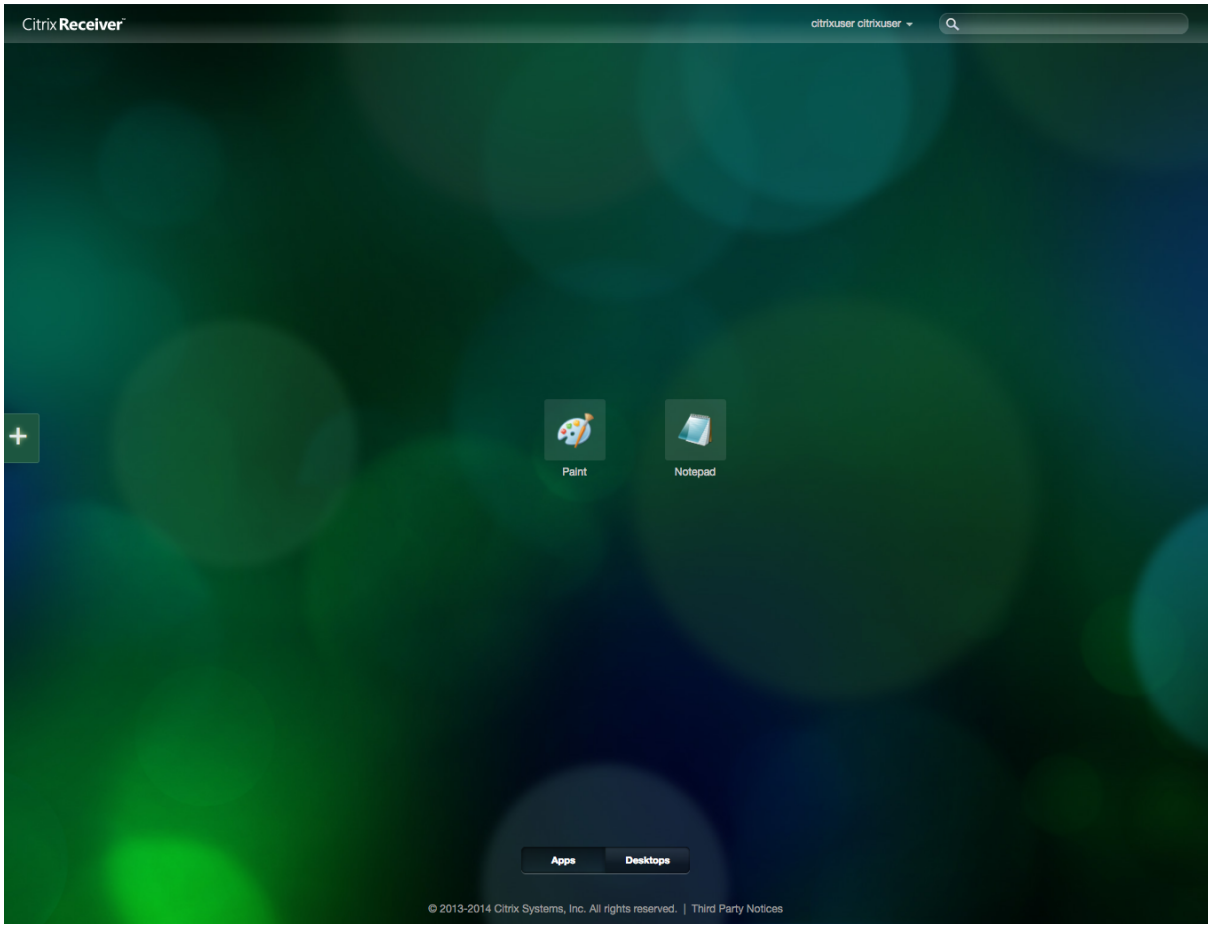
4. Kliknij *Zapisz*.

Nawiązanie połączenia

1. W przeglądarce internetowej wprowadź adres IP `10.0.8.65:7003`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu Citrix StoreFront.

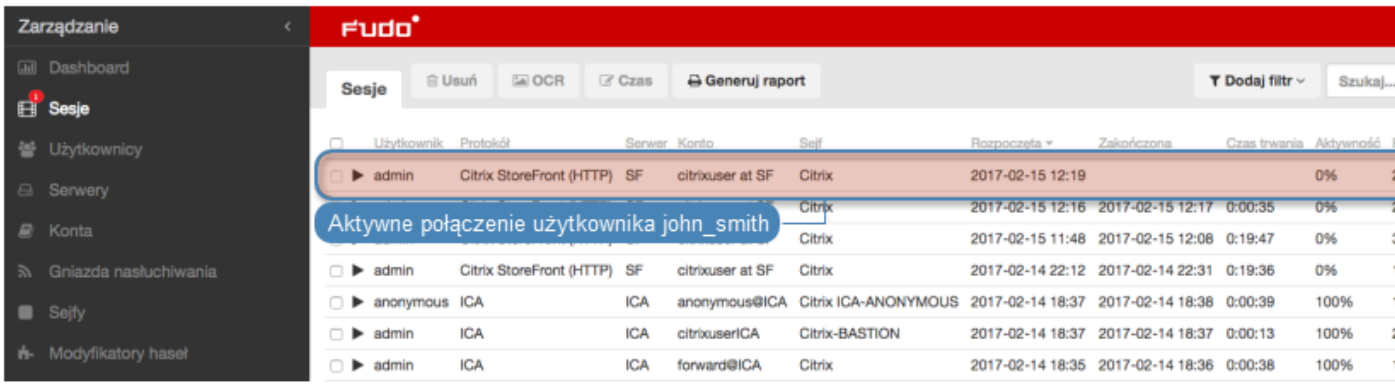


3. Kliknij wybrany element, aby nawiązać połączenie z zasobem.



Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP `10.0.8.65`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu panelu zarządzającego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Model danych*
- *Dodawanie serwera Citrix*

- *Dodawanie gniazda nasłuchiwania Citrix*
- *Citrix StoreFront (HTTP)*

4.10 VNC

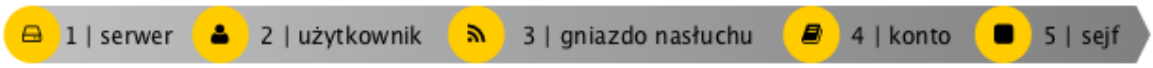
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń VNC ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *VNC* uwierzytelnia się na Wheel Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Wheel Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła.

Informacja: Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.

4.10.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

4.10.2 Konfiguracja



Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	vnc_server
Zablokowane	✗
Protokół	`VNC`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.40.230`
Port	`5900`
Adres źródłowy	`Dowolny`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`vnc_listener`
Zablokowane	✗
Protokół	`VNC`
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`5900`

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_vnc_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`vnc_server`
Dane uwierzytelniające	
Domena	✗
Login	✗
Zastąp sekret	`hasłem`
Hasło	`root`
Powtórz hasło	`root`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użyj istniejące konto	✗
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

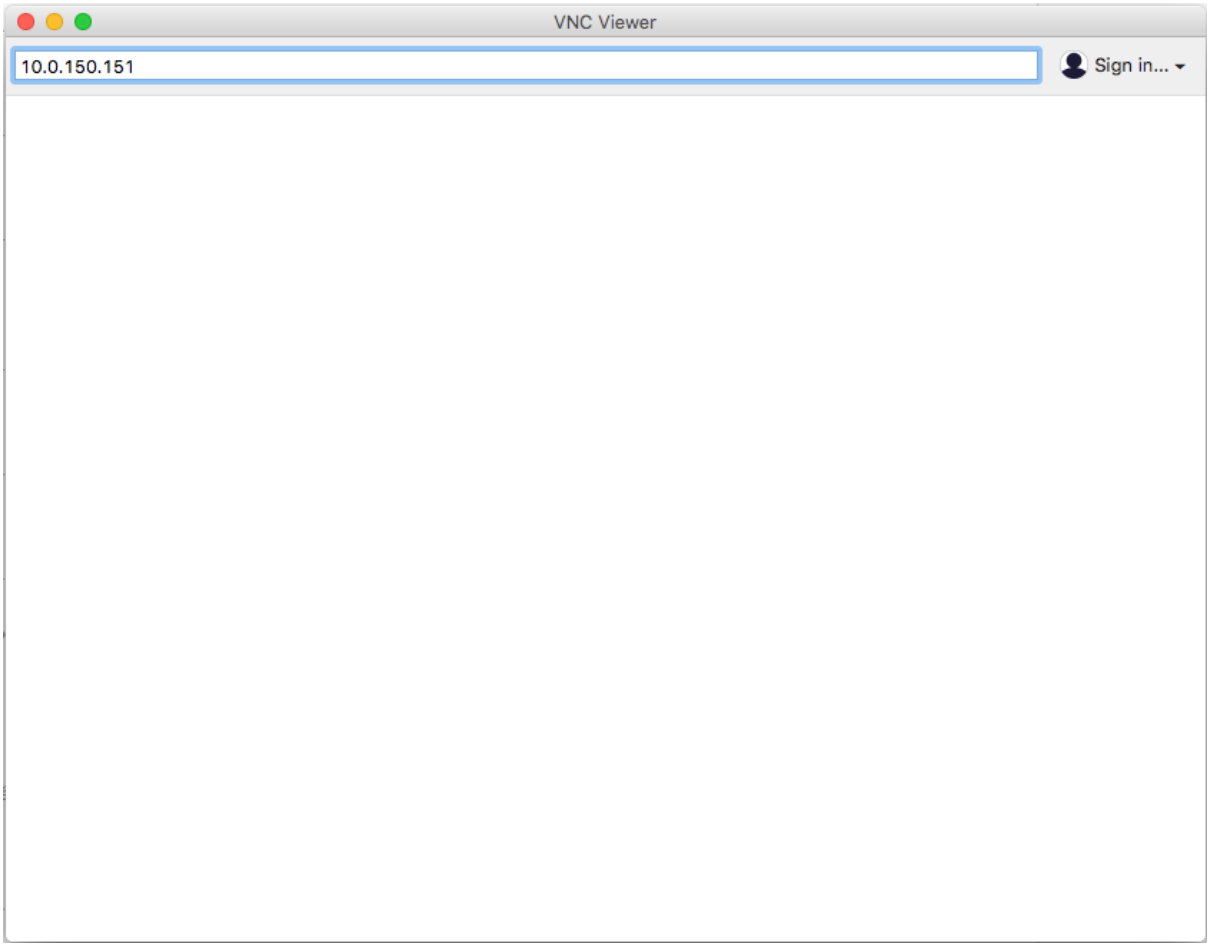
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`vnc_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Użytkownicy	`john_smith`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✓
Uprawnienia	
Uprawnieni użytkownicy	✗
Powiązania obiektu	
`admin_vnc_server`	`vnc_listener`

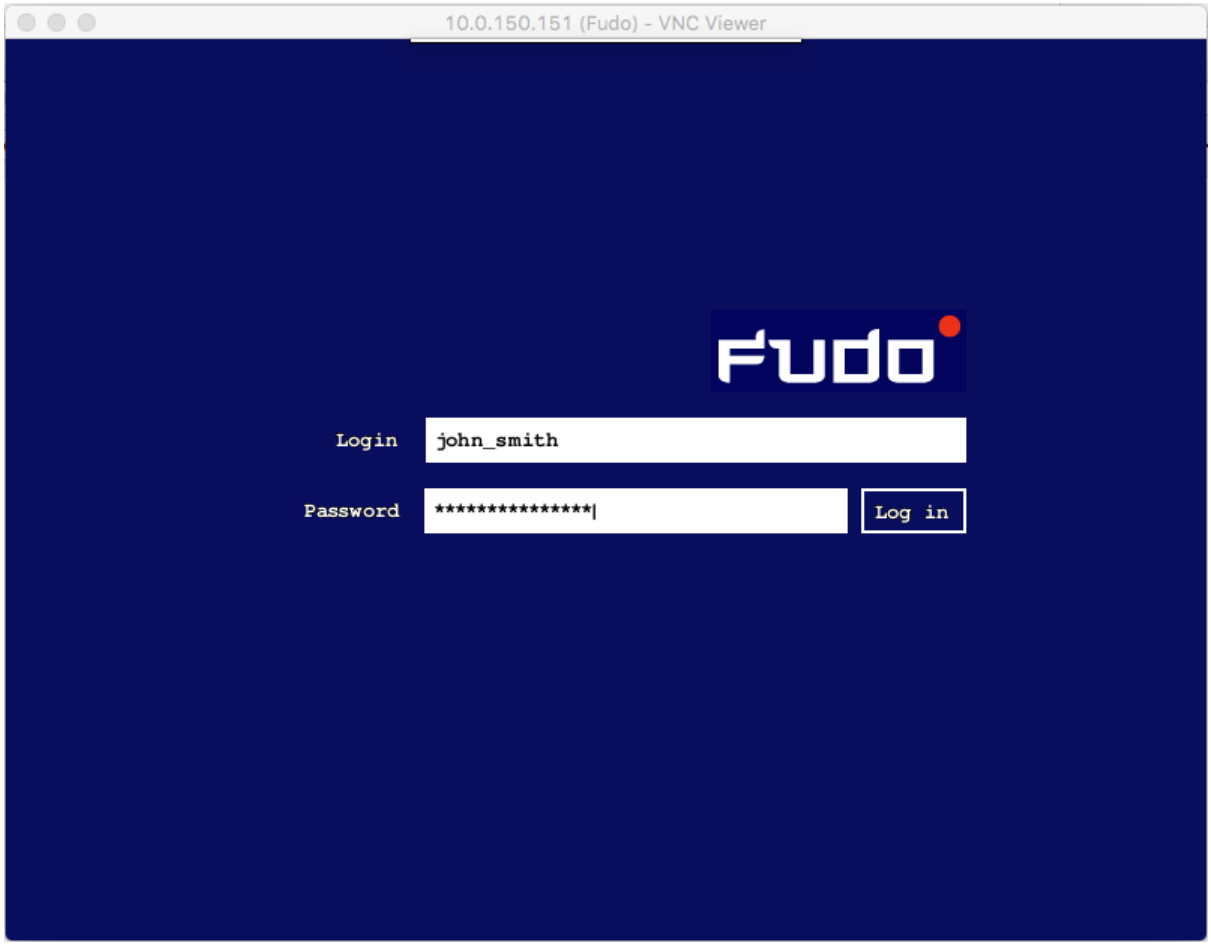
4. Kliknij *Zapisz*.

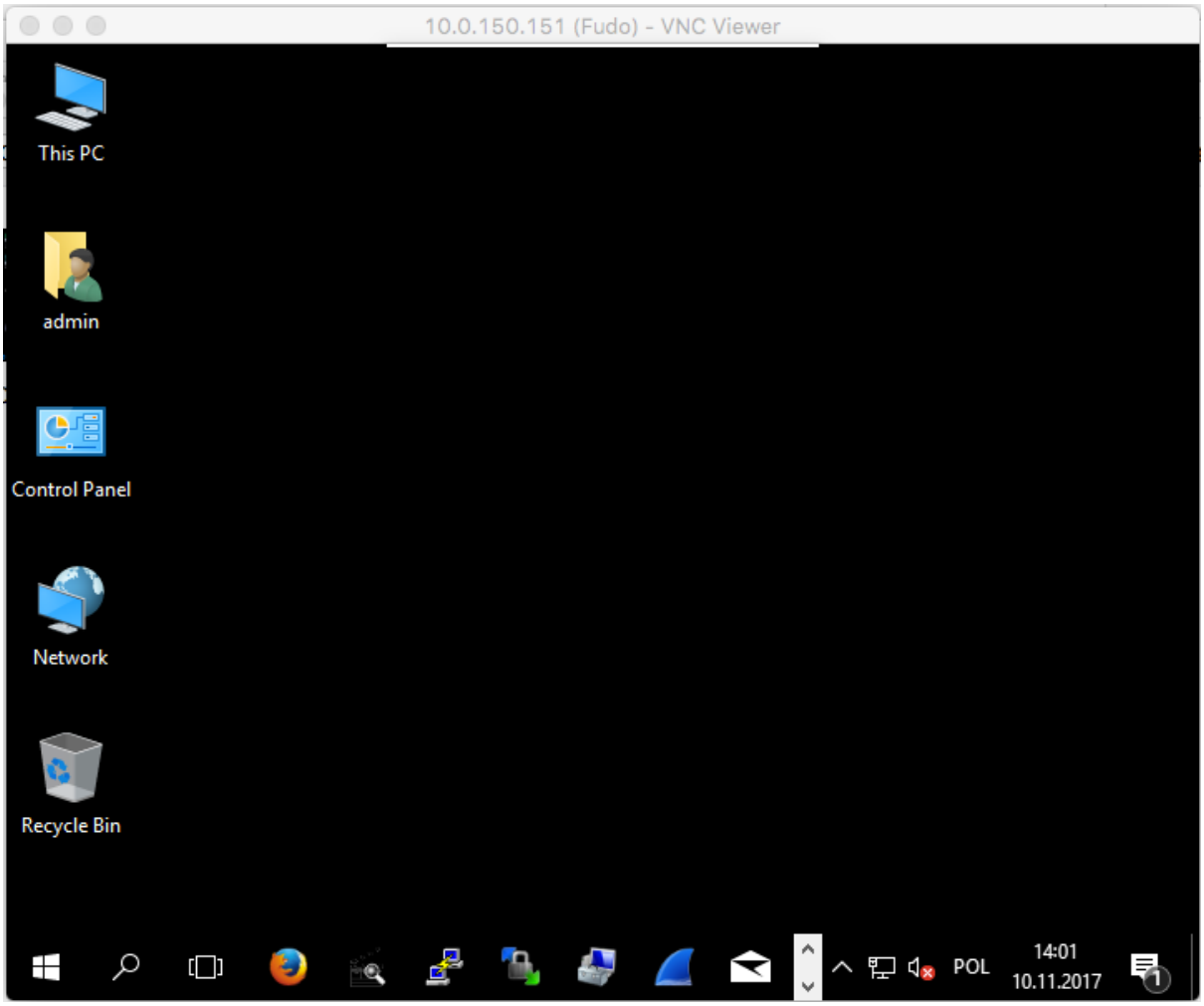
4.10.3 Nawiązanie połączenia

1. Uruchom aplikację kliencką *VNC Viewer* i w polu adresu wprowadź `10.0.150.151`.



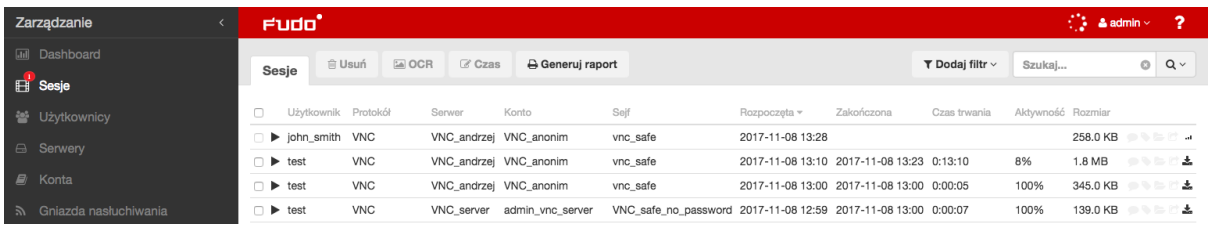
2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in



4.10.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.151`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *VNC Viewer*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*

- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*
- Konfiguracja

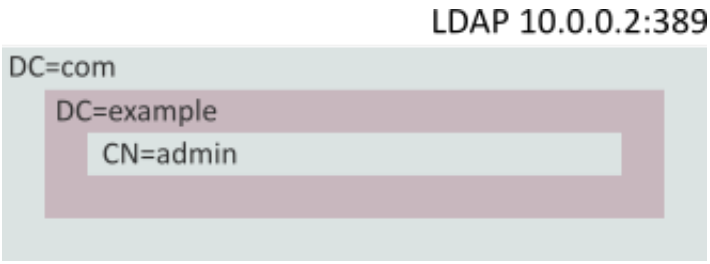
4.11 Uwierzytelnienie użytkowników w katalogu LDAP

W tym rozdziale przedstawiony jest przykład konfigurowania usługi LDAP jako zewnętrznego źródła uwierzytelnienia i wykorzystanie definicji do uwierzytelnienia użytkownika zdefiniowanego w lokalnym modelu danych systemu Wheel Fudo PAM.

4.11.1 Założenia

Poniższy opis zakłada, że dane uwierzytelniające użytkownika `admin` sprawdzane są na serwerze LDAP, dostępnym pod adresem 10.0.0.2 i na domyślnym numerze portu usługi LDAP tj. 389.

Definicja użytkownika znajduje się pod ścieżką `cn=admin,dc=example,dc=com`.



4.11.2 Konfiguracja

Dodanie zewnętrznego źródła uwierzytelnienia

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnienie*.
2. Kliknij + *Dodaj zewnętrzne źródło uwierzytelnienia*.
3. Uzupełnij parametry konfiguracyjne usługi:

Parametr	Wartość
Typ	`LDAP`
Adres hosta	`10.0.0.2`
Port	`389`
Wysyłaj żądania z	`10.0.0.10`
Bind DN	`dc=example,dc=com` **Informacja:** Alternatywnie, określ pełną ścieżkę miejsca przechowywania definicji kont użytkowników `cn=##username##, dc=example,dc=com` i pozostaw pole *Baza LDAP* w konfiguracji użytkowników puste.
Połączenie szyfrowane	✗
Usuń	✗

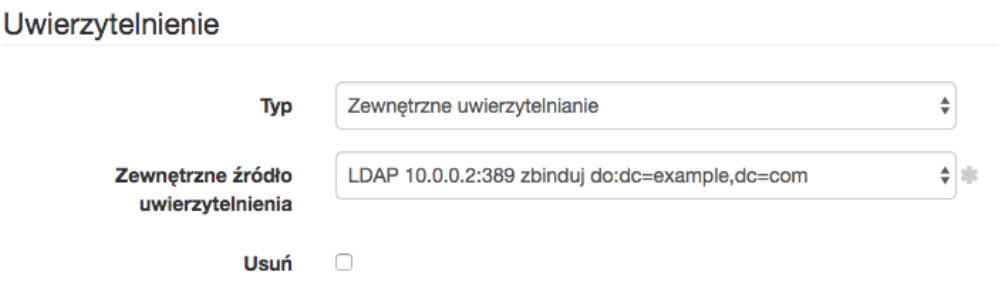
4. Kliknij *Zapisz*.

Dodanie metody uwierzytelnienia użytkownika

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i kliknij użytkownika `admin`.
3. W polu *Baza LDAP* wprowadź ciąg definiujący obiekt *admin* w strutkurze katalogowej `cn=admin,dc=example,dc=com`.

Informacja: Pozostaw pole *Baza LDAP* puste, jeśli w konfiguracji zewnętrznego źródła uwierzytelnienia podana została pełna ścieżka miejsca przechowywania kont użytkowników w drzewie katalogów (`cn=##username##,dc=example,dc=com`).

4. Kliknij *+ Dodaj metodę uwierzytelnienia*.
5. Z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie`.
6. Z listy rozwijalnej *Zewnętrzne źródło uwierzytelnienia*, wybierz `LDAP 10.0.0.10:389 zbinduj do:dc=example,dc=com`.



7. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Dodawanie użytkownika*
- *Konfigurowanie monitorowania połączeń SSH*

ROZDZIAŁ 5

Użytkownicy

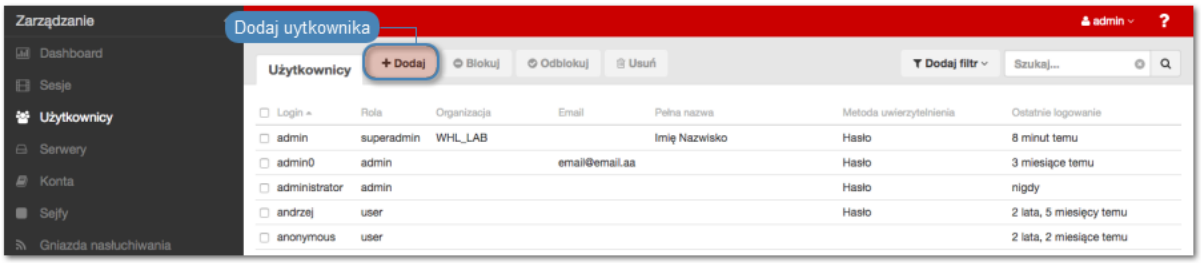
Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

5.1 Dodawanie użytkownika

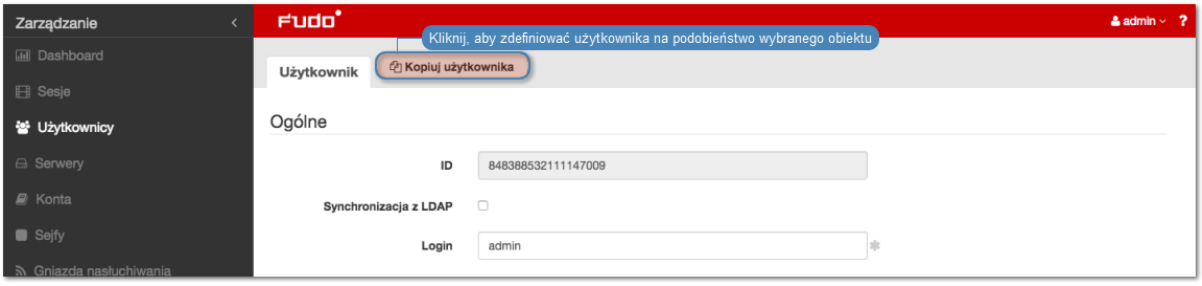
Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

Aby dodać definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.



Informacja: Wheel Fudo PAM umożliwia tworzenie użytkowników na podstawie istniejących definicji. Otwórz formularz edycji istniejącego użytkownika i kliknij *Kopiuj użytkownika*, aby stworzyć nowy obiekt na podstawie wybranej definicji.



3. Wprowadź nazwę użytkownika.

Informacja:

- Model danych dopuszcza istnienie więcej niż jednego obiektu o tym samym loginie, z zachowaniem unikalności kombinacji loginu i domeny.
- Pole *Login* nie rozróżnia wielkości liter.

4. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi zalogowanie zaraz po utworzeniu konta.
5. Określ ważność tworzonego konta.
6. Zdefiniuj rolę, determinującą prawa dostępu użytkownika.

Informacja: Określone rolą uprawnienia, dotyczą także dostępu do modelu danych poprzez interfejs API.

Rola	Prawa dostępu
user	• łączenie z serwerami w ramach zdefiniowanych sejfów, do których użytkownik został przypisany • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
service	• monitorowanie stanu systemu poprzez protokół SNMP
operator	• logowanie do panelu administracyjnego • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • włączanie/wyłączanie powiadomień email • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
admin	• logowanie do panelu administracyjnego • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału • włączanie/wyłączanie powiadomień email • zarządzanie politykami • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia • zarządzanie modyfikatorami haseł • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

superadmin	• zarządzanie obiektami bez ograniczeń • zarządzanie konfiguracją urządzenia bez ograniczeń • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

7. Określ preferowany język panelu administracyjnego Wheel Fudo PAM.
8. Dodaj sejfy z kontami uprzywilejowanymi, do których użytkownik będzie miał dostęp.

Informacja:

- Przeciągnij i upuść sejf, żeby określić kolejność użycia danych przechowywanych w sejfie przy zestawianiu połączenia.
- SSH_sejf wskazuje, że opcja Pokaż hasło jest wyłączona.
- RDP_sejf oznacza, że opcja Pokaż hasło jest włączona.
- Kliknij sejf, aby zdefiniować *politykę czasu dostępu*.

9. Wprowadź pełną nazwę użytkownika, która umożliwi jego jednoznaczną identyfikację.
10. Wprowadź adres email użytkownika.

Informacja: Na podany adres email, Wheel Fudo PAM wysyła subskrybowane raporty cykliczne.

11. Wprowadź nazwę organizacji, do której przynależy użytkownik.
12. Podaj numer telefonu użytkownika.
13. Wprowadź domenę *AD*, do której należy konto użytkownika.
14. Wprowadź parametr bazowy usługi katalogowej LDAP (*Base DN*).

Informacja:

- Parametr bazowy LDAP jest wymagany do uwierzytelnienia użytkownika w usłudze Active Directory.
- Dla użytkownika `admin` w przykładowej domenie `example.com`, parametr powinien przyjąć postać `cn=admin,dc=example,dc=com`.

15. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania tworzonym obiektem.
16. W sekcji *Uwierzytelnienie*, określ sposób uwierzytelnienia użytkownika.

Hasło

- Z listy rozwijalnej *Typ*, wybierz `Hasło`.

- Wprowadź hasło w polu *Hasło*.
- Powtórnie wprowadź hasło w polu *Powtórz hasło*.

Zewnętrzne uwierzytelnienie

- Z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie`.
- Z listy rozwijalnej *Zewnętrzne źródło uwierzytelnienia* wybierz źródło, które zostanie użyte do uwierzytelnienia użytkownika.

Informacja: Procedura definiowanie zewnętrznych źródeł uwierzytelnienia opisana jest w rozdziale *Zewnętrzne serwery uwierzytelniania*.

Klucz SSH

- Z listy rozwijalnej *Typ*, wybierz `Klucz SSH`.
- Kliknij ikonę w polu tekstowym *Klucz publiczny* i wskaż plik z definicją klucza publicznego użytkownika, który zostanie użyty do zweryfikowania jego tożsamości.

Hasło jednorazowe

Ostrzeżenie: Opcja logowania za pomocą hasła jednorazowego ma zastosowanie w implementacjach mechanizmu bezpiecznej wymiany haseł pomiędzy aplikacjami (*AAPM*).

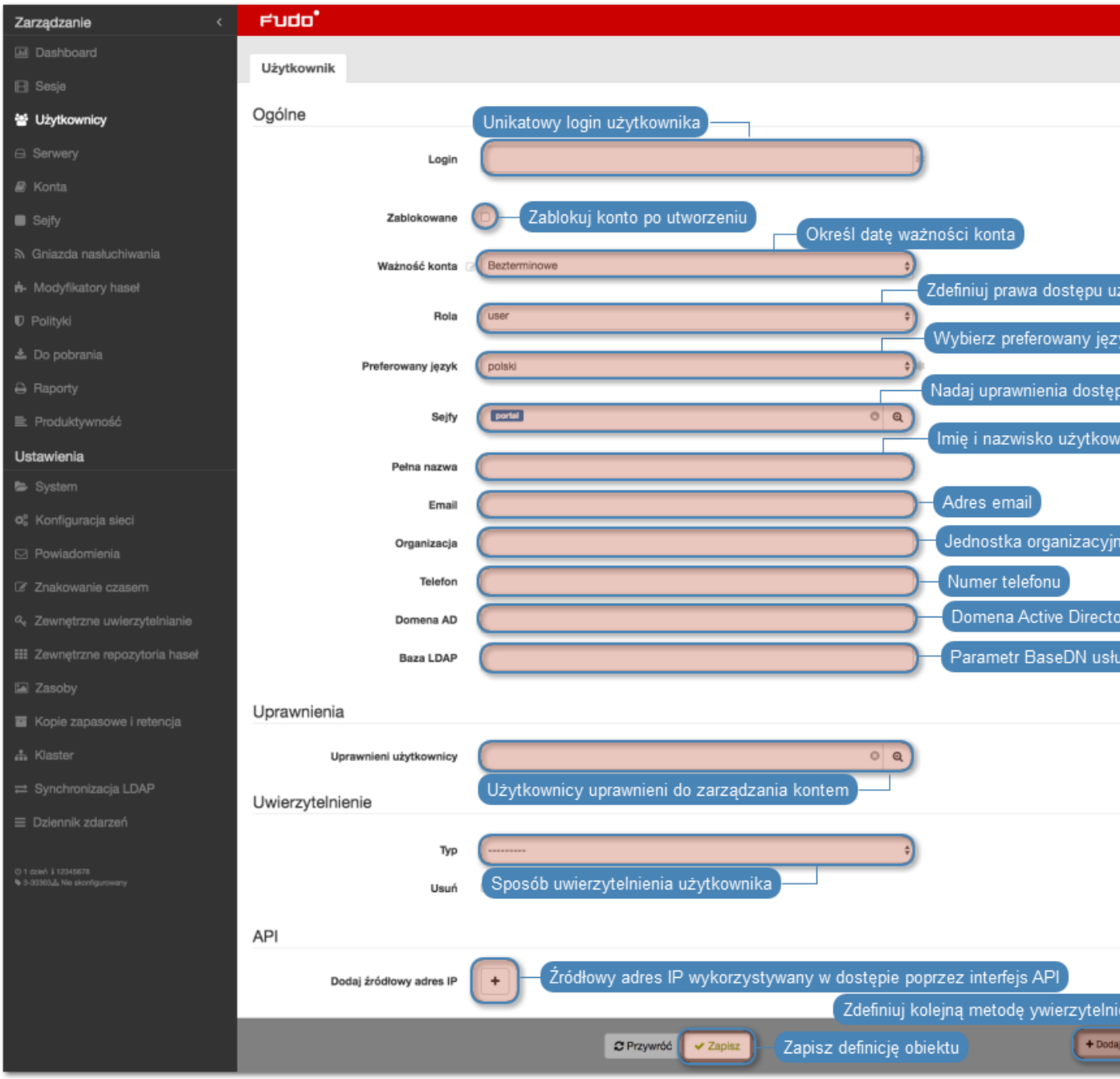
- Z listy rozwijalnej *Typ*, wybierz `Hasło jednorazowe`.

17. Kliknij *+ Dodaj metodę uwierzytelnienia*, aby zdefiniować kolejną metodę uwierzytelnienia.

Informacja: W procesie uwierzytelnienia, Wheel Fudo PAM dokonuje sprawdzenia danych logowania użytkownika w oparciu o źródła uwierzytelnienia w kolejności w jakiej zostały zdefiniowane. W przypadku niepowodzenia uwierzytelnienia za pomocą pierwszej metody, Wheel Fudo PAM próbuje uwierzytelnić użytkownika za pomocą kolejnych.

---

18. W sekcji *API* kliknij  , aby dodać adres IP, z którego system wykorzystujący API będzie nawiązywał połączenia, uwierzytelniając się za pomocą definiowanego konta użytkownika.
19. Kliknij *Zapisz*.



Tematy pokrewne:

- *Synchronizacja użytkowników z LDAP*
- *Dodawanie urządzenia mobilnego*
- *Polityka czasowa dostępu do sejfów*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*
- *Akceptowanie połączeń oczekujących*

- *Odrzucanie połączeń oczekujących*

5.2 Modyfikowanie użytkownika

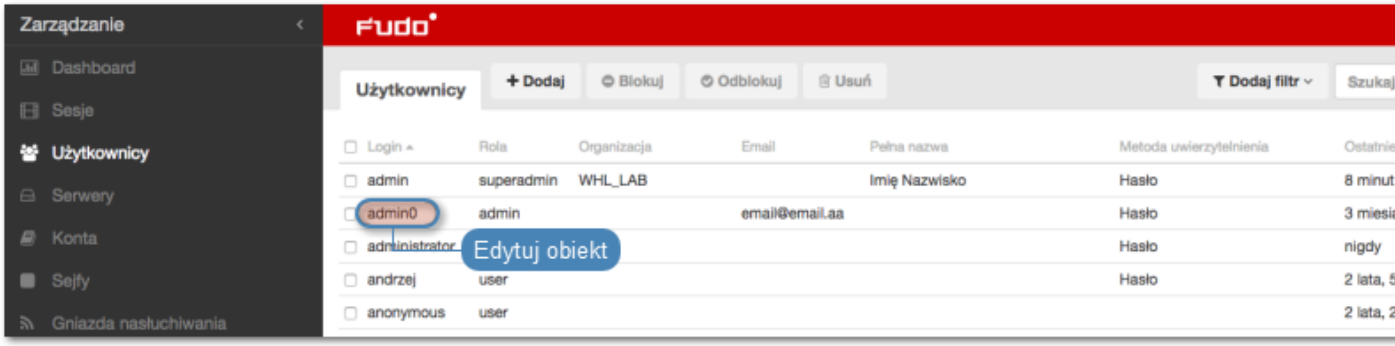
Aby zmodyfikować definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście definicję konta, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

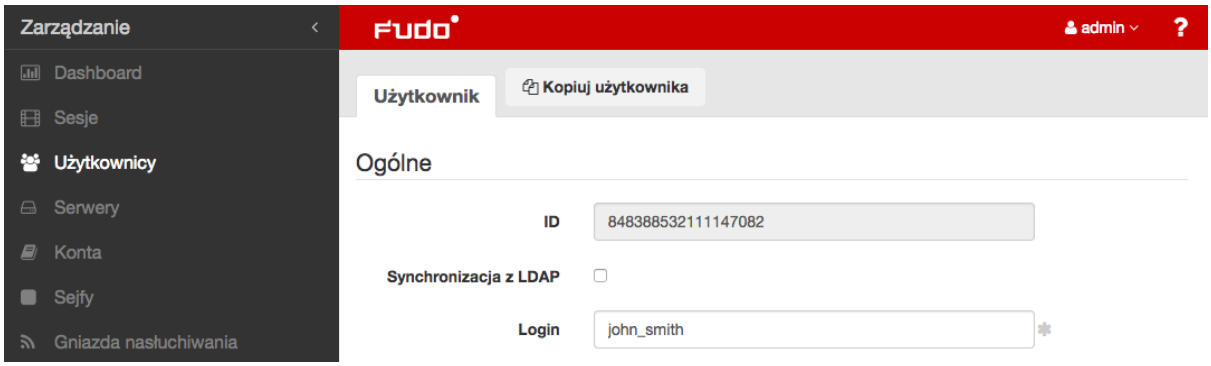
3. Kliknij nazwę konta.



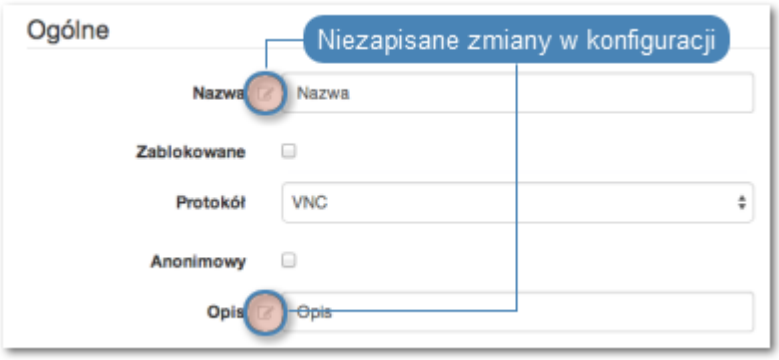
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja:

- ID użytkowika jest identyfikatorem obiektu nadawanym automatycznie przez Wheel Fudo PAM i jest parametrem tylko do odczytu.



- Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną .



5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

5.3 Blokowanie użytkownika

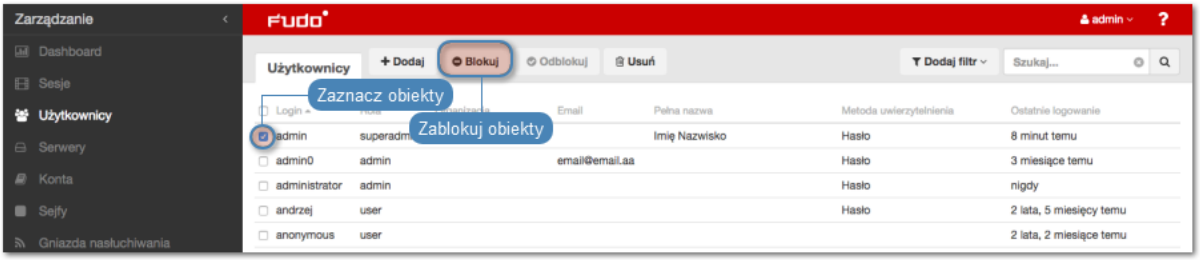
Aby zablokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

Ostrzeżenie: Zablokowanie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

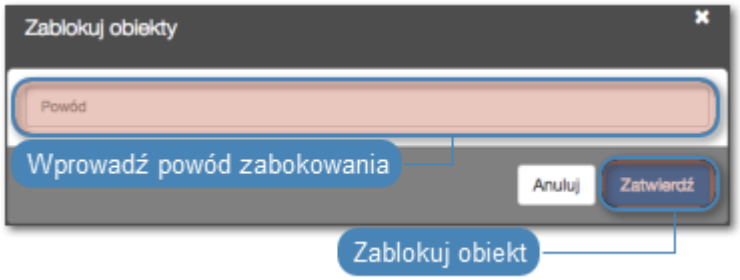
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz użytkownika, którego chcesz zablokować/odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować użytkownikowi możliwość nawiązywania połączeń.



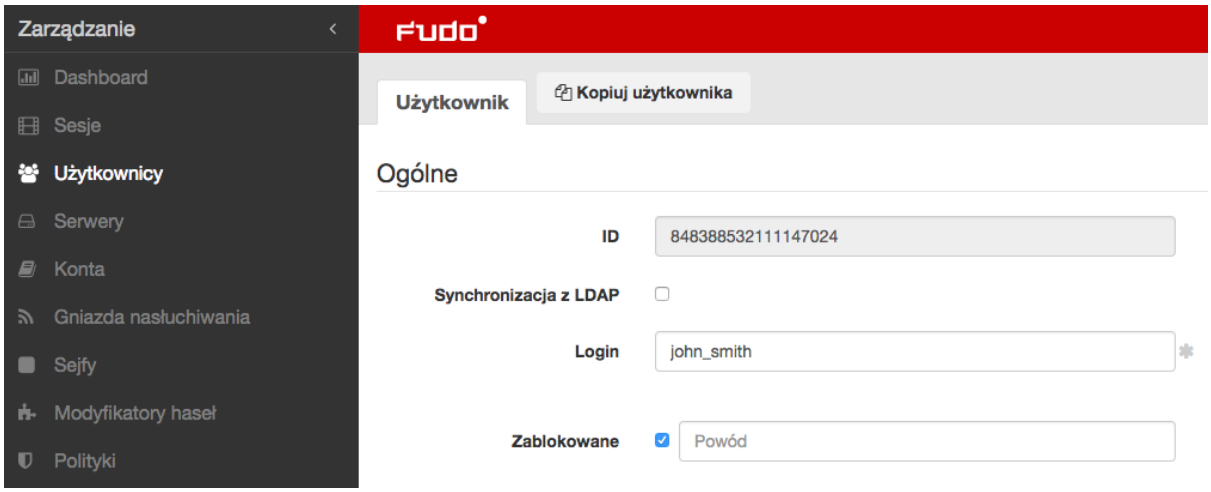
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.



Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Informacja: Konto użytkownika może zostać również zablokowane z poziomu formularza edycji obiektu.

- Zaznacz opcję *Zablokowane*.
- Opcjonalnie, wprowadź powód zablokowania.



- Kliknij *Zapisz*.

Tematy pokrewne:

- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

5.4 Odblokowanie użytkownika

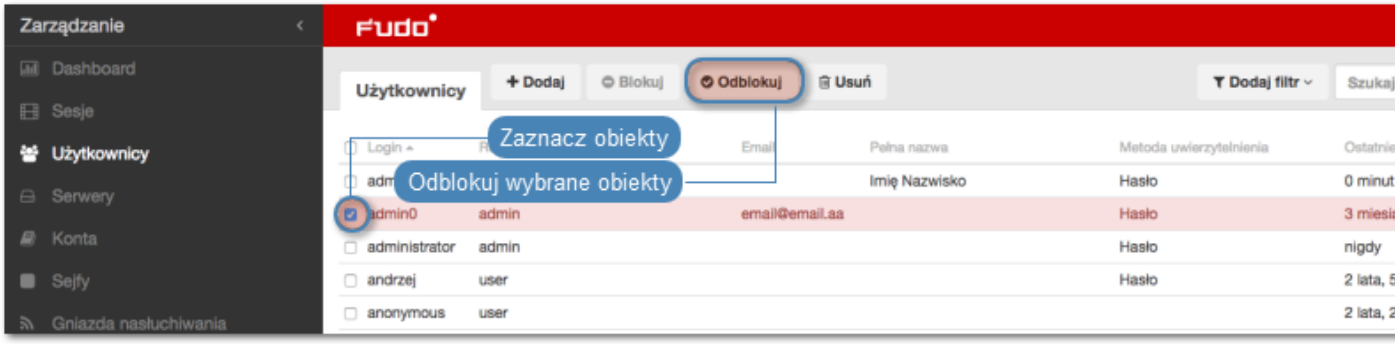
Aby odblokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować/odblokować.

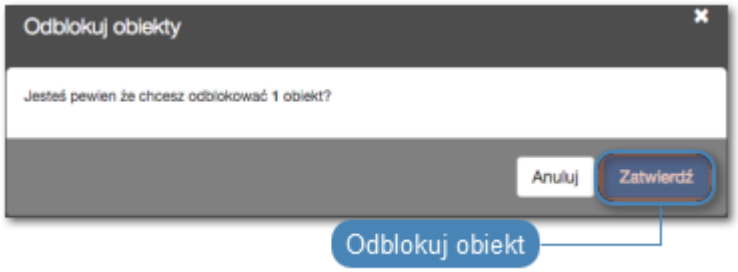
Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

3. Kliknij *Odblokuj*, aby umożliwić nawiązywanie połączeń za pośrednictwem wybranego konta.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.



Tematy pokrewne:

- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

5.5 Usuwanie użytkownika

Aby usunąć definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

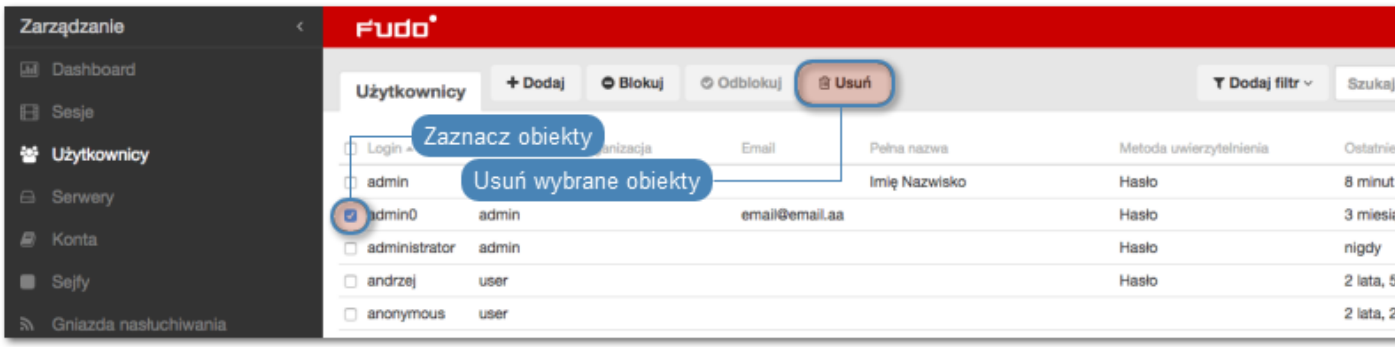
Informacja: Usunięcie definicji użytkownika nie skutkuje usunięciem skojarzonych, zarejestrowanych sesji. Sesje usuniętych użytkowników charakteryzują się przekreślonym loginem użytkownika.

Ostrzeżenie: Usunięcie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

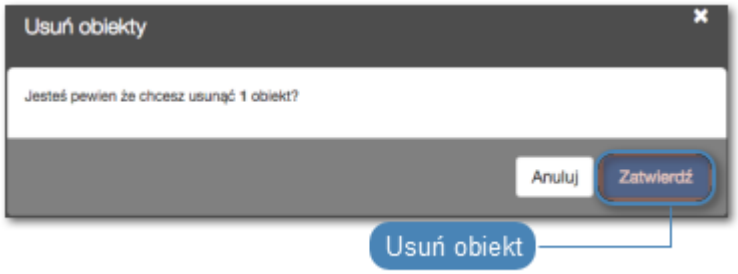
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz konta, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.



4. Potwierdź operację usunięcia zaznaczonych obiektów.



Tematy pokrewne:

- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

5.6 Polityka czasowa dostępu do sejfów

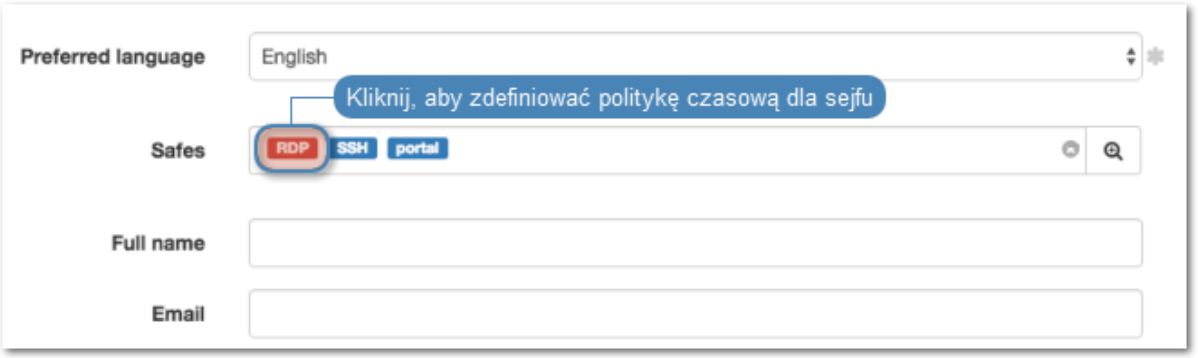
Wheel Fudo PAM pozwala na regulowanie dostępu do sejfów na podstawie definiowanych ram czasowych.

Aby zdefiniować politykę czasu dostępu do sejfu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście definicję użytkownika.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

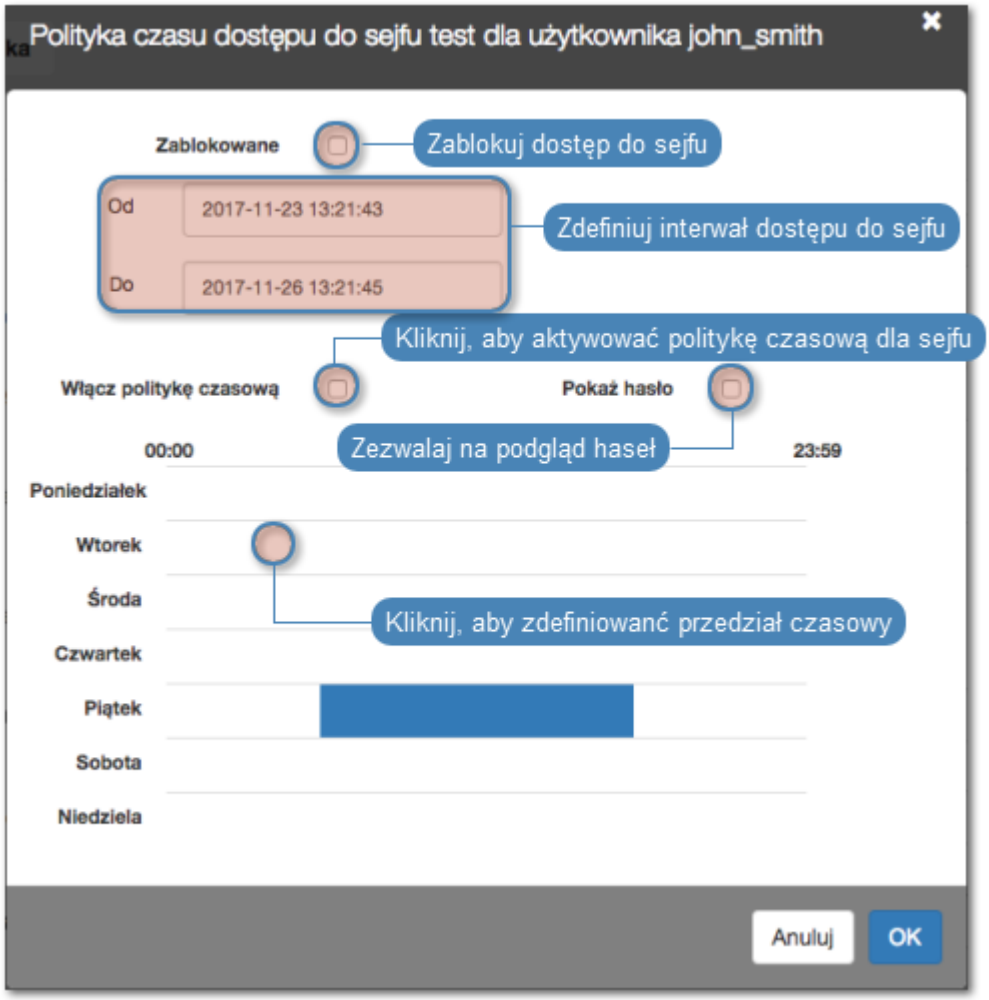
3. Kliknij nazwę użytkownika.
4. Kliknij wybrany sejf.



5. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi nawiązywanie połączeń poprzez wybrany sejf.
6. W polach *Od* i *Do* określ interwał czasu, w którym użytkownik będzie mógł nawiązywać połączenia za pośrednictwem wybranego sejfu.

Informacja: Pozostaw pola kalendarza puste, aby dostęp do sejfu był bezterminowy.

7. Zaznacz opcję *Włącz politykę czasową*, aby użytkownik mógł nawiązywać połączenia tylko w wyznaczonych godzinach.
8. Zaznacz opcję *Pokaż hasło*, aby zezwolić użytkownikowi na podgląd haseł w *Portalu Użytkownika*.
9. Kliknij kalendarz, aby zdefiniować przedziały czasowe, w których użytkownik będzie mógł się łączyć poprzez konta przypisane do wybranego sejfu.



10. Kliknij *OK*.
11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *ServiceNow - przyznawanie dostępu*
- *Sejfy*

5.7 Role użytkownika

Role użytkownika umożliwiają regulowanie dostępu do obiektów zarządzanych i monitorowanych przez Wheel Fudo PAM.

Rola	Prawa dostępu
user	• łączenie z serwerami w ramach zdefiniowanych sejfów, do których użytkownik został przypisany • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
service	• monitorowanie stanu systemu poprzez protokół SNMP
operator	• logowanie do panelu administracyjnego • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • włączanie/wyłączanie powiadomień email • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
admin	• logowanie do panelu administracyjnego • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału • włączanie/wyłączanie powiadomień email • zarządzanie politykami • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, gniazdo nasłuchiwania, konto), do których użytkownik posiada uprawnienia • zarządzanie modyfikatorami haseł • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

superadmin	• zarządzanie obiektami bez ograniczeń • zarządzanie konfiguracją urządzenia bez ograniczeń • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

Tematy pokrewne:

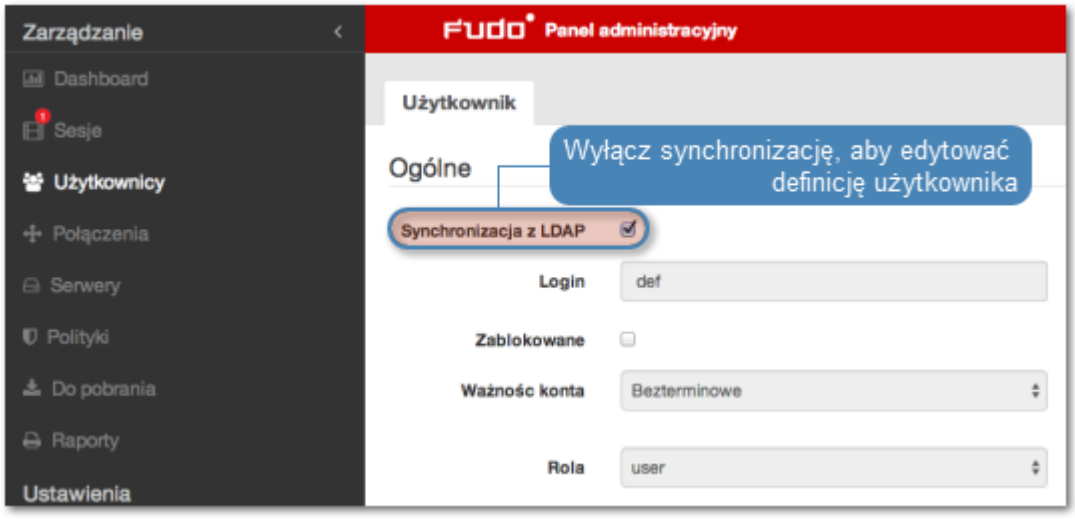
- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

5.8 Synchronizacja użytkowników z LDAP

Użytkownik jest jednym z podstawowych elementów *modelu danych*. Tylko zdefiniowani użytkownicy mogą nawiązywać połączenia z monitorowanymi serwerami. Wheel Fudo PAM pozwala na automatyczną synchronizację definicji użytkowników z serwerem *Active Directory* lub innymi zgodnymi z protokołem *LDAP*.

Definicje nowych użytkowników oraz zmiany w istniejących obiektach pobierane są z serwera usług katalogowych co 5 minut. Odzwierciedlenie zmiany polegającej na usunięciu użytkownika z serwera *AD* lub *LDAP* wymaga pełnej synchronizacji. Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00, lub może zostać wyzwolona ręcznie.

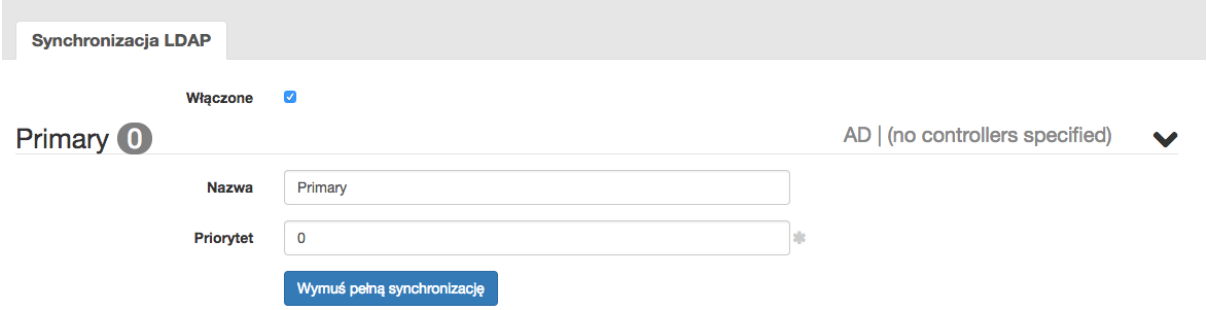
Informacja: Dane użytkowników synchronizowanych z serwerem usług katalogowych nie mogą być poddawane edycji. Aby zmienić definicję użytkownika synchronizowanego z serwerem LDAP lub AD, wyłącz opcję `Synchronizacja z LDAP` dla danego użytkownika.



Konfiguracja usługi synchronizacji użytkowników

1. Wybierz z lewego menu *Ustawienia* > *Synchronizacja LDAP*.
2. Zaznacz opcję *Włączone*.
3. W przypadku *konfiguracji klastrowej*, z listy rozwijalnej *Aktywny węzeł klastra*, wybierz węzeł, który będzie dokonywał synchronizacji obiektów z usługą LDAP.
4. Kliknij *+ Dodaj domenę LDAP*.
5. Wprowadź nazwę domeny.
6. Określ priorytet, który determinuje kolejność odpytywania domen.

Informacja: Mniejsza liczba oznacza wyższy priorytet.



7. W sekcji *Usługa katalogowa*, wybierz z listy rozwijalnej *Rodzaj serwera* typ usługi katalogowej.
8. Podaj informacje uwierzytelniające użytkownika uprawnionego do przeglądania katalogu.
9. Podaj nazwę domeny, do której należą użytkownicy podlegający synchronizacji.
10. Określ miejsce przechowywania użytkowników w strukturze katalogowej (np. `dc=devel, dc=whl`).

Informacja: Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

- użycia nakładki *memberOf*
- użycia grup *objectClass*: `groupOfNames`
- zdefiniowania ciągu parametru base DN w postaci: `uid=##username##,ou=people, dc=ldap,dc=test`.

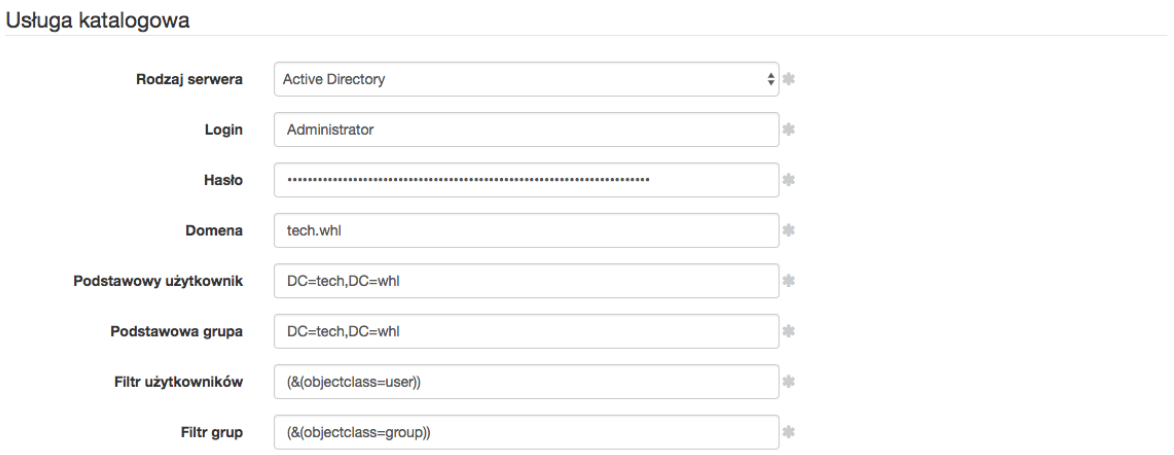
---

11. Określ miejsce przechowywania grup w strukturze katalogowej.

Informacja: Parametr DN nie powinien zawierać zbędnych znaków białych, tj. spacji, tabulatorów, itp.

---

12. Zdefiniuj filtr dla rekordów użytkowników, których definicje mają zostać zsynchronizowane (lub pozostaw wartość domyślną).
13. Zdefiniuj filtr dla grup użytkowników, których definicje mają zostać zsynchronizowane (lub pozostaw wartość domyślną).



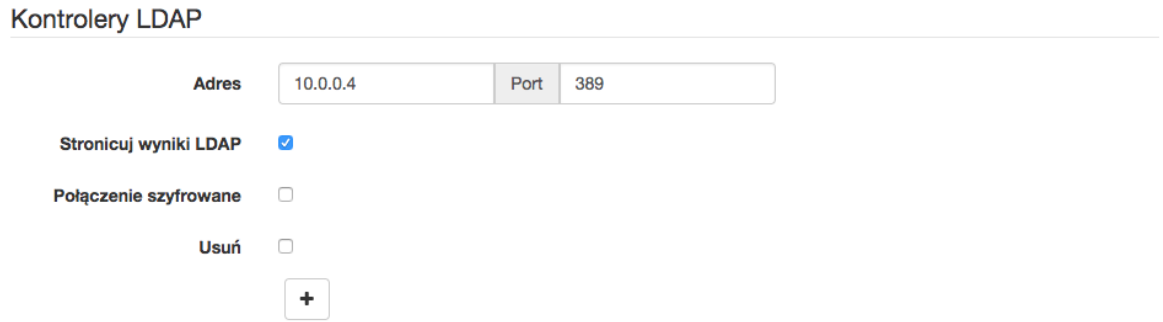
14. Kliknij + w sekcji *Kontrolery LDAP*, aby zdefiniować host usługi katalogowej.
15. Wprowadź adres IP serwera oraz numer portu, na którym dostępna jest usługa katalogowa.

Informacja: W przypadku połączeń szyfrowanych, w polu adresu serwera, wprowadź jego nazwę domenową (np. `tech.ldap.com`) zamiast adresu IP, aby zapewnić poprawność weryfikacji certyfikatu serwera. Upewnij się, że nazwa domenowa jest ujęta w polu *Common Name* w certyfikacie.

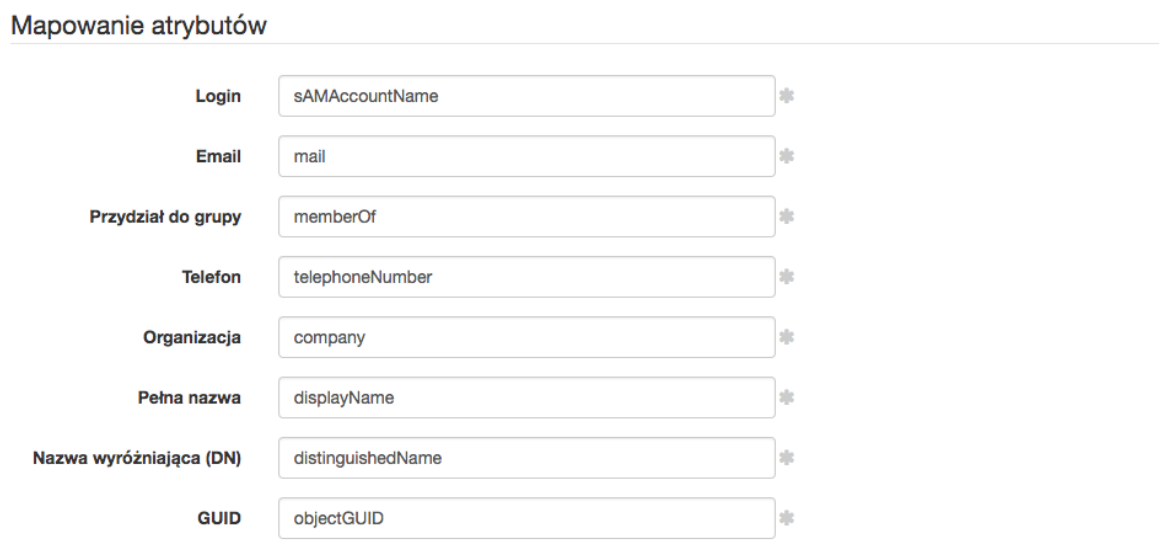
---

16. Zaznacz opcję *Stronicuj wyniki LDAP*, aby włączyć stronicowanie danych zwracanych przez serwer LDAP.
17. Zaznacz opcję *Połączenie szyfrowane* i wgraj certyfkat CA, aby włączyć szyfrowanie transmisji z serwerem LDAP.

Informacja: Kliknij +, aby wskazać kolejny serwer usług katalogowych.

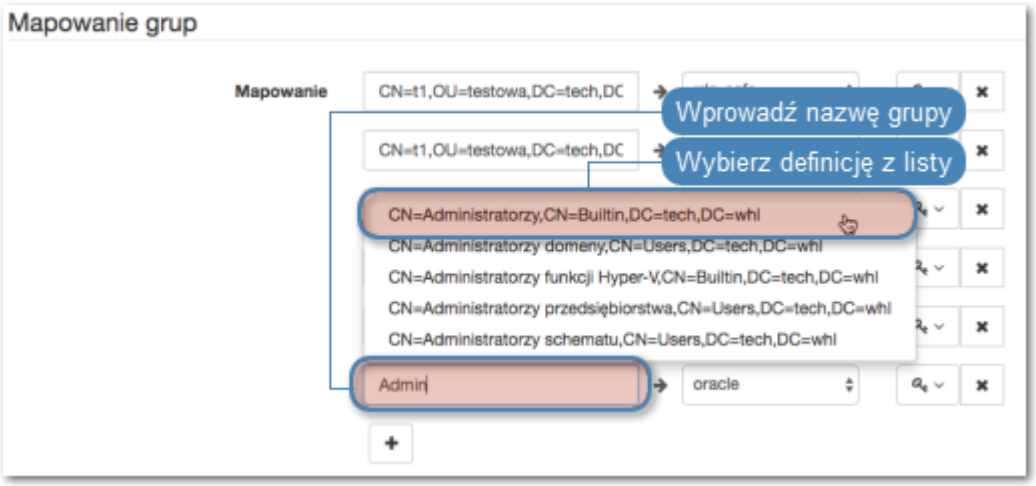


18. Zdefiniuj mapowanie pól atrybutów definicji użytkowników.



Informacja: Mapowanie pól pozwala na pobranie informacji o użytkownikach z atrybutów o niestandardowych nazwach, np. numeru telefonu zdefiniowanego w atrybucie *mobile* zamiast standardowego *telephoneNumber*.

19. Kliknij + w sekcji *Mapowanie grup*, aby dodać mapowanie grupy użytkowników.
20. Wprowadź nazwę grupy i kliknij wybrany element na liście.



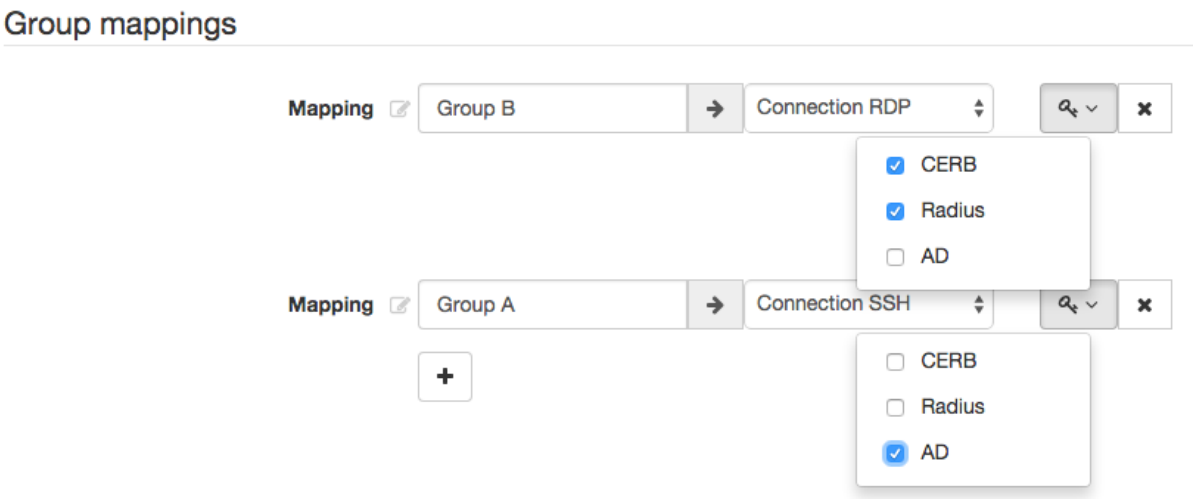
21. Określ przypisanie grup użytkowników do sejfów.
22. Przypisz źródła uwierzytelnienia do grup użytkowników.

Informacja: Źródła uwierzytelnienia przypisywane są użytkownikom w kolejności definiowania mapowań. Jeśli użytkownik znajduje się w więcej niż jednej grupie, w pierwszej kolejności będzie uwierzytelniany w oparciu o źródła uwierzytelniania przypisane do pierwszego zdefiniowanego mapowania, w którym się znajduje.

Na przykład:

Użytkownik przypisany jest do grup A i B. Dla grupy B, zdefiniowane jest mapowanie z połączeniem `Sejf RDP` i przypisanymi źródłami uwierzytelnienia `CERB` i `Radius`. Grupa A, mapowana

jest w drugiej kolejności, na połączenie `Sejf SSH` i ma przypisane źródło uwierzytelnienia `AD`.



Wheel Fudo PAM uwierzytelniając użytkownika będzie wysyłać zapytania do zewnętrznych źródeł uwierzytelniania w następującej kolejności:

1. CERB.
2. Radius.
3. AD.

---

23. Kliknij *Zapisz*.

Informacja: Opcja *Wymuś pełną synchronizację* pozwala na przetworzenie zmian po stronie serwera usług katalogowych, które nie są odwzorowywane w procesie okresowej synchronizacji, tj. usunięcie zdefiniowanej grupy, lub usunięcie obiektu użytkownika.

Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00.

Informacja: Wheel Fudo PAM wspiera zagnieżdżone grupy LDAP.

Tematy pokrewne:

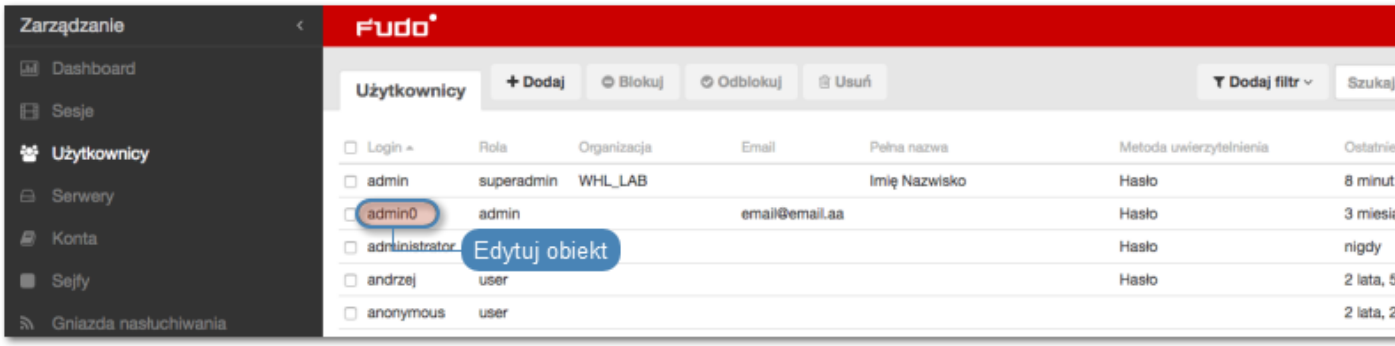
- *Uwierzytelnienie użytkowników w katalogu LDAP*
- *Zarządzanie użytkownikami*
- *Zarządzanie serwerami*
- *Sejfy*

5.9 Dodawanie urządzenia mobilnego

Urządzenie mobilne umożliwia akceptowanie/odrzucanie połączeń oczekujących, wymagających autoryzacji przez administratora.

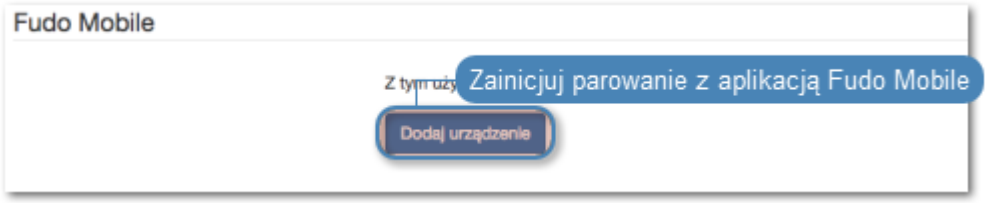
Informacja: Przed dodaniem urządzenia należy skonfigurować usługę proxy. Więcej na temat konfigurowania proxy dla mechanizmu uwierzytelnienia 4-Eyes, znajdziesz w rozdziale *Konfiguracja serwerów proxy*.

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM, na konto użytkownika, któremu chcesz dodać urządzenie mobilne.
2. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
3. Odszukaj na liście i kliknij definicję użytkownika.



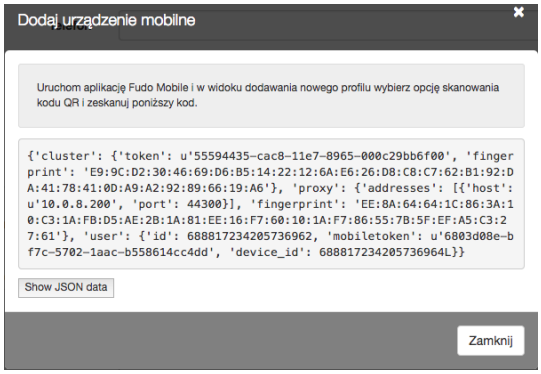
Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

4. W sekcji *Fudo Mobile*, kliknij *Dodaj urządzenie*.



5. Uruchom aplikację *Fudo Mobile*.
6. W prawym górnym rogu ekranu wybierz *+*, aby stworzyć profil.
7. Wybierz opcję *Skanuj* i zeskanuj wyświetlony kod QR.

Informacja: Alternatywnie, kliknij *Pokaż dane w formacie JSON*, w widoku dodawania profilu wybierz *Wklej* i wklej ciąg znaków definiujący profil.



8. Nadaj profilowi nazwę i wybierz *Zapisz*.
9. Kliknij *OK*, aby ukryć okno z kodem QR.
10. Kliknij *Zapisz*.

Tematy pokrewne:

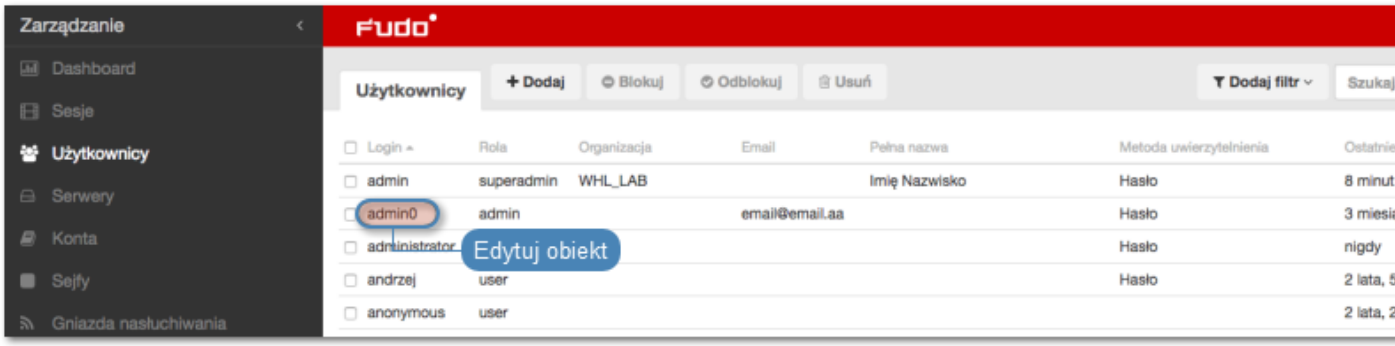
- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja serwerów proxy*
- *Usuwanie powiązanego urządzenia mobilnego*
- *Dodawanie użytkownika*
- *Model danych*

5.10 Usuwanie powiązanego urządzenia mobilnego

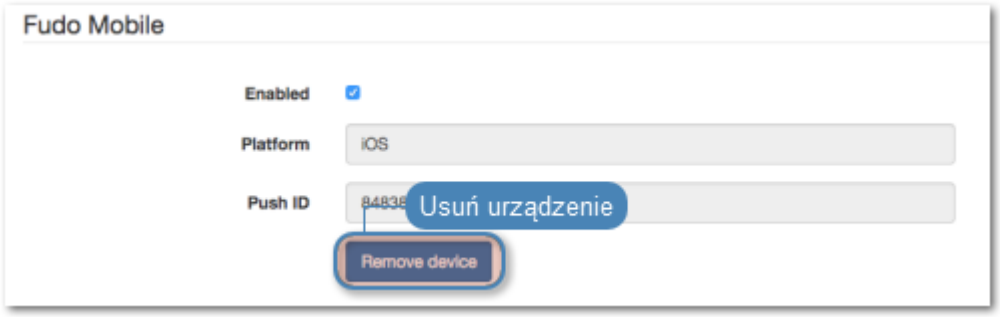
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście definicję konta, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę konta.



4. W sekcji *Fudo Mobile*, kliknij *Usuń urządzenie*.



5. Potwierdź usunięcie urządzenia.
6. Kliknij *Zapisz*.

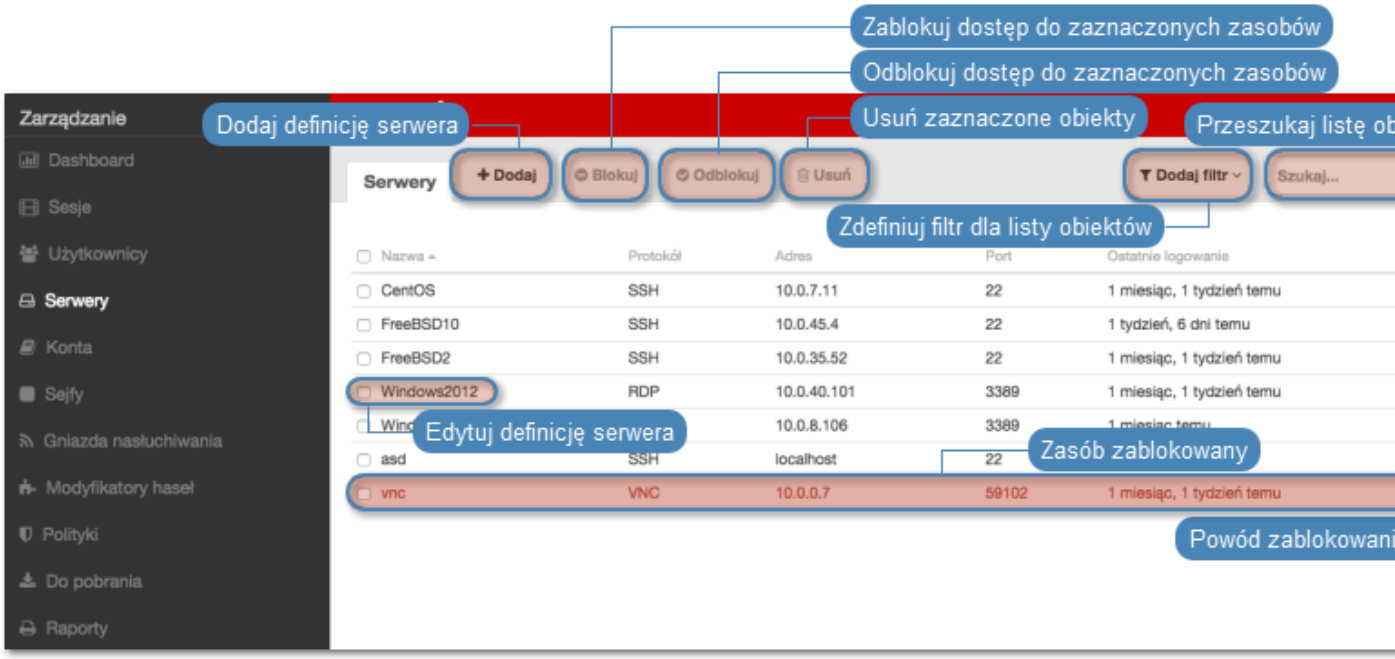
Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja serwerów proxy*
- *Dodawanie urządzenia mobilnego*
- *Dodawanie użytkownika*

ROZDZIAŁ 6

Serwery

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.



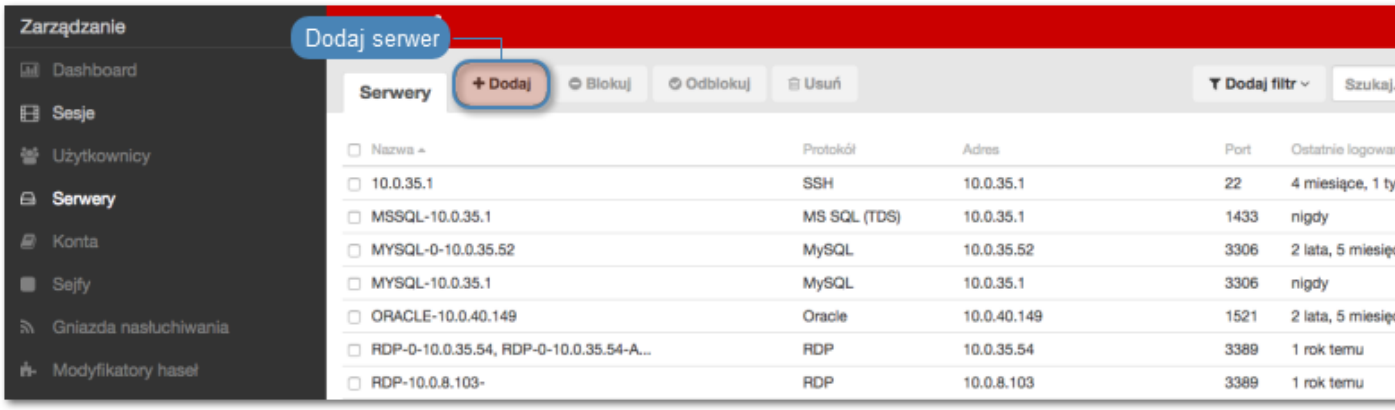
6.1 Dodawanie serwera

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

6.1.1 Serwery statyczne

6.1.1.1 Dodawanie serwera Citrix

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



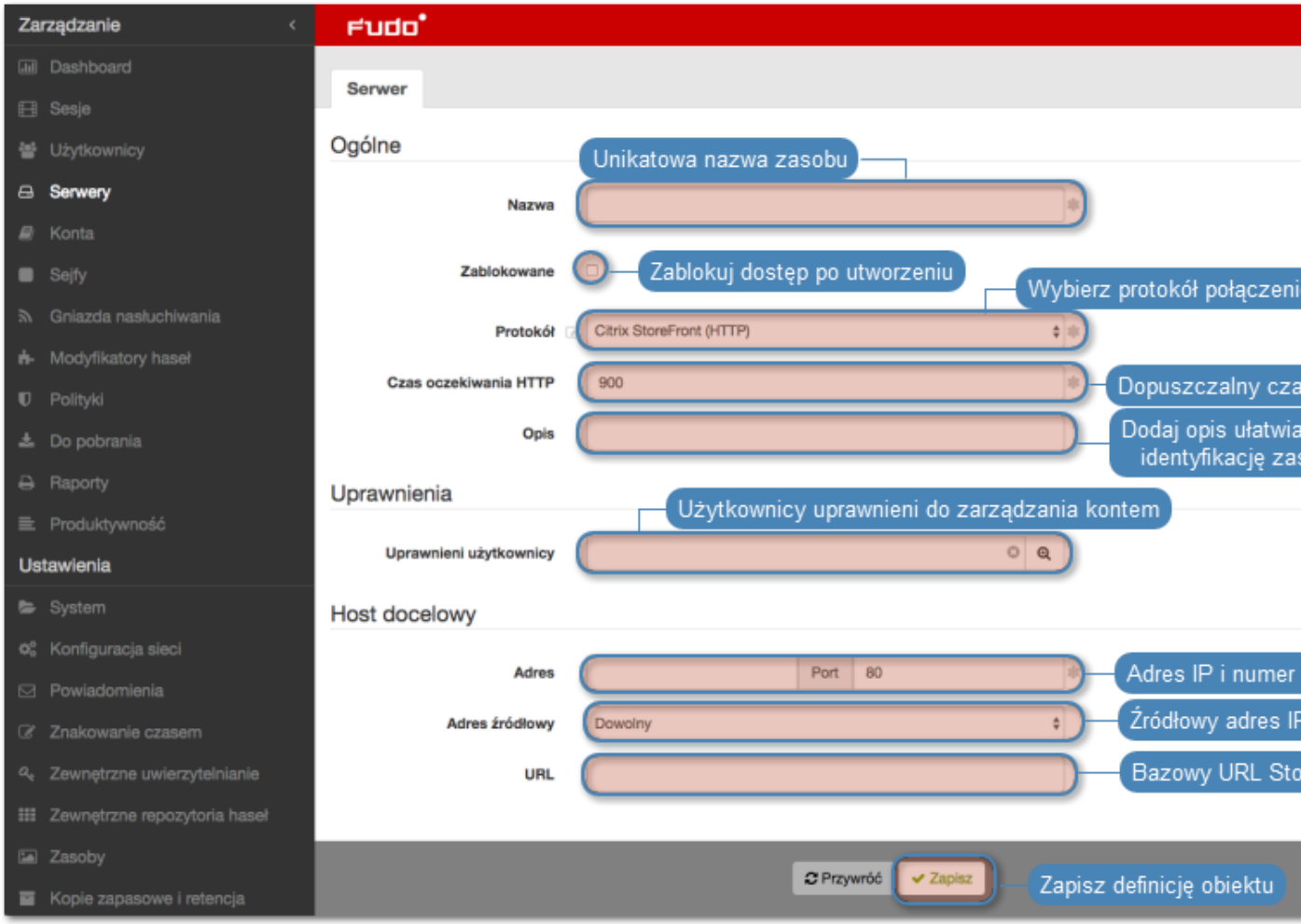
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Citrix StoreFront (HTTP)`.
6. Wprowadź wartość parametru *Czas oczekiwania HTTP* - wyrażony w sekundach czas bezczynności, po upłynięciu którego, połączenie będzie wymagało ponownego uwierzytelnienia.
7. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu połączeń HTTP.
10. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

11. W polu *URL* wprowadź bazowy URL Citrix StoreFront.
12. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Dodawanie gniazda nasłuchiwania Citrix*
- *Citrix StoreFront*
- *Plik konfiguracyjny połączenia ICA*

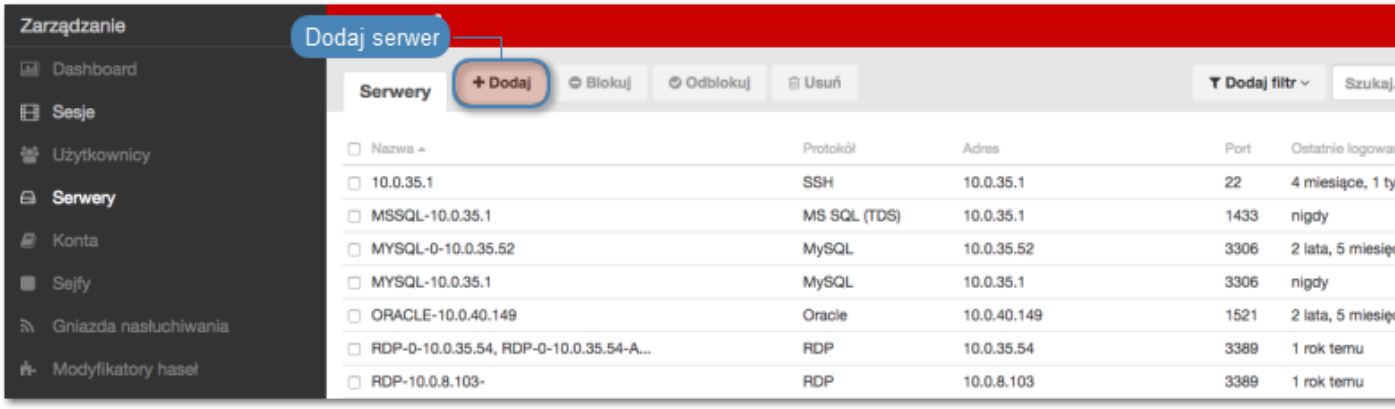
6.1.1.2 Dodawanie serwera HTTP

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.



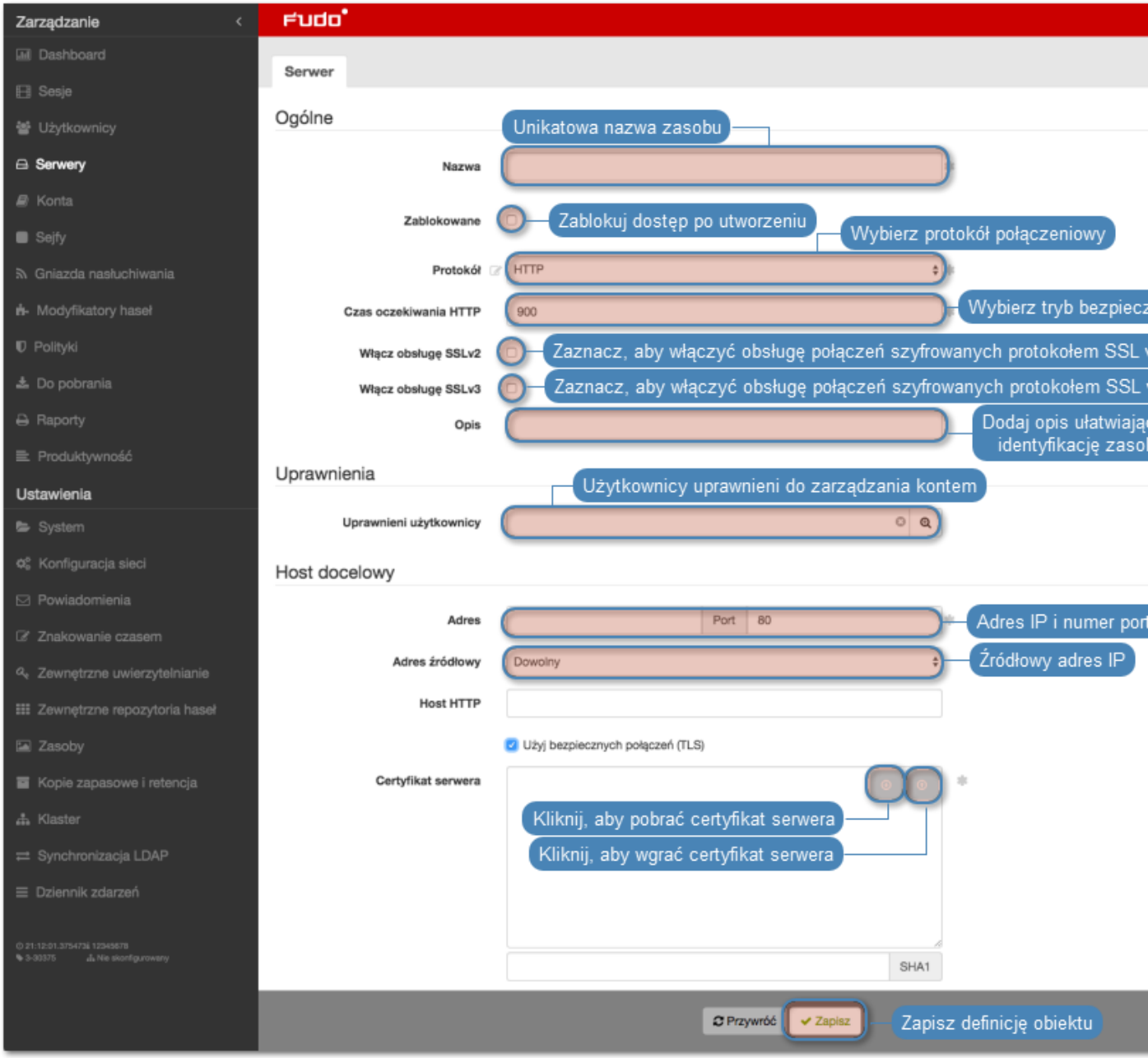
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `HTTP`.
6. Wprowadź wartość parametru *Czas oczekiwania HTTP* - wyrażony w sekundach czas bezczynności, po upłynięciu którego, połączenie będzie wymagało ponownego uwierzytelnienia.
7. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
8. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
9. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
10. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
11. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu połączeń HTTP.
12. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

13. W polu *Host HTTP* wprowadź ścieżkę zasobu na serwerze, który ma podlegać monitorowaniu.
14. Opcjonalnie, zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*.
15. Kliknij ikonę wgrywania, aby wgrać certyfikat serwera, lub ikonę pobierania, aby pobrać certyfikat hosta.
16. Kliknij *Zapisz*.

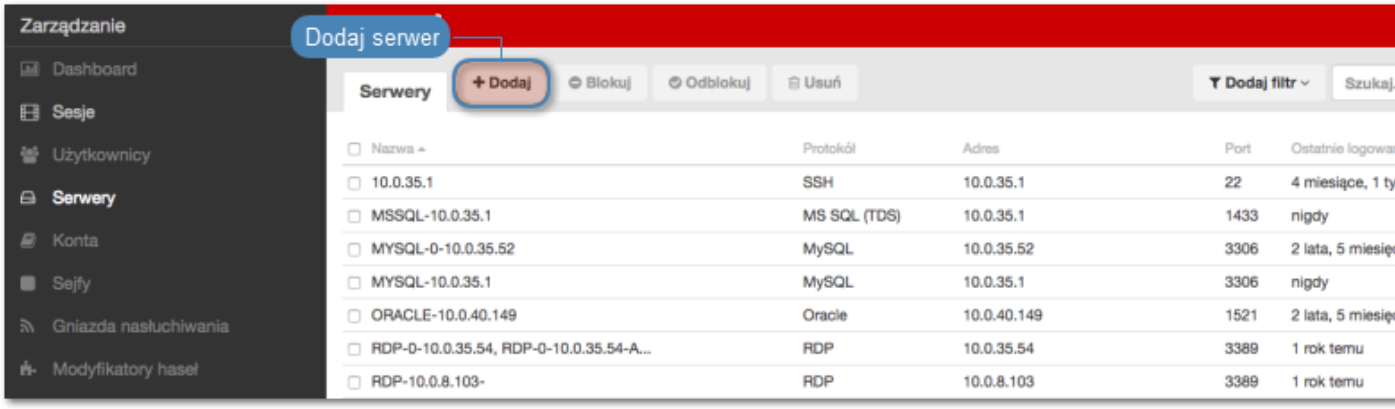


Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.3 Dodawanie serwera ICA

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



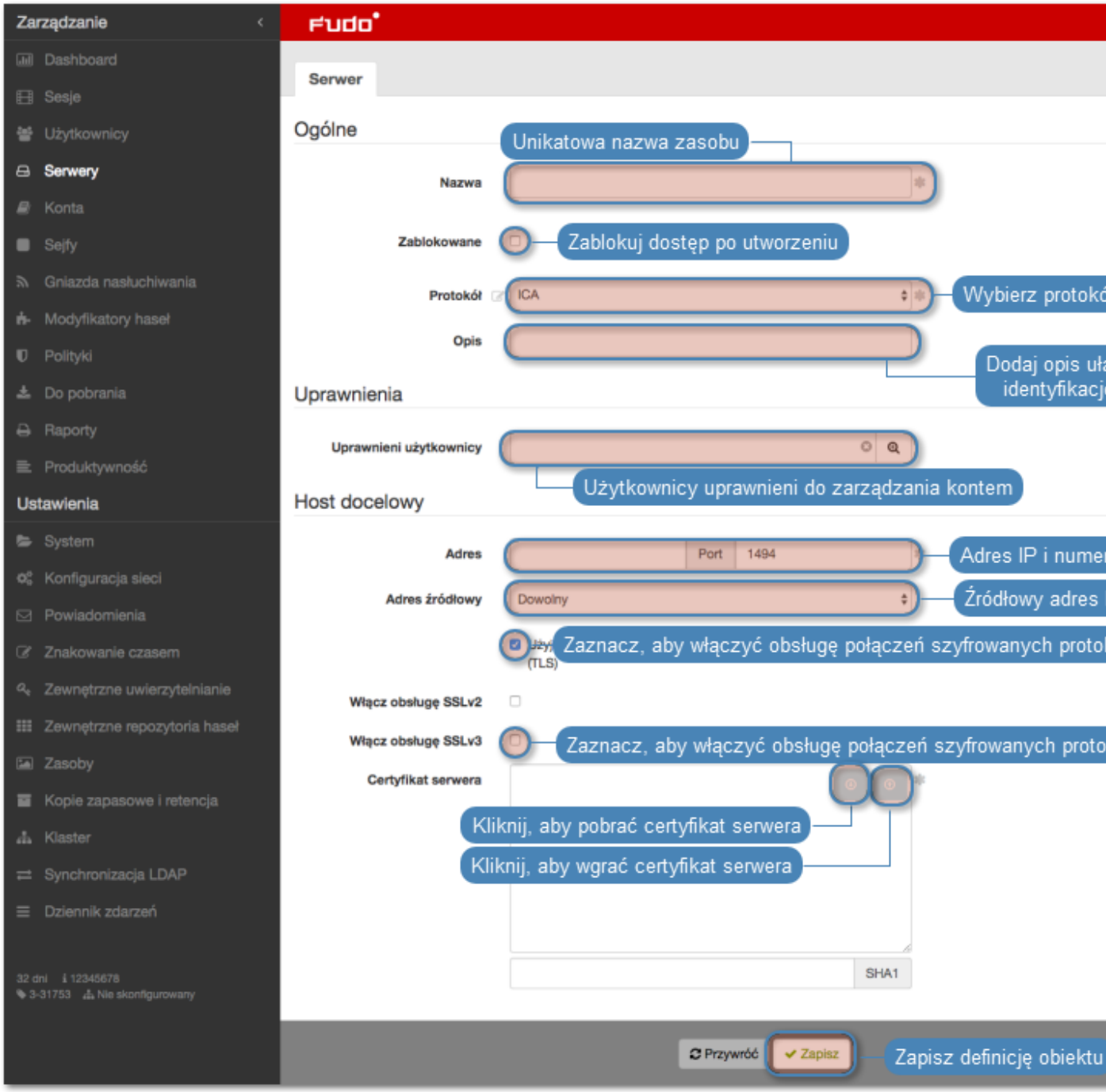
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `ICA`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Opcjonalnie, zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*.
11. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
12. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
13. Kliknij ikonę wgrywania, aby wgrać certyfikat serwera, lub ikonę pobierania, aby pobrać certyfikat hosta.
14. Kliknij *Zapisz*.



Tematy pokrewne:

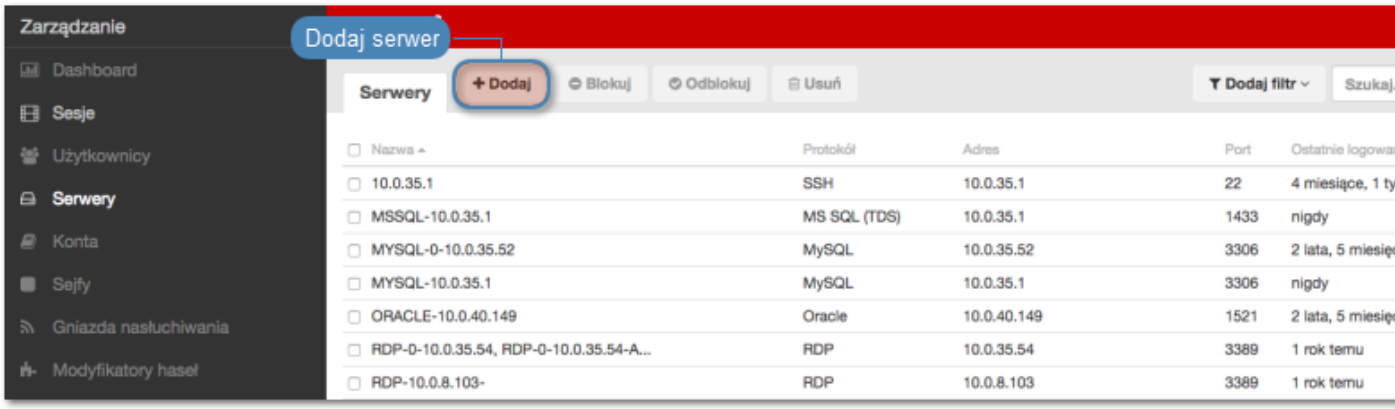
- *Protokół ICA*
- *Model danych*
- *Dodawanie gniazda nasłuchiwania ICA*
- *Plik konfiguracyjny połączenia ICA*
- *Szybki start - ICA*

6.1.1.4 Dodawanie serwera Modbus

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.

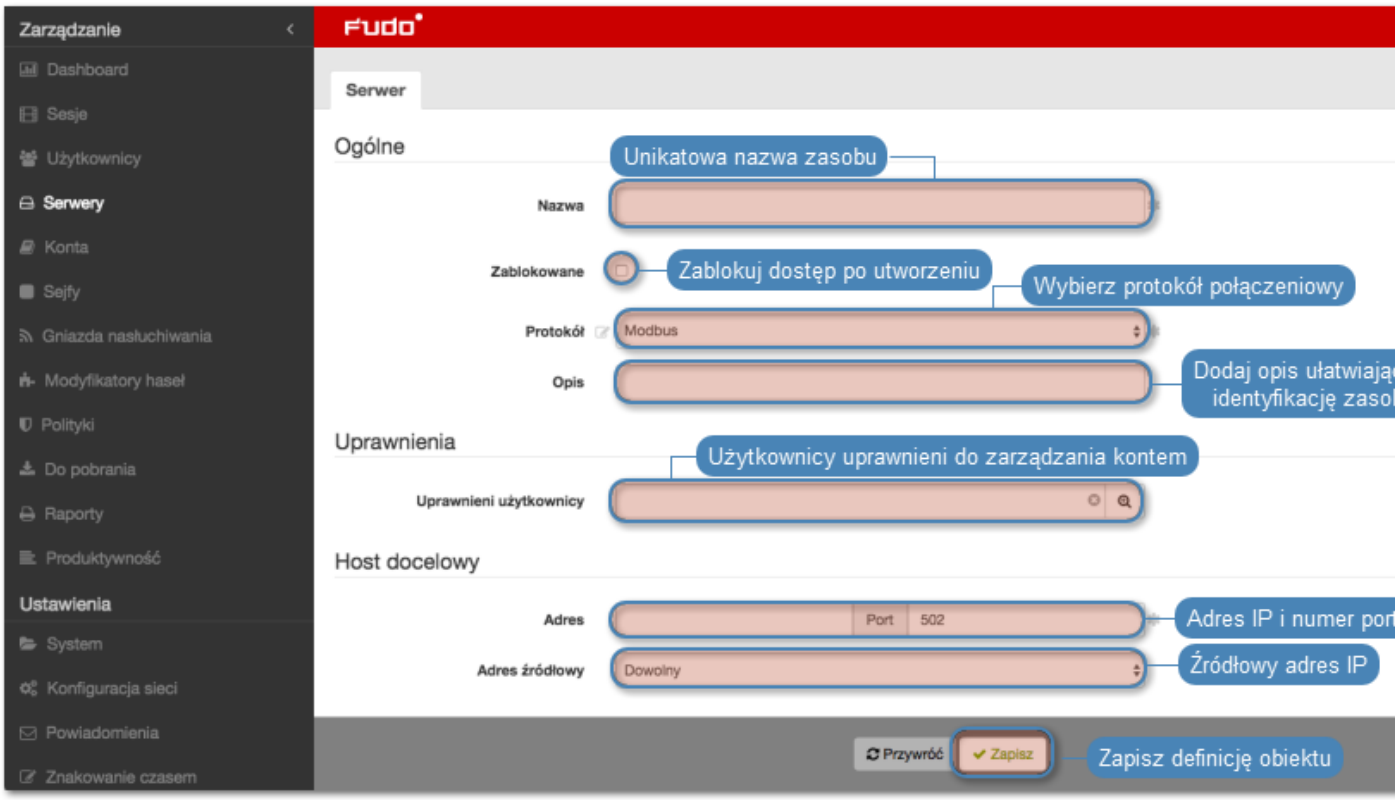


3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Modbus`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

10. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

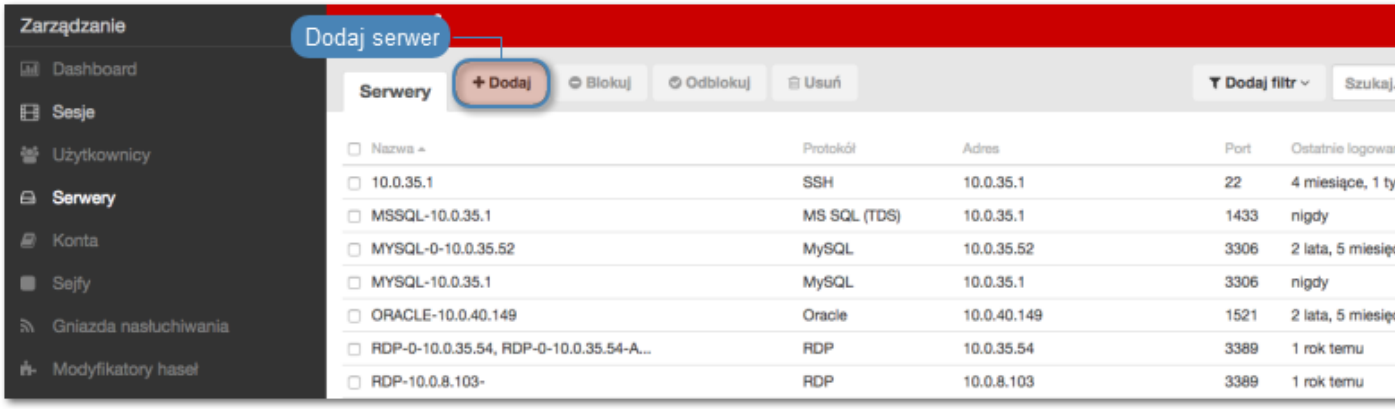
6.1.1.5 Dodawanie serwera MS SQL

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



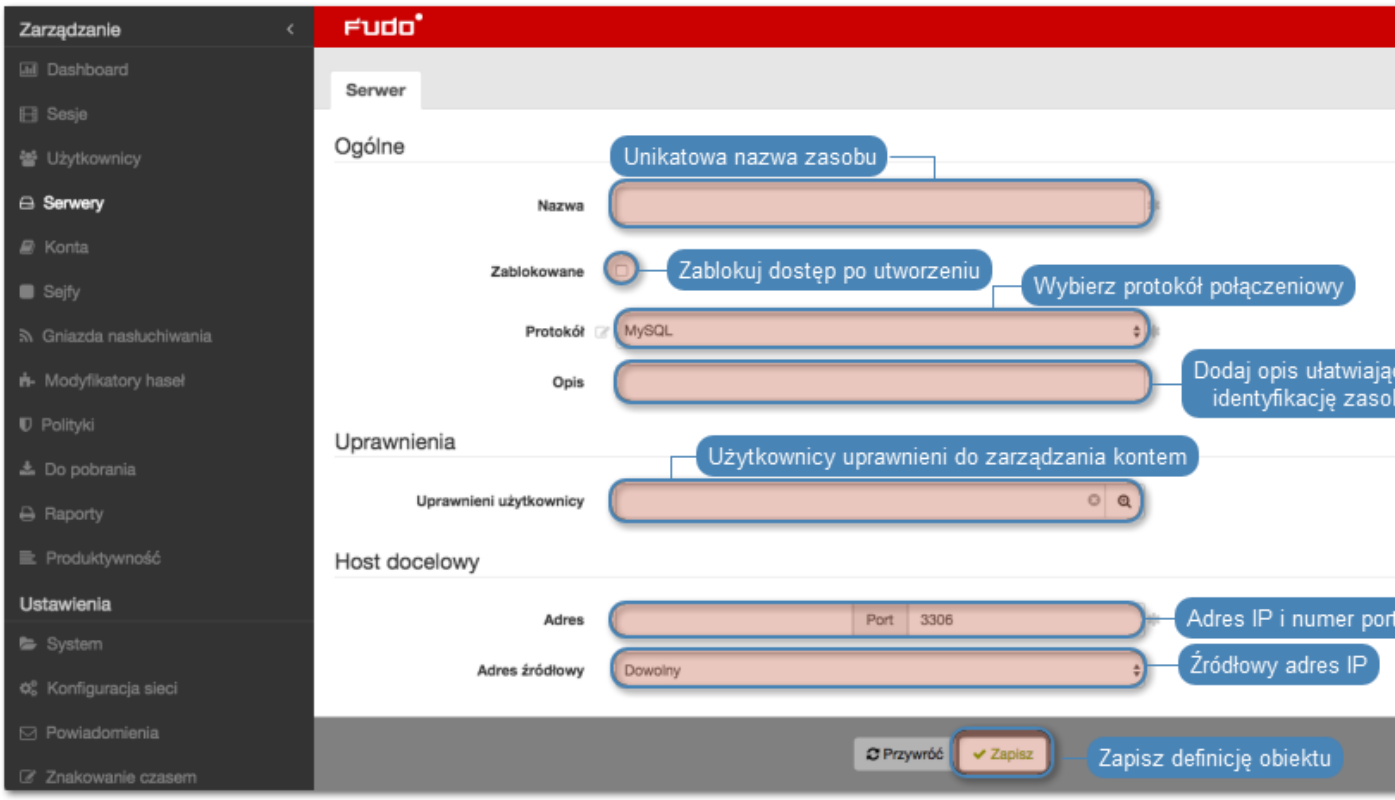
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `MS SQL (TDS)`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

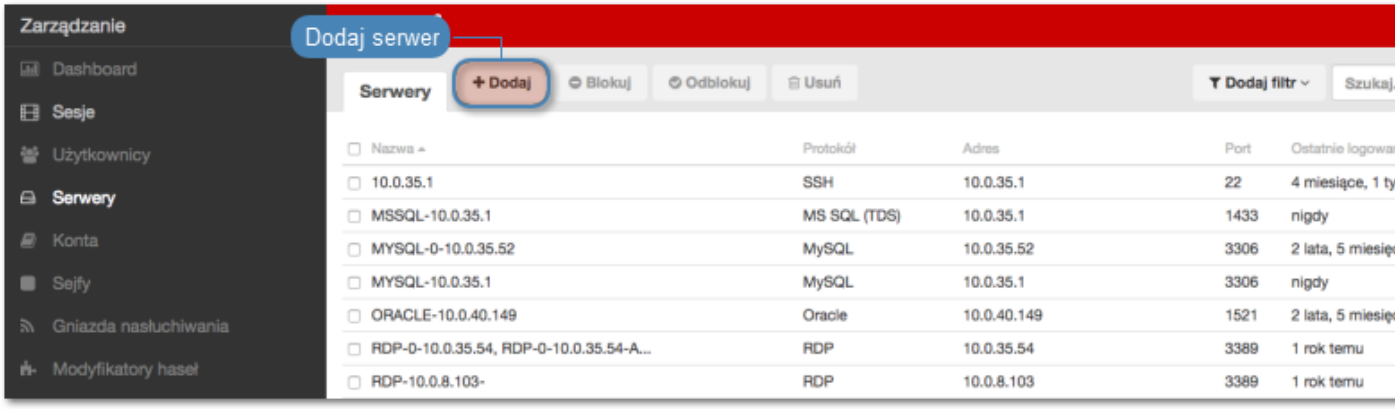
6.1.1.6 Dodawanie serwera MySQL

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



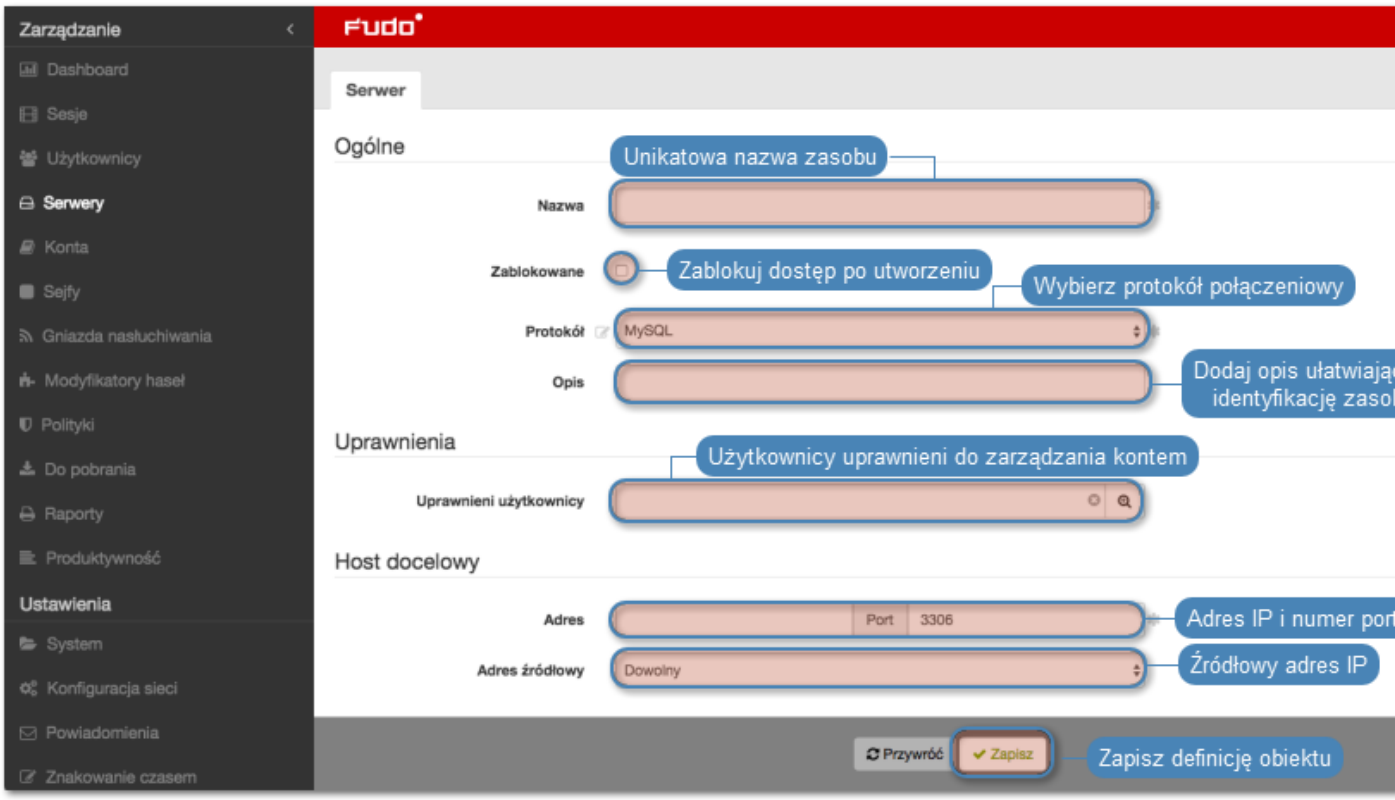
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `MySQL`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

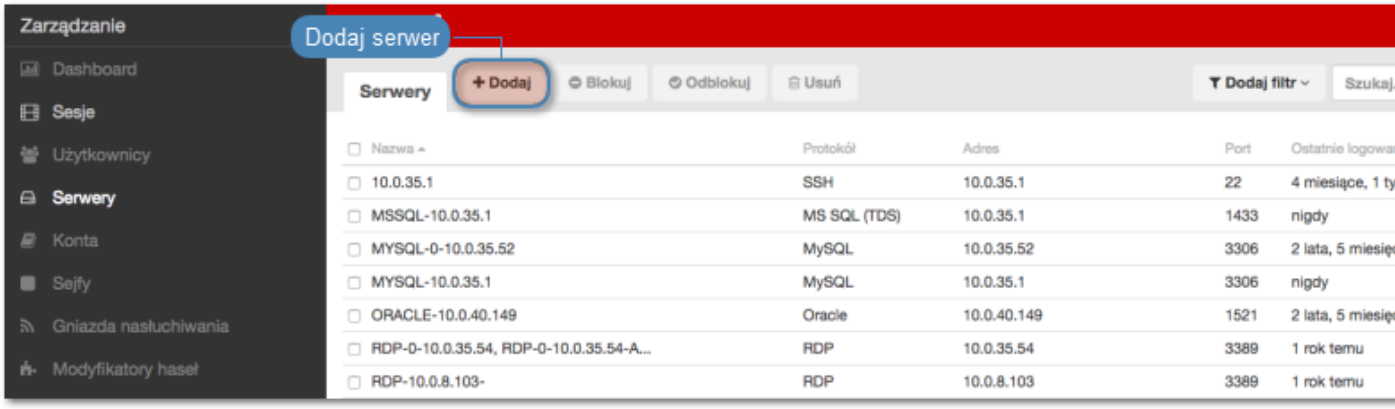
6.1.1.7 Dodawanie serwera Oracle

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



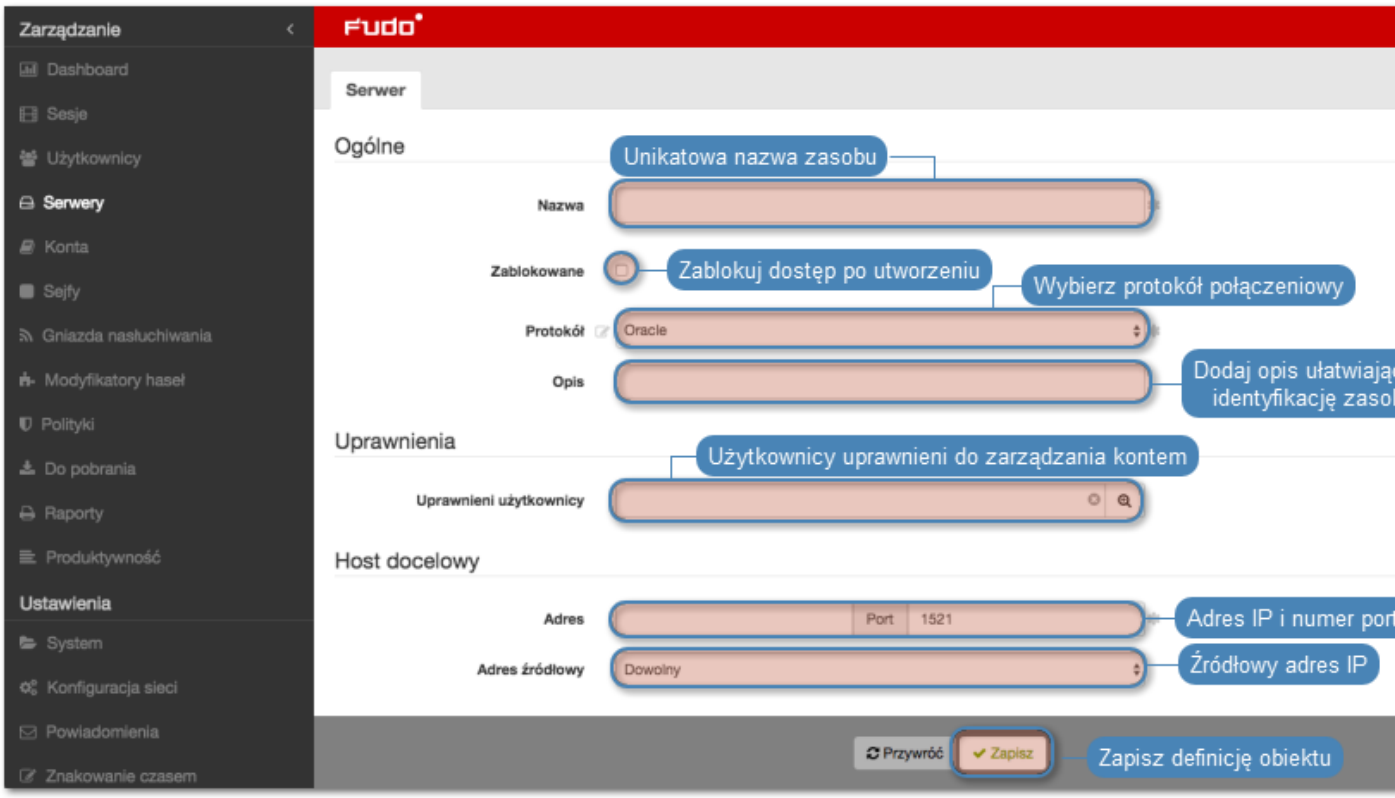
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Oracle`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

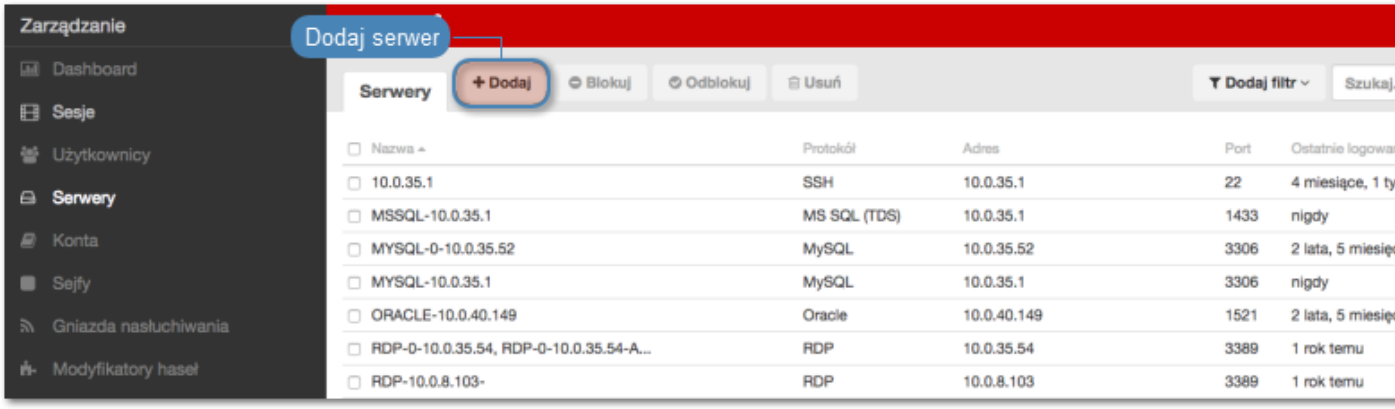
6.1.1.8 Dodawanie serwera RDP

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



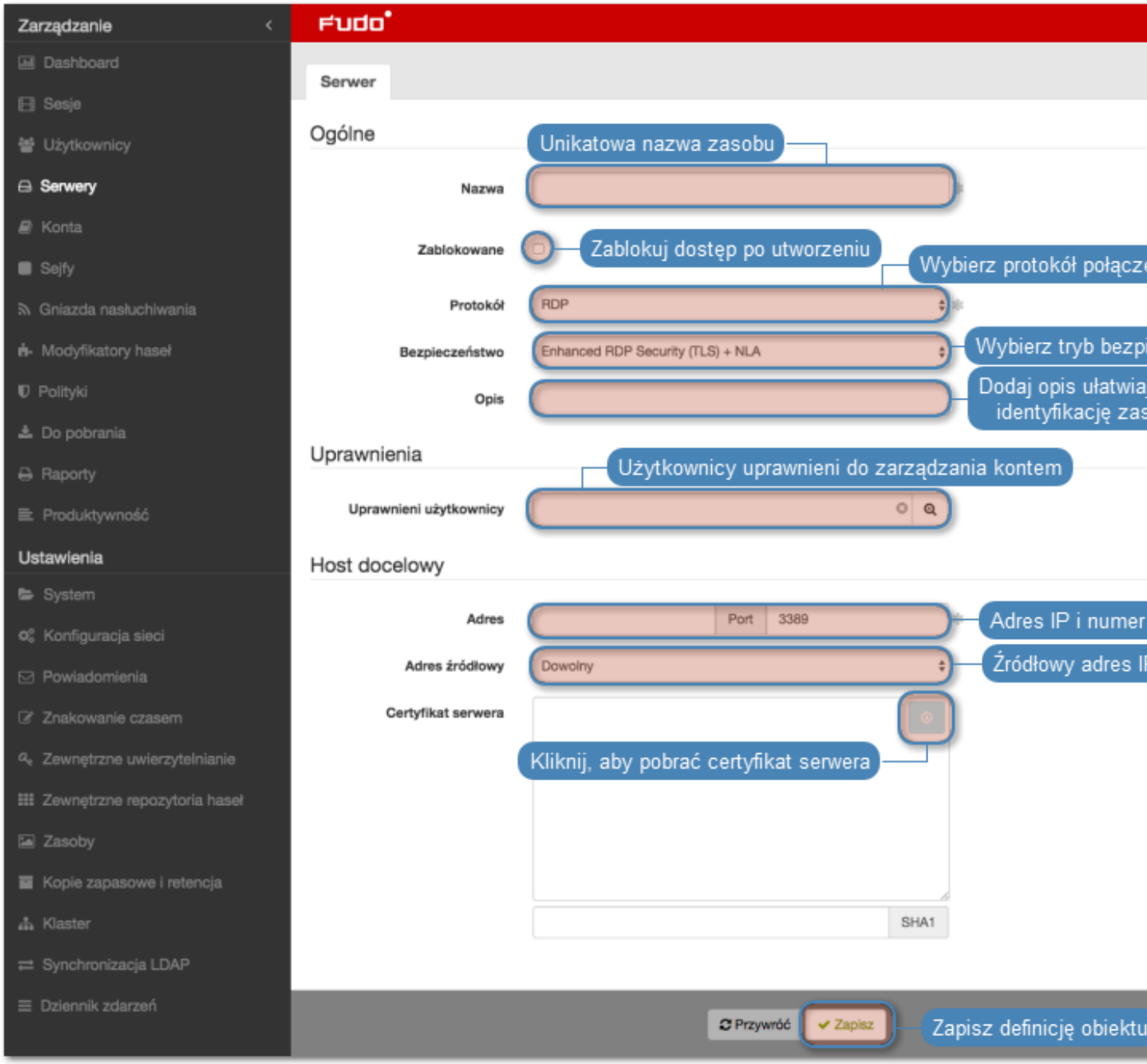
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `RDP`.
6. Z listy rozwijalnej *Bezpieczeństwo*, wybierz tryb bezpieczeństwa prodokołu RDP.
7. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu połączeń RDP.
10. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Kliknij ikonę pobierania, aby pobrać certyfikat serwera.
11. Kliknij *Zapisz*.



Tematy pokrewne:

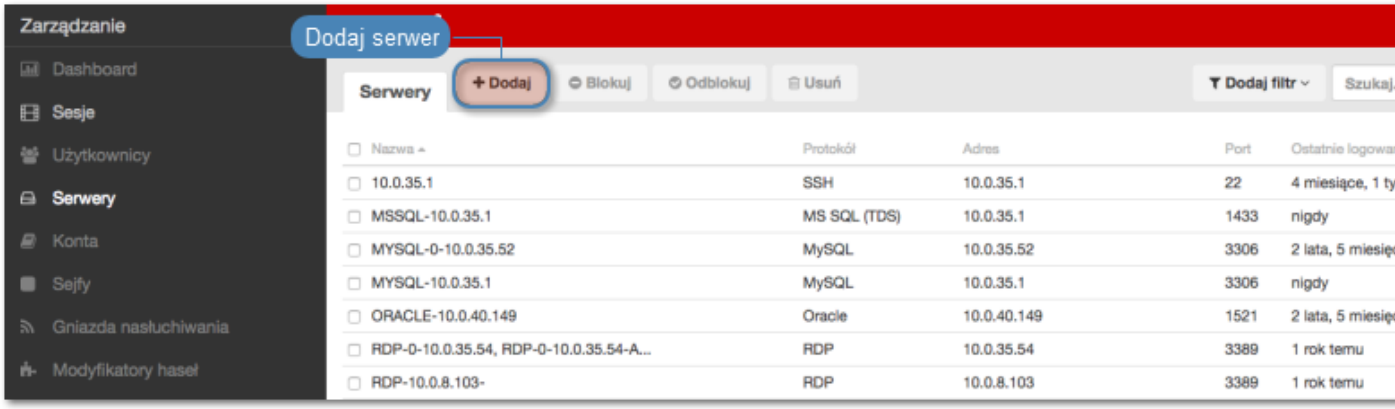
- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.9 Dodawanie serwera SSH

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.

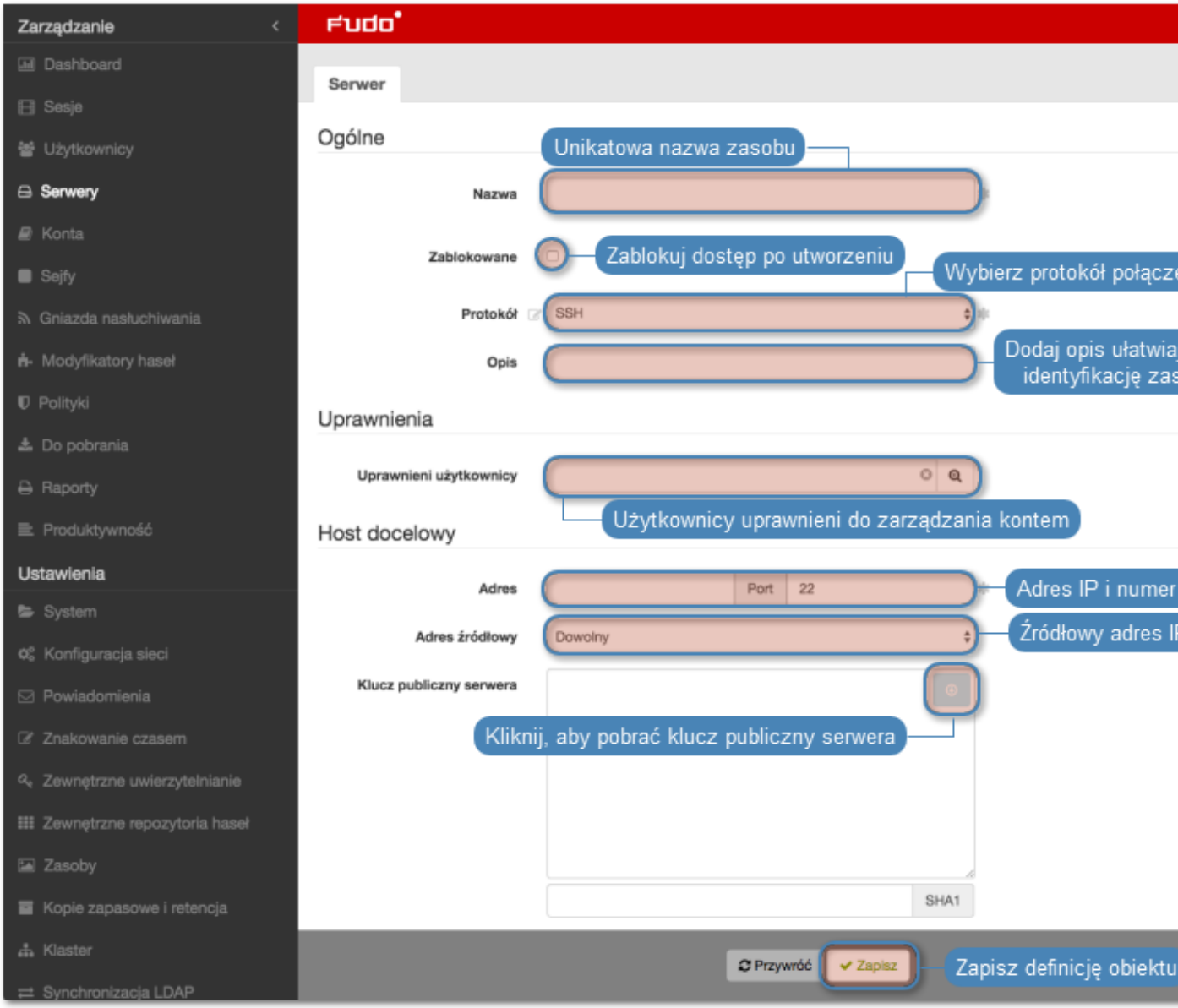


3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `SSH`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera i numer portu, na którym nasłuchuje usługa SSH.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

10. Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
11. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.10 Dodawanie serwera Telnet

Dodawanie definicji serwera

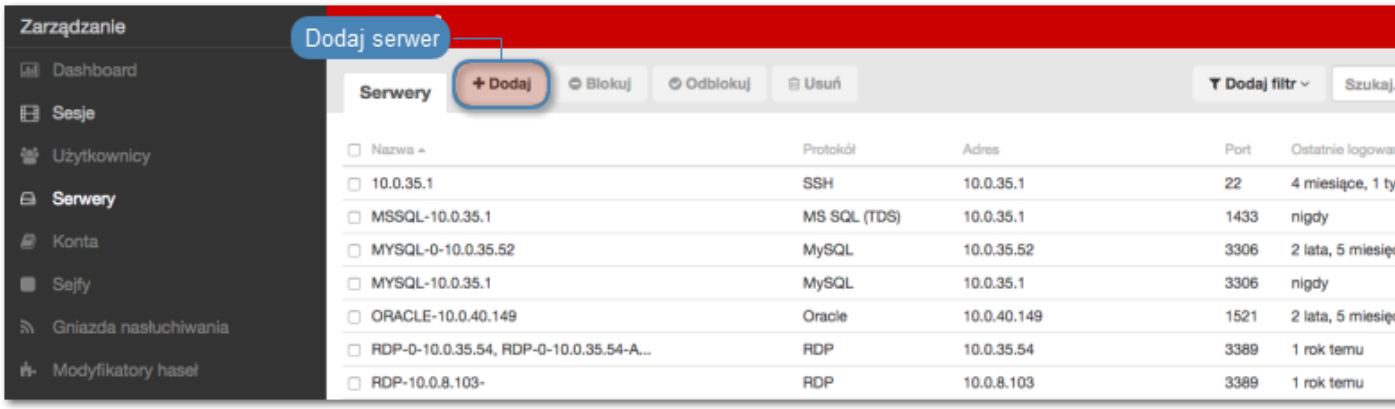
Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.

- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Wheel Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

---

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.



3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Telnet`.
6. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
7. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
8. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
11. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

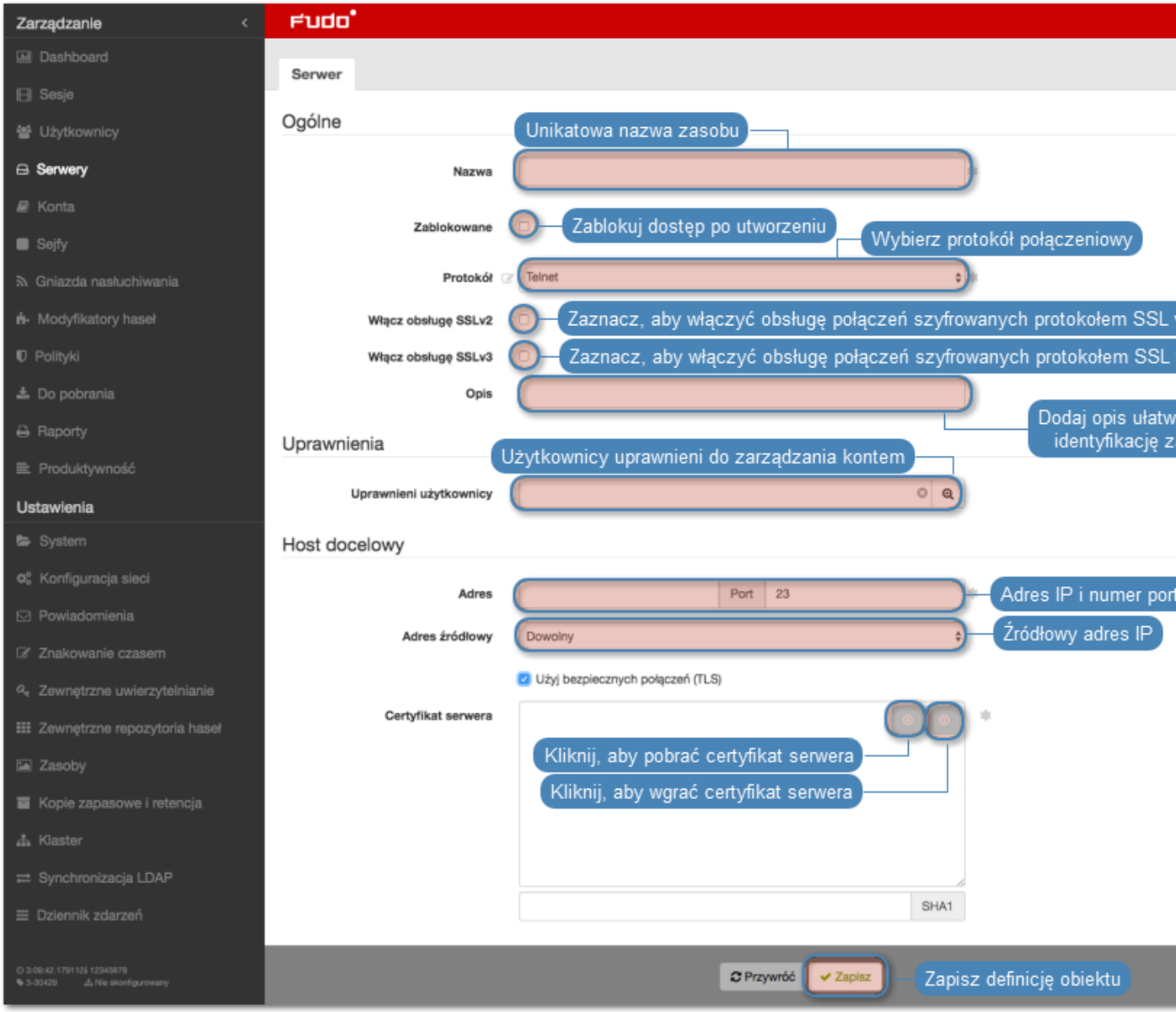
Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

12. Opcjonalnie, zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*.

13. Kliknij ikonę wgrywania, aby wgrać certyfikat serwera, lub ikonę pobierania, aby pobrać certyfikat hosta.
14. Kliknij *Zapisz*.



Tematy pokrewne:

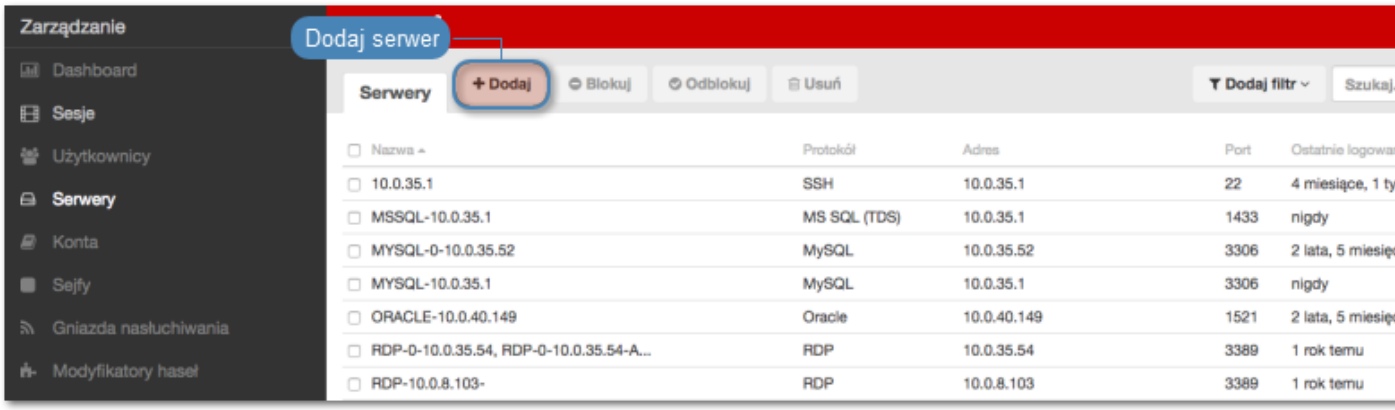
- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.11 Dodawanie serwera Telnet 3270

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Wheel Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.

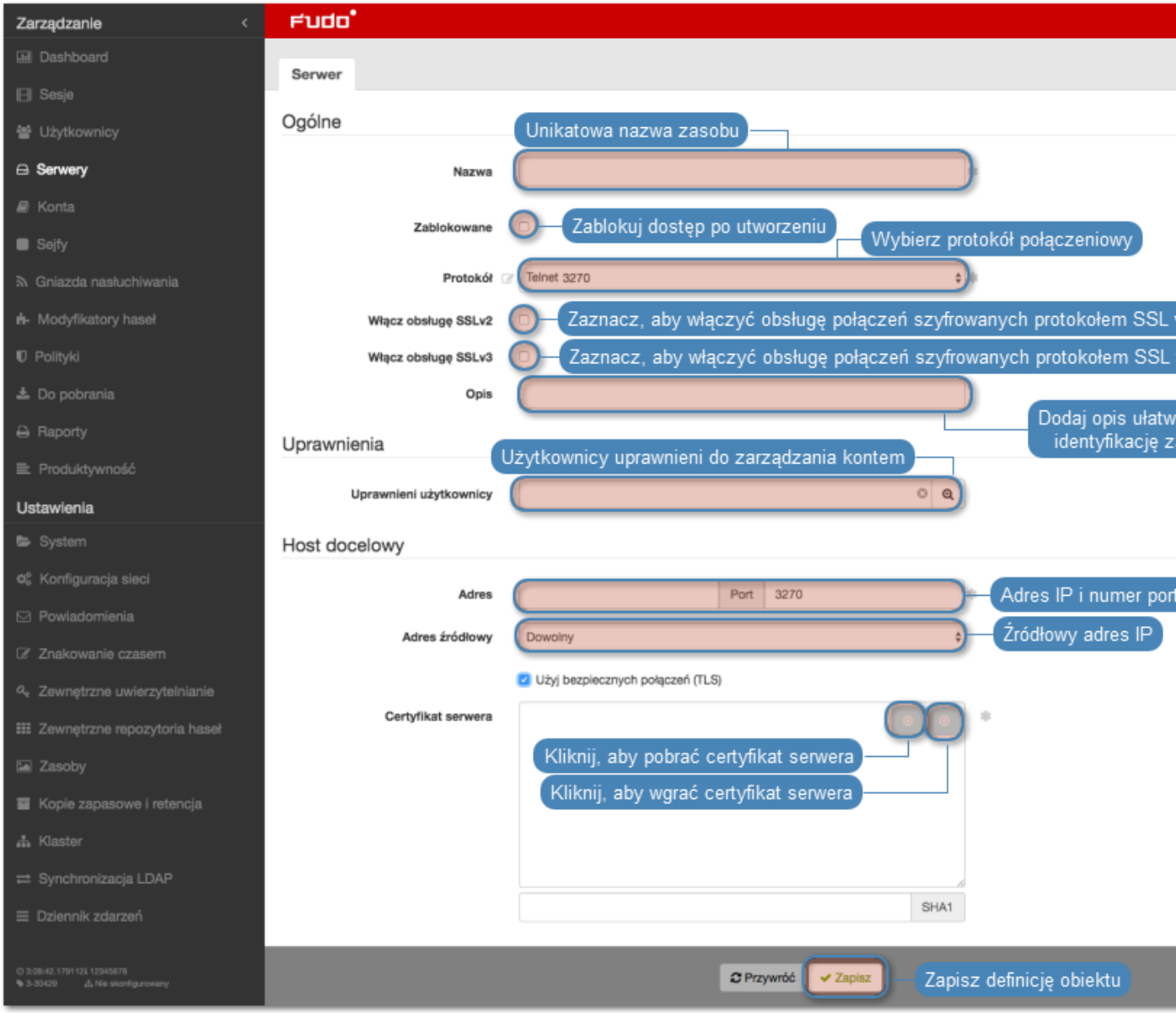


3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Telnet 3270`.
6. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
7. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
8. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
11. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

12. Opcjonalnie, zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*.
13. Kliknij ikonę wgrywania, aby wgrać certyfikat serwera, lub ikonę pobierania, aby pobrać certyfikat hosta.
14. Kliknij *Zapisz*.



Tematy pokrewne:

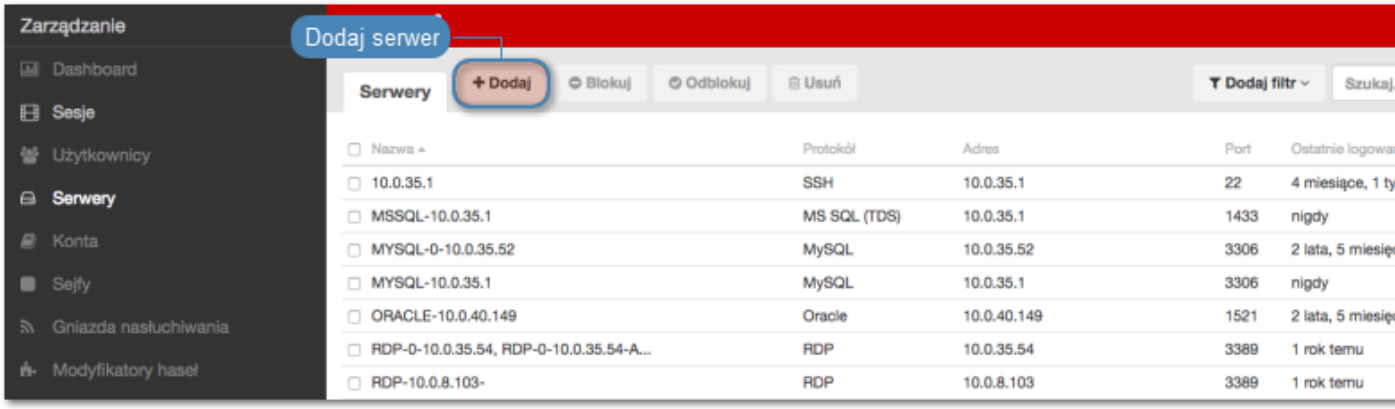
- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.12 Dodawanie serwera Telnet 5250

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Wheel Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `Telnet 5250`.
6. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
7. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
8. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
11. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.

- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

12. Opcjonalnie, zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*.
13. Kliknij ikonę wgrywania, aby wgrać certyfikat serwera, lub ikonę pobierania, aby pobrać certyfikat hosta.
14. Kliknij *Zapisz*.

Tematy pokrewne:

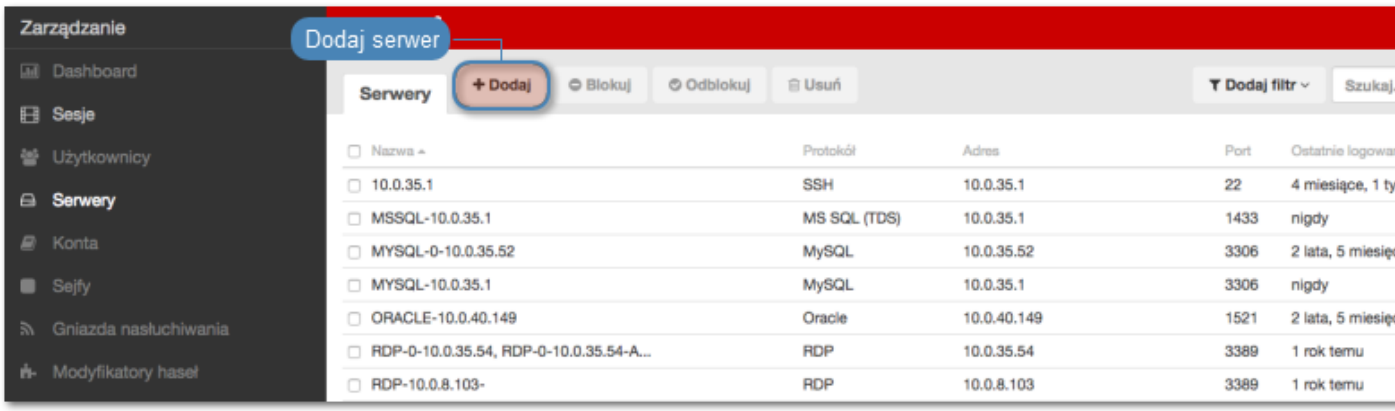
- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.1.1.13 Dodawanie serwera VNC

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `VNC`.
6. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.

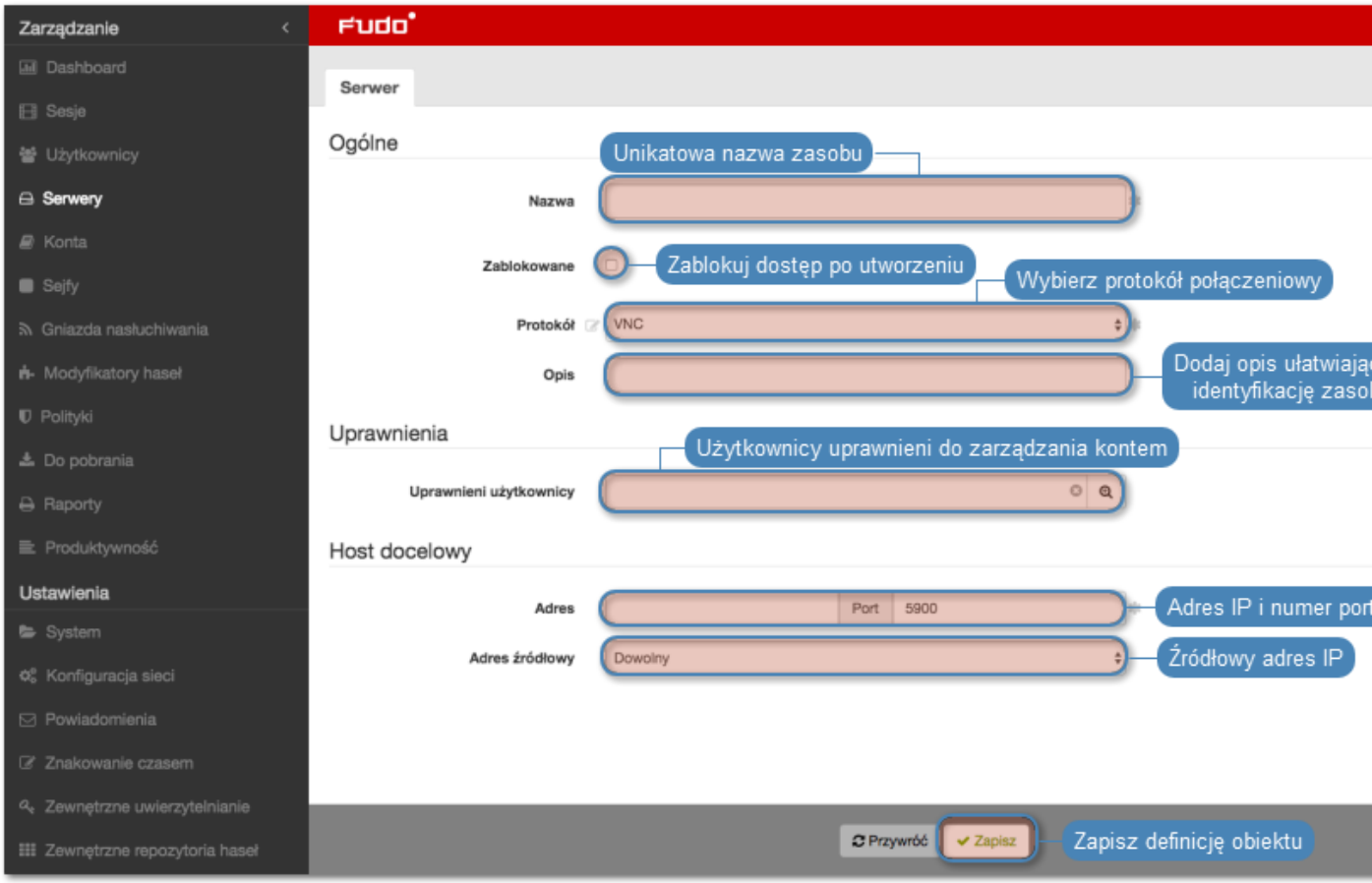
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Host docelowy*, wprowadź adres serwera oraz numer portu.
9. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

10. Kliknij *Zapisz*.



Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*

- *Sejfy*
- *Konta*

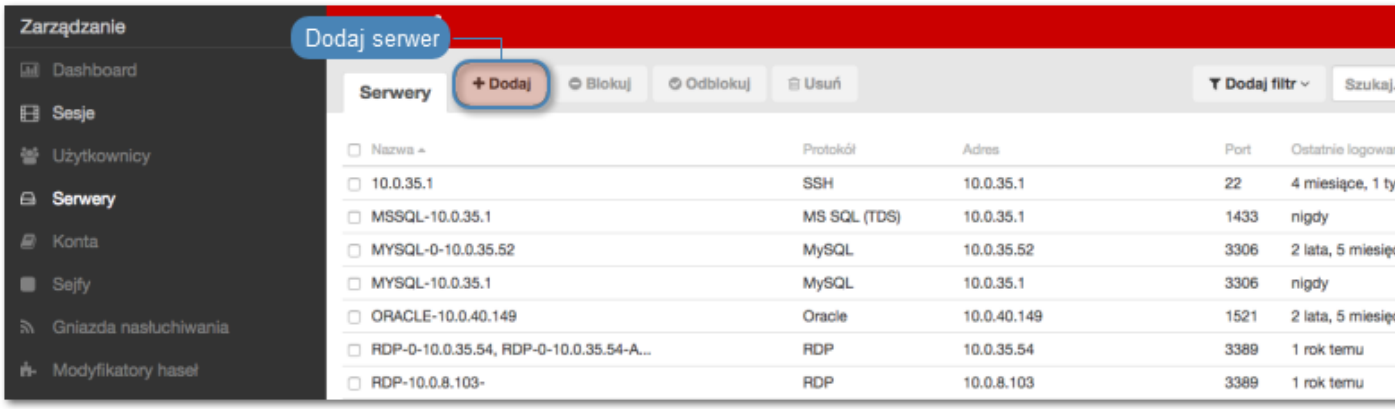
6.1.2 Serwery dynamiczne

Wheel Fudo PAM umożliwia zdefiniowanie grupy serwerów w postaci podsieci, w której znajdują się maszyny docelowe. Z chwilą gdy użytkownik dokonuje próby nawiązania połączenia z systemem znajdującym się w wybranej podsieci, Wheel Fudo PAM dokona sprawdzenia czy dany podmiot ma stosowne prawa dostępu, automatycznie doda definicję serwera w ramach istniejącego obiektu, pobierze certyfikat serwera i zestawi monitorowane połączenie.

6.1.2.1 Definiowanie grupy serwerów

Aby dodać dynamiczną grupę serwerów, postępuj zgodnie z poniższą procedurą.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.



3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz protokół serwera i skonfiguruj parametry charakterystyczne dla wybranego typu.
6. W sekcji *Host docelowy*, wprowadź adres podsieci, maskę w notacji CIDR i numer portu.
7. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja: Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych*.

---

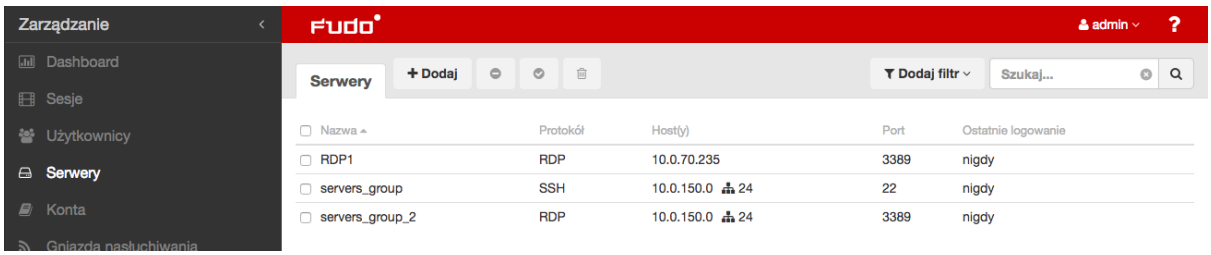
8. Uzupełnij pozostałe właściwości protokołu i kliknij *Zapisz*.

6.1.2.2 Definiowanie pojedynczego hosta w ramach grupy serwerów

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.

2. Odszukaj i kliknij definicję grupy dynamicznych serwerów.

Informacja: Obiekty grupujące serwery wyróżnione są ikoną .



3. Kliknij przycisk *+ Dodaj host*.
4. Wprowadź adres IP serwera.
5. Kliknij ikonę , aby pobrać klucz serwera.
6. Zdefiniuj dodatkowe parametry konfiguracji.
7. Kliknij *Zapisz*.

Tematy pokrewne:

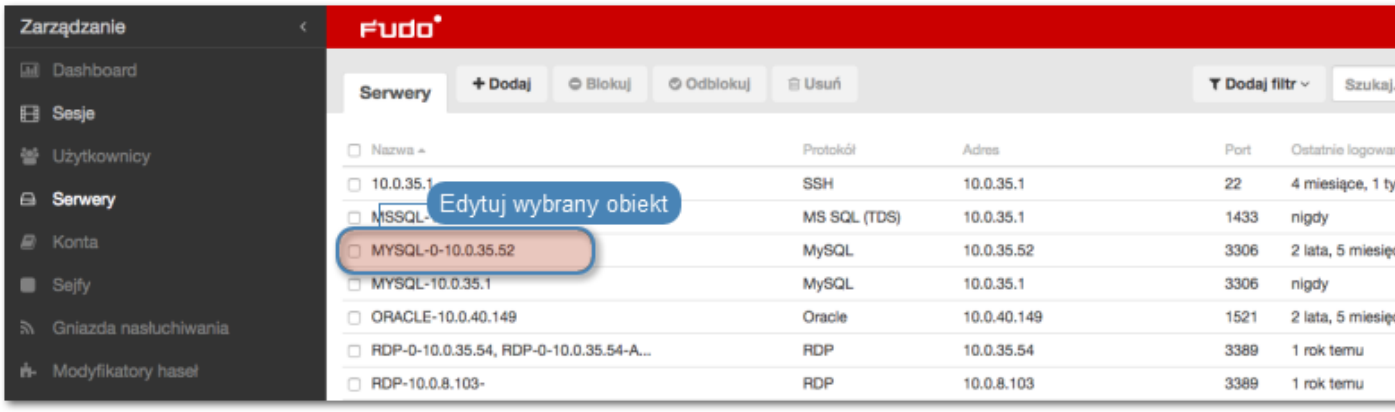
- *Model danych*
- *Serwery statyczne*

6.2 Modyfikowanie serwera

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście definicję obiektu, który chcesz edytować.

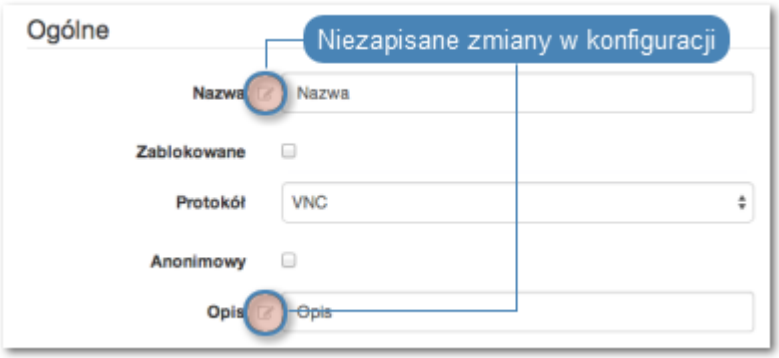
Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę obiektu.



4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną .



5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Dodawanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

6.3 Blokowanie serwera

Blokowanie i odblokowanie serwera

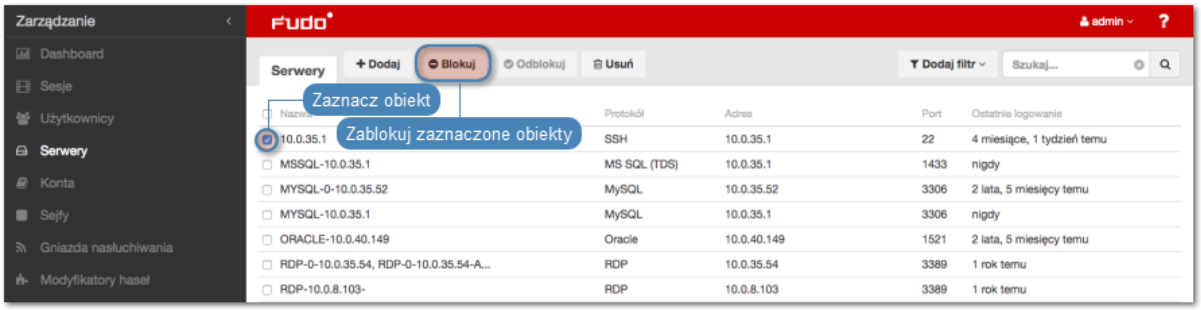
Wheel Fudo PAM pozwala na zablokowanie wszystkim użytkownikom możliwości nawiązywania połączeń z wybranym serwerem.

Ostrzeżenie: Zablokowanie serwera spowoduje zerwanie aktualnie trwających sesji połączeniowych z danym zasobem.

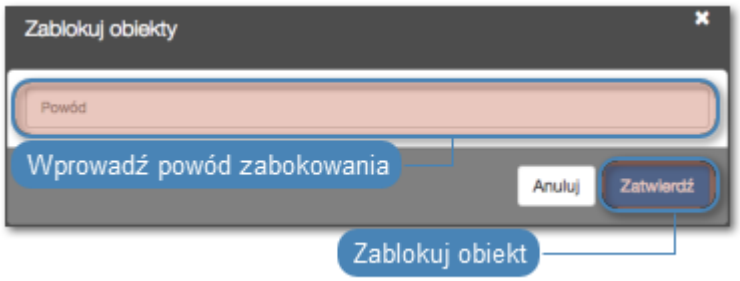
1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz serwer, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z wybranymi zasobami.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.



Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

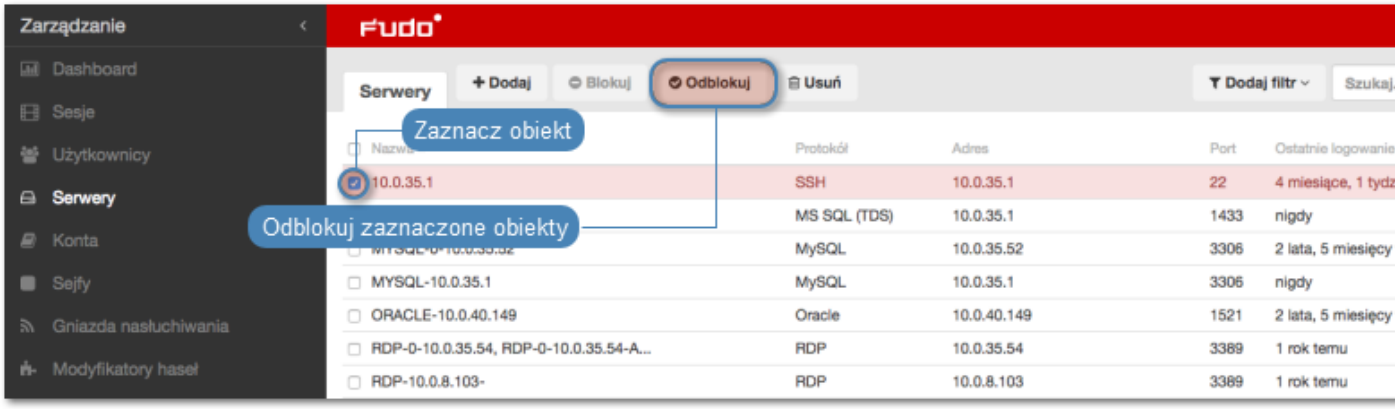
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

6.4 Odblokowanie serwera

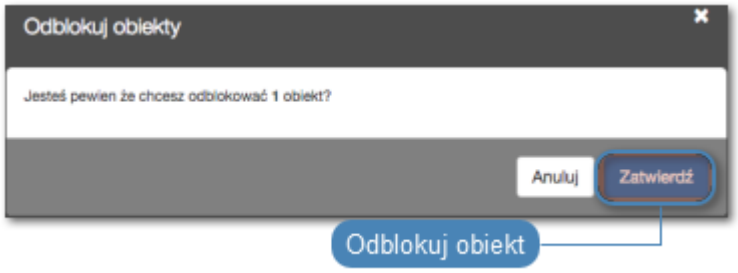
1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń z serwerami.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektów.



Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

6.5 Usuwanie serwera

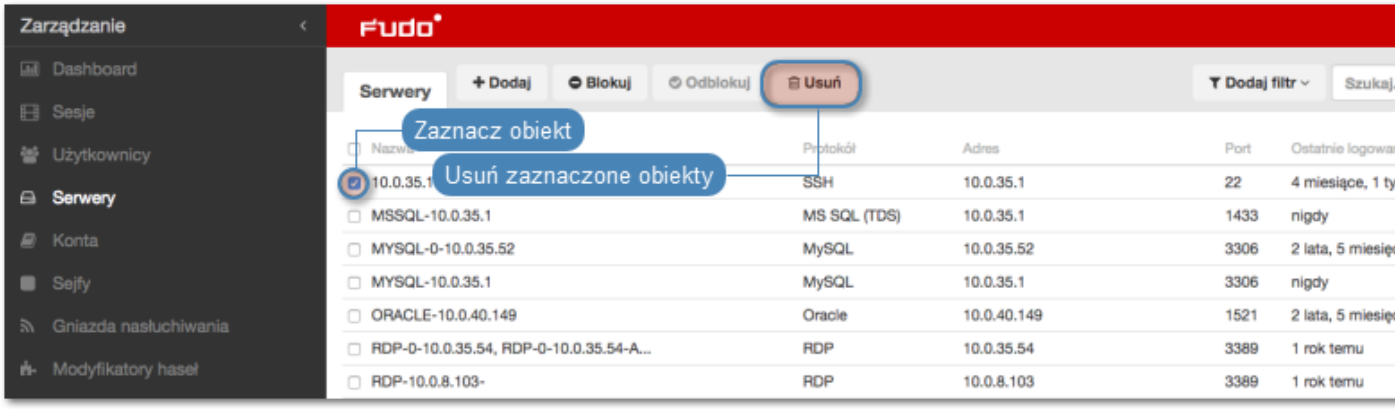
Ostrzeżenie: Usunięcie serwera spowoduje przerwanie aktualnie trwających sesji połączeniowych z danym zasobem.

6.5.1 Usuwanie definicji serwera

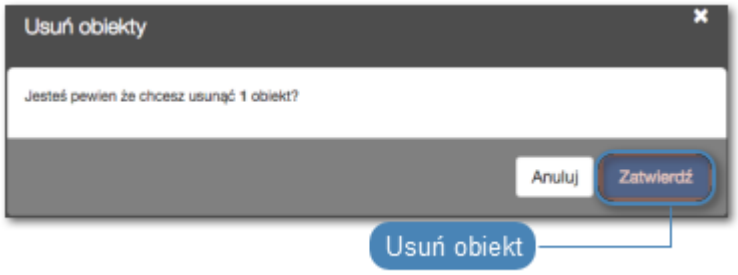
1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz serwer, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.

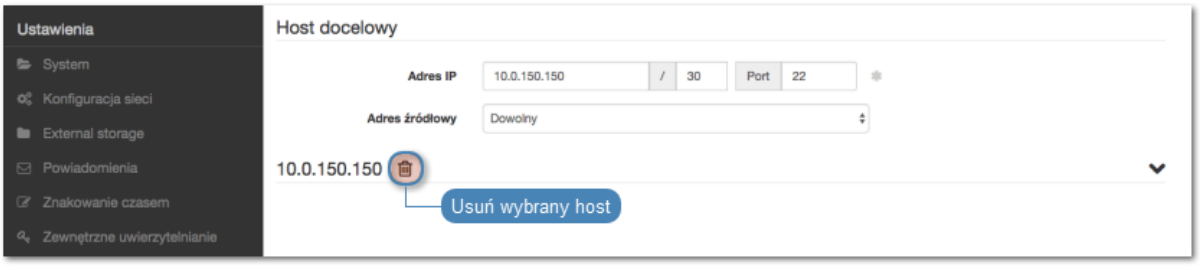


4. Potwierdź operację usunięcia zaznaczonych obiektów.



6.5.2 Usuwanie wybranego hosta z grupy serwerów dynamicznych

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i kliknij obiekt reprezentujący serwery dynamiczne.
3. W sekcji *Host docelowy* znajdź wybrany serwer i kliknij ikonę .



4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

ROZDZIAŁ 7

Konta

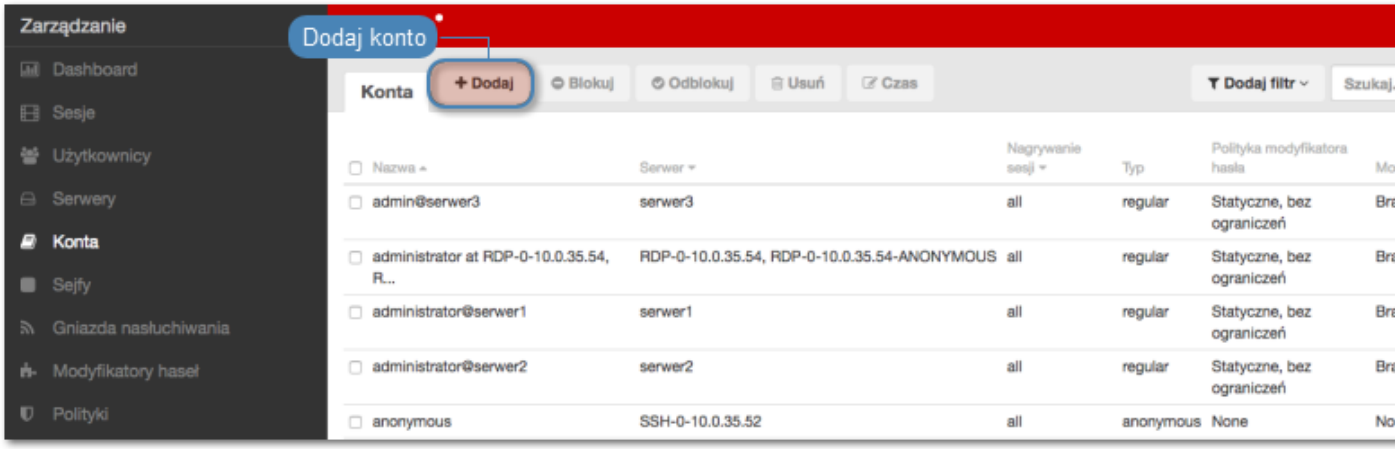
Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

7.1 Dodawanie konta

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

7.1.1 Dodawanie konta typu *anonymous*

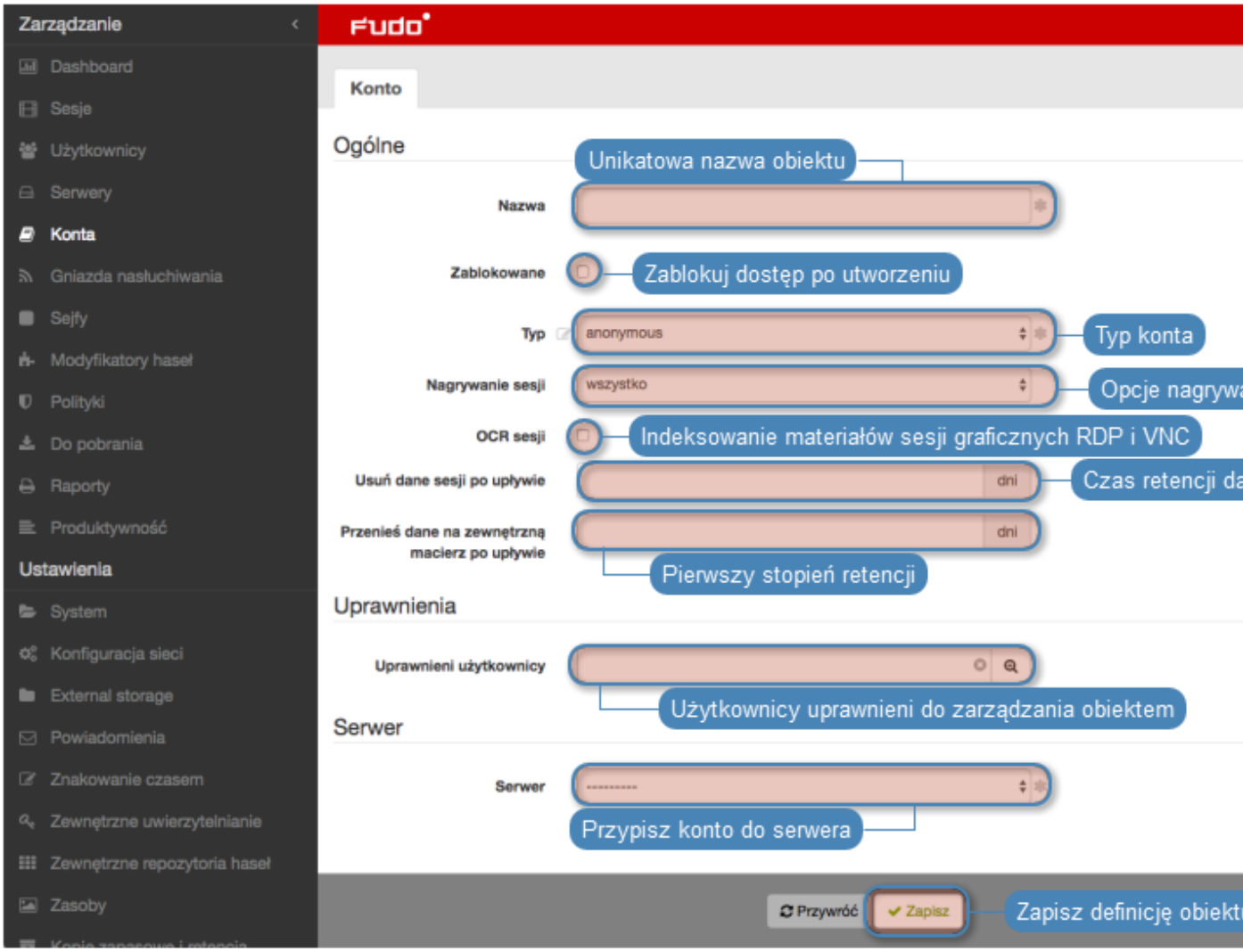
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Typ*, wybierz `anonymous`.
6. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.

- `wszystko` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze odtworzenie materiału w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.
- `raw` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w odtwarzaczu sesji.
- `brak` - Wheel Fudo PAM jedynie odnotowuje fakt, że połączenie miało miejsce, jednak nie rejestruje wymiany danych pomiędzy użytkownikiem i serwerem.

7. Zaznacz opcję *OCR sesji*, aby włączyć kompletne indeksowanie treści połączeń graficznych RDP i VNC.
8. W polu *Usuń dane sesji po upływie*, określ liczbę dni, po których dane sesji zostaną usunięte.
9. W polu *Przenieś dane na zewnętrzną macierz po upływie*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz.
10. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
11. W sekcji *Serwer*, z listy rozwijlanej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
12. Kliknij *Zapisz*.



Modyfikowanie konta

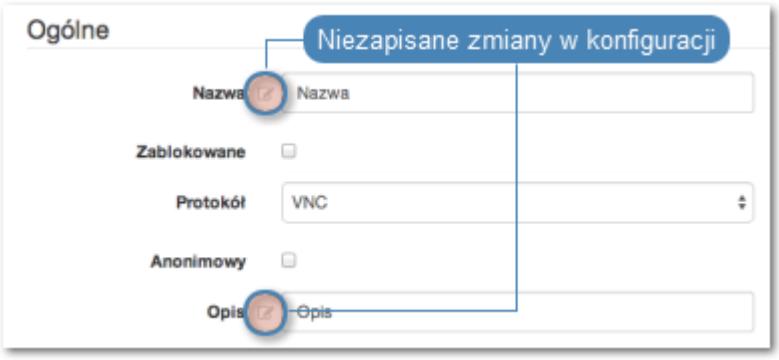
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście definicję konta, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

3. Kliknij nazwę konta.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



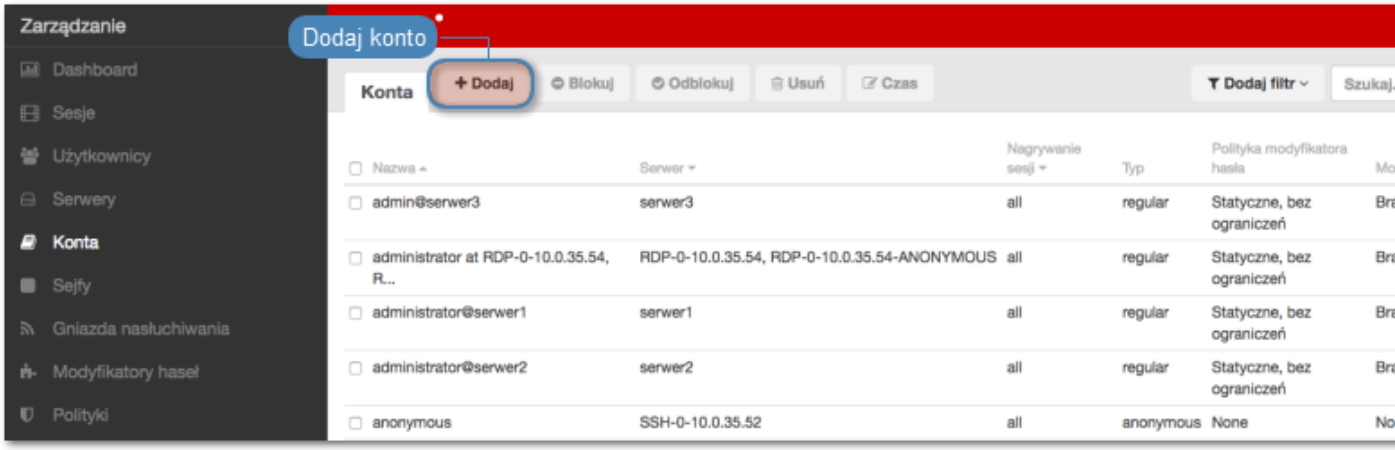
5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

7.1.2 Dodawanie konta typu *forward*

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Typ*, wybierz `forward`.
6. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.

- `wszystko` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze odtworzenie materiału w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.
- `raw` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w odtwarzaczu sesji.

- `brak` - Wheel Fudo PAM jedynie odnotowuje fakt, że połączenie miało miejsce, jednak nie rejestruje wymiany danych pomiędzy użytkownikiem i serwerem.

7. Zaznacz opcję *OCR sesji*, aby włączyć kompletne indeksowanie treści połączeń graficznych RDP i VNC.
8. Wybierz języki, które zdefiniują słowniki użyte przy przetwarzaniu OCR.
9. W polu *Usuń dane sesji po upływie*, określ liczbę dni, po których dane sesji zostaną usunięte.
10. W polu *Przenieś dane na zewnętrzną macierz po upływie*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz.
11. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
12. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
13. W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz żądaną opcję.

`innym kontem`

- Z listy rozwijalnej *Konto* wybierz obiekt, z którego pobrane zostanie hasło w celu uwierzytelnienia użytkownika podczas zestawiania połączenia.

Informacja: Lista zawiera obiekty, do których zalogowany użytkownik ma stosowne prawa dostępu.

`kluczem`

- Kliknij ikonę  i wybierz typ klucza SSH.
- Kliknij ikonę  i wskaż plik z kluczem do wgrania.

`hasłem`

- W polu *Hasło*, wprowadź hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.
- W polu *Powtórz hasło*, wprowadź ponownie hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.

Informacja: *Podwójne uwierzytelnienie*

Funkcjonalność podwójnego uwierzytelnienia polega na dwukrotnym żądaniu wprowadzenia danych logowania podczas nawiązywania połączenia. Pierwsze zapytanie dotyczy uwierzytelnienia użytkownika przed Wheel Fudo PAM, drugie służy uwierzytelnieniu przed systemem docelowym.

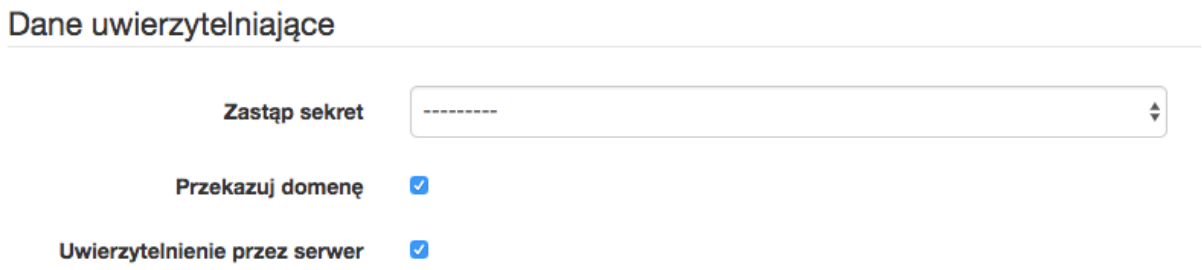
Aby aktywować funkcję podwójnego uwierzytelnienia, z listy rozwijalnej *Zastąp sekret* wybierz opcję `hasłem` i nie wypełniaj pól definiujących hasło oraz login.

`hasłem z zewnętrznego repozytorium`

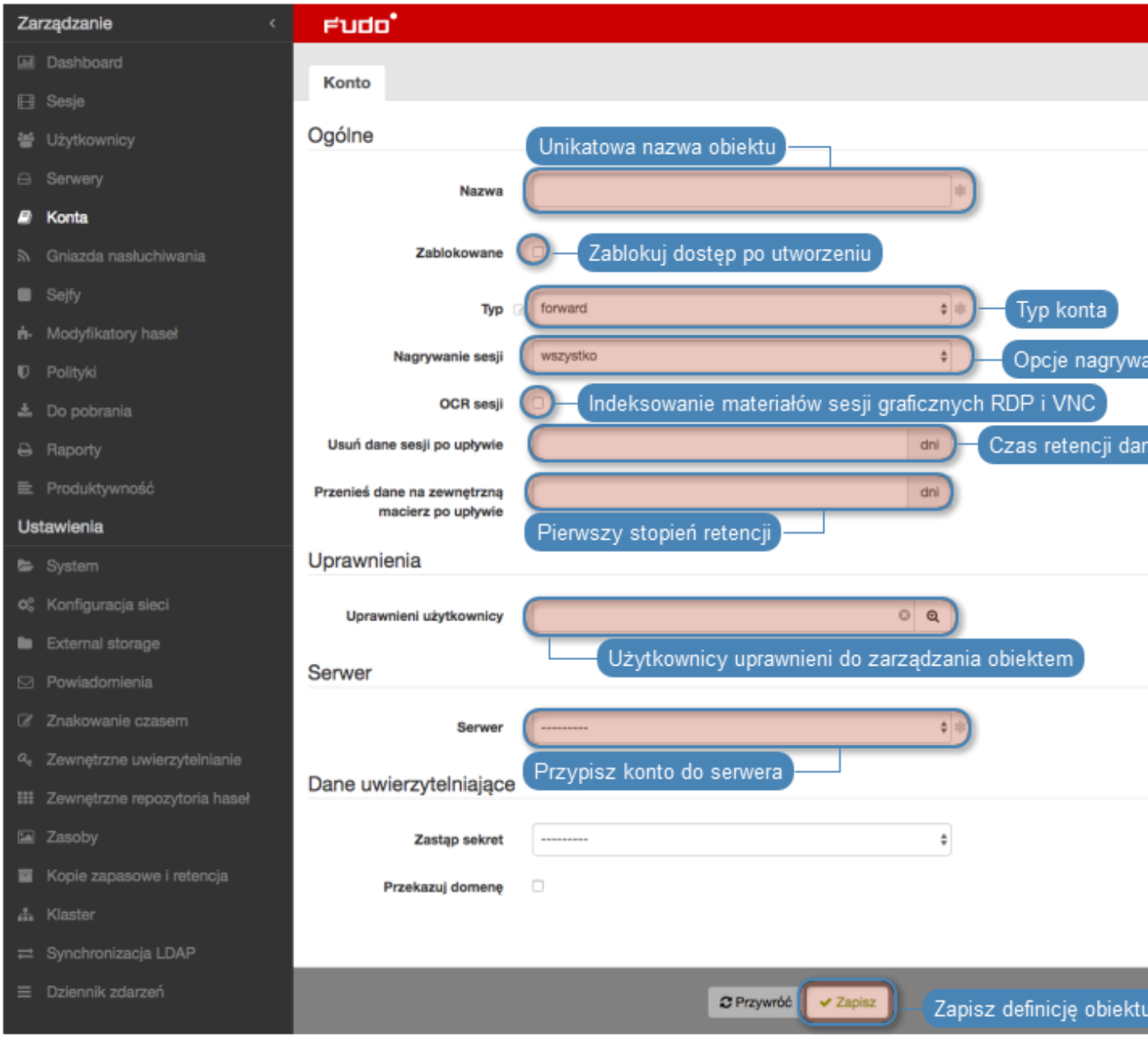
- Z listy rozwijalnej, wybierz zewnętrzne repozytorium haseł, z którego pobrane zostanie hasło podczas zestawiania połączenia.

Informacja: *Uwierzytelnienie przez serwer*

W trybie uwierzytelnienia przez serwer, Fudo nie weryfikuje poprawności danych logowania, tylko przekazuje je do serwera docelowego, który przeprowadza proces uwierzytelnienia. Aby włączyć uwierzytelnienie przez serwer, zaznacz opcję *Uwierzytelnienie przez serwer* w sekcji *Dane uwierzytelniające* (dostępne tylko dla serwerów SSH oraz RDP w trybie bezpieczeństwa *Enhanced RDP Security (TLS) + NLA*.



13. Zaznacz opcję *Przekazuj domenę*, aby nazwa domeny była przekazywana razem z ciągiem identyfikującym użytkownika.
14. Kliknij *Zapisz*.

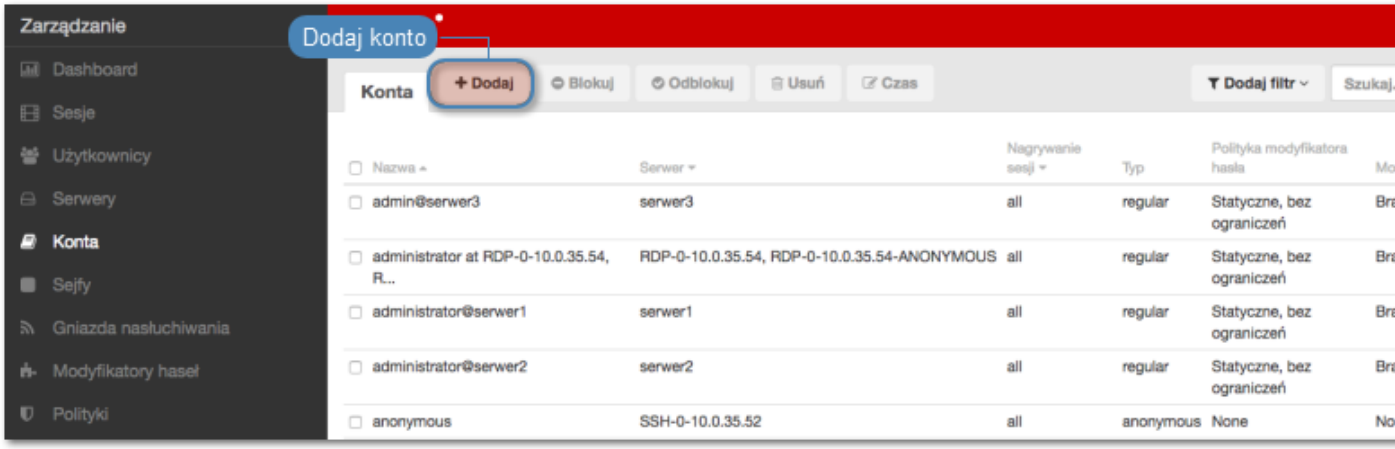


Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

7.1.3 Dodawanie konta typu *regular*

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Typ*, wybierz `regular`.
6. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.

- `wszystko` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze odtworzenie materiału w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.
- `raw` - Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w odtwarzaczu sesji.
- `brak` - Wheel Fudo PAM jedynie odnotowuje fakt, że połączenie miało miejsce, jednak nie rejestruje wymiany danych pomiędzy użytkownikiem i serwerem.

7. Zaznacz opcję *OCR sesji*, aby włączyć kompletne indeksowanie treści połączeń graficznych RDP i VNC.

Informacja: Zindeksowanie sesji umożliwia późniejsze pełnotekstowe przeszukiwanie zarejestrowanego materiału.

---

8. Wybierz języki jakie zostaną użyte przy indeksowaniu sesji.
9. W polu *Usuń dane sesji po upływie*, określ liczbę dni, po których dane sesji zostaną usunięte.
10. W polu *Przenieś dane na zewnętrzną macierz po upływie*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz.
11. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
12. W sekcji *Serwer*, z listy rozwijlanej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
13. W sekcji *Dane uwierzytelniające*, w polu *Domen*, wprowadź domenę konta użytkownika uprzywilejowanego, na serwerze docelowym.
14. W polu *Login*, wprowadź login użytkownika uprzywilejowanego na serwerze docelowym.
15. Z listy rozwijalnej *Zastąp sekret*, wybierz żądaną opcję.

```
innym kontem
```

- Z listy rozwijalnej *Konto* wybierz obiekt, z którego pobrane zostanie hasło w celu uwierzytelnienia użytkownika podczas zestawiania połączenia.

`kluczem`

- Kliknij ikonę  i wybierz typ klucza SSH.
- Kliknij ikonę  i wskaż plik z kluczem prywatnym, niezabezpieczony frazą szyfrującą.

`hasłem`

- W polu *Hasło*, wprowadź hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.
- W polu *Powtórz hasło*, wprowadź ponownie hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.

Informacja: *Podwójne uwierzytelnienie*

Funkcjonalność podwójnego uwierzytelnienia polega na dwukrotnym żądaniu wprowadzenia danych logowania podczas nawiązywania połączenia. Pierwsze zapytanie dotyczy uwierzytelnienia użytkownika przed Wheel Fudo PAM, drugie służy uwierzytelnieniu przed systemem docelowym.

Aby aktywować funkcję podwójnego uwierzytelnienia, z listy rozwijalnej *Zastąp sekret* wybierz opcję `hasłem` i nie wypełniaj pól definiujących hasło oraz login.

`hasłem z zewnętrzengo repozytorium`

- Z listy rozwijalnej, wybierz zewnętrzne repozytorium haseł, z którego pobrane zostanie hasło podczas zestawiania połaczenia.

16. Z listy rozwijalnej *Polityka modyfikatora haseł*, wybierz zdefiniowaną wcześniej politykę zmiany haseł do konta uprzywilejowanego.
17. W sekcji *Modyfikator hasła*, z listy rozwijalnej *Modyfikator hasła*, wybierz właściwy dla hosta docelowego sposób zmiany haseł i uzupełnij parametry konfiguracyjne.

Konto Unix poprzez SSH

- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

Konto Windows poprzez WMI

- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

Konto użytkownika MySQL na serwerze Unix poprzez SSH

- Wprowadź nazwę użytkownika SSH.
- Wprowadź hasło do konta użytkownika SSH.
- Podaj adres serwera SSH.
- Wpisz port usługi SSH.

- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

Konto CISCO poprzez Telnet

- Wprowadź hasło trybu uprzywilejowanego.
- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

CISCO Enable Password poprzez Telnet

- Wprowadź hasło trybu uprzywilejowanego.
- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

Konto CISCO poprzez SSH

- Wprowadź hasło trybu uprzywilejowanego.
- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

CISCO Enable Password poprzez Telnet

- Wprowadź hasło trybu uprzywilejowanego.
- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

LDAP

- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.
- Wprowadź parametr bazowy LDAP (LDAP base).
- Wgraj certyfikat CA serwera LDAP.

WinRM

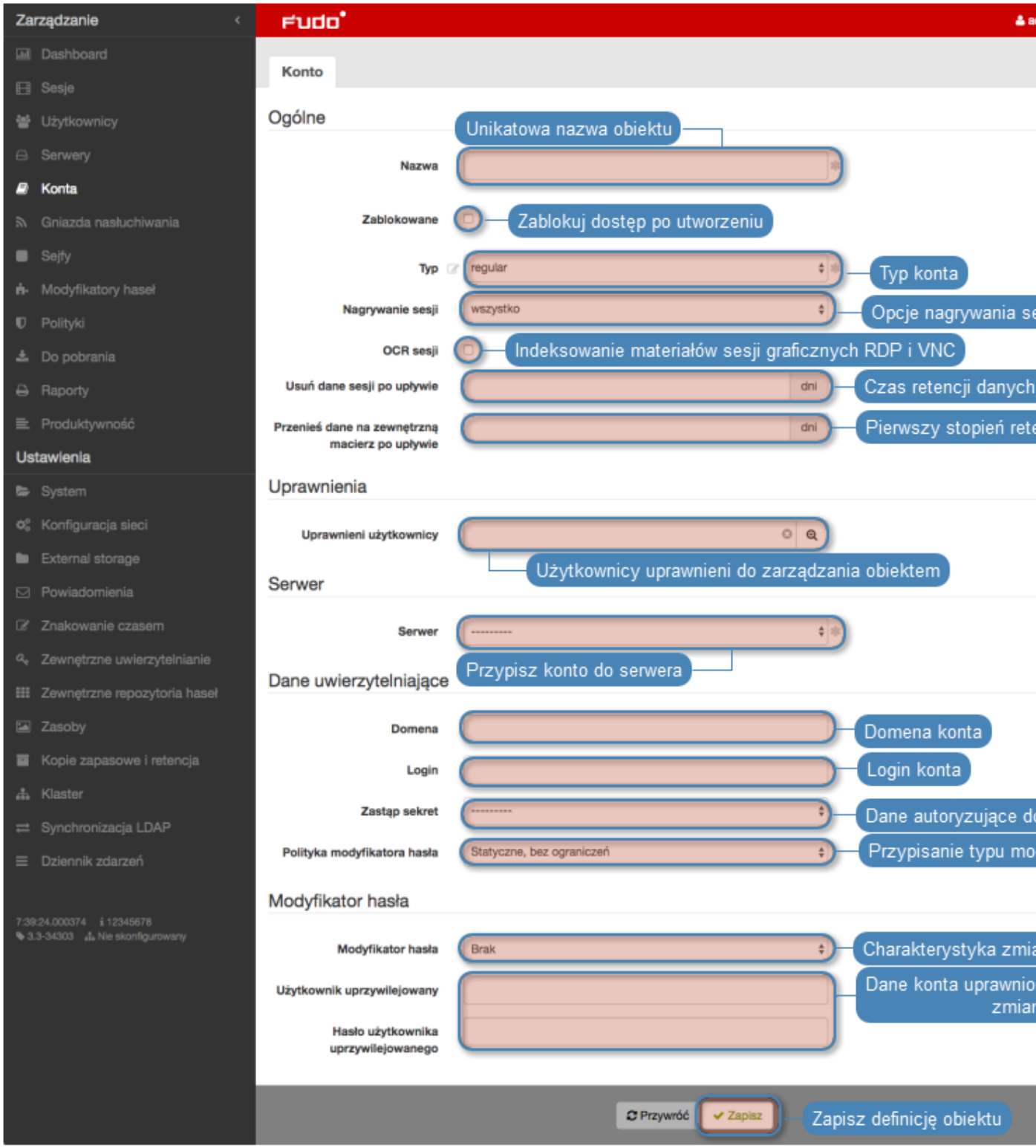
- Wybierz język serwera docelowego.
- Wprowadź nazwę konta użytkownika uprzywilejowanego.
- Wprowadź hasło użytkownika uprzywilejowanego.

Informacja:

- Zaznacz opcję *Użyj istniejące konto* i wybierz z listy rozwijalnej wcześniej zdefiniowane konto, aby użyć je w charakterze konta uprzywilejowanego.
- Konto uprzywilejowane wykorzystywane jest do zmiany hasła w przypadku wykrycia jego nieautoryzowanej zmiany.

---

18. Kliknij *Zapisz*.



Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

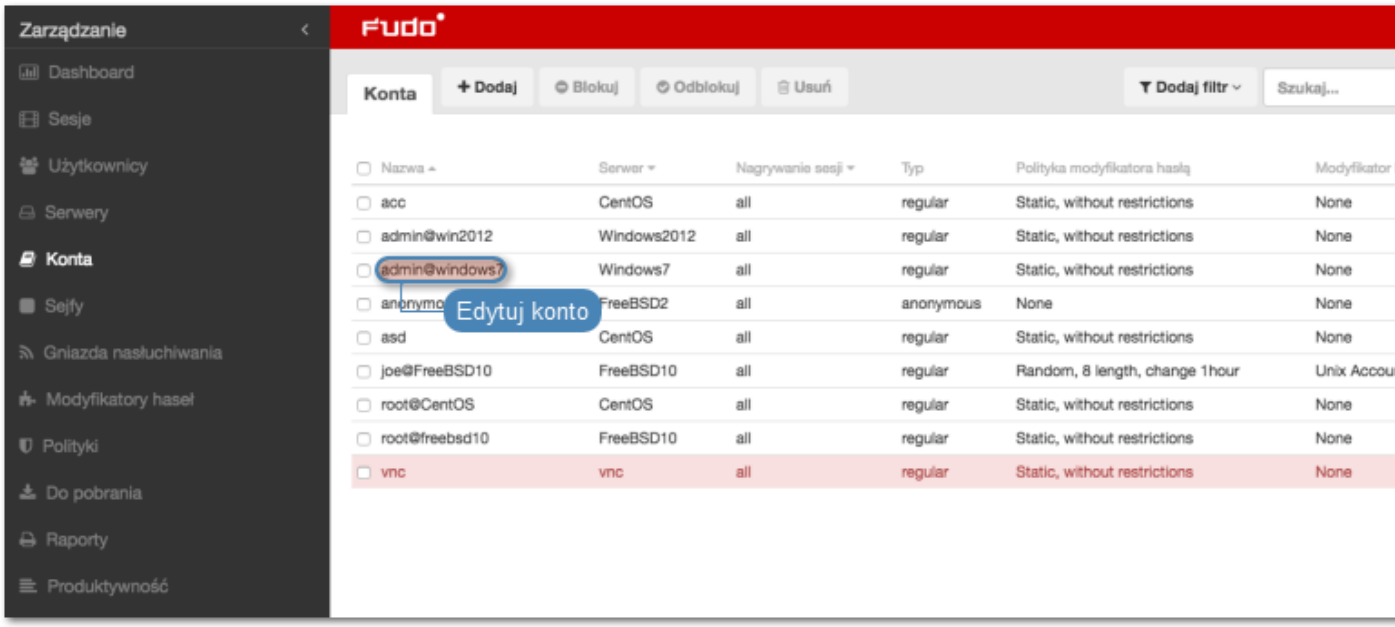
7.2 Edytowanie konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście definicję konta, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

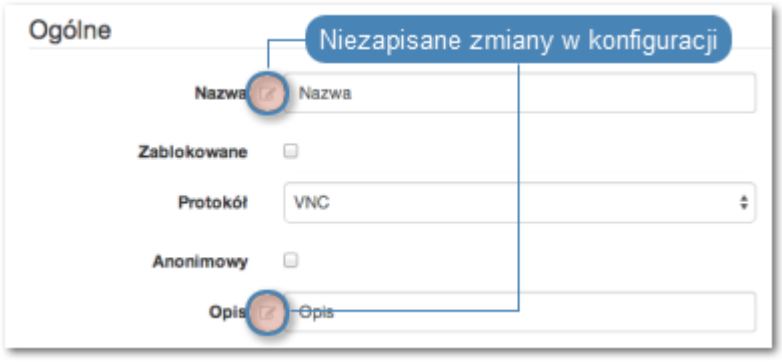
---

3. Kliknij nazwę konta.



4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną .



---

5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie konta*
- *Edytowanie konta*
- *Odblokowanie konta*

- *Usuwanie konta*

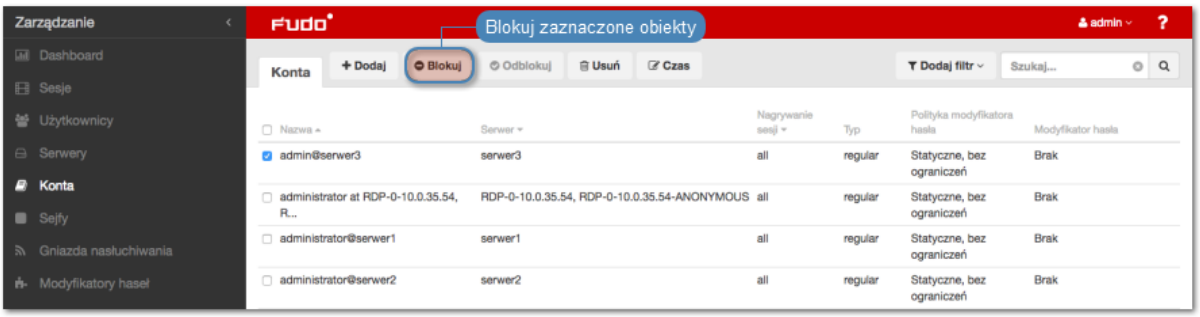
7.3 Blokowanie konta

Ostrzeżenie: Zablokowanie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązanym serwerem.

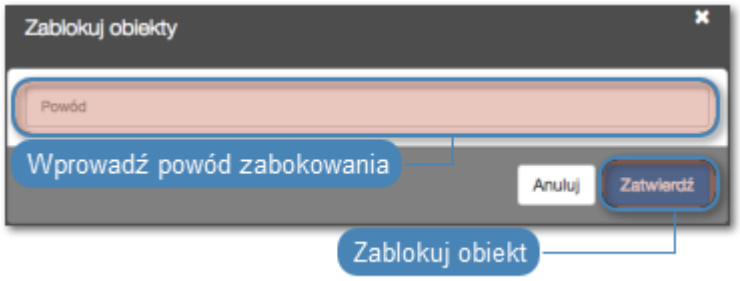
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerem za pośrednictwem z wybranego konta.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.



Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

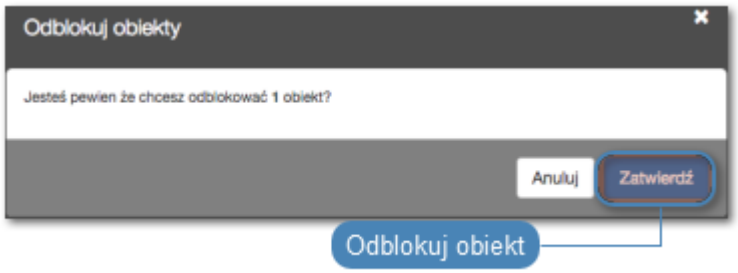
- *Odblokowanie konta*
- *Dodawanie konta*
- *Edytowanie konta*
- *Usuwanie konta*

7.4 Odblokowanie konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby umożliwić nawiązywanie połączeń za pośrednictwem wybranego konta.
4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.



Tematy pokrewne:

- *Blokowanie konta*
- *Dodawanie konta*
- *Edytowanie konta*
- *Usuwanie konta*

7.5 Usuwanie konta

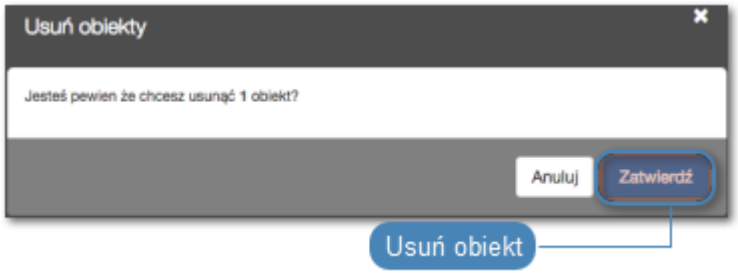
Ostrzeżenie: Usunięcie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązanym serwerem.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.

4. Potwierdź operację usunięcia zaznaczonych obiektów.



Tematy pokrewne:

- *Dodawanie konta*
- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*

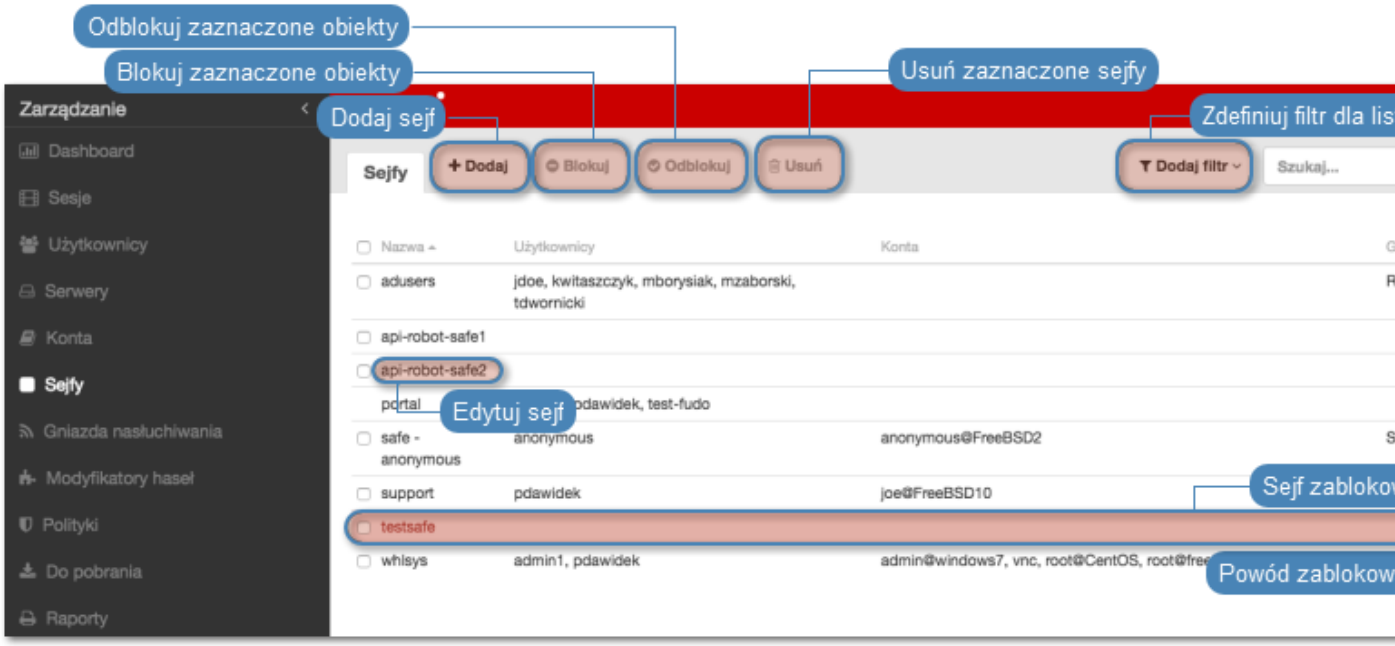
ROZDZIAŁ 8

Sejfy

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

Informacja:

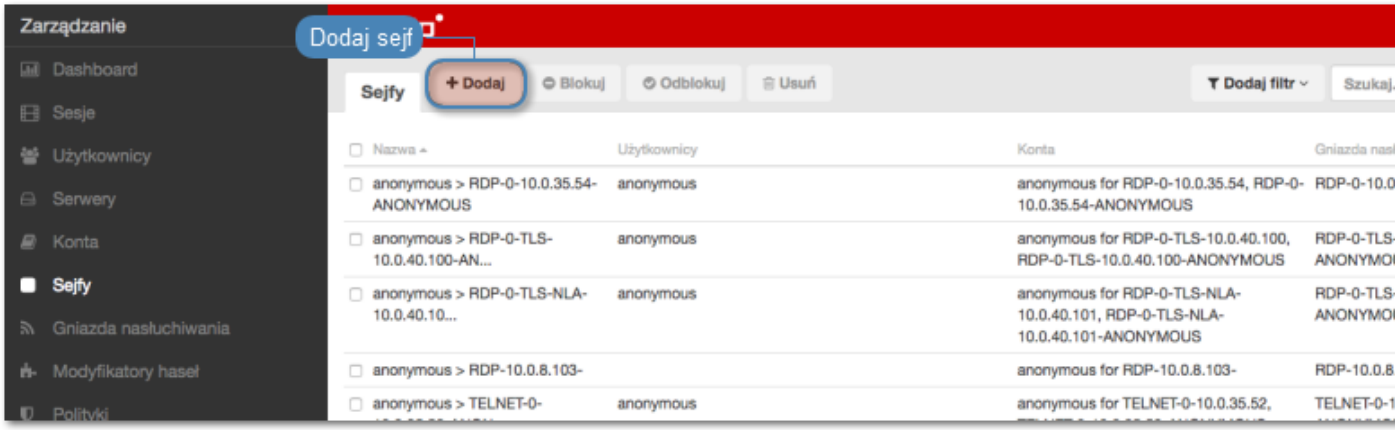
- Sejf `system` może mieć przypisane tylko konto `system`.
- Sejf `portal` może mieć przypisane tylko konto `portal`.
- Użytkownik o roli `operator`, `admin` lub `superadmin` zawsze posiada dostęp do sejfu `system`.
- Użytkownik o roli `user` nie może posiadać dostępu do sejfu `system`.
- Użytkownik anonimowy musi mieć dostęp do sejfów, które zawierają konta anonimowe.



8.1 Dodawanie sejfu

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.



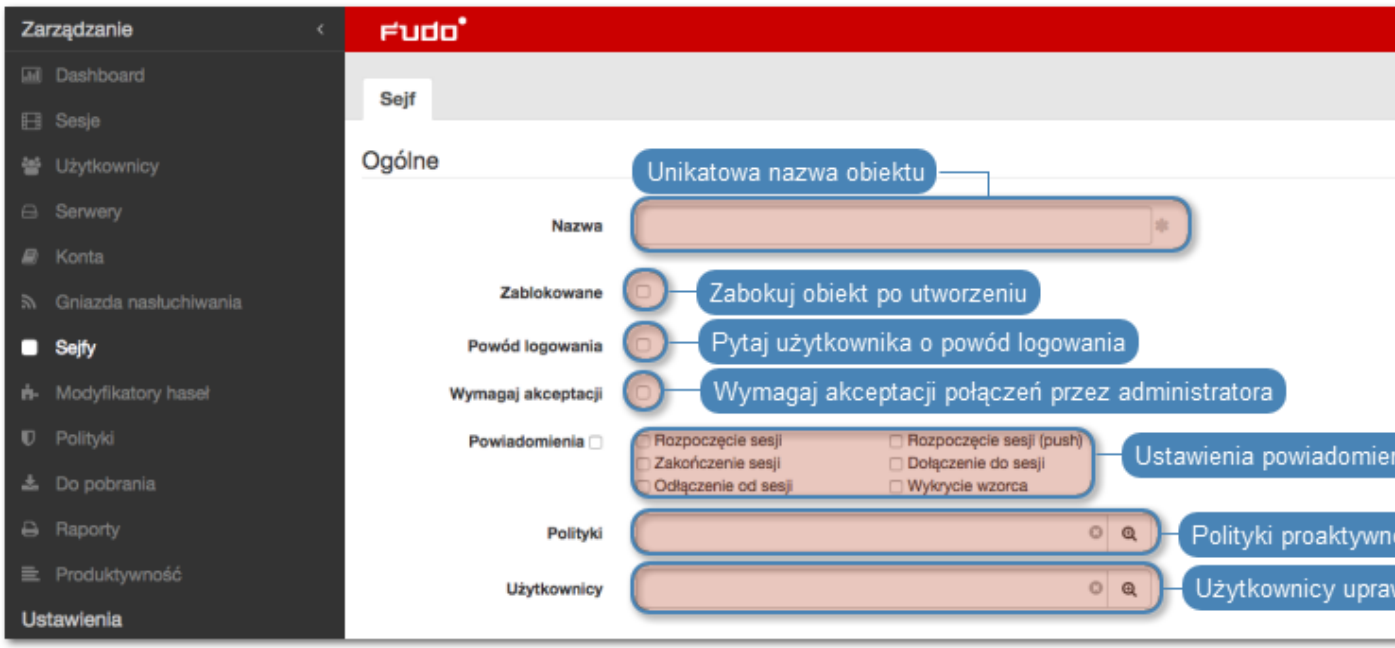
3. Wpisz nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby użytkownicy nie mieli dostępu do kont przypisanych do sejfu, zaraz po jego utworzeniu.
5. Zaznacz opcję *Powód logowania*, aby wyświetlić użytkownikowi monit o podanie powodu logowania do systemu docelowego.

6. Zaznacz opcję *Wymagaj akceptacji*, aby połączenia z serwerami realizowane za pośrednictwem wybranego sejfu, wymagały potwierdzenia przez osobę do tego upoważnioną.
7. Zaznacz opcję *Powiadomienia* i wybierz zdarzenia systemowe, o których informowani będą administratorzy.

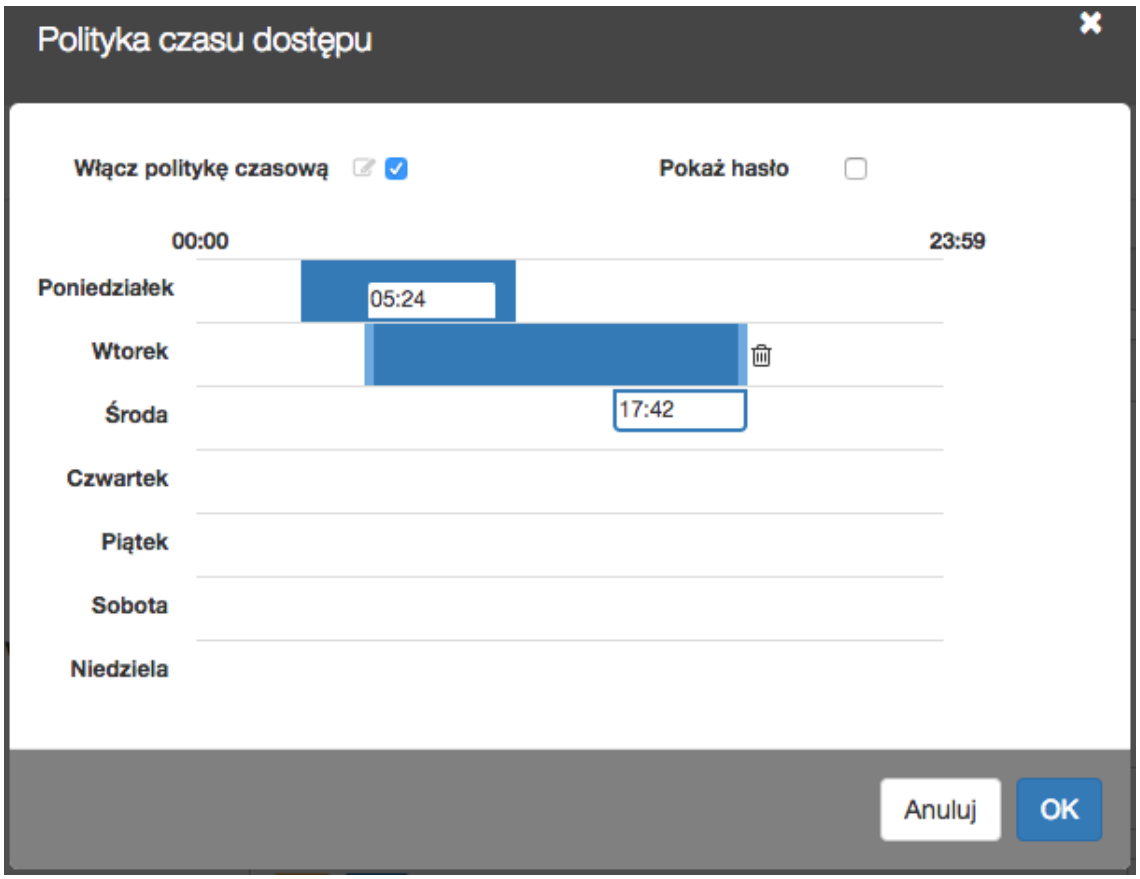
Informacja: Powiadomienie o rozpoczęciu sesji wysyłane do aplikacji *Fudo Mobile* za pośrednictwem mechanizmu push wymaga skonfigurowania usługi proxy. Więcej informacji na temat konfigurowania serwera proxy znajdziesz w rodzaiale *Konfiguracja serwerów proxy*.

---

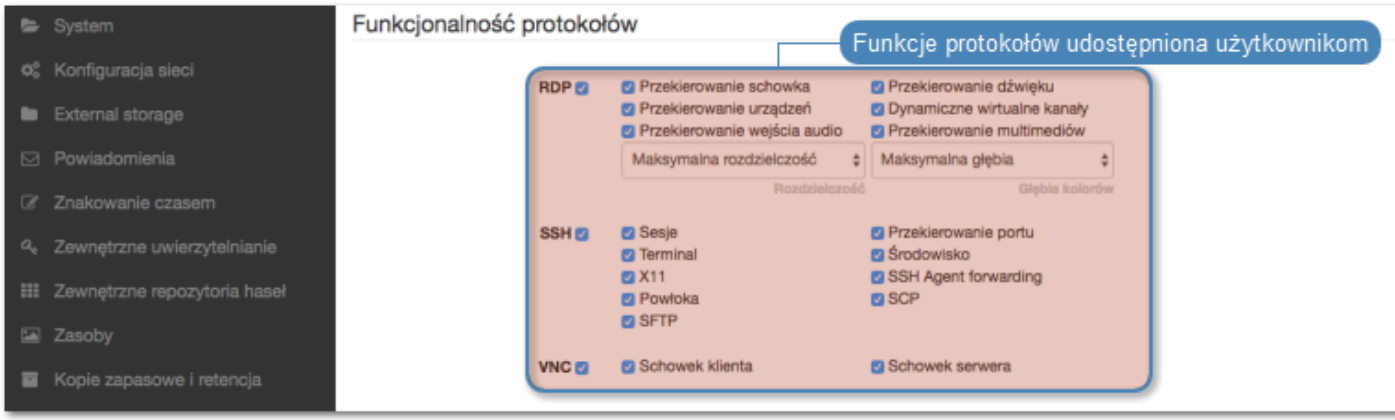
8. Przypisz do sejfu *polityki bezpieczeństwa*.
9. W polu *Użytkownicy*, przypisz użytkowników, którzy będą uprawnieni do nawiązywania połączeń z serwerami, za pośrednictwem tego sejfu.



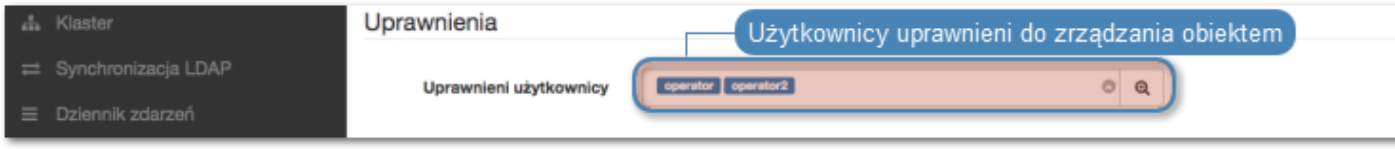
Informacja: Kliknij element reprezentujący użytkownika, aby zdefiniować politykę czasową lub włączyć możliwość podglądu haseł w Portalu Użytkownika.



10. W sekcji *Funkcjonalność protokołów*, zaznacz dozwolone w połączeniach funkcjonalności protokołów.



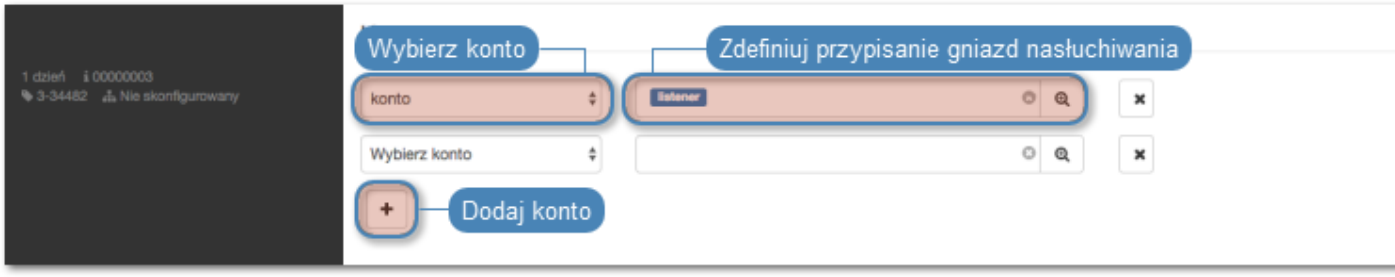
11. W sekcji *Uprawnienia*, dodaj użytkowników (administratorów, operatorów) uprawnionych do zarządzania obiektem.



12. W sekcji *Konta*, kliknij ikonę  .

13. Z listy rozwijalnej wybierz konto, a w sąsiednim polu wybierz gniazda nasłuchiwania, które

mogą zostać użyte w nawiązaniu połączenia z serwerem docelowym, za pośrednictwem wybranego konta.



14. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*

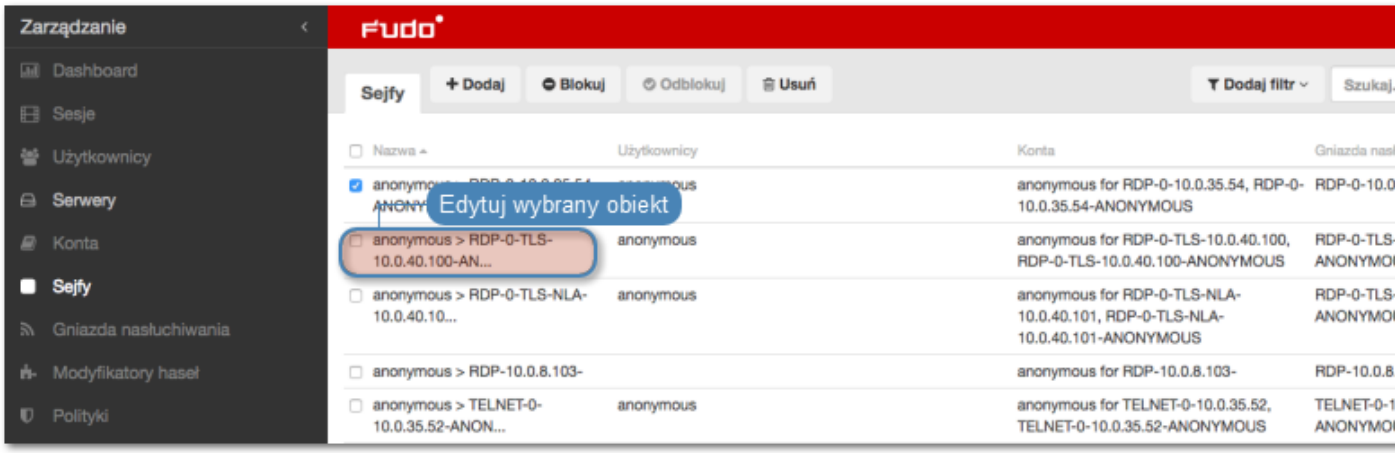
8.2 Modyfikowanie sejfu

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście definicję sejfu, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

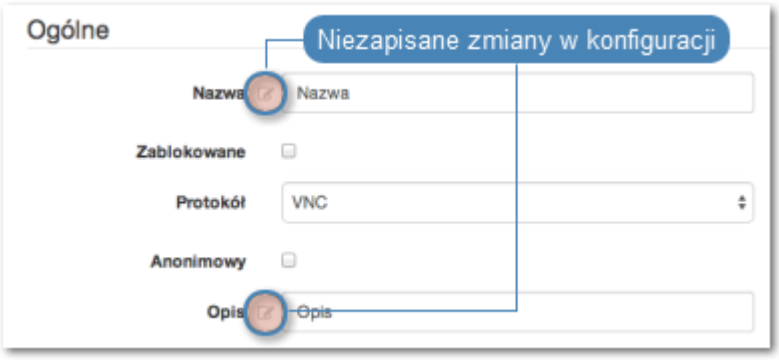
---

3. Kliknij nazwę sejfu.



4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną .



5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Dodawanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*

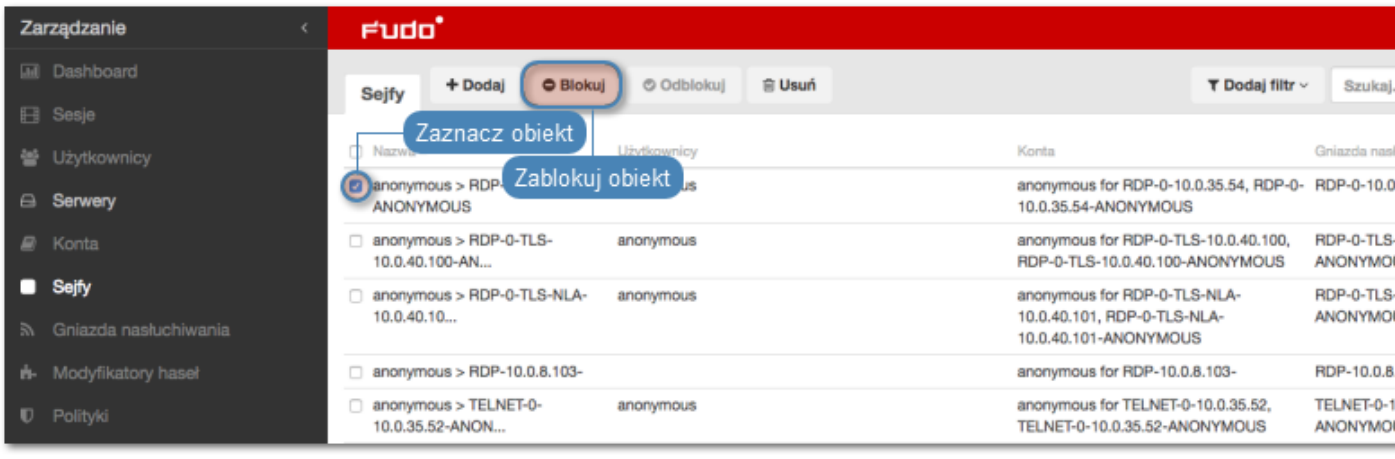
8.3 Blokowanie sejfu

Ostrzeżenie: Zablokowanie sejfu spowoduje zerwanie aktualnie trwających sesji połączeniowych, wykorzystujących konta przypisane wybranego obiektu.

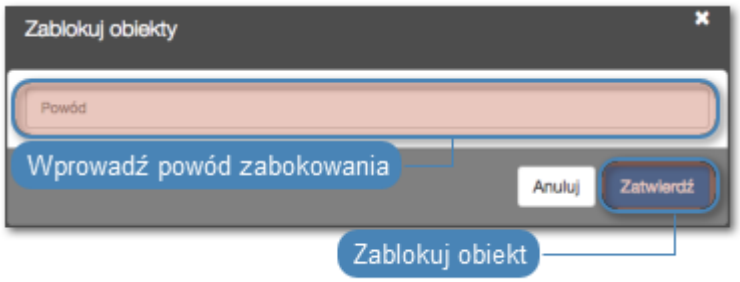
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerami z wykorzystaniem kont uprzywilejowanych przypisanych do wybranego sejfu.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.



Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

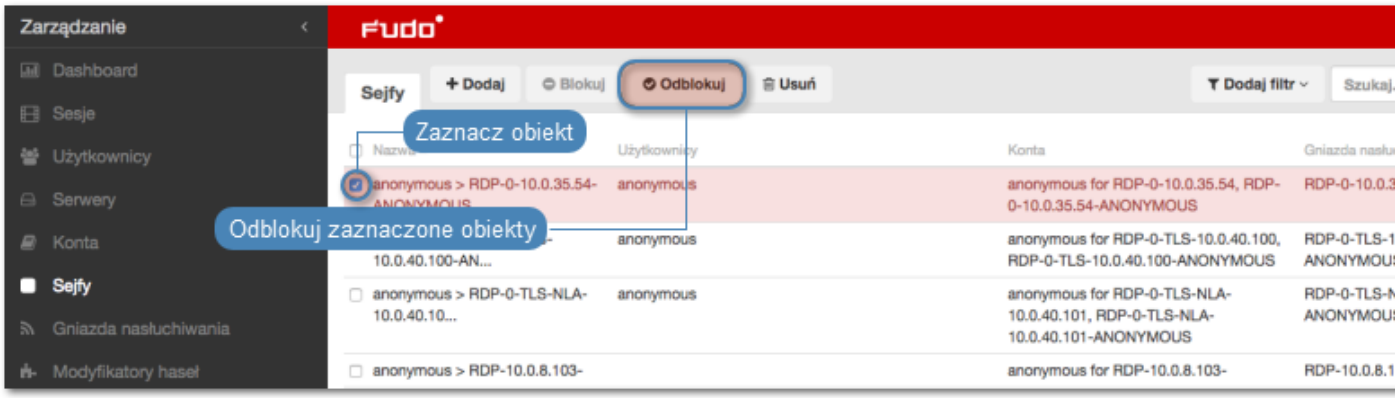
- *Odblokowanie sejfu*
- *Model danych*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*

8.4 Odblokowanie sejfu

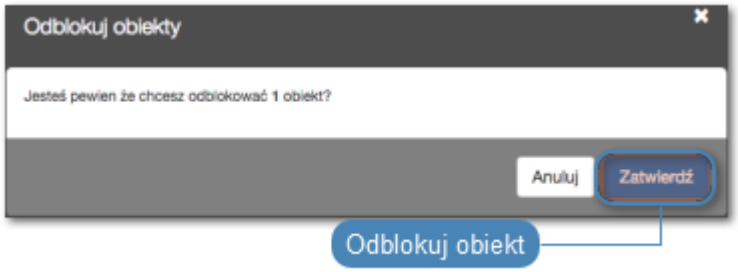
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń z serwerami z wykorzystaniem kont uprzywilejowanych przypisanych do wybranego sejfu.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektów.



Tematy pokrewne:

- *Model danych*
- *Blokowanie sejfu*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*
- *Usuwanie sejfu*

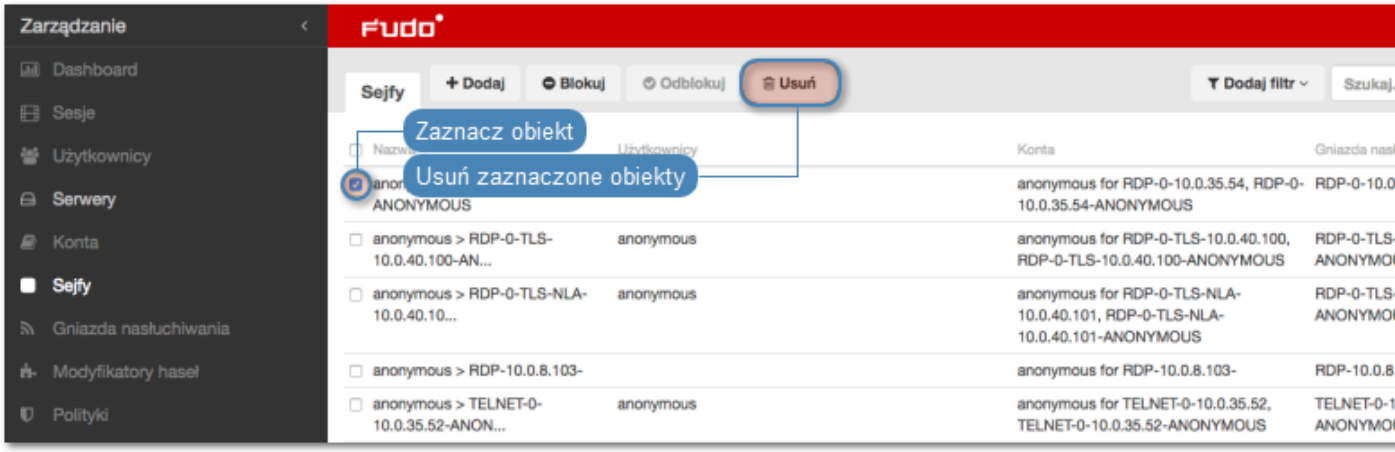
8.5 Usuwanie sejfu

Ostrzeżenie: Usunięcie sejfu spowoduje przerwanie aktualnie trwających sesji z serwerami, do połączenia z którymi zostały wykorzystane konta przypisane do sejfu.

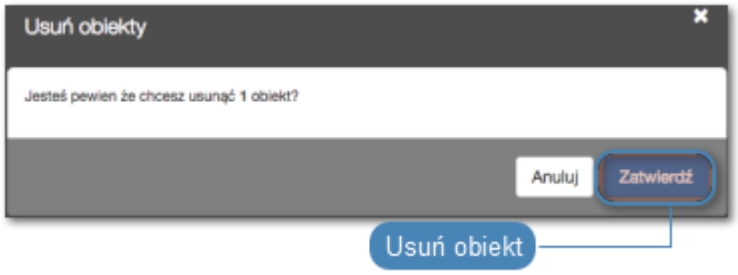
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz sejfy, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.



4. Potwierdź operację usunięcia zaznaczonych obiektów.



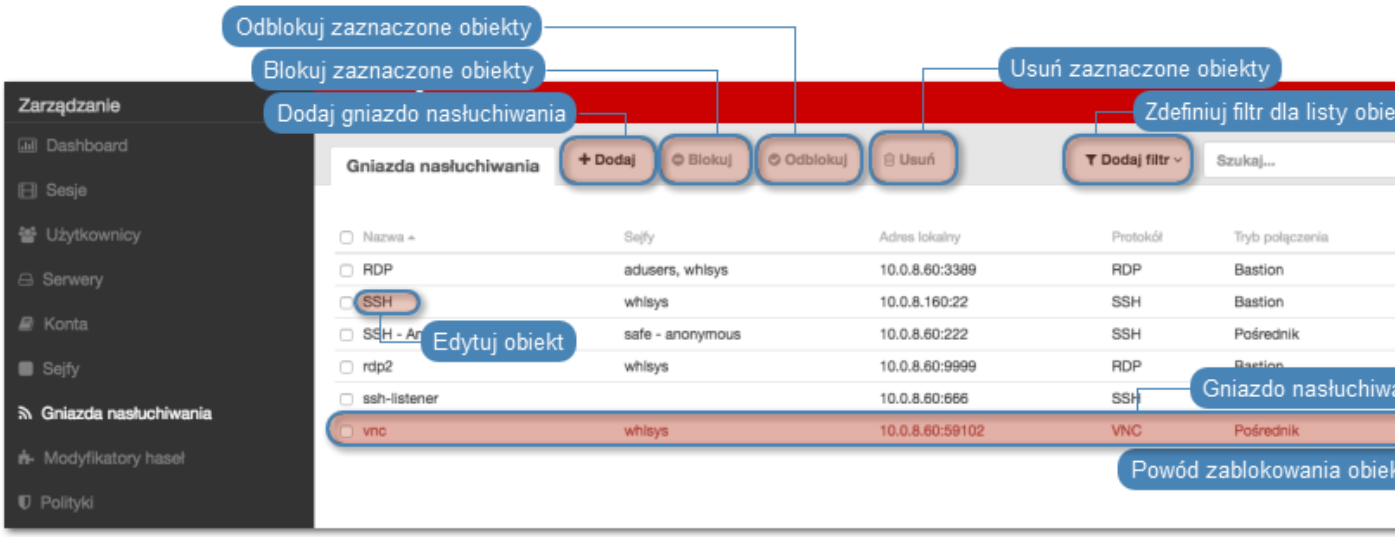
Tematy pokrewne:

- *Model danych*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*
- *Blokowanie sejfu*
- *Odblokowanie sejfu*

ROZDZIAŁ 9

Gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.



9.1 Dodawanie gniazda nasłuchiwania

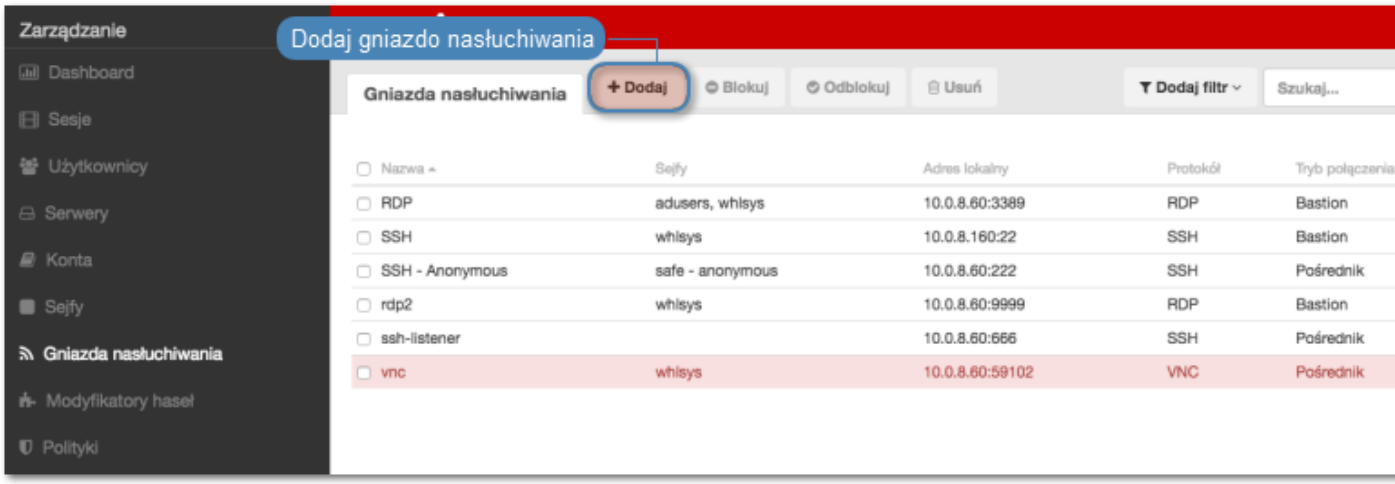
Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

Informacja:

- Gniazdo nasłuchiwania nie może być skojarzone z kontem przypisanym do serwera o protokole innym niż protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania typu *pośrednik* może być skojarzone tylko z jednym serwerem.
- Gniazdo nasłuchiwania typu *bastion* nie może być skojarzone z kontem anonimowym.
- Gniazdo nasłuchiwania nie może być przypisane do jednego konta anonimowego poprzez dwa sejfy.
- Gniazdo nasłuchiwania nie może zawierać konta anonimowego i *regular* lub *forward* do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania nie może być przypisane do dwóch kont do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania, do których jeden użytkownik ma dostęp.

9.1.1 Dodawanie gniazda nasłuchiwania Citrix

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `Citrix StoreFront (HTTP)`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo

PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

8. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.
9. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
10. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
11. Wgraj lub wygeneruj certyfikat TLS.

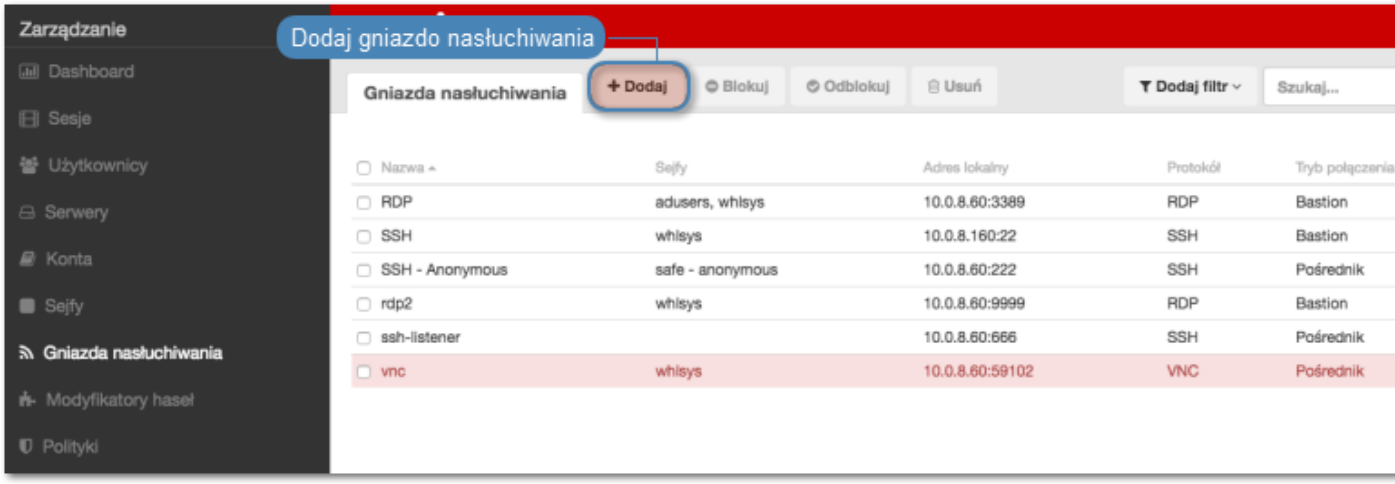
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Citrix StoreFront*
- *ICA*
- *Plik konfiguracyjny połączenia ICA*

9.1.2 Dodawanie gniazda nasłuchiwania HTTP

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `HTTP`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.

- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

8. Zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*, aby połączenie było szyfrowane.
9. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
10. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
11. W polu *Certyfikat TLS*, kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
12. Kliknij *Zapisz*.

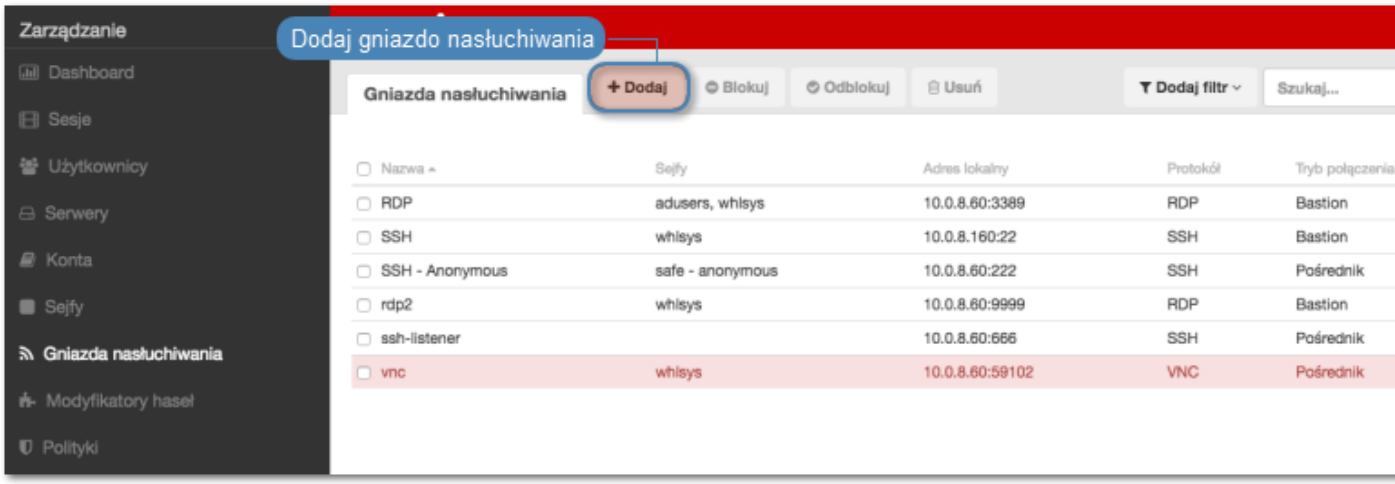
Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*

- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.3 Dodawanie gniazda nasłuchiwania ICA

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `ICA`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Bastion`

Informacja: Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

8. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.
9. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.

10. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
11. Wgraj lub wygeneruj certyfikat TLS.

Informacja: W przypadku połączeń szyfrowanych, Fudo zwraca klientowi Citrix *plik konfiguracyjny .ica*, w którym adresem FQDN serwera (*Address*) jest nazwa zwyczajowa (*Common Name*) z certyfikatu TLS.

---

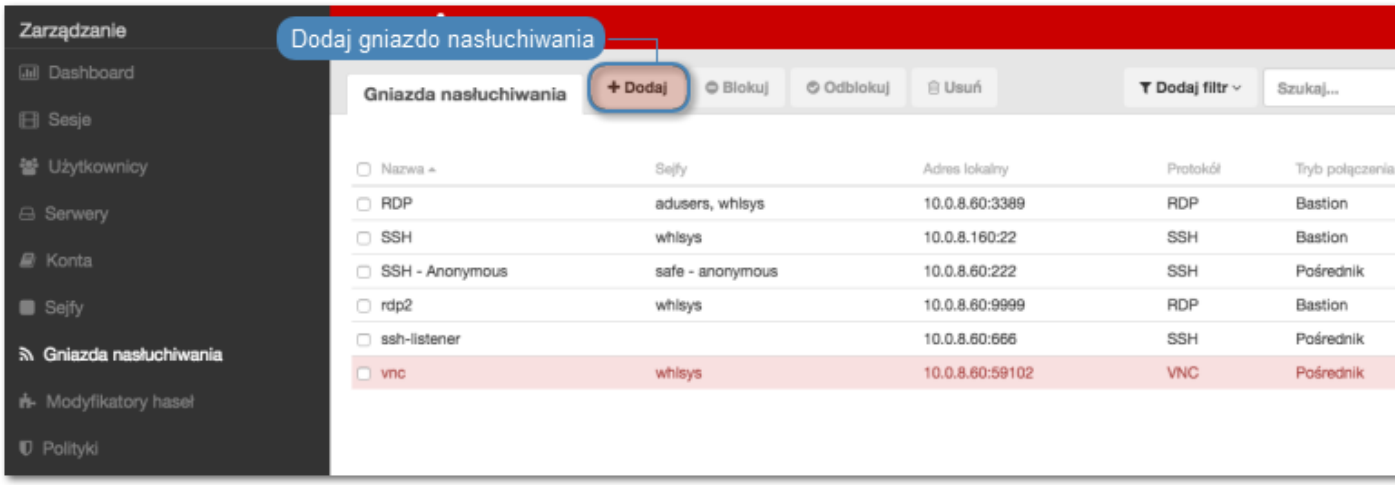
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *ICA*
- *Model danych*
- *Citrix StoreFront*
- *ICA*
- *Plik konfiguracyjny połączenia ICA*

9.1.4 Dodawanie gniazda nasłuchiwania Modbus

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `Modbus`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne > Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

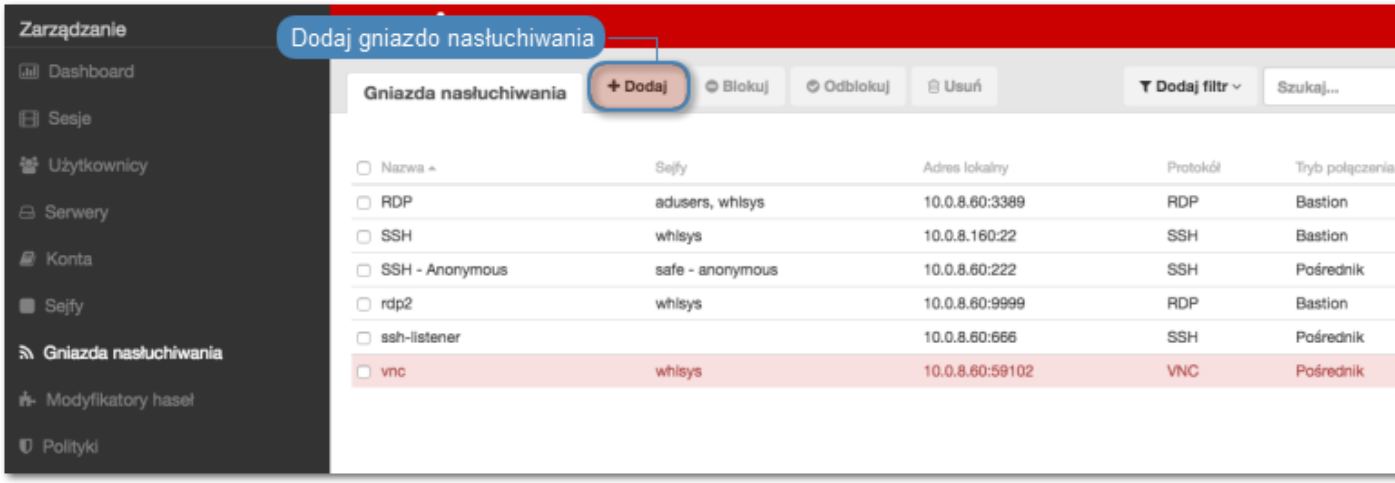
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.5 Dodawanie gniazda MySQL

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `MySQL`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.

- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

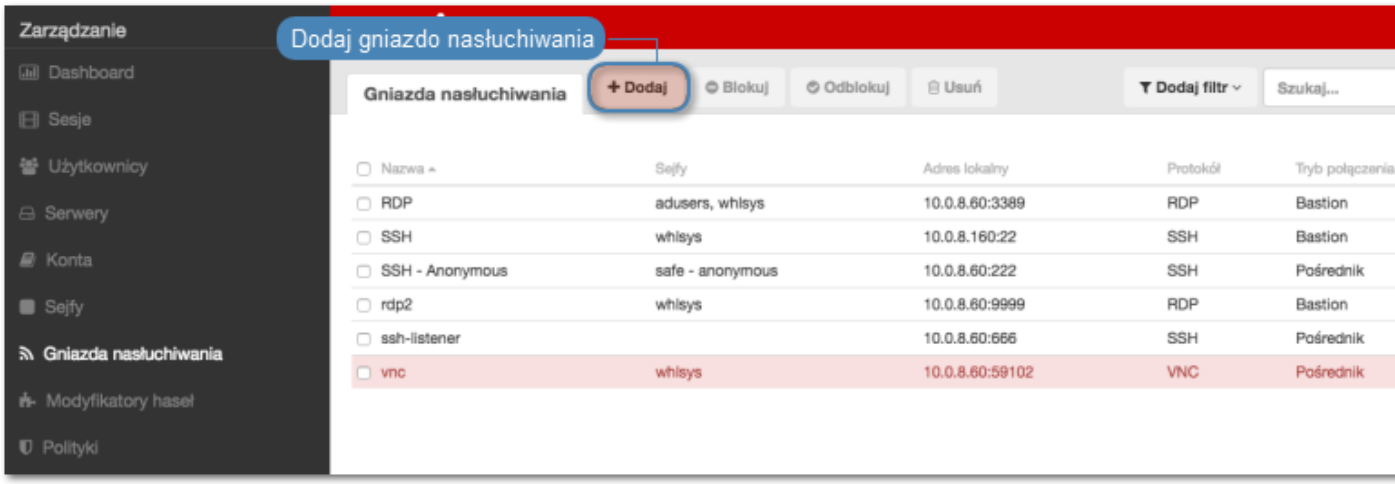
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.6 Dodawanie gniazda Oracle

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `Oracle`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

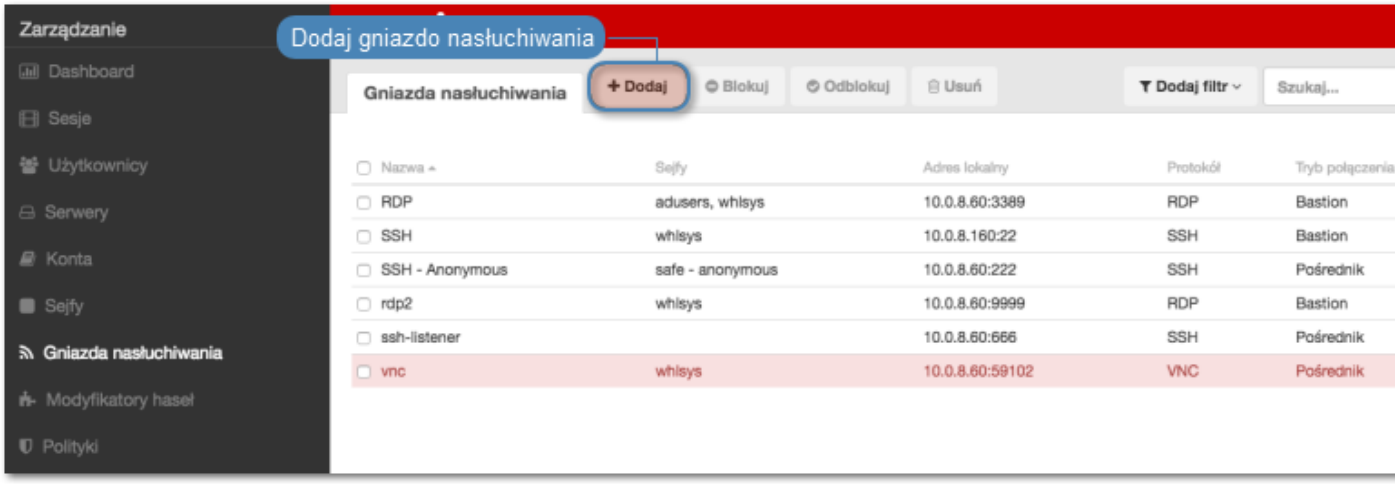
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.7 Dodawanie gniazda RDP

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `RDP`.
6. Z listy rozwijalnej *Bezpieczeństwo*, wybierz tryb bezpieczeństwa prodokołu RDP.
7. W polu *Komunikat*, wprowadź informację, która będzie wyświetlana użytkownikom na ekranie logowania.
8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Bastion`

Informacja: Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

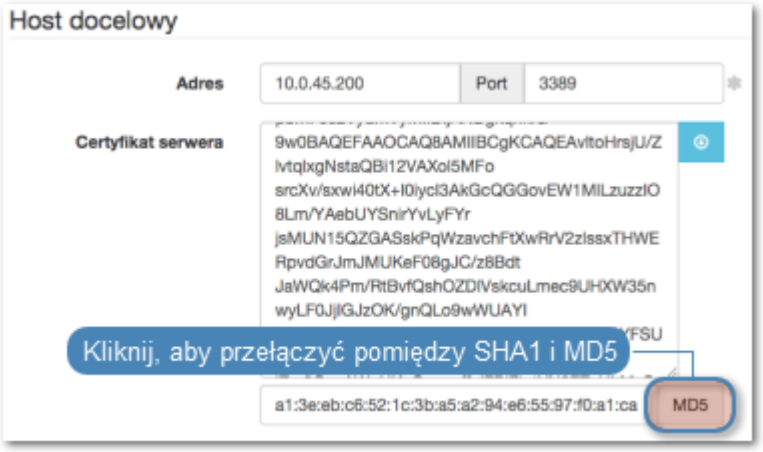
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

Informacja: Kliknij specyfikator funkcji skrótu, aby przełączyć pomiędzy wyświetlaniem skrótu klucza wygenerowanego przez algorytm SHA1 lub MD5.



---

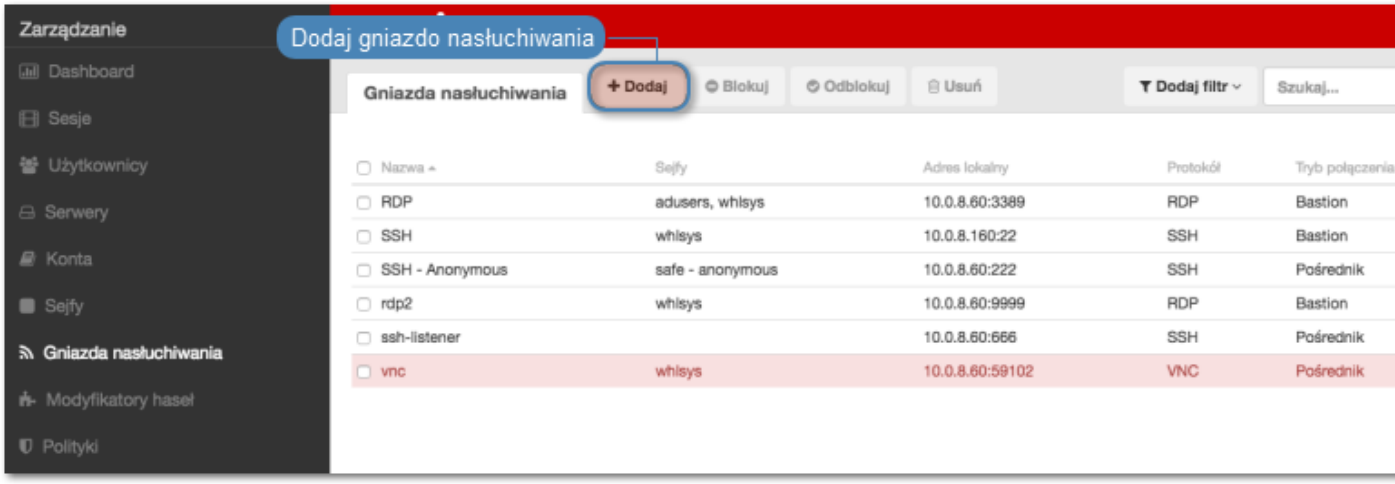
10. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.8 Dodawanie gniazda SSH

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `SSH`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Bastion`

Informacja: Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

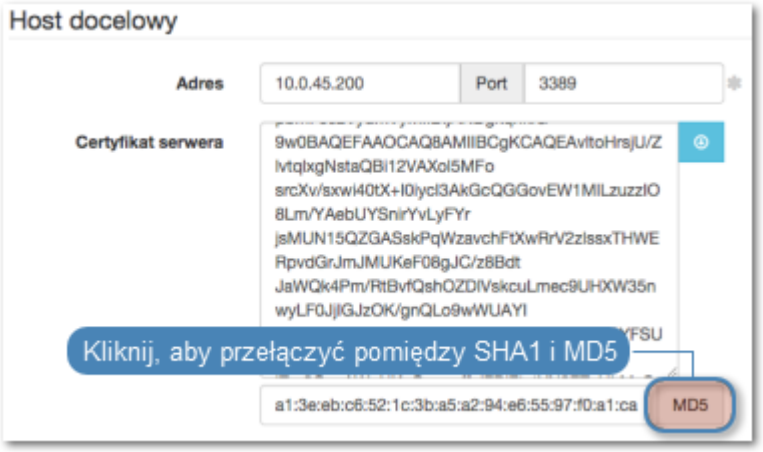
`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.

- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
- Kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
- Kliknij *Zapisz*.

Informacja: Kliknij specyfikator funkcji skrótu, aby przełączyć pomiędzy wyświetlaniem skrótu klucza wygenerowanego przez algorytm SHA1 lub MD5.



---

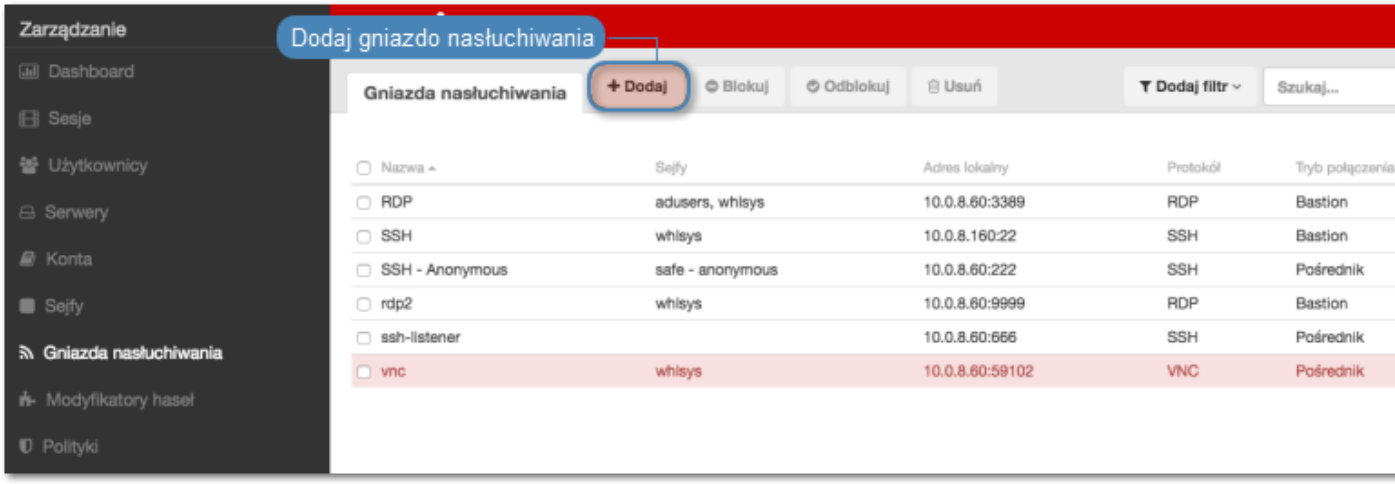
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.9 Dodawanie gniazda MS SQL

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `MS SQL (TDS)`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

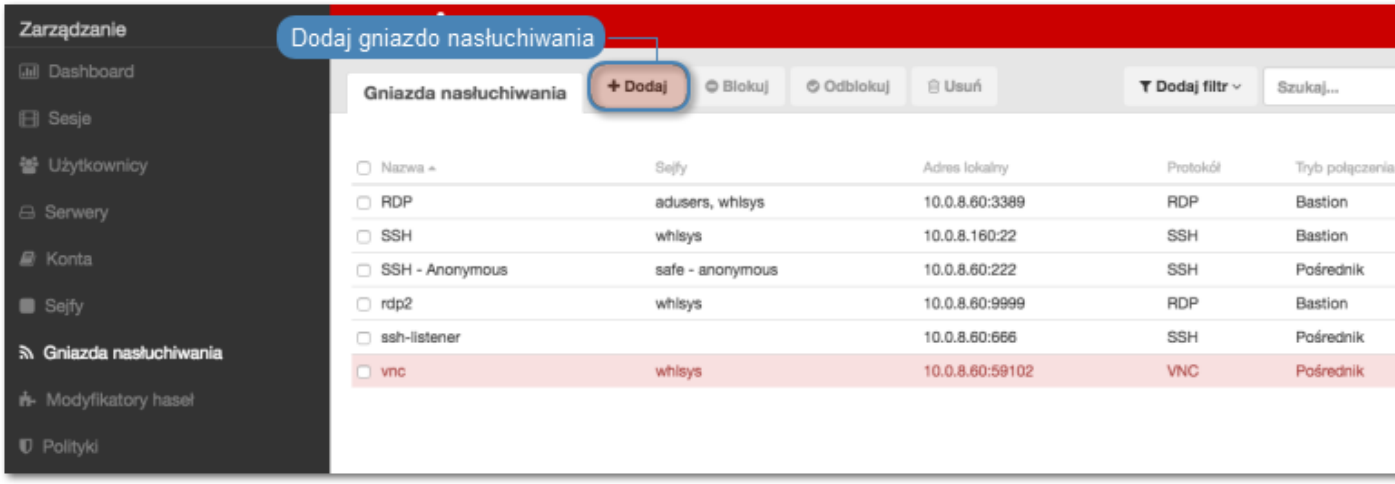
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.10 Dodawanie gniazda nasłuchiwania Telnet

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `Telnet`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

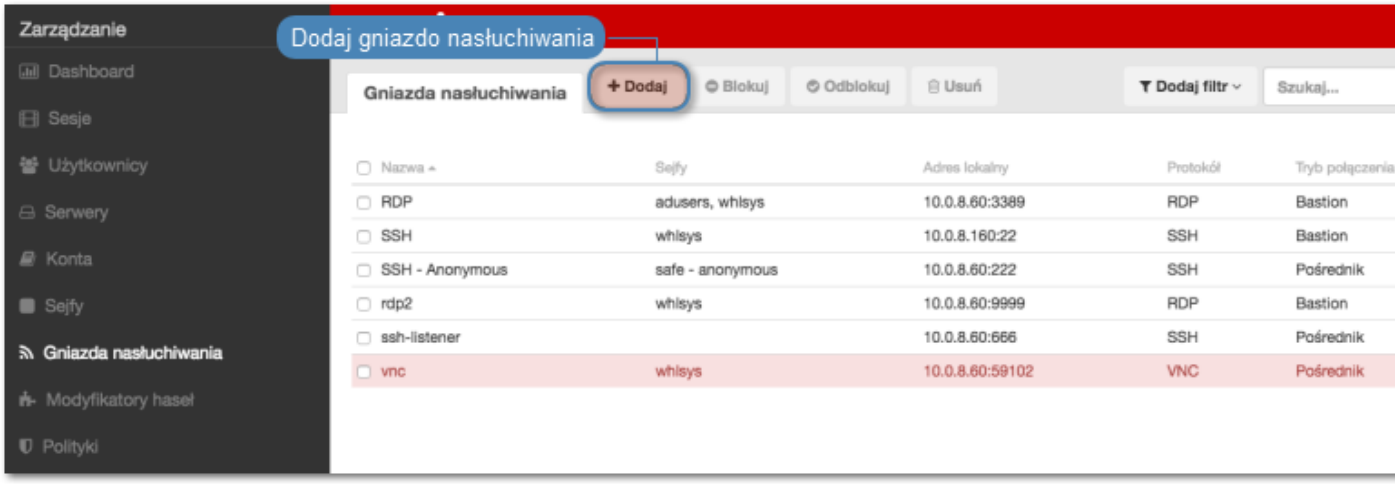
8. Zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*, aby połączenie było szyfrowane.
9. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
10. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
11. W polu *Certyfikat TLS*, kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.11 Dodawanie gniazda nasłuchiwania Telnet 3270

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `Telnet 3270`.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

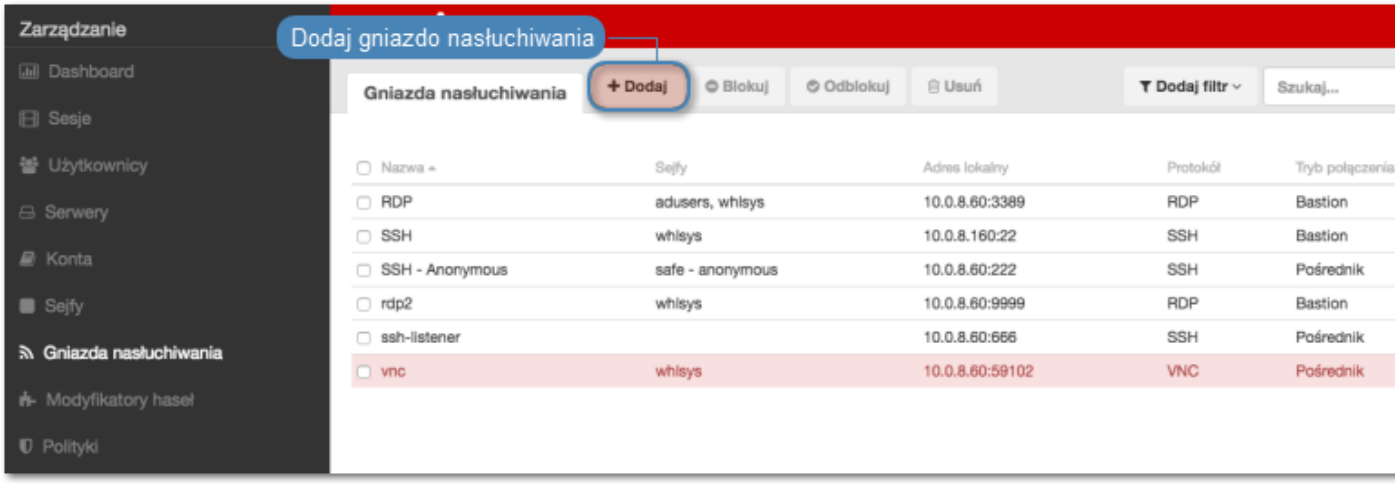
8. Zaznacz opcję *Użyj bezpiecznych połączeń (TLS)*, aby połączenie było szyfrowane.
9. Zaznacz opcję *Włącz obsługę SSLv2*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
10. Zaznacz opcję *Włącz obsługę SSLv3*, aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 3.
11. W polu *Certyfikat TLS*, kliknij ikonę pobierania, aby pobrać klucz publiczny serwera.
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.1.12 Dodawanie gniazda nasłuchiwania VNC

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.



3. Wprowadź nazwę obiektu.
4. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
5. Z listy rozwijalnej *Protokół*, wybierz `VNC`.
6. W polu *Komunikat*, wprowadź informację, która będzie wyświetlana użytkownikom na ekranie logowania.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Informacje ogólne* > *Scenariusze wdrożenia*.

`Brama`

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

`Pośrednik`

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

`Przezroczysty`

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

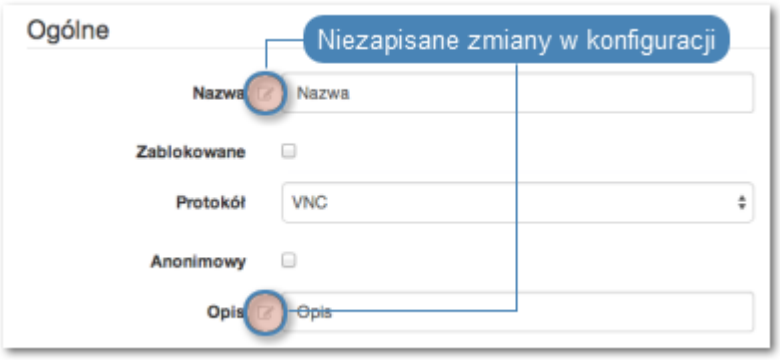
9.2 Modyfikowanie gniazda nasłuchiwania

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście definicję gniazda nasłuchiwania, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę gniazda nasłuchiwania.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną .



5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

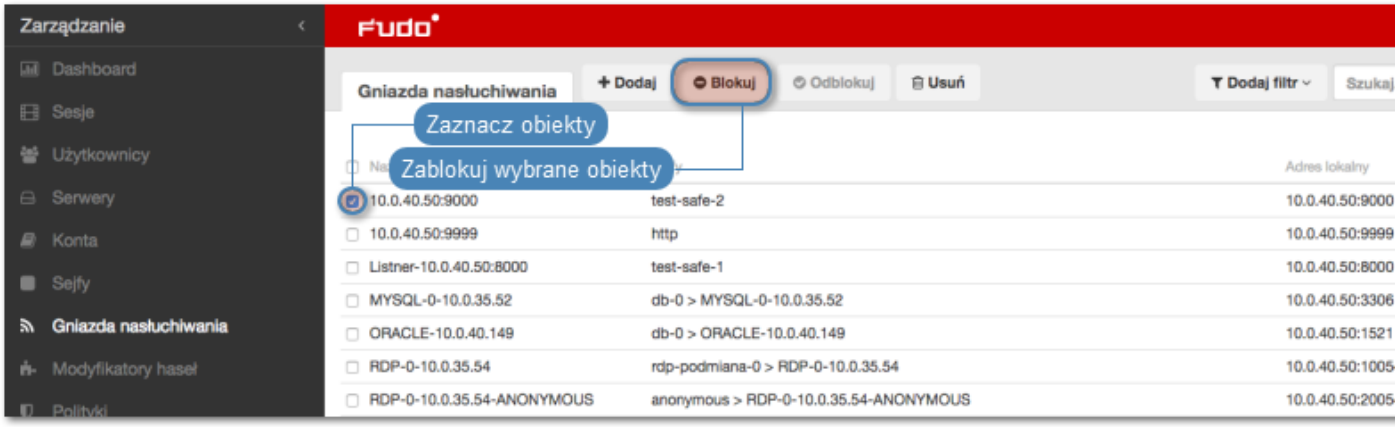
9.3 Blokowanie gniazda nasłuchiwania

Ostrzeżenie: Zablokowanie gniazda spowoduje zerwanie aktualnie trwających sesji z serwerami, w połączeniach z którymi pośredniczy wybrane gniazdo nasłuchiwania.

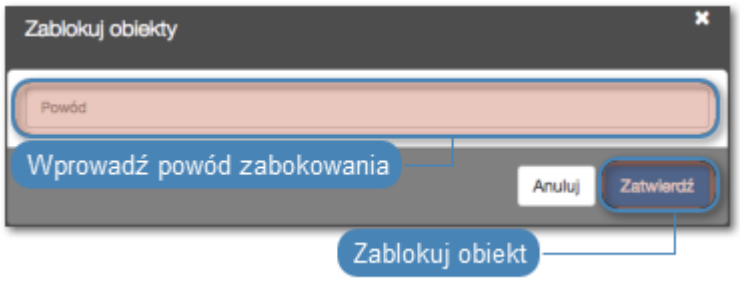
1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerami, z którymi połączenia realizowane są za pośrednictwem danego gniazda nasłuchiwania.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.



Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

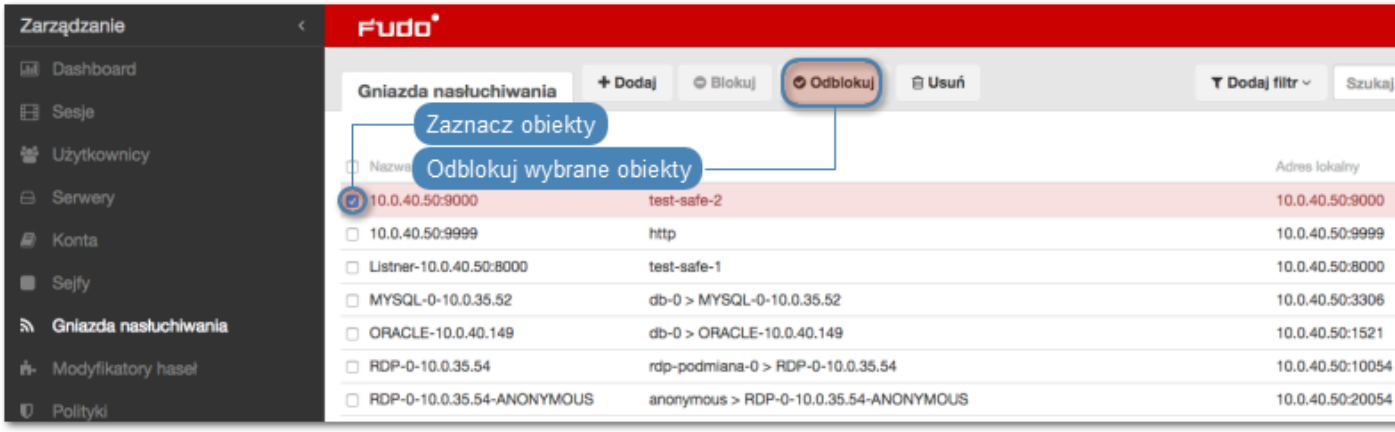
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

9.4 Odblokowanie gniazda nasłuchiwania

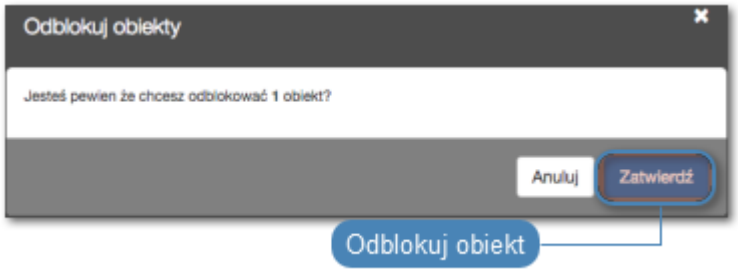
1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.



Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

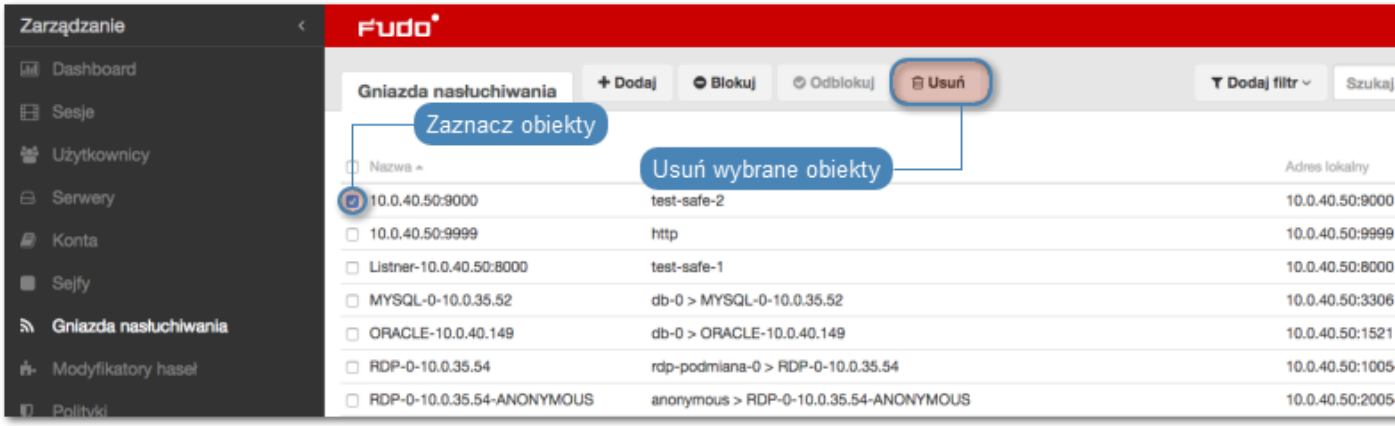
9.5 Usuwanie gniazda nasłuchiwania

Ostrzeżenie: Usunięcie gniazda nasłuchiwania spowoduje przerwanie aktualnie trwających sesji połączeniowych korzystających z usuniętego obiektu.

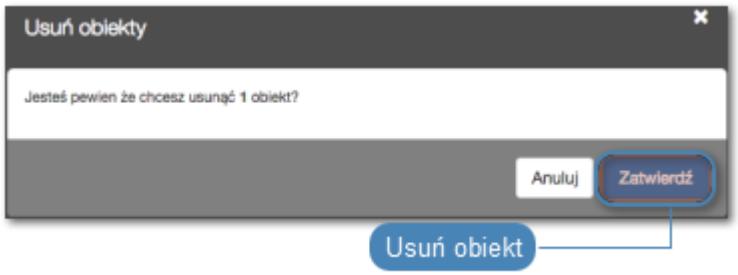
1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.



4. Kliknij *Zatwierdź*, aby potwierdzić usunięcie zaznaczonych obiektów.



Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

ROZDZIAŁ 10

Modyfikatory haseł

Wheel Fudo PAM umożliwia zarządzanie hasłami dostępu do kont uprzywilejowanych zdefiniowanych na monitorowanych systemach. Funkcjonalność modyfikatorów haseł wspiera następujące scenariusze:

- Unix poprzez SSH
- MySQL na serwerze Unix poprzez SSH
- Cisco poprzez SSH i Telnet
- Cisco Enable Password poprzez SSH i Telnet
- Microsoft Windows poprzez WMI
- LDAP

10.1 Polityki haseł

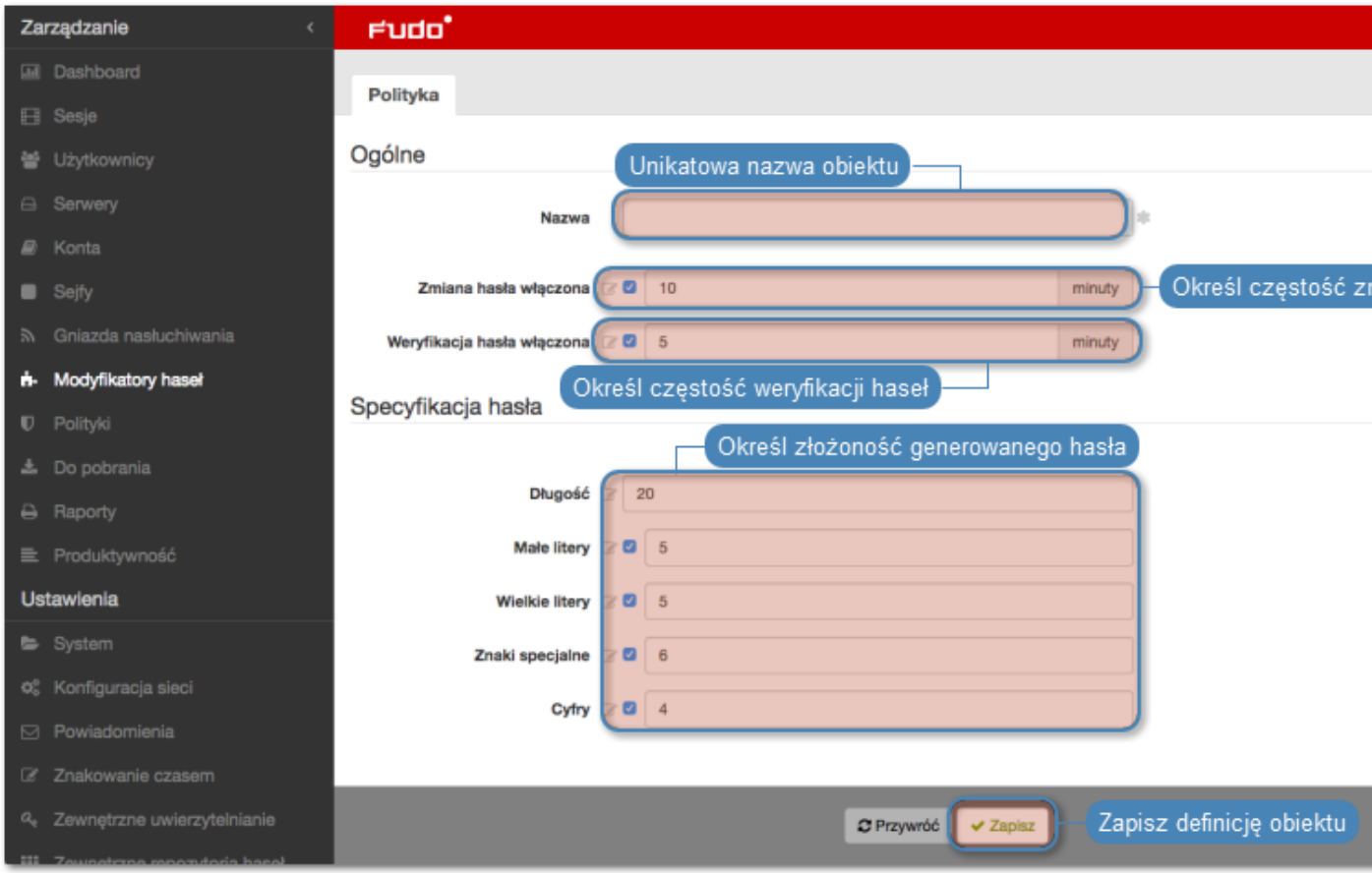
Polityka zmiany haseł określa częstotliwość zmiany hasła oraz jego złożoność.

10.1.1 Dodawanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij + *Dodaj*.
3. Wprowadź nazwę dla modyfikatora haseł.
4. Zaznacz opcję *Zmiana hasła włączona* i zdefiniuj jak często hasło ma być zmieniane.
5. Zaznacz opcję *Weryfikacja hasła włączona* i zdefiniuj jak często sprawdzane będzie, czy hasło nie zostało zmienione w sposób nieuprawiony.
6. W sekcji *Specyfikacja hasła*, określ złożoność generowanego ciągu znaków.

Parametr	Opis
Długość	Liczba znaków hasła.
Małe litery	Określ, czy hasło ma zawierać małe litery i ich minimalną liczbę.
Duże litery	Określ, czy hasło ma zawierać wielkie litery i ich minimalną liczbę.
Znaki specjalne	Określ, czy hasło ma zawierać znaki specjalne i ich minimalną liczbę.
Cyfry	Określ, czy hasło ma zawierać cyfry i ich minimalną liczbę.

7. Kliknij *Zapisz*.



10.1.2 Edytowanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Odszukaj i kliknij wybraną politykę.
3. Zmodyfikuj parametry konfiguracyjne.
4. Kliknij *Zapisz*.

10.1.3 Usuwanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Zaznacz wybrane polityki zmiany haseł.

3. Kliknij *Usuń*.
4. Potwierdź usunięcie obiektów.

Tematy pokrewne:

- *Model danych*
- *Konta*
- *Uniwersalne modyfikatory haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

10.2 Uniwersalne modyfikatory haseł

Uniwersalne modyfikatory haseł umożliwiają zdefiniowanie sekwencji komend, które zostaną wykonane na zdalnej maszynie w celu zmiany hasła.

10.2.1 Dodawanie uniwersalnego modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Kliknij *+ Dodaj*.
4. Zdefiniuj nazwę modyfikatora haseł.
5. Kliknij *+*, aby dodać komendę.
6. Wprowadź komendę.

Informacja: W komendach można stosować zmienne wymienione w sekcji *Lista zmiennych*. Ciąg znaków definiujący zmienną, zawarty pomiędzy znakami **%%**, zostanie zamieniony w każdej komendzie (np. `%%host%%`).

- *host* - adres IP lub nazwa mnemoniczna serwera docelowego (użycie nazwy mnemonicznej wymaga skonfigurowania serwera DNS)
- *port* - numer portu
- *login* - login użytkownika
- *secret* - aktualne hasło użytkownika
- *new_secret* - nowe hasło użytkownika

---

7. Dodaj opcjonalny opis.
8. Powtarzaj kroki 5-7, aby dodać kolejne komendy.

Informacja: Przeciągnij i upuść komendy aby zmieniać kolejność ich wykonania.

---

9. Powtarzaj kroki 5-8, aby zdefiniować weryfikator hasła w sekcji *Lista komend weryfikatora haseł*.

10. Kliknij *Zapisz*.
11. *Zdefiniuj politykę haseł* i *dodaj modyfikator do konta*.

Informacja: Przykład

W przykładowym modyfikatorze haseł, zmiana sekeretu wywoływana jest komendą `passwd`, która wymaga podania aktualnego hasła `secret` i dwókrotnego wprowadzenia nowego sekretu `new_secret`. Ostatnia komenda tworzy plik, który umożliwia późniejsze stwierdzenie pomyślnej zmiany hasła.

Zmiana hasła

1. passwd
2. %%secret%%
3. %%new_secret%%
4. %%new_secret%%
5. touch /tmp/%%login%%.passwd-changed

Weryfikacja

1. stat /tmp/%%login%%.passwd-changed | | exit 1
2. touch /tmp/%%login%%.passwd-verified

10.2.2 Edytowanie uniwersalnego modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Znajdź i kliknij wybrany modyfikator.
4. Zmień wybrane komendy.
5. Kliknij *X*, aby usunąć komendę.
6. Kliknij *Zapisz*.

10.2.3 Usuwanie modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Zaznacz wybrane obiekty i kliknij *Usuń*.
4. Potwierdź usunięcie wybranych obiektów.

Tematy pokrewne:

- *Model danych*
- *Konta*
- *Polityki haseł*

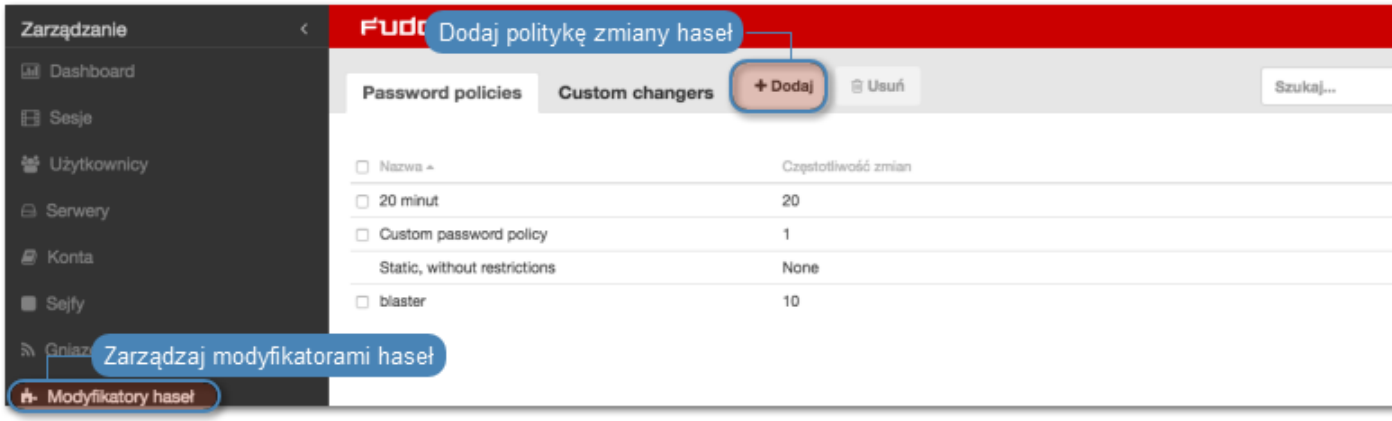
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

10.3 Konfigurowanie modyfikatora haseł Unix poprzez SSH

W tym rozdziale przedstawiony jest przykład konfigurowania automatycznej zmiany haseł na serwerze Unix.

Dodanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij + *Dodaj*.

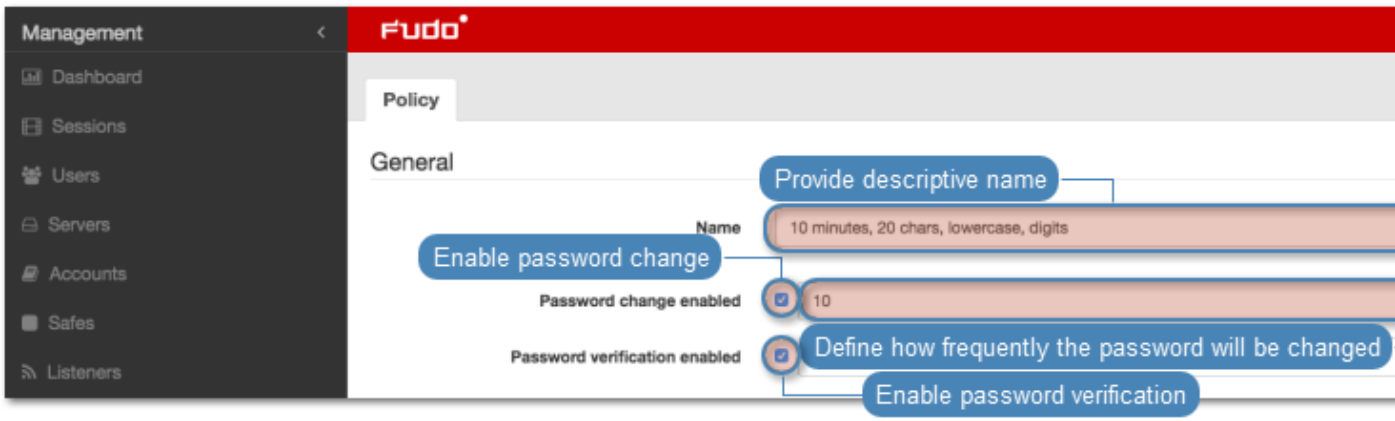


3. Wprowadź nazwę polityki zmany haseł.

Informacja: Opisowa nazwa pozwoli osobom administrującym Wheel Fudo PAM, szybko zorientować się w charakterystyce polityki zmiany haseł, np. `10 minut, 20 znaków, znaki specjalne, wielkie litery`.

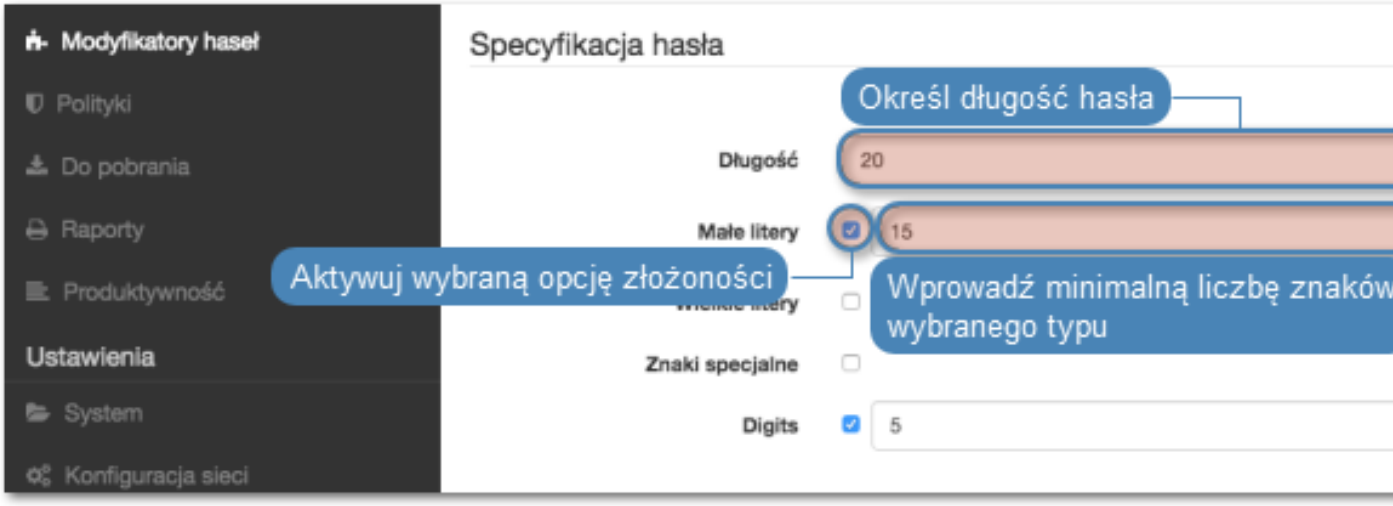
---

4. Zaznacz opcję *Zmiana haseł włączona* i zdefiniuj częstotliwość zmiany haseł.
5. Zaznacz opcję *Weryfikacja haseł włączona* i zdefiniuj jak często mechanizm będzie weryfikował, czy hasło nie zostało zmienione w sposób nieuprawniony.



6. Wprowadź liczbę znaków hasła.

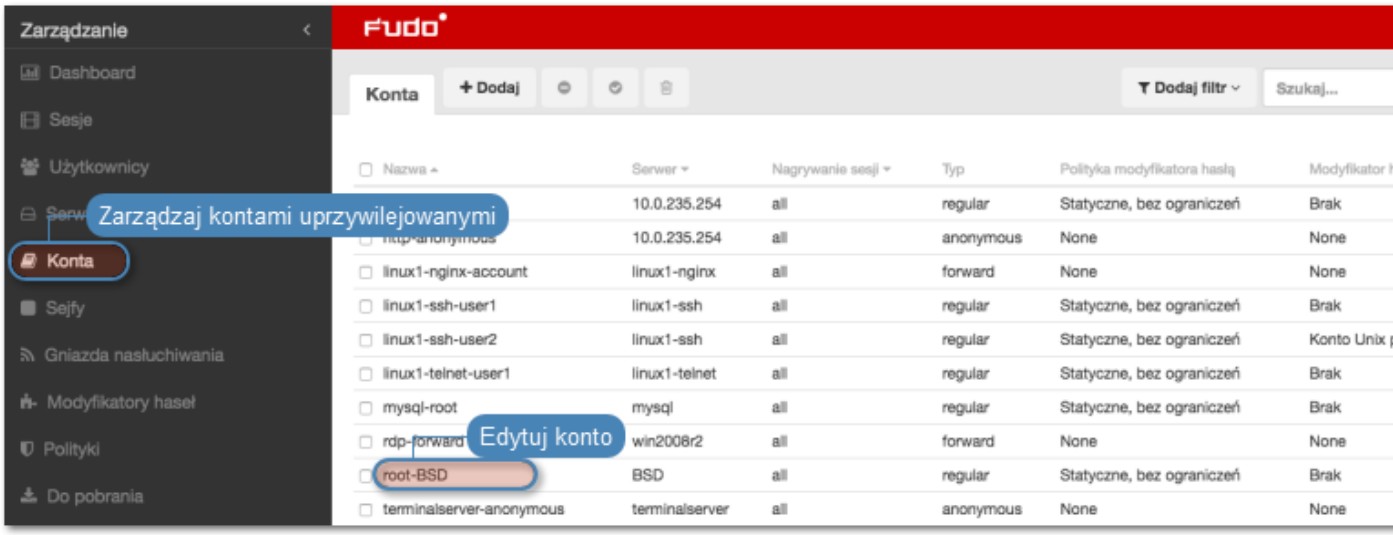
7. Zaznacz wybrane opcje złożoności hasła i wprowadź minimalną liczbę znaków dla każdej z nich.



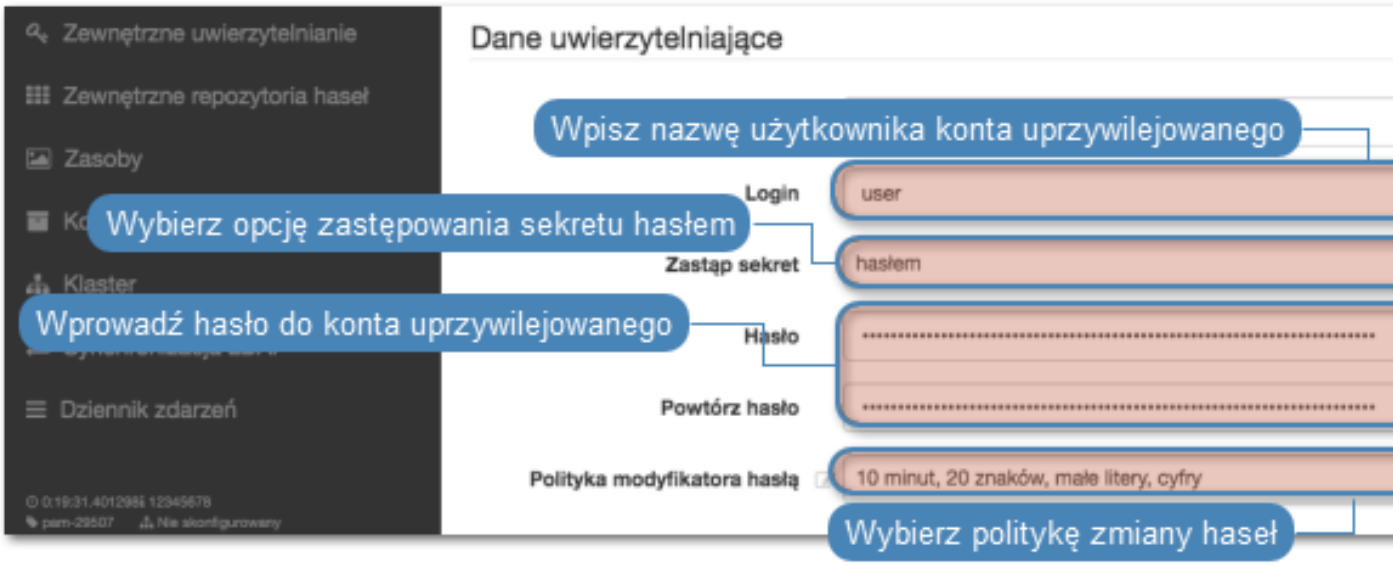
8. Kliknij *Zapisz*, aby zapisać politykę zmiany haseł.

Przypisanie modyfikatora haseł do konta uprzywilejowanego

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i kliknij wybrany obiekt.



3. W sekcji *Dane uwierzytelniające*, wprowadź login konta uprzywilejowanego.
4. Z listy rozwijalnej *Zastąp sekret*, wybierz `hasłem`.
5. Wprowadź hasło konta uprzywilejowanego.
6. Z listy rozwijalnej *Polityka modyfikatora hasła*, wybierz wcześniej zdefiniowaną politykę.



7. W sekcji *Modyfikator hasła*, wybierz `Unix Account over SSH`.
8. Uzupełnij dane logowania superużytkownika.

Informacja: Konto superużytkownika umożliwia resetowanie hasła w sytuacji, w której moduł *Secret manager* stwierdzi nieautoryzowaną zmianę hasła.

---

9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*
- Konfiguracja

10.4 Konfigurowanie modyfikatora haseł Windows WMI

W tym rozdziale przedstawiony jest przykład konfigurowania automatycznej zmiany haseł do konta na systemie Microsoft Windows poprzez WMI.

Informacja: Modyfikator haseł Windows WMI

Zastosowanie modyfikator haseł Windows WMI wymaga nadania zwykłym użytkownikom stosownych uprawnień.

- Wykonaj polecenie `winrm quickconfig`, aby wykryć ewentualne problemy, włączyć opcję *LocalAccountTokenFilterPolicy* i odblokować porty na wewnętrznym firewallu.
- Jeśli *winrm* nie jest dostępne, wykonaj komendę `cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f`

  Dodatkowo odblokuj porty dla WMI i DCOM oraz zmień typ interfejsu na *Sieć biurowa*.

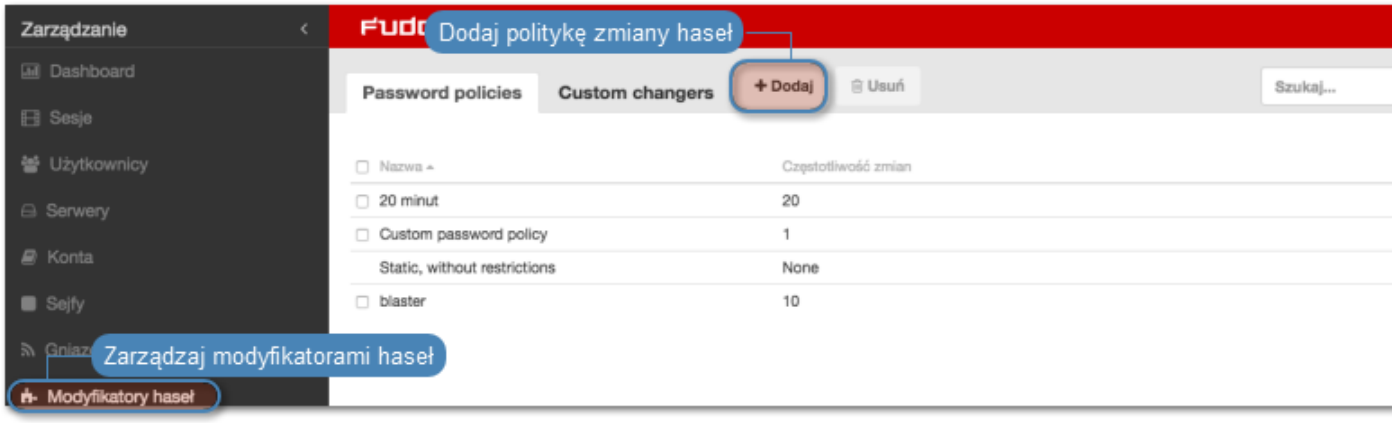
Jeśli żadna z powyższych metod nie przyniesie spodziewanych rezultatów, należy jawnie nadać użytkownikowi lub grupie uprawnienia do WMI i DCOM za pomocą *wmimgmt.msc* i *dcomcnfg*:

- http://www-01.ibm.com/support/docview.wss?uid=swg21681046
- https://technet.microsoft.com/en-us/library/cc771551(v=ws.11).aspx

---

Dodanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij + *Dodaj*.



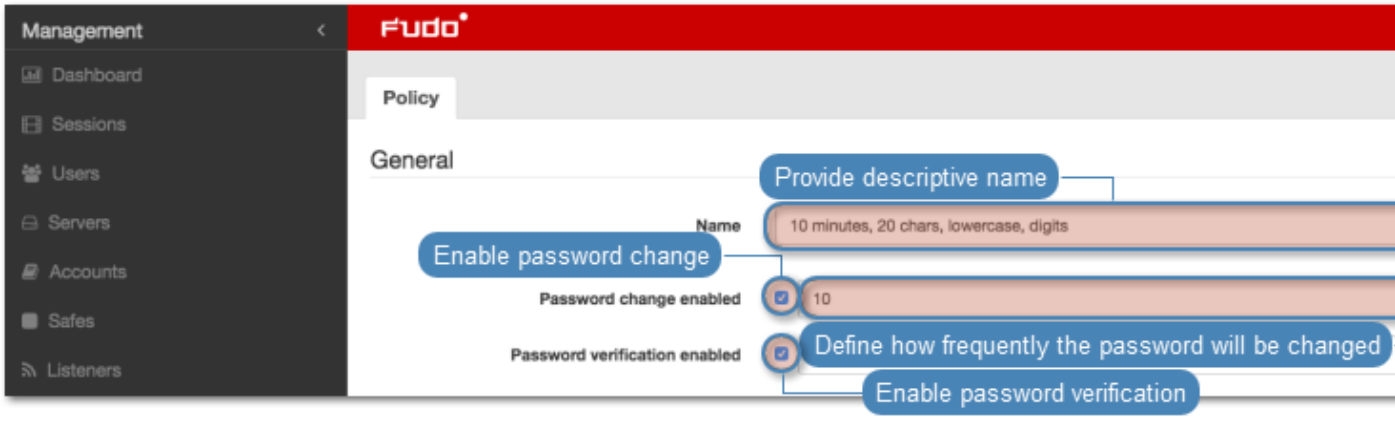
3. Wprowadź nazwę polityki zmany haseł.

Informacja: Opisowa nazwa pozwoli osobom administrującym Wheel Fudo PAM, szybko zorientować się w charakterystyce polityki zmiany haseł, np. `10 minut, 20 znaków, znaki specjalne, wielkie litery`.

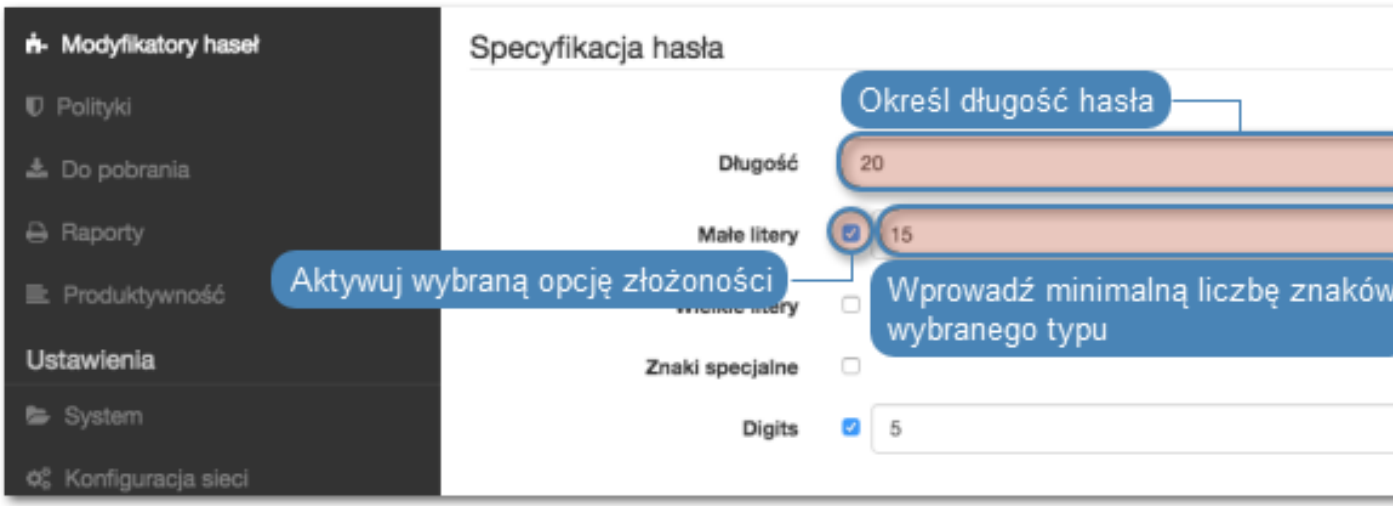
---

4. Zaznacz opcję *Zmiana haseł włączona* i zdefiniuj częstotliwość zmiany haseł.

5. Zaznacz opcję *Weryfikacja haseł włączona* i zdefiniuj jak często mechanizm będzie weryfikował, czy hasło nie zostało zmienione w sposób nieuprawniony.



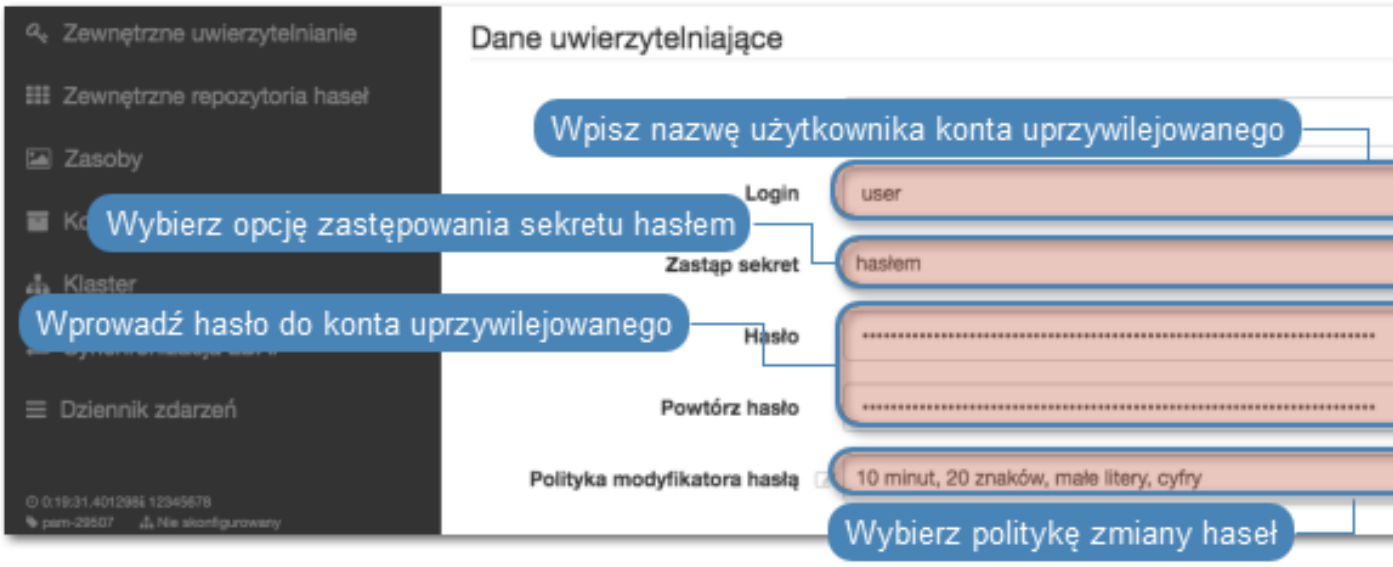
6. Wprowadź liczbę znaków hasła.
7. Zaznacz wybrane opcje złożoności hasła i wprowadź minimalną liczbę znaków dla każdej z nich.



8. Kliknij *Zapisz*, aby zapisać politykę zmiany haseł.

Przypisanie modyfikatora haseł do konta uprzywilejowanego

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i kliknij wybrany obiekt.
3. W sekcji *Dane uwierzytelniające*, wprowadź login konta uprzywilejowanego.
4. Z listy rozwijalnej *Zastąp sekret*, wybierz `hasłem`.
5. Wprowadź hasło konta uprzywilejowanego.
6. Z listy rozwijalnej *Polityka modyfikatora hasła*, wybierz wcześniej zdefiniowaną politykę.



7. W sekcji *Modyfikator hasła*, wybierz `Windows Account over WMI`.
8. Uzupełnij dane logowania superużytkownika.

Informacja: Konto superużytkownika umożliwia resetowanie hasła w sytuacji, w której moduł *Secret manager* stwierdzi nieautoryzowaną zmianę hasła.

---

9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia RDP*
- *Wymagania*
- *Model danych*
- Konfiguracja

ROZDZIAŁ 11

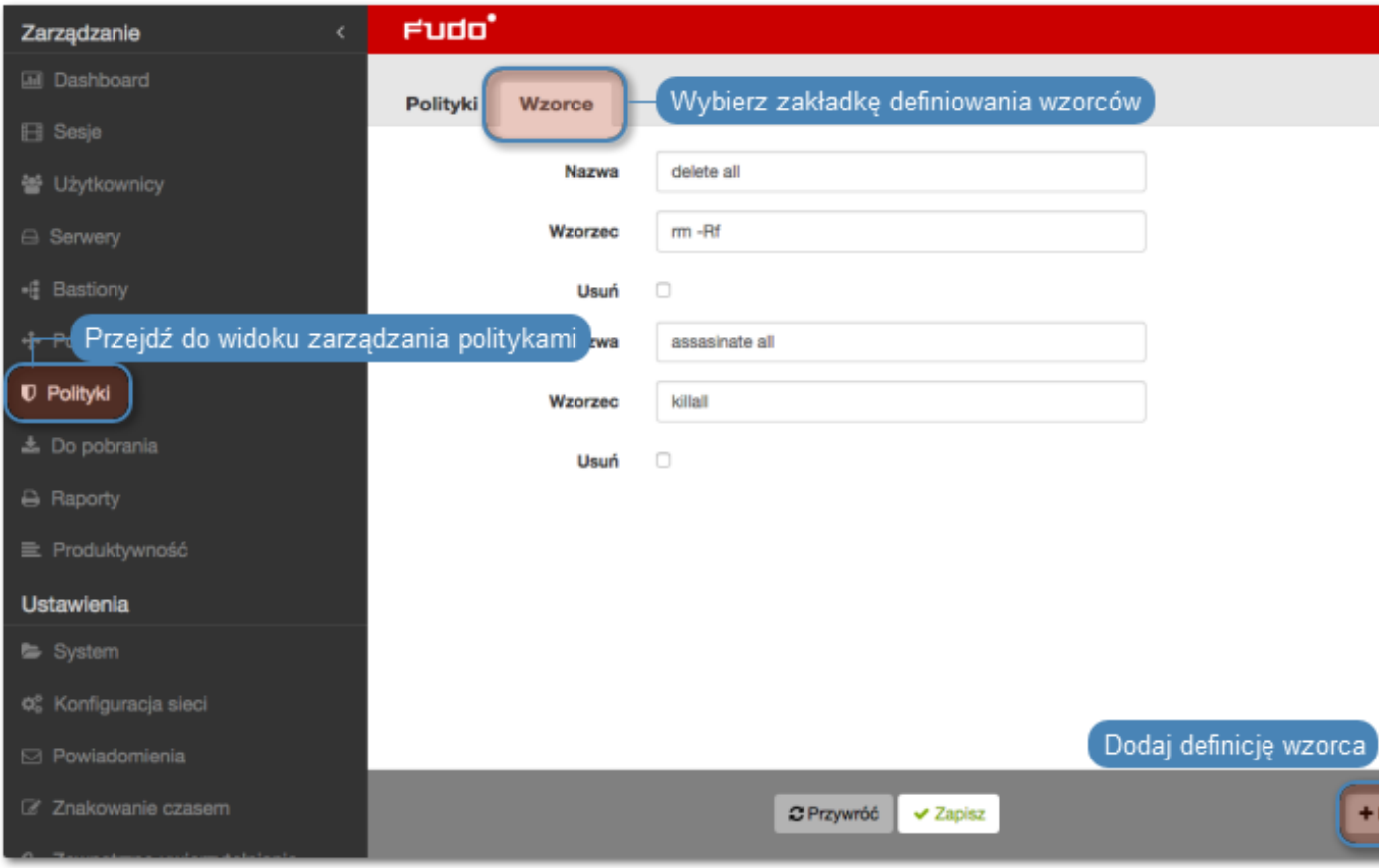
Polityki

Polityki to grupy definicji wzorców pozwalające na proaktywny monitoring przebiegu sesji. W przypadku wykrycia wzorca, Wheel Fudo PAM pozwala na automatyczne wstrzymanie sesji, zakończenie połączenia, zablokowanie użytkownika i wysłanie stosownego powiadomienia do administratora.

Definiowanie wzorców

Informacja: Wheel Fudo PAM wspiera wyrażenia regularne opisane standardem *POSIX Extended*.

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Wybierz zakładkę *Wzorce*.
3. Kliknij *+ Dodaj wzorzec*.

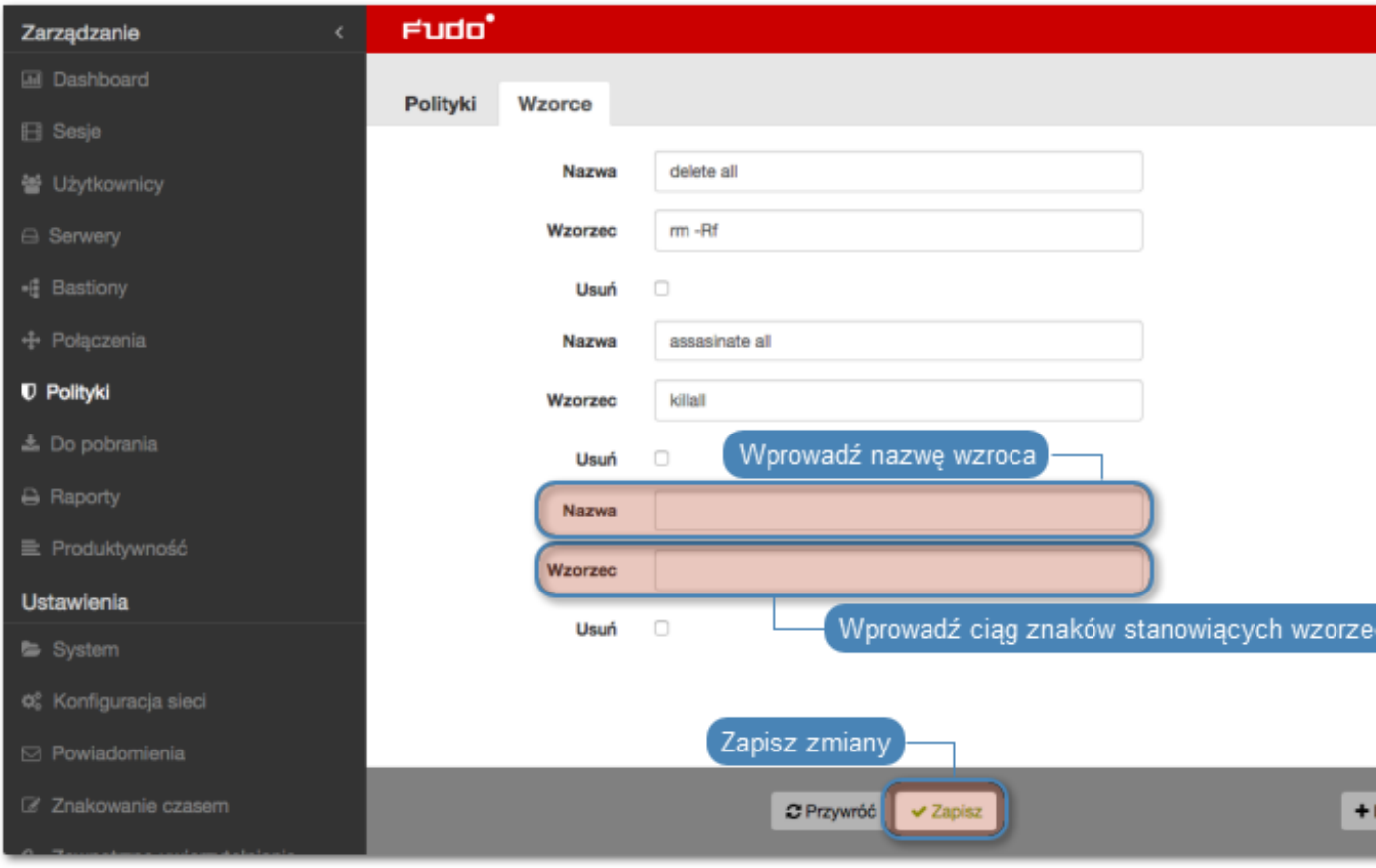


4. Zdefiniuj nazwę i ciąg znaków stanowiący wzorzec.

Informacja: Wheel Fudo PAM nie rozpoznaje wzorców zdefiniowanych z użyciem znaku \ (backslash); np. `\d`, `\D`, `\w`, `\W`.

---

5. Powtarzaj kroki 3-5, aby zdefiniować kolejne wzorce.
6. Kliknij *Zapisz*.



Informacja: Przykłady wyrażeń regularnych

Komenda `rm`

```
(^|[^a-zA-Z])rm[[:space:]]
```

Komenda `rm -rf` (*także* `-fr`; `-Rf`; `-fR`)

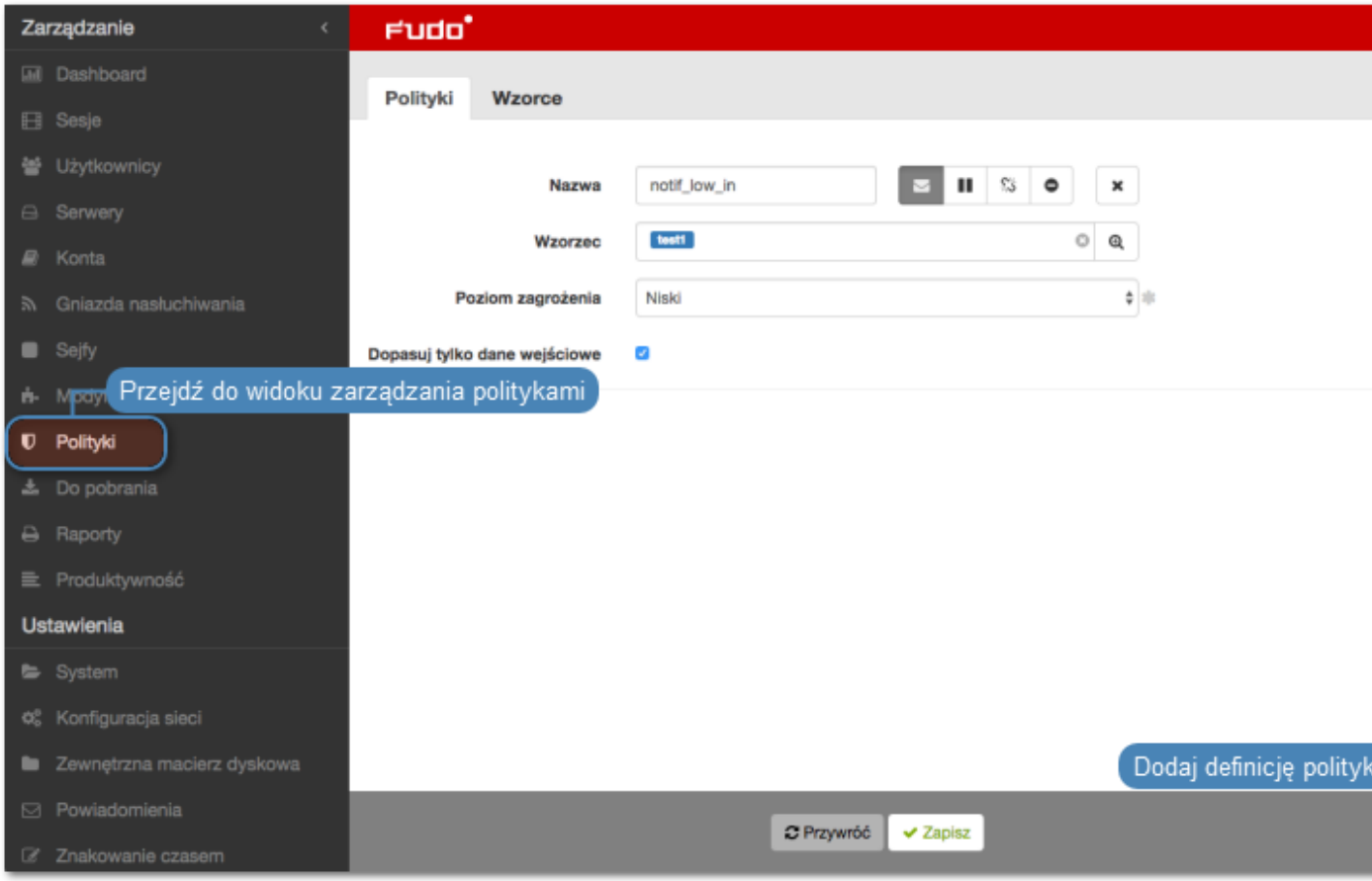
```
(^|[^a-zA-Z])rm[[:space:]]+-([rR]f|f[rR])
```

Komenda `rm file`

```
(^|[^a-zA-Z])rm[[:space:]]+([^[:space:]]+[[:space:]]*)?/full/path/to/a/
file([[:space:]]|\;|$) (^|[^a-zA-Z])rm[[:space:]]+.*justafilename
```

Definiowanie polityk

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Kliknij + *Dodaj politykę*.



3. Wprowadź nazwę dla definiowanej polityki.
4. Określ akcje, które Wheel Fudo PAM podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców.

	Wyślij powiadomienie email do administratora systemu.
	Wstrzymaj połączenie.
	Przerwij połączenie.
	Zablokuj konto użytkownika.

Informacja:

- Wysyłanie powiadomień wymaga skonfigurowania *usługi powiadomień* oraz zaznaczonej opcji *Wykrycie wzorca* w *ustawieniach sejfu*.
- Zablokowanie użytkownika powoduje automatyczne przerwanie połączenia.

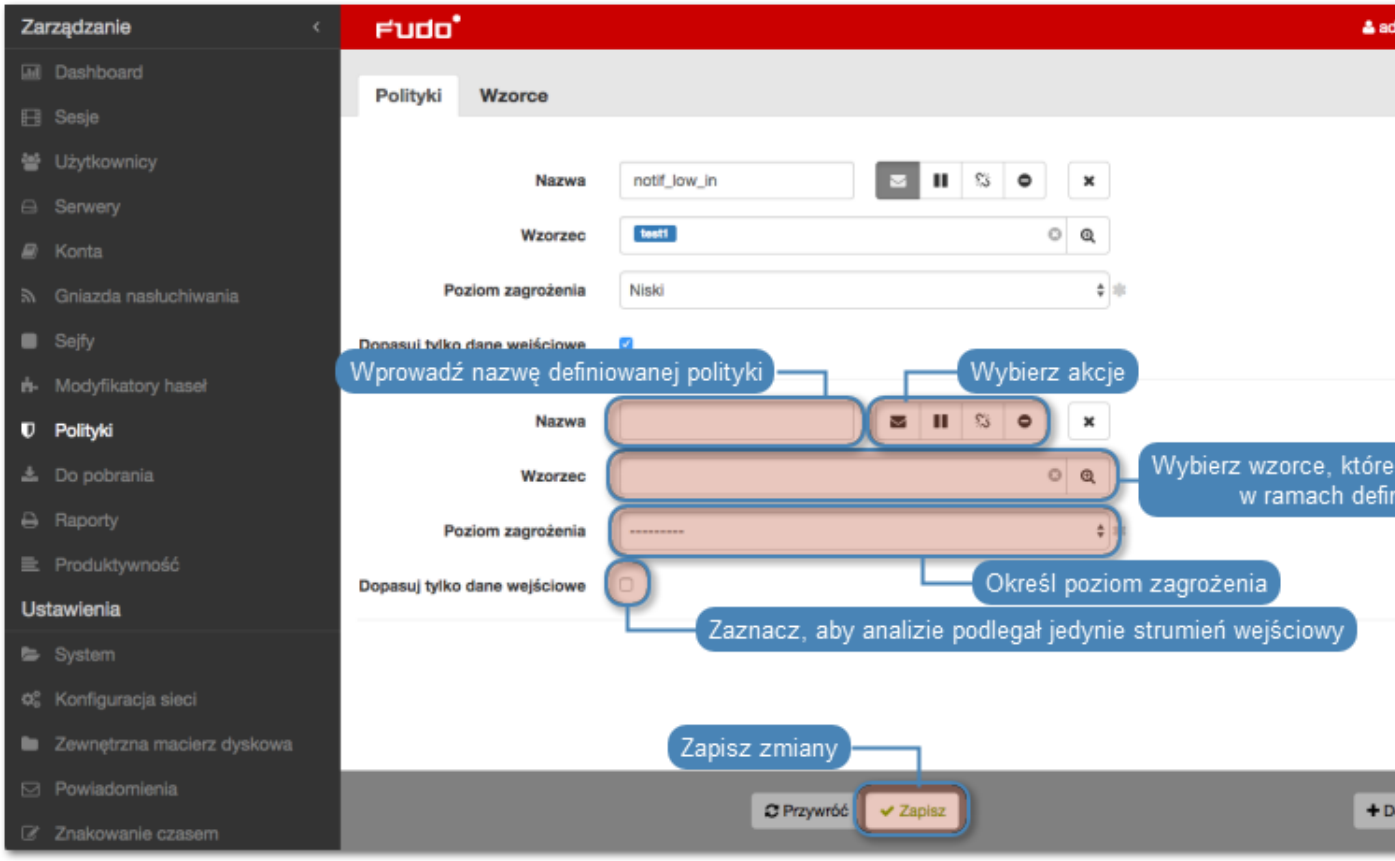
5. Wybierz wzorce śledzone w ramach danej polityki.
6. Określ poziom zagrożenia dla dodawanej polityki.

Informacja: Informacja o poziomie zagrożenia zawarta jest w treści powiadomienia.

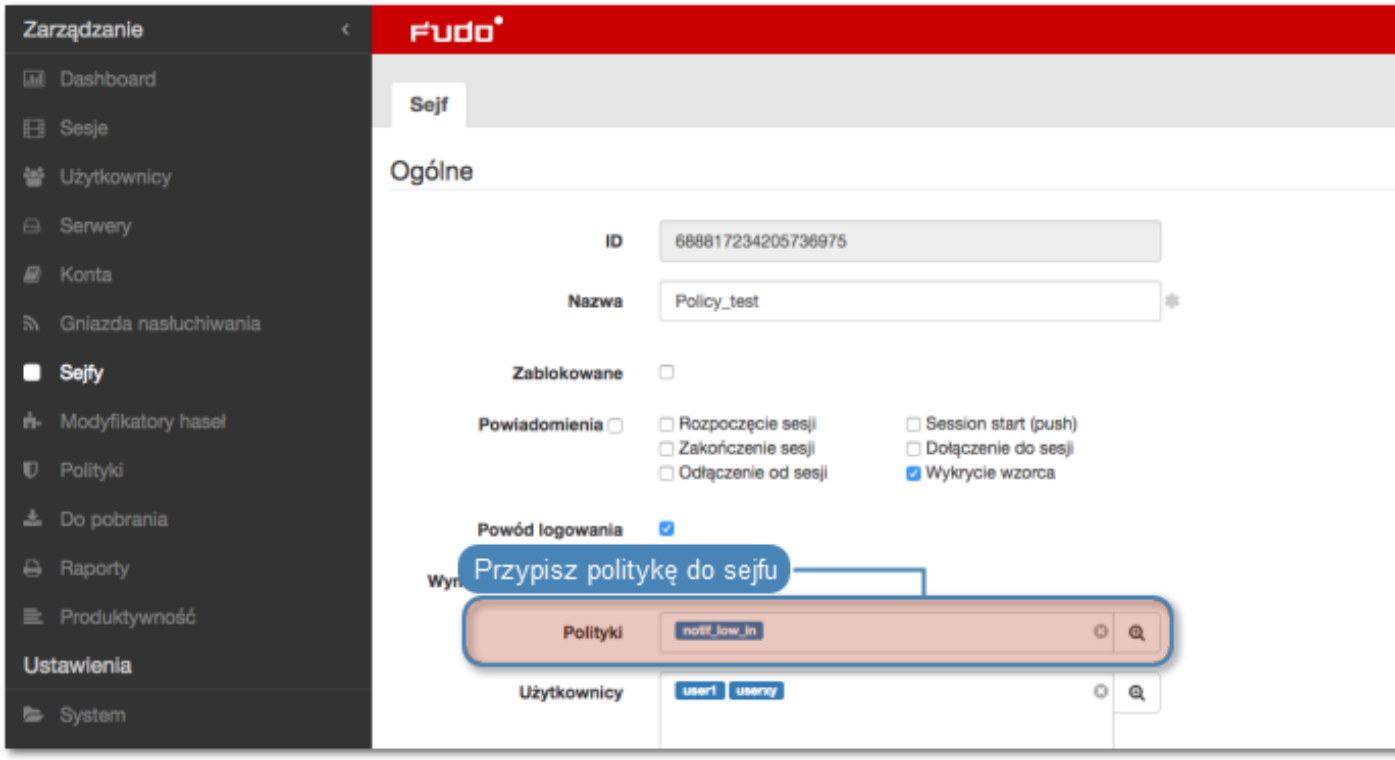
7. Zaznacz opcję *Dopasuj tylko dane wejściowe*, aby system reagował tylko na treści wprowadzone przez użytkownika.

Informacja: W przypadku protokołów RDP, VNC i MySQL, przetwarzaniu podlegają tylko dane wejściowe.

8. Kliknij *Zapisz*.

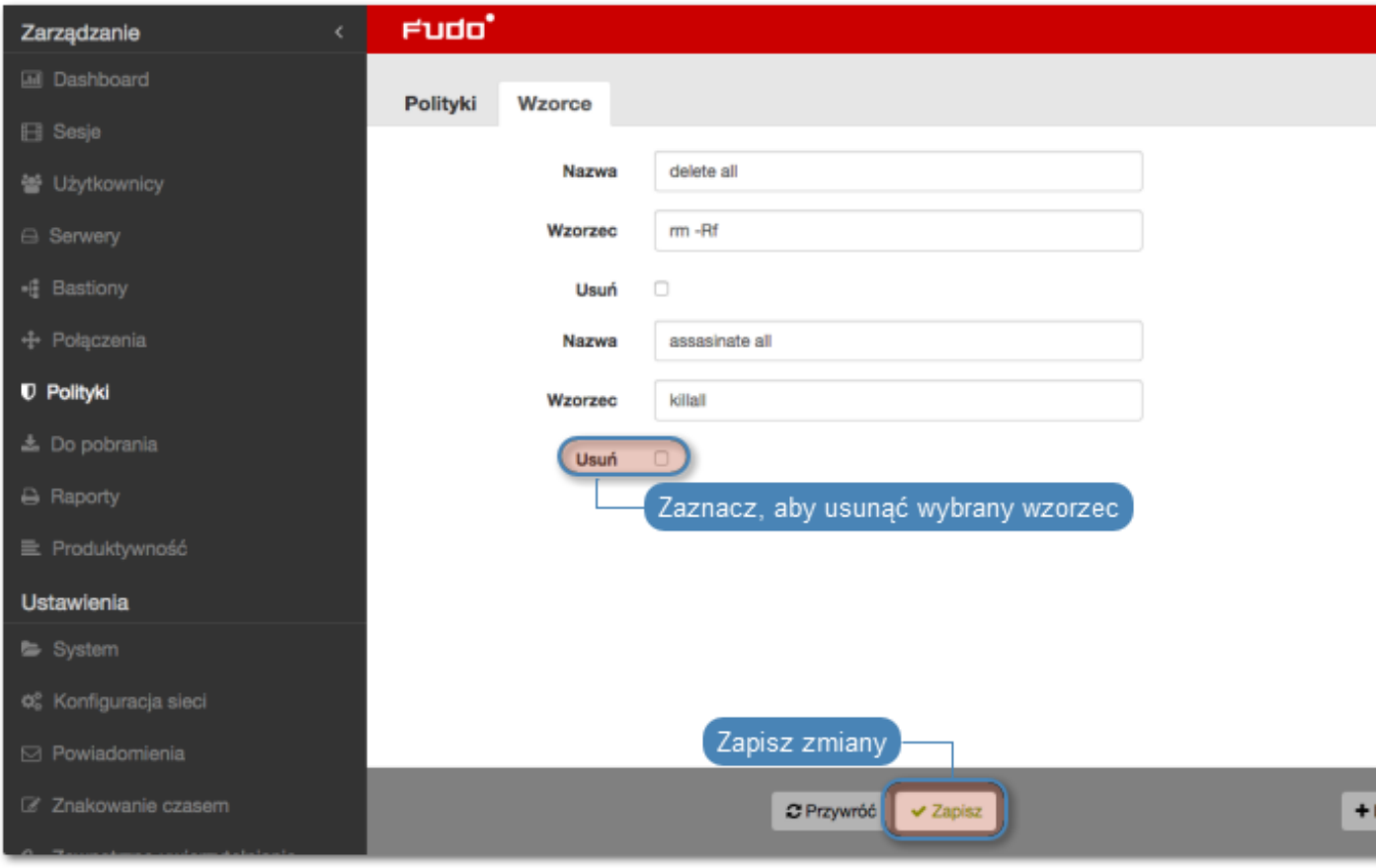


Informacja: Po utworzeniu polityki, przypisz ją do wybranego sejfu.



Usuwanie definicji wzorców

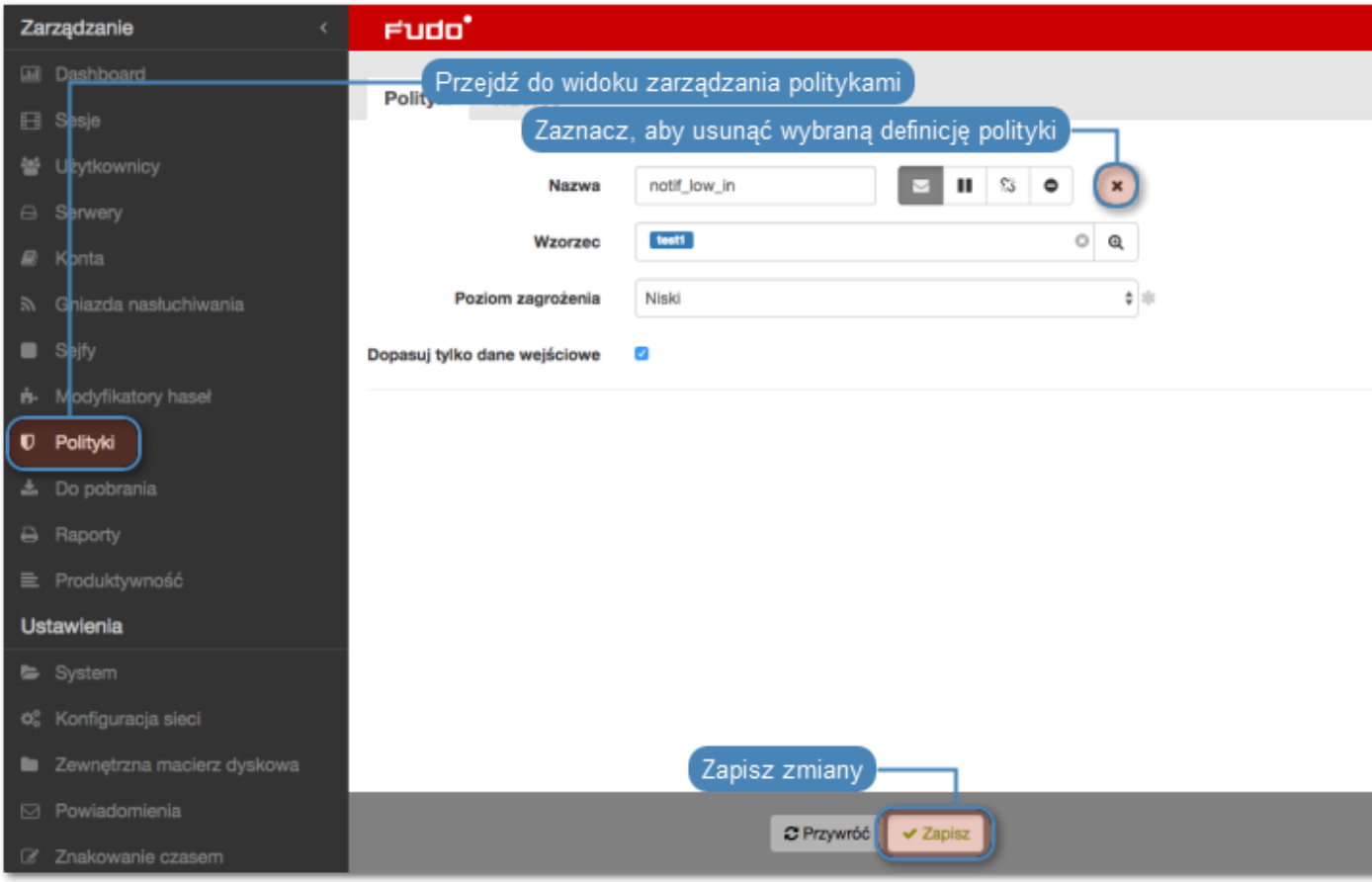
1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Wybierz zakładkę *Wzorce*.
3. Zaznacz opcję *Usuń* przy wybranym wzorcu.
4. Kliknij *Zapisz*.



Usuwanie definicji polityk

Aby usunąć definicję polityki, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Zaznacz opcję *Usuń* przy wybranej polityce.
3. Kliknij *Zapisz*.



Tematy pokrewne:

- *Przerywanie połączenia*
- *Powiadomienia*
- *Sejfy*
- *Bezpieczeństwo*

ROZDZIAŁ 12

Sesje

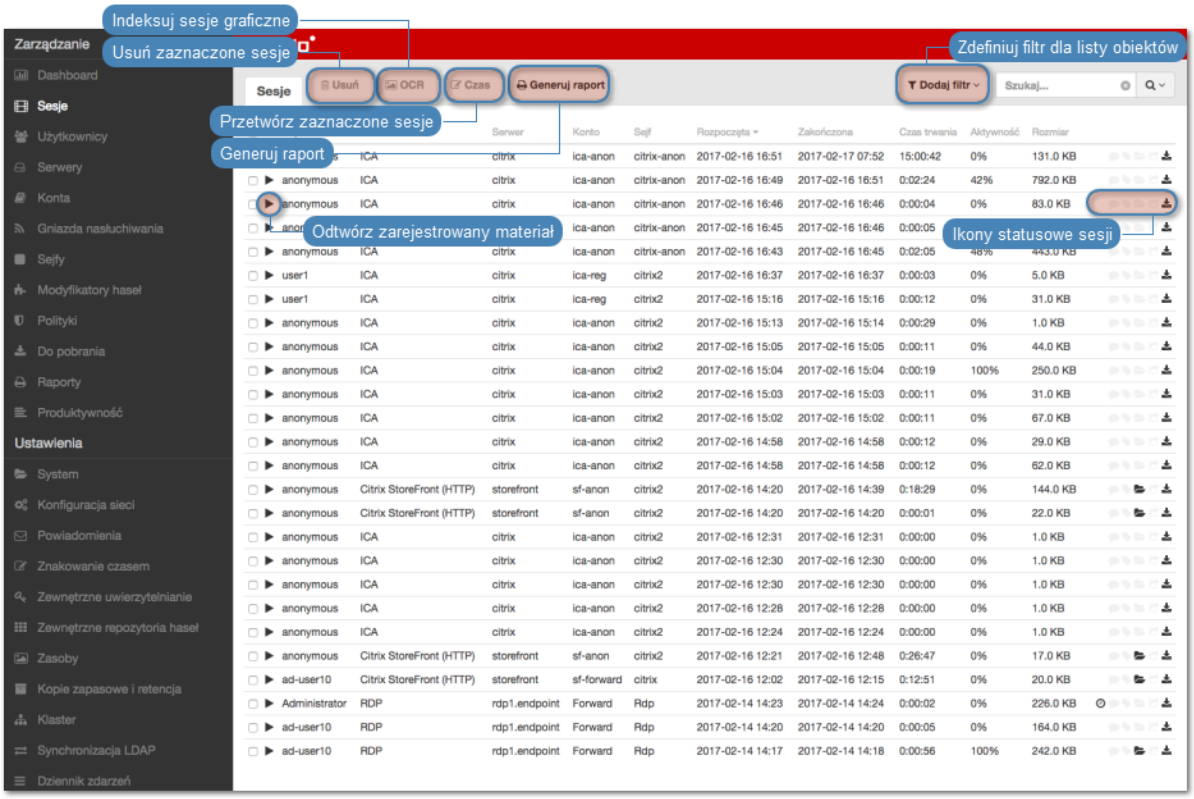
Wheel Fudo PAM przechowuje wszystkie nagrane sesje administracyjne, dając możliwość ich odtworzenia, przejrzenia, kasowania oraz eksportowania.

Widok zarządzania sesjami pozwala na filtrowanie zapisanych sesji, podgląd sesji aktualnie trwających oraz pobranie zapisanych sesji dostępu. Widok dostrcza także informacji statusowych na temat każdej z sesji oraz pozwala zarządzać wygenerowanymi wcześniej odnośnikami.

Ikona	Opis
▶	Odtwarzaj sesję (*dotyczy sesji nagranych z opcją rejestrowania pełnego ruchu*).
	Sesja opatrzona znacznikiem czasu.
	Powód nawiązania sesji.
	Sesja zawiera naniesione komentarze.
	Sesja została przetworzona na potrzeby przeszukiwania pełnotesktowego.
	Otwórz zarządzanie udostępnianiem sesji.
	Pobierz materiał sesji w wybranym formacie (*dotyczy sesji nagranych z opcją rejestrowania pełnego lub surowego ruchu*).
	Monitor aktywności użytkownika (*dotyczy sesji aktualnie trwających*).
	Nazwa użytkownika, który zaakceptował sesję wymagającą autoryzacji.
✔	Akceptacja połączenia oczekującego.
✖	Odrzucenie połączenia oczekującego.
?	Sesja oczekująca na akceptację.
✚	Element agregujący połączenia nawiązane w ramach tej samej sesji.

Aby przejść do widoku zarządzania sesjami wybierz z lewego menu opcję *Zarządzanie* > *Sesje*.

Informacja: Wheel Fudo PAM przechowuje materiał sesji w formie skompresowanej, z czego wynikać mogą różnice pomiędzy podawanym a faktycznym rozmiarem sesji.

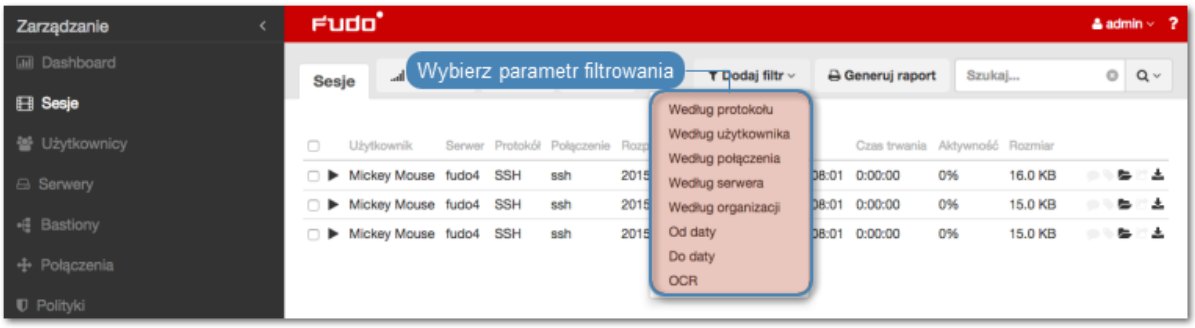


12.1 Filtrowanie sesji

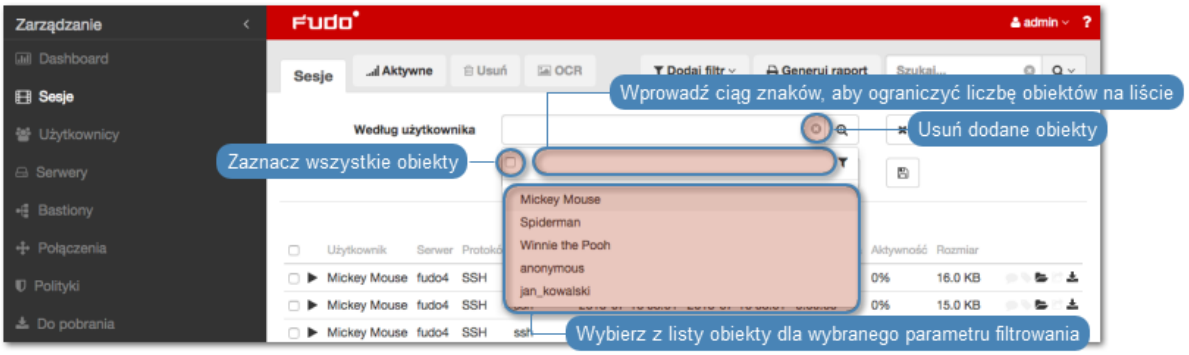
Filtrowanie pozwala na łatwiejsze odnalezienie żądanej sesji dzięki ograniczeniu ilości pozycji na liście zarejestrowanych sesji. Opcje filtrowania pozwalają na wybranie wielu obiektów jednego typu a zdefiniowany zestaw filtrów może zostać zapisany dla wygody operatora systemu.

12.1.1 Definiowanie filtrów

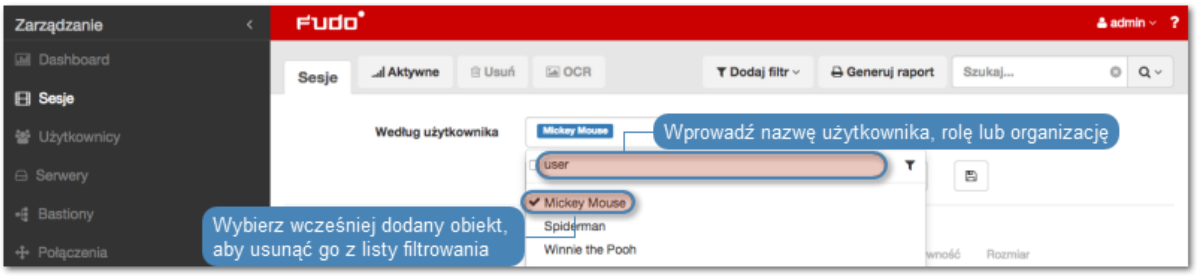
1. Kliknij *Dodaj filtr* i wybierz z listy rozwijalnej typ parametru filtrowania.



2. Wybierz wartości dla wcześniej dodanego parametru filtrowania.



Informacja: Wprowadź ciąg znaków, aby ograniczyć liczbę pozycji na liście. W przypadku użytkowników, zawartość listy można ograniczyć do użytkowników o przypisanej roli lub należących do określonej organizacji.



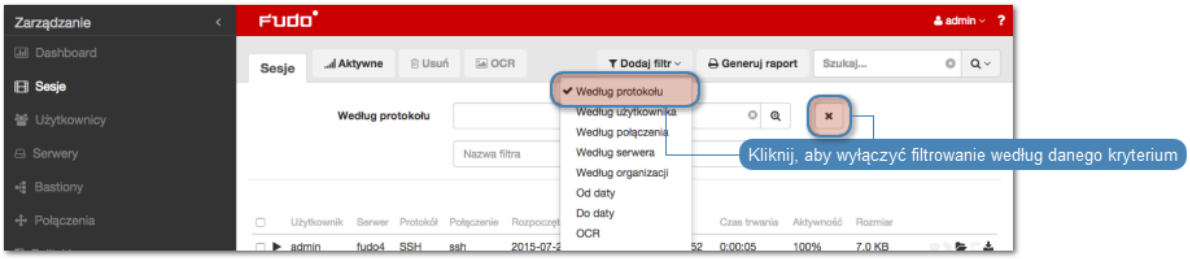
Ponownie wybierz wcześniej dodany obiekt, aby usunąć go z listy.

Dla parametrów filtrowania według protokołu, użytkownika, połączenia, serwera, organizacji możliwe jest wybranie wielu obiektów danego typu.

3. Powtarzaj kroki 1. i 2., aby zdefiniować kolejne kryteria filtrowania.

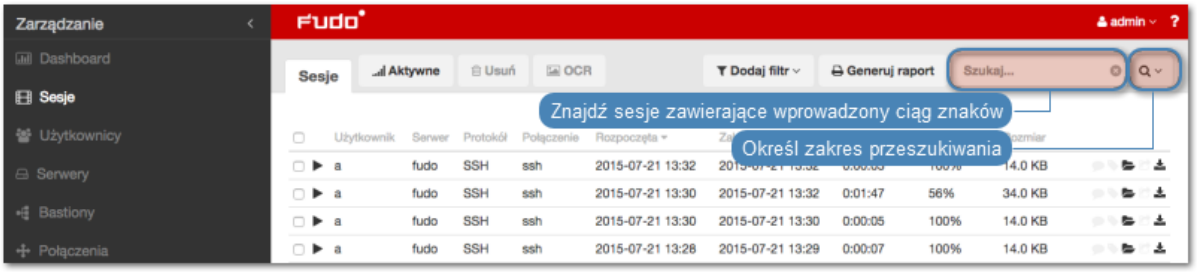
Informacja: Na liście sesji wyświetlone zostaną tylko pozycje, które spełniają wszystkie warunki filtrowania.

4. Kliknij *Dodaj filtr* i wybierz ponownie wcześniej zaznaczony parametr filtrowania, aby wyłączyć filtrowanie według zadanego parametru.



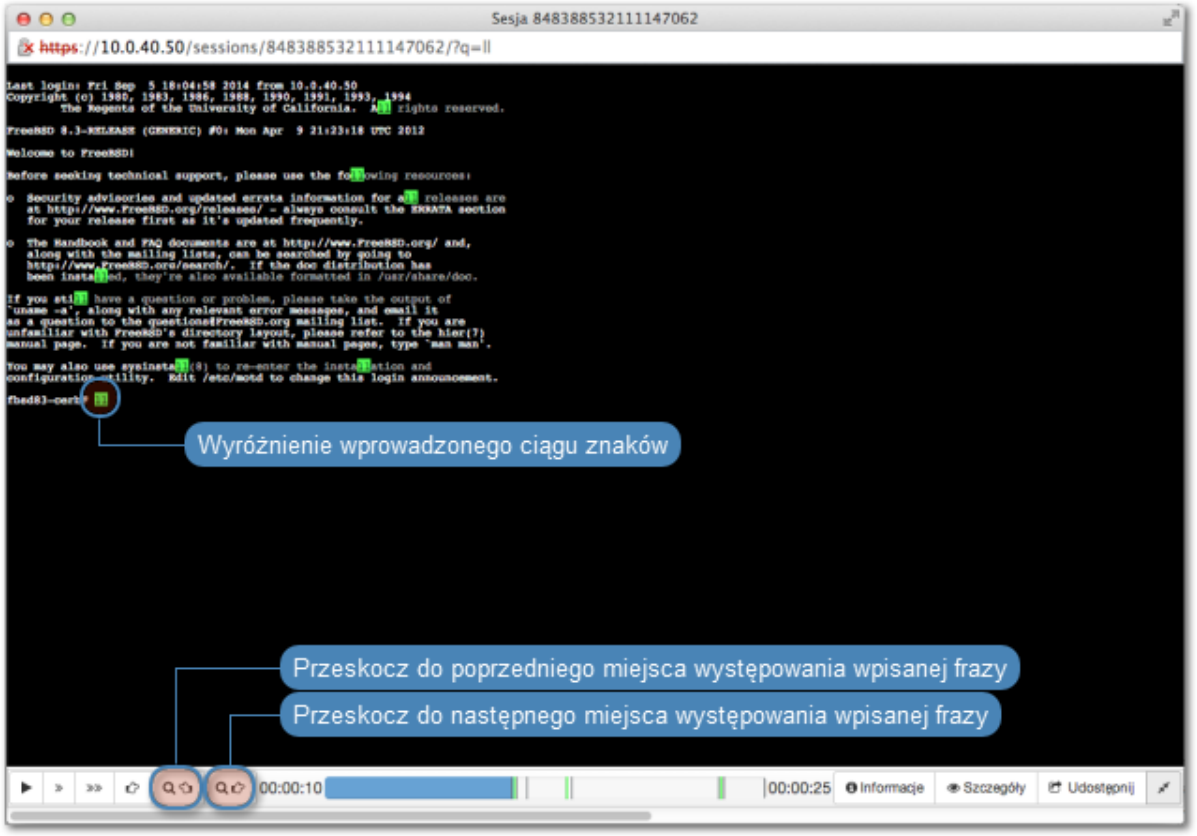
12.1.2 Przeszukiwanie pełnotekstowe

Wheel Fudo PAM pozwala na przeszukiwanie zapisanego materiału, ograniczając listę sesji do pozycji zawierających wskazany ciąg znaków.



Informacja: Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.

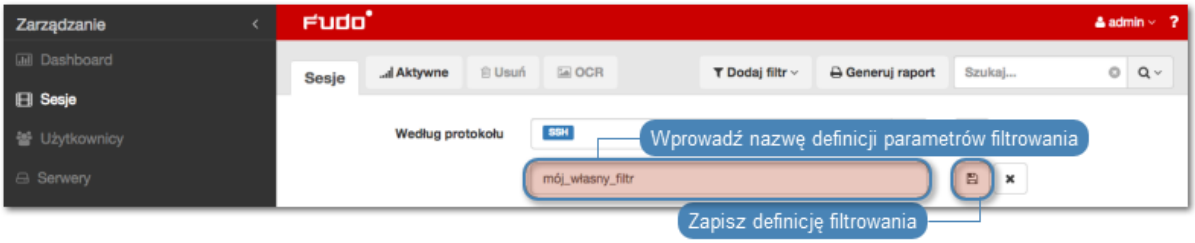


12.1.3 Zarządzanie definicjami filtrowania

Aktualne parametry filtrowania mogą zostać zapisane z wybraną nazwą dla wygody operatora systemu.

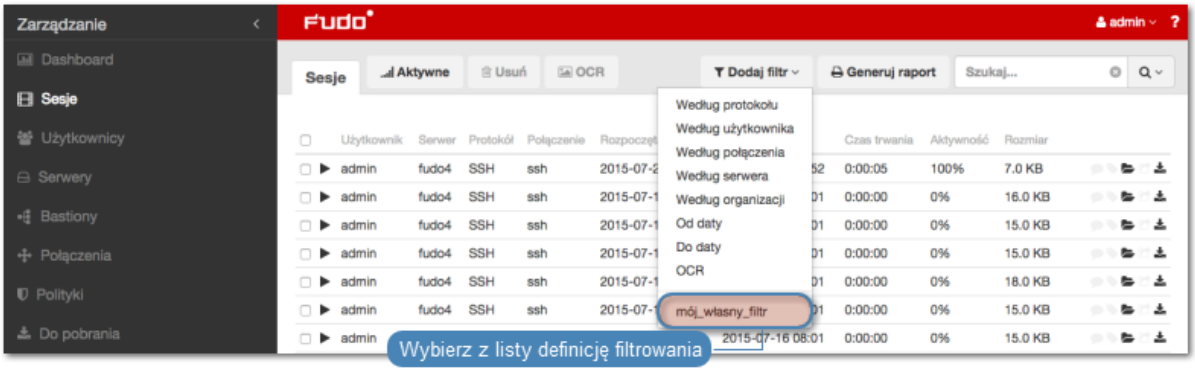
Zapisywanie definicji filtrowania

1. Zdefiniuj parametry filtrowania zgodnie z procedurą opisaną w sekcji *Filtrowanie sesji*.
2. Wprowadź nazwę definicji filtrowania.
3. Kliknij ikonę zapisu ustawień.



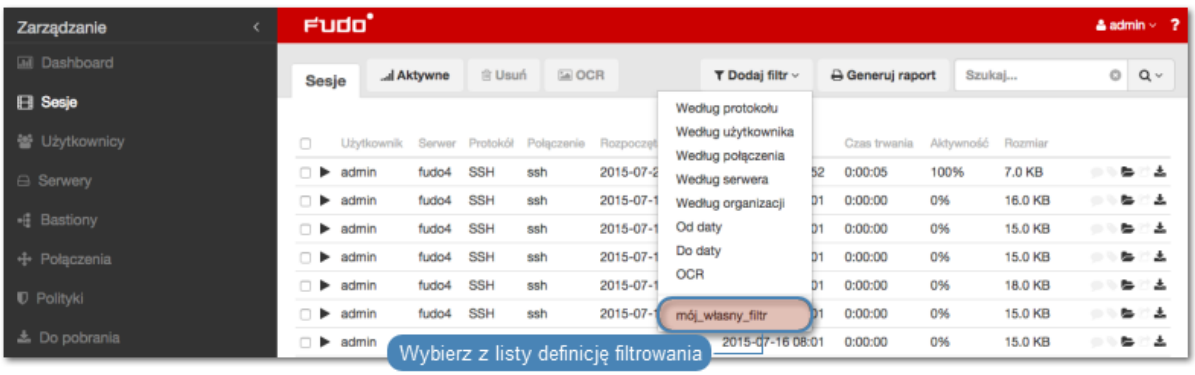
Edycja definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.
2. Zmodyfikuj opcje filtrowania zgodnie z potrzebą.
3. Kliknij ikonę zapisu ustawień.

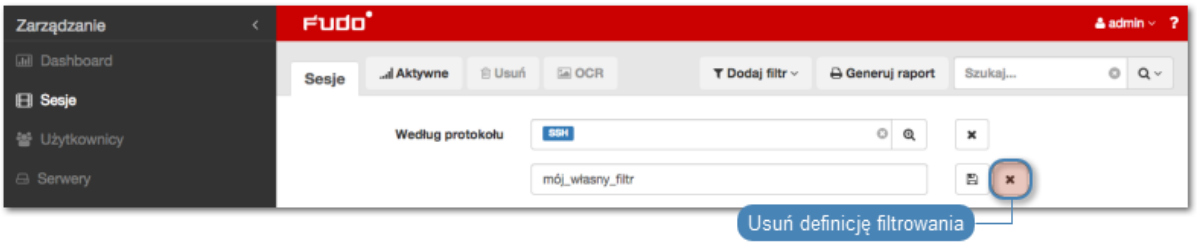


Usuwanie definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.



2. Kliknij ikonę usunięcia definicji filtrowania.



3. Potwierdź usunięcie wybranej definicji filtrowania.

Tematy pokrewne:

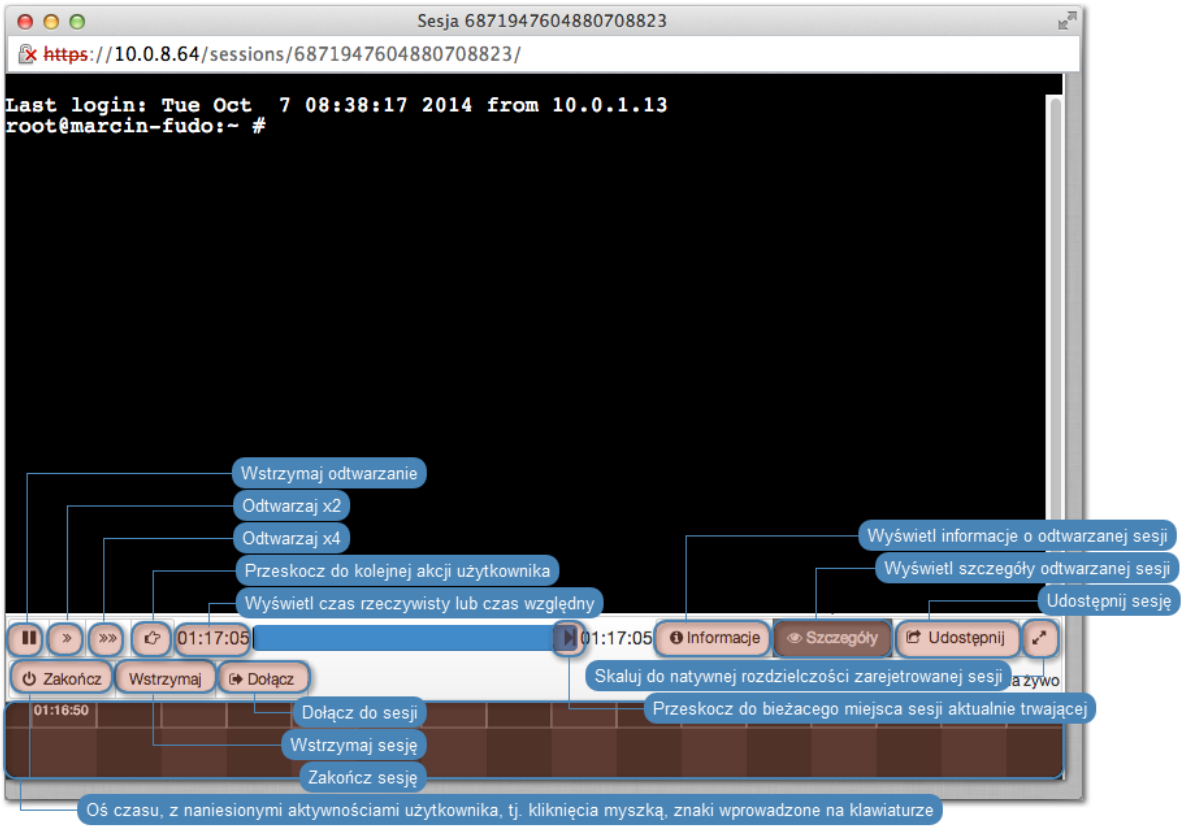
- *Widok zarządzania sesjami*
- *Opis systemu*
- *Raporty*

12.2 Odtwarzanie sesji

Wheel Fudo PAM pozwala zarówno na odtwarzanie zarejestrowanych sesji połączeniowej jak i podgląd aktualnie trwających połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj na liście żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.

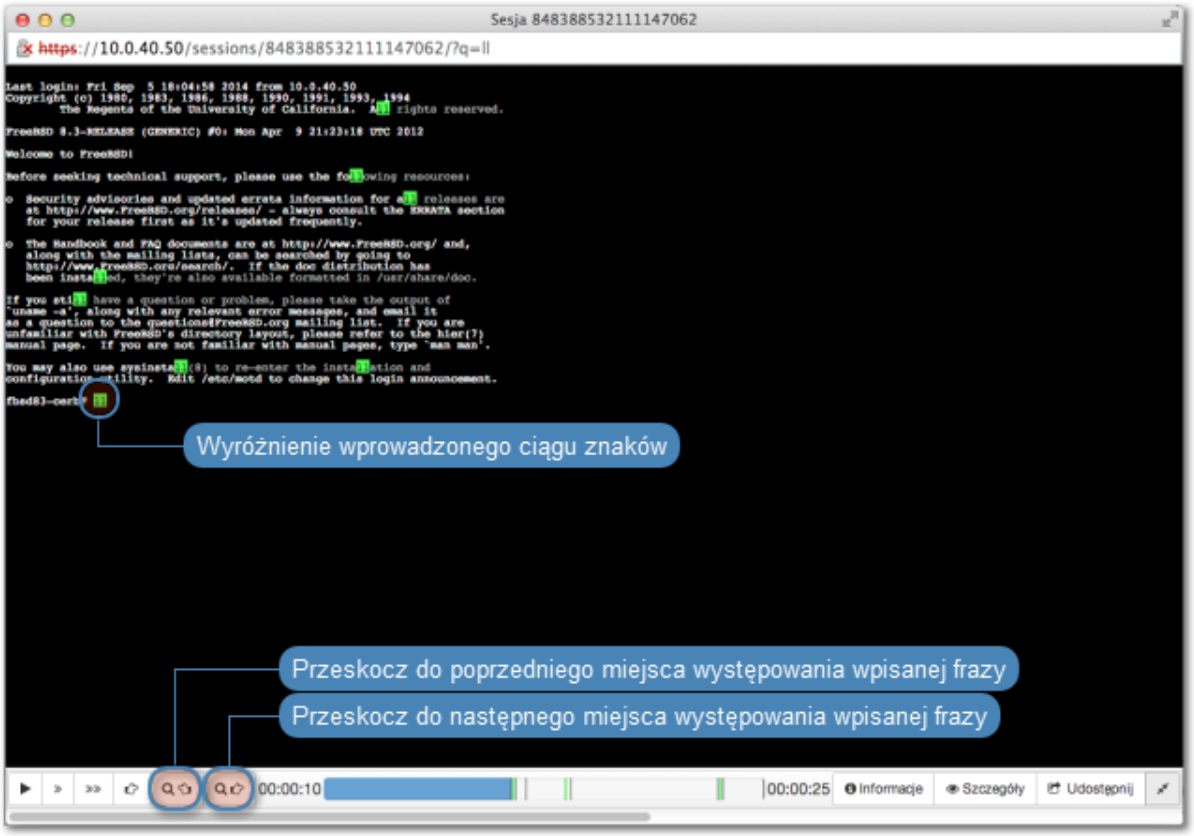
Opcje odtwarzacza



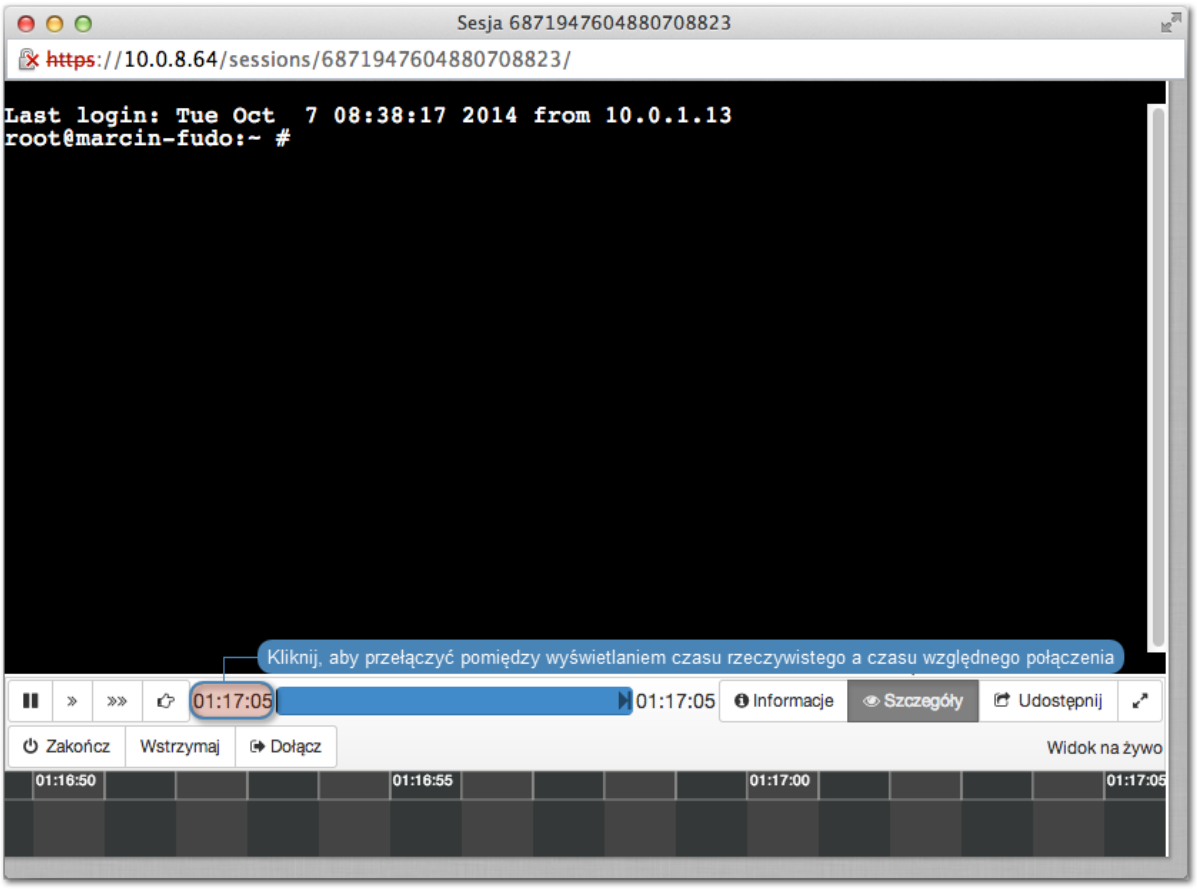
Informacja: Niektóre funkcje dostępne są tylko dla podglądu sesji aktualnie trwających.

Informacja: Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



Informacja: Kliknij w zegar odmierzający czas odtwarzanej sesji, aby przełączyć pomiędzy czasem bezwzględnym i względnym.



Tematy pokrewne:

- *Funkcjonalności wrażliwe*

12.3 Podgląd trwających sesji

Wheel Fudo PAM umożliwia podgląd sesji aktualnie trwających, co pozwala na bieżącą kontrolę aktywności użytkowników.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj żądaną sesję i kliknij ikonę odtwarzania, aby otworzyć *okno odtwarzacza*.

Tematy pokrewne:

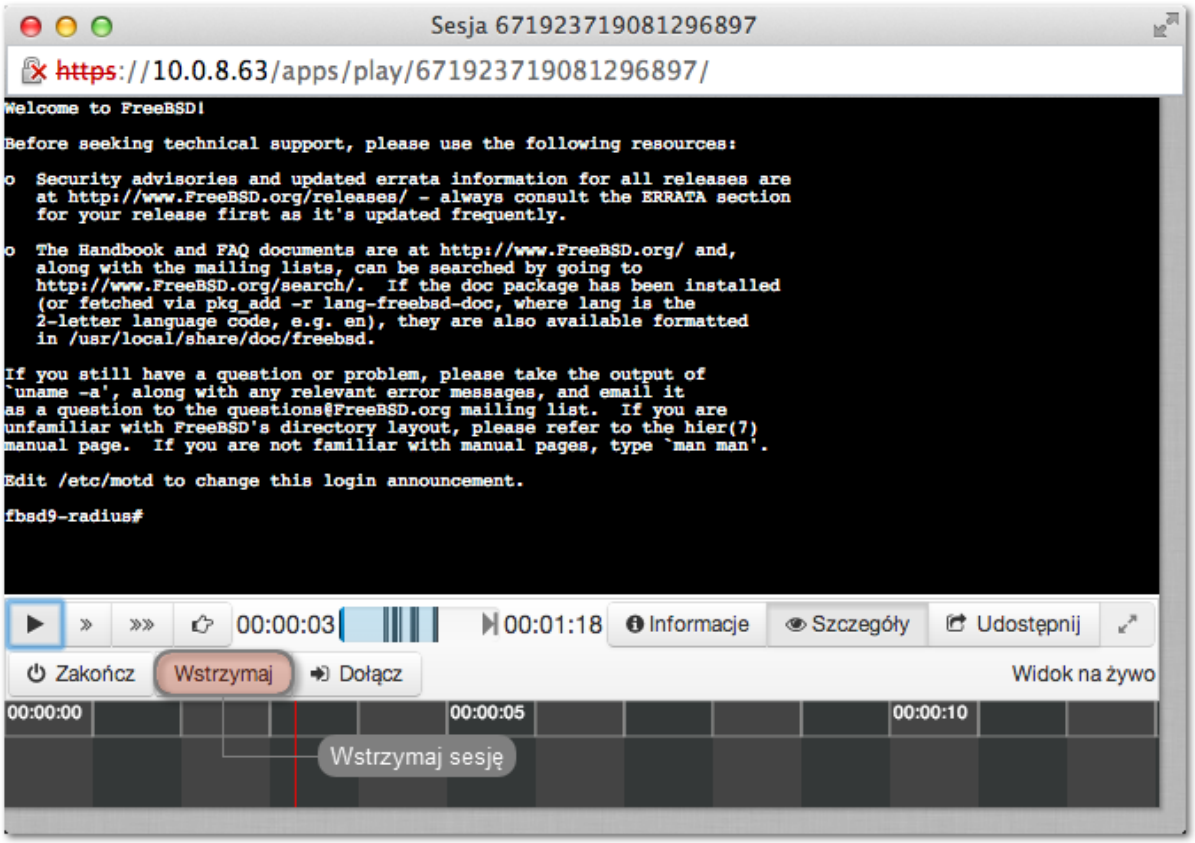
- *Filtrowanie sesji*

12.4 Wstrzymywanie połączenia

W przypadku gdy aktualne akcje użytkownika wymagają analizy, połączenie może zostać wstrzymane.

Informacja: Wstrzymanie połączenia powoduje czasowe wstrzymanie transmisji pakietów. W przypadku wznowienia połączenia, akcje wykonane przez użytkownika w czasie wstrzymania sesji zostaną przesłane do serwera.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj i kliknij żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.
5. Kliknij *Wstrzymaj*.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Dołączanie do sesji*
- *Filtrowanie sesji*

12.5 Przerywanie połączenia

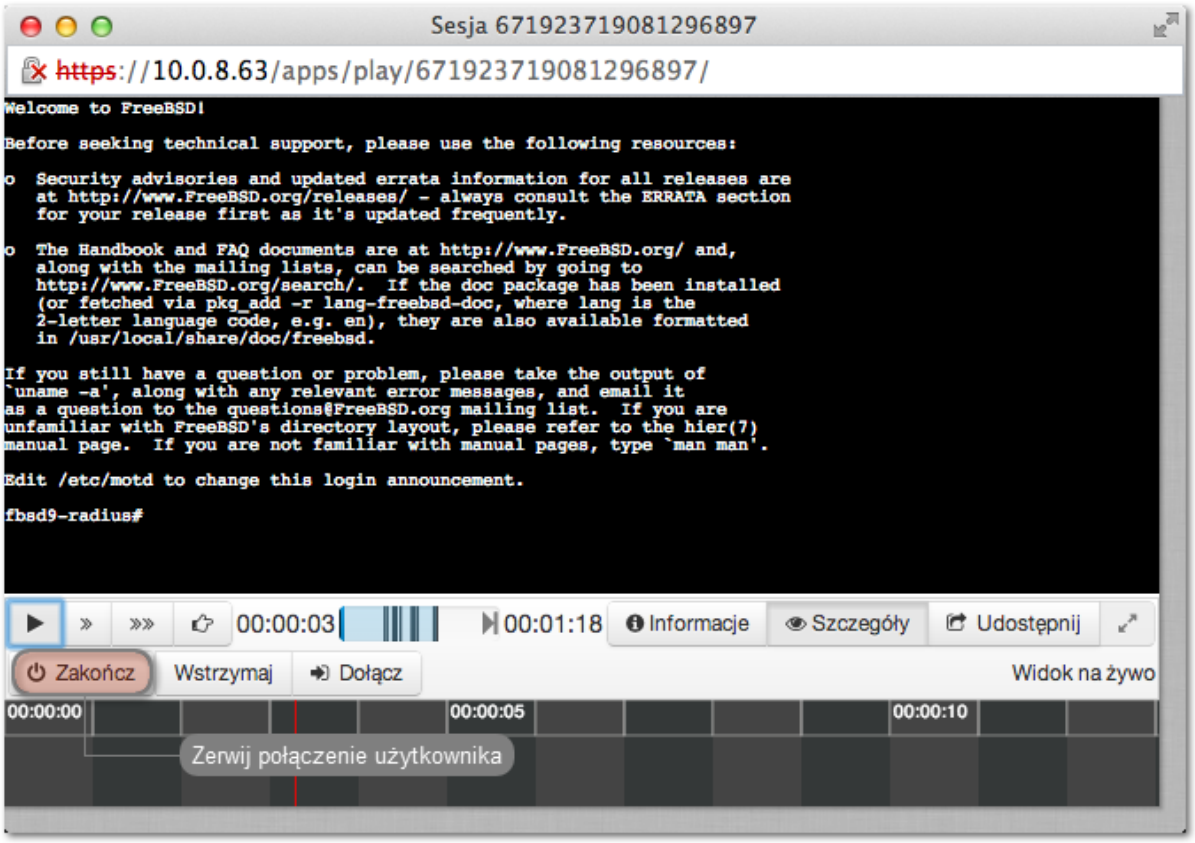
W przypadku gdy administrator stwierdzi nadużycie praw dostępu, może przerwać sesję połączeniową użytkownika.

Informacja: Wheel Fudo PAM umożliwia automatyczne zablokowanie użytkownika, z chwilą

wykrycia zdefiniowanego ciągu znaków. Więcej informacji na temat polityk i wzorców znajdziesz w rozdziale *Polityki*.

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij *Zakończ*, aby przerwać połączenie.

Informacja: Zerwanie połączenia automatycznie blokuje konto użytkownika.



6. Zdecyduj czy użytkownik powinien pozostać zablokowany.

Tematy pokrewne:

- *Polityki*
- *Mechanizmy bezpieczeństwa*
- *Dołączanie do sesji*
- *Udostępnianie sesji*
- *Filtrowanie sesji*

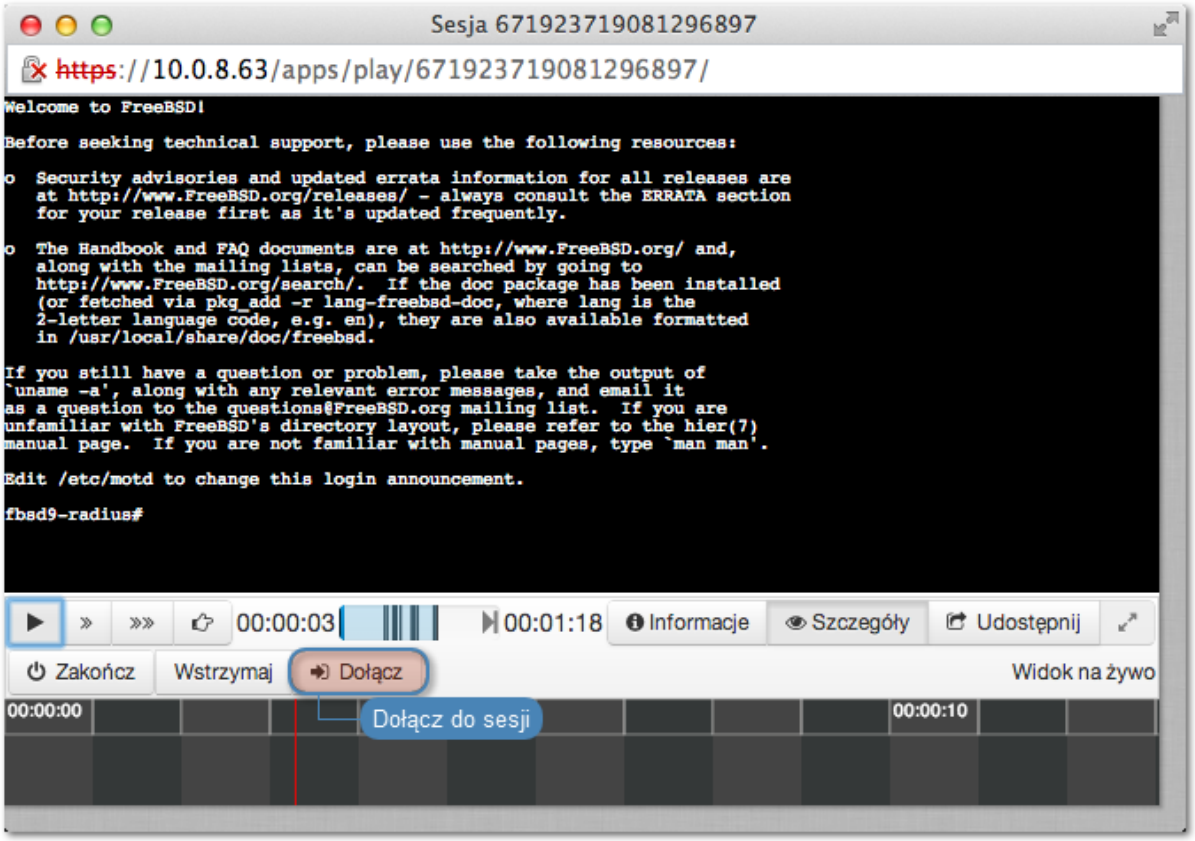
12.6 Dołączanie do sesji

Wheel Fudo PAM pozwala administratorowi na dołączenie do aktualnie trwającej sesji i jednoczesną pracę z użytkownikiem.

Informacja: Funkcja dołączania do sesji nie jest dostępna dla połączeń realizowanych za pośrednictwem protokołu X11.

Aby dołączyć do aktualnie trwającej sesji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij przycisk *Dołącz*.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Udostępnianie sesji*
- *Filtrowanie sesji*

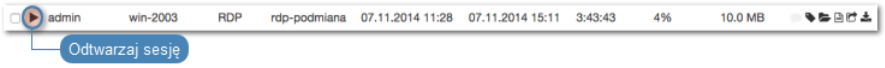
12.7 Udostępnianie sesji

Wheel Fudo PAM umożliwia udostępnienie innemu użytkownikowi sesji zapisanej oraz aktualnie trwającej.

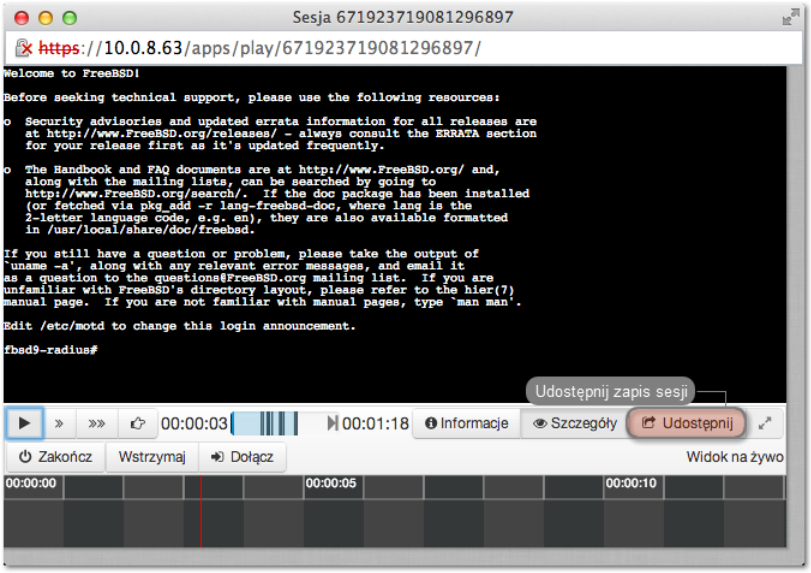
Udostępnianie sesji

Aby udostępnić sesję, postępuj zgodnie z poniższą instrukcją.

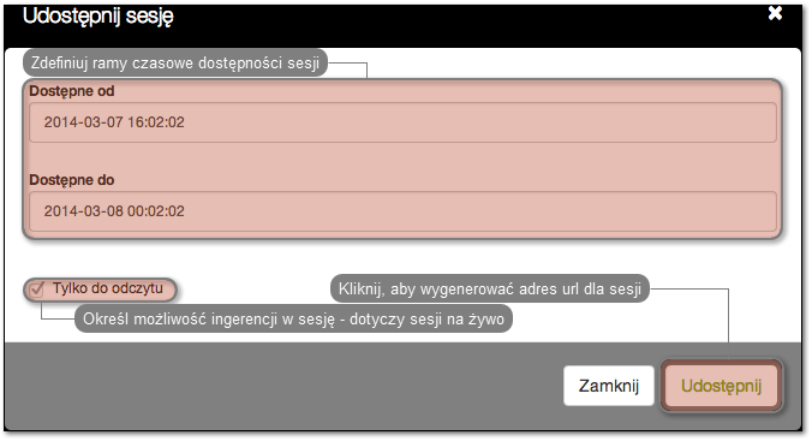
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.



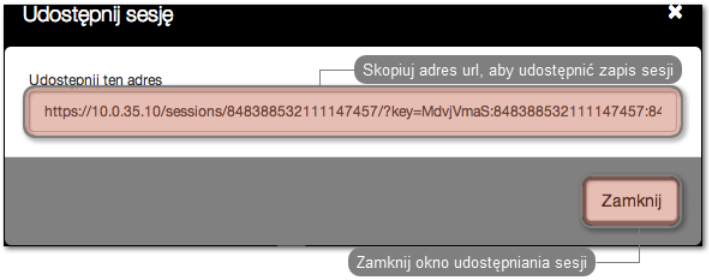
3. Kliknij *Udostępnij*.



4. Określ ramy czasowe dostępności sesji i kliknij *Zatwierdź*, aby wygenerować adres URL, pod którym udostępniony zostanie zapis sesji.

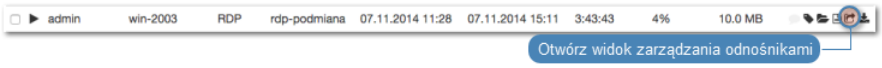


5. Skopiuj odnośnik i kliknij *Zamknij*.

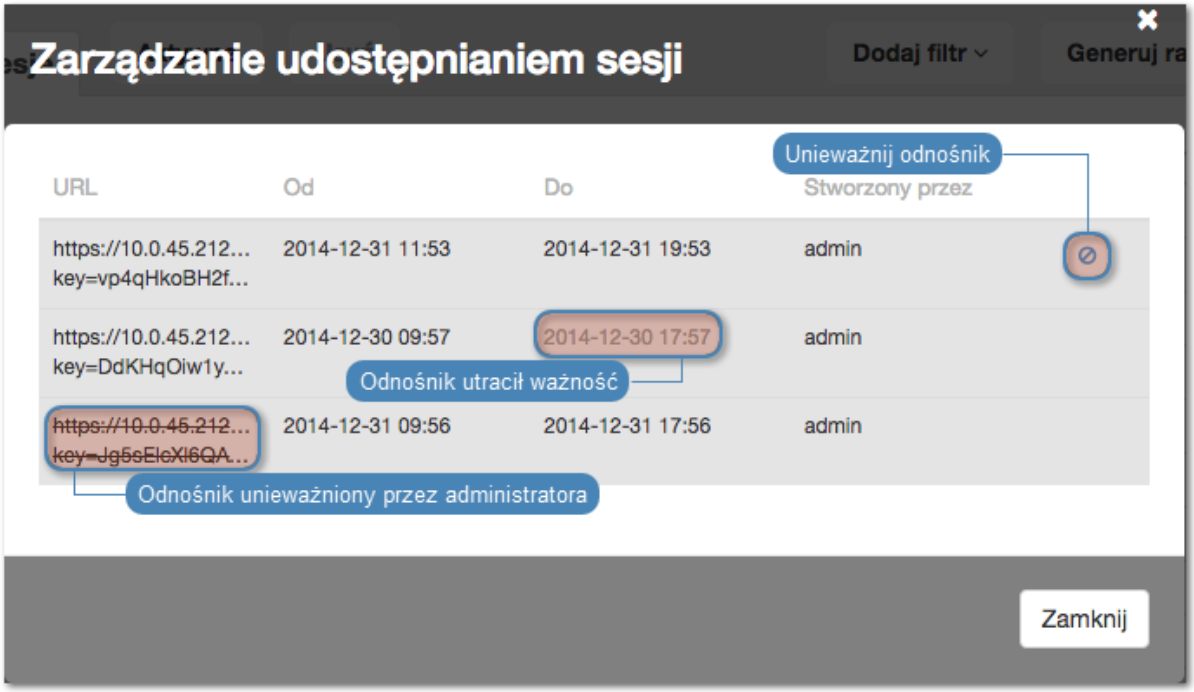


Unieważnienie odnośnika

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź żądaną sesję i kliknij ikonę udostępniania, aby otworzyć okno zarządzania odnośnikami.



3. Kliknij ikonę unieważnienia odnośnika.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Dołączanie do sesji*
- *Filtrowanie sesji*

12.8 Komentowanie sesji

Wheel Fudo PAM pozwala na dodawanie komentarzy i znaczników do zarejestrowanych sesji.

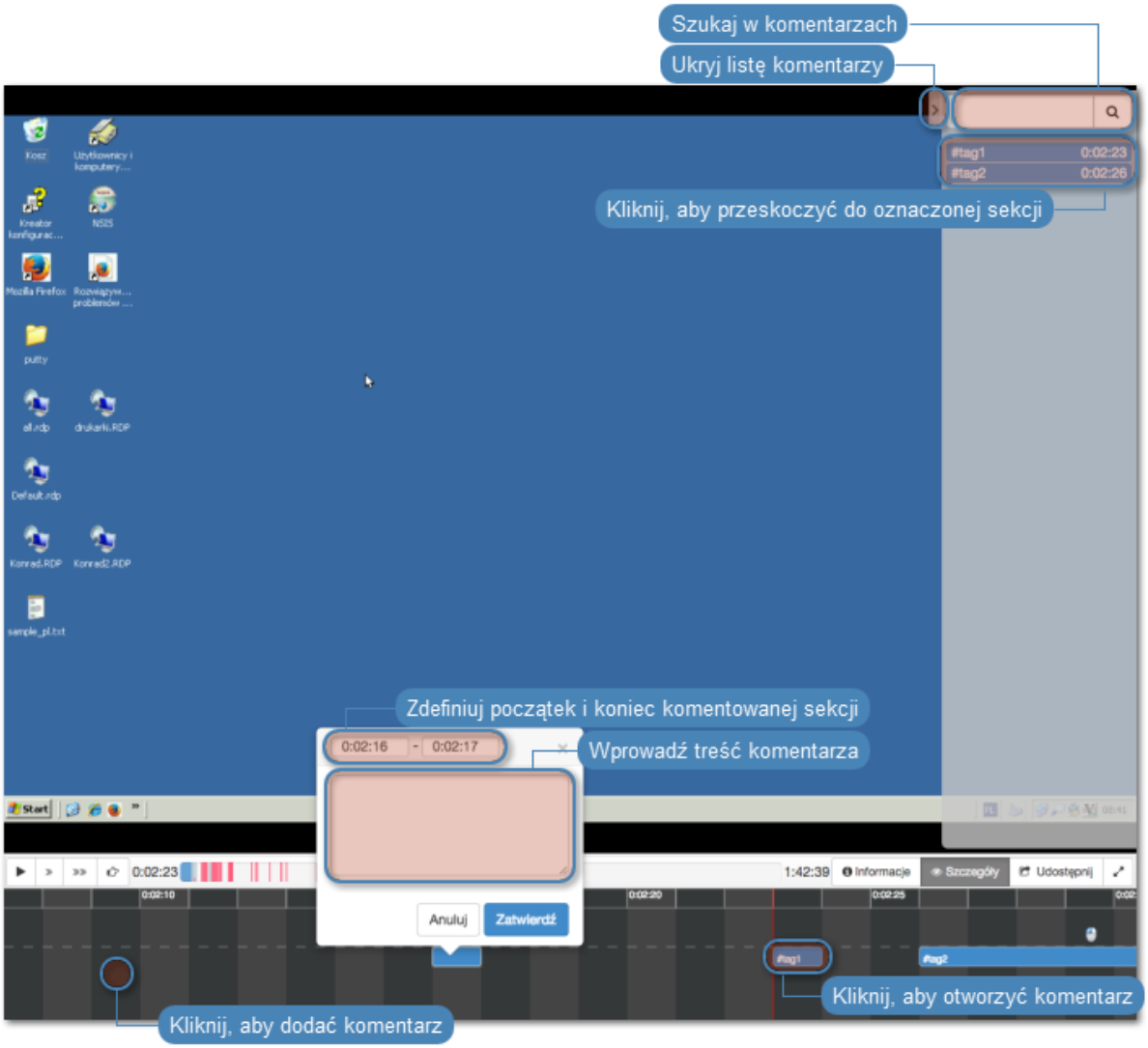
Dodawanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.

2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Kliknij w dolnym obszarze osi czasu, aby dodać komentarz.
5. Zdefiniuj przedział czasu, którego dotyczy dodawany komentarz.

Informacja: Kliknij i przeciągnij bok prostokąta, aby zmienić ramy czasowe komentarza.

6. Dodaj treść komentarza.
7. Kliknij *Zatwierdź*.



Edytowanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.

5. Kliknij ikonę edycji komentarza.
6. Wprowadź zmiany i kliknij *Zatwierdź*.

Usuwanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.
5. Kliknij ikonę kosza.
6. Kliknij *Usuń*.

Dodawanie odpowiedzi do komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.
5. Kliknij *Odpowiedz*.
6. Wprowadź treść odpowiedzi i kliknij *Zatwierdź*.

Tematy pokrewne:

- *Funkcjonalności wrażliwe*

12.9 Eksportowanie sesji

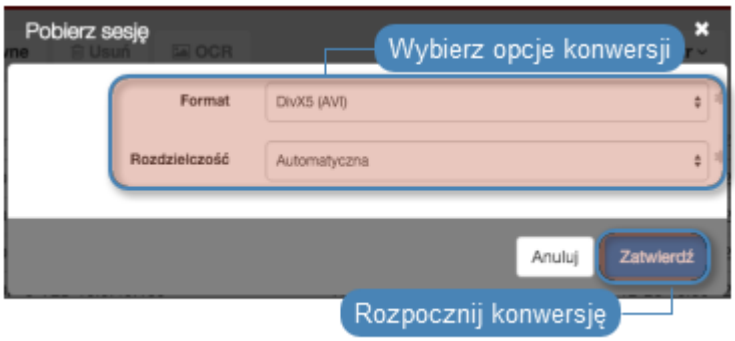
Wheel Fudo PAM pozwala na konwersję zapisanej sesji do jednego ze wspieranych formatów wyjściowych.

Aby wyeksportować sesję, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź żądaną sesję i kliknij ikonę eksportu zarejestrowanego materiału.

3. Wybierz format pliku wyjściowego.

Informacja: Format pliku wyjściowego oraz rozdzielczość obrazu wideo wpływają na czas trwania konwersji oraz rozmiar pliku wynikowego.



4. Wybierz rozdzielczość w jakiej zapisany ma być strumień wideo (*nie dotyczy konwersji materiału do formatu tekstowego*).

Informacja: Wybór opcji `Automatyczna` spowoduje wybór rozdzielczości odpowiadający rozdzielczości ekranu użytkownika z zapisanej sesji.

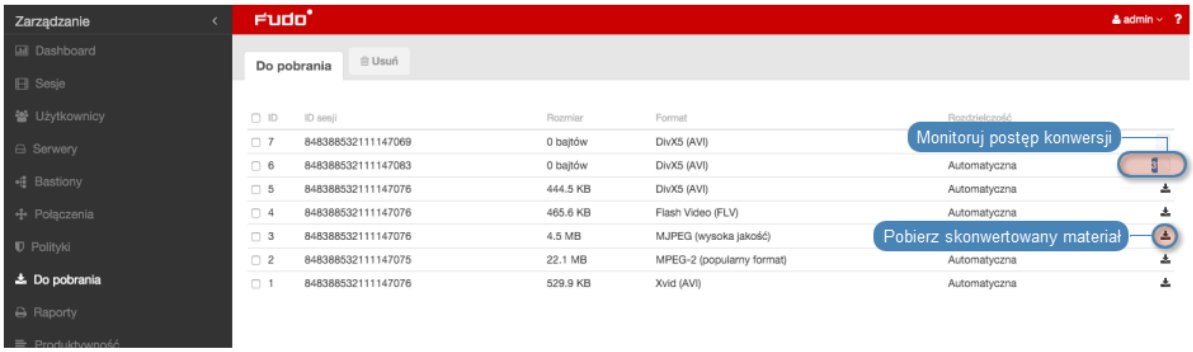
---

5. Kliknij *Zatwierdź*, aby rozpocząć konwersję i przejść do widoku *Do pobrania*.

Informacja: Widok *Do pobrania* umożliwia monitorowanie postępu konwersji.

---

6. Kliknij ikonę pobrania sesji.



Tematy pokrewne:

- *Filtrowanie sesji*
- *Udostępnianie sesji*
- *Odtwarzanie sesji*
- *Dołączanie do sesji*

12.10 Usuwanie sesji

Aby usunąć zarejestrowaną sesję, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź i zaznacz żądaną sesję.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia sesji.

Informacja: Wheel Fudo PAM może automatycznie usuwać dane sesji po upływie czasu zadanego parametrem retencji. Więcej informacji znajdziesz w rozdziale *Kopie bezpieczeństwa i retencja danych*.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Współdzielenie sesji*
- *Odtwarzanie sesji*
- *Eksportowanie sesji*

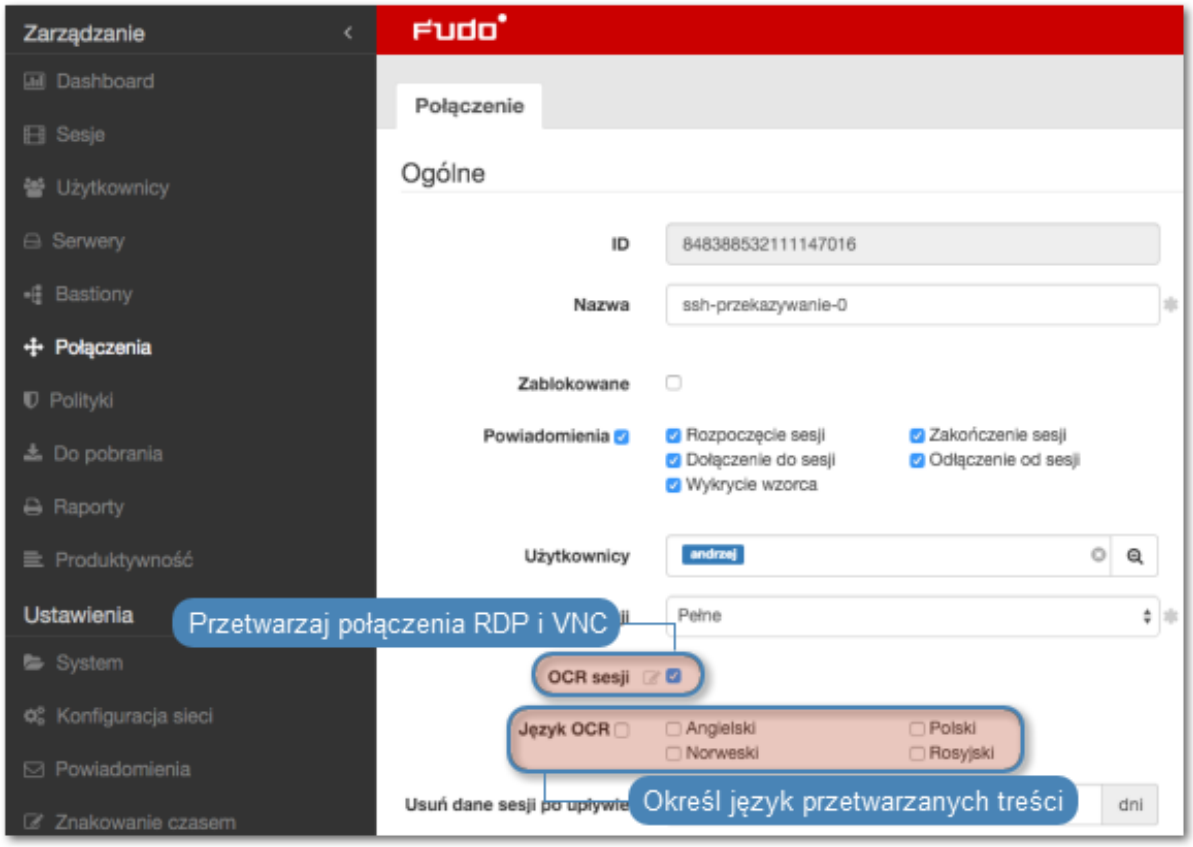
12.11 Przetwarzanie OCR sesji

Zarejestrowany materiał sesji RDP i VNC może być indeksowany na potrzeby przeszukiwania pełnotekstowego.

Automatyczne przetwarzanie OCR sesji w ramach wybranego połączenia

Aby włączyć przetwarzanie OCR sesji w ramach wybranego połączenia, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Połączenia*.
2. Znajdź i wybierz żądane połączenie.
3. Zaznacz opcję *OCR sesji*.
4. Wybierz język przetwarzanych treści.

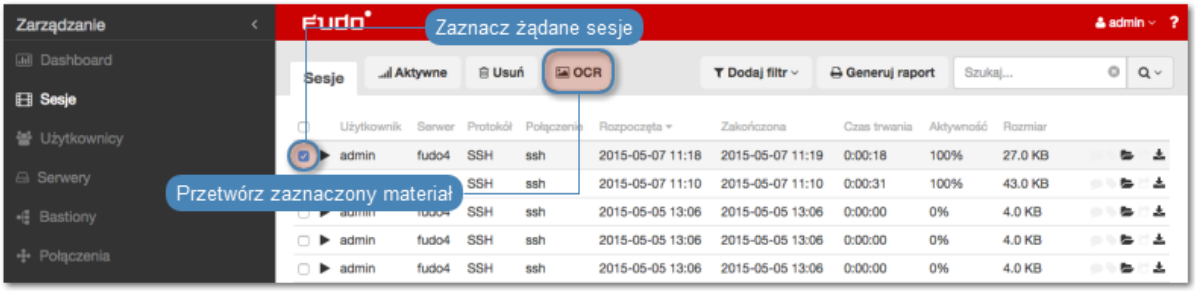


5. Kliknij *Zapisz*.

Przetwarzanie OCR wybranych sesji

Aby przetworzyć wybrane sesje, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje i kliknij *OCR*.



Informacja: Opcje filtrowania sesji pozwalają na wybranie obiektów przetworzonych lub

nieprzetworzonych.

3. Zatwierdź przetwarzanie wybranych sesji.

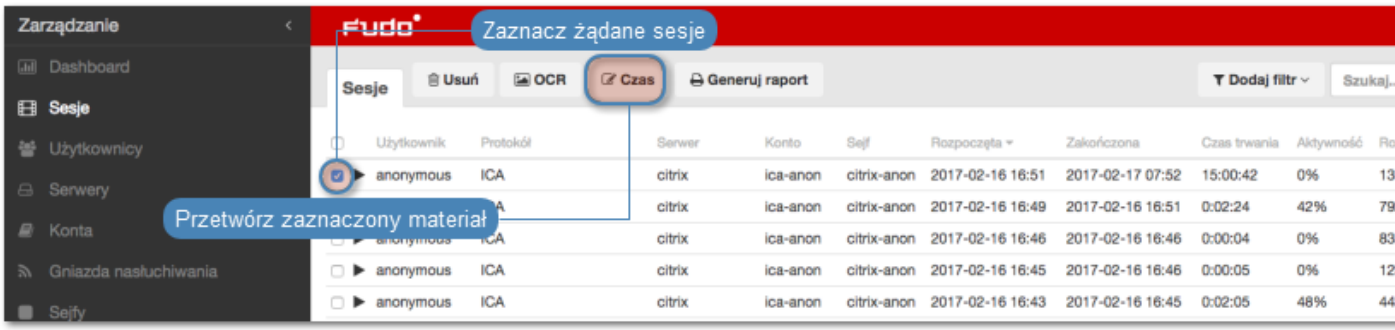
Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

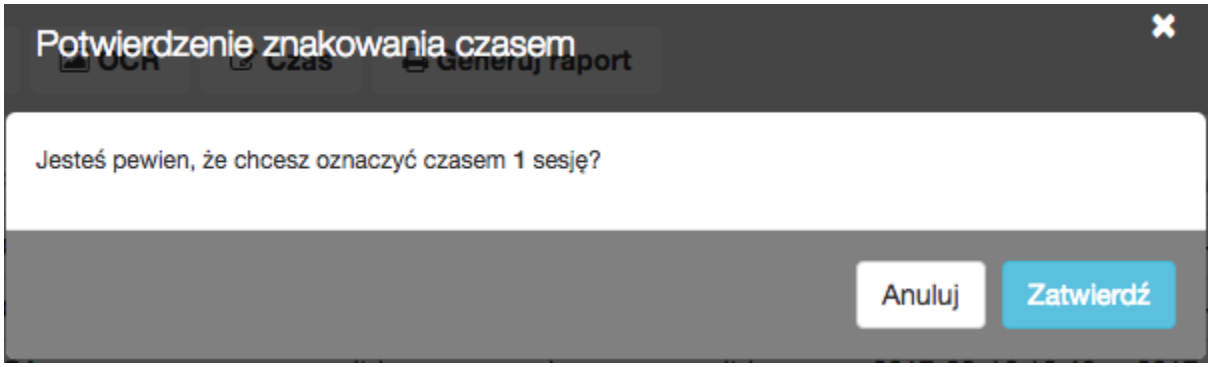
12.12 Znakowanie czasem wybranych sesji

Aby opatrzyć znacznikiem czasu wybrane sesje, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje i kliknij *Czas*.



3. Kliknij *Zatwierdź*.



Informacja: Aby wyświetlić znacznik czasu, kliknij ikonę .

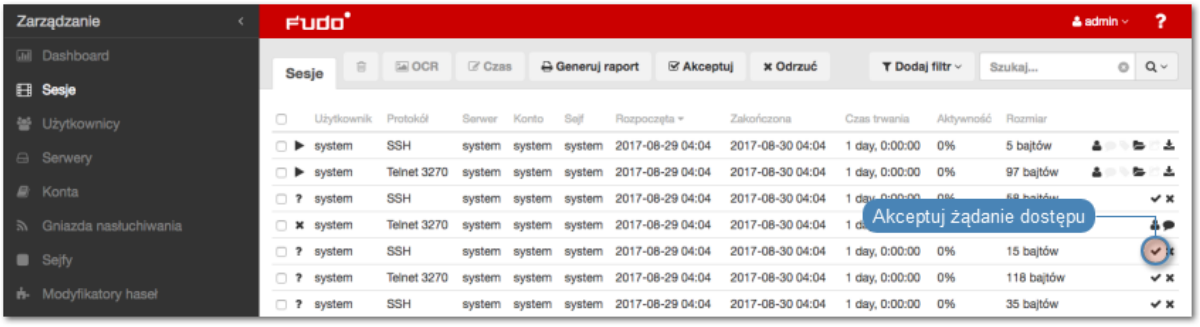
Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

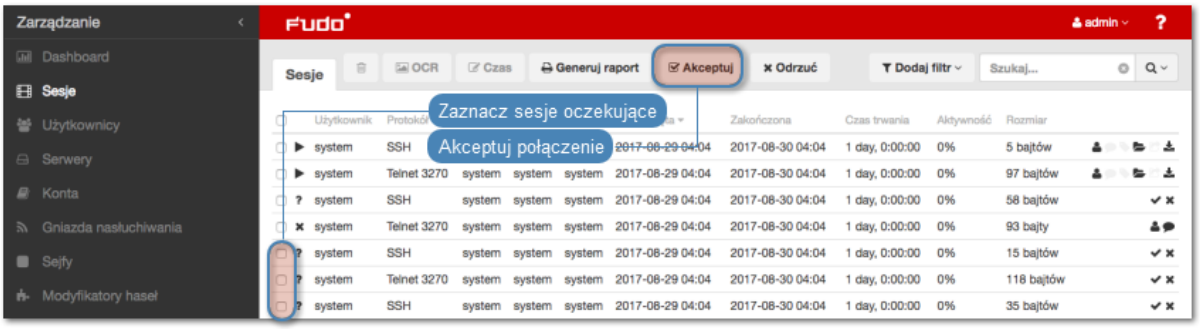
12.13 Akceptowanie połączeń oczekujących

12.13.1 Interfejs administracyjny Fudo

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ✔ przy wybranym połączeniu



lub zaznacz żądane sesje oczekujące i kliknij *Akceptuj*.



12.13.2 Fudo Mobile

1. Uruchom i zaloguj się do aplikacji *Fudo Mobile*.
2. Wybierz profil, z którego chcesz wyświetlić listę połączeń.
3. Wybierz połączenie oczekujące, a następnie opcję *Akceptuj* lub przesuń palcem w prawo na wybranej pozycji i wybierz opcję ☑.

Tematy pokrewne:

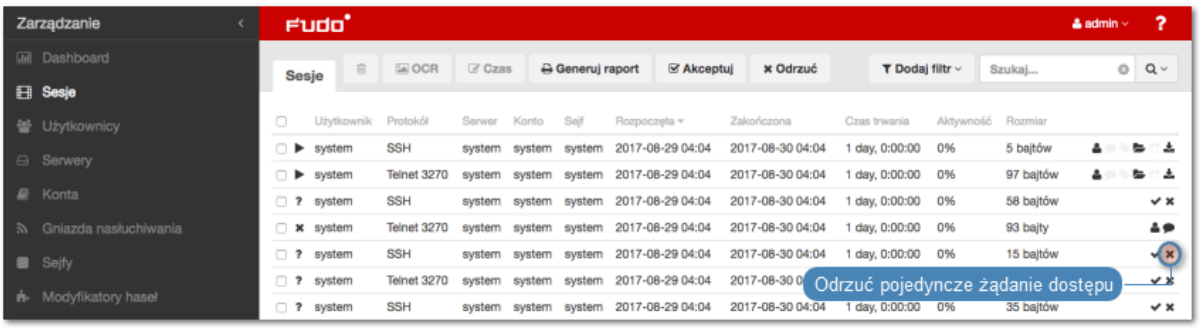
- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

12.14 Odrzucanie połączeń oczekujących

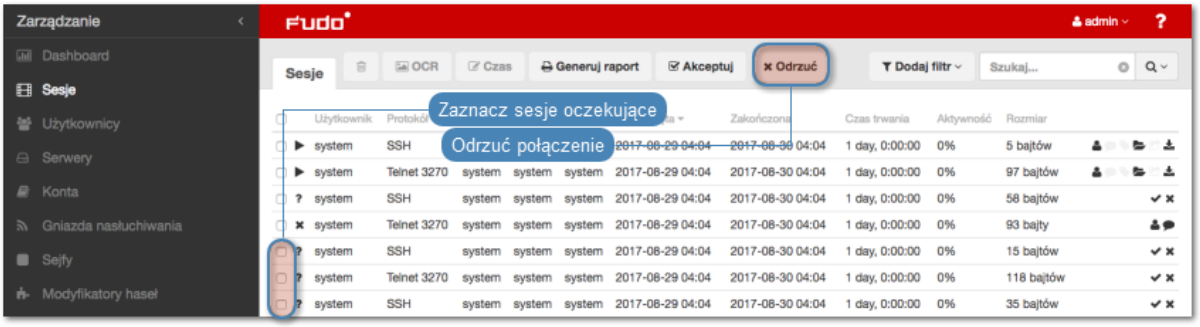
12.14.1 Interfejs administracyjny Fudo

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.

2. Kliknij ✖ przy wybranym połączeniu



lub zaznacz żądane sesje oczekujące i kliknij *Odrzuć*.

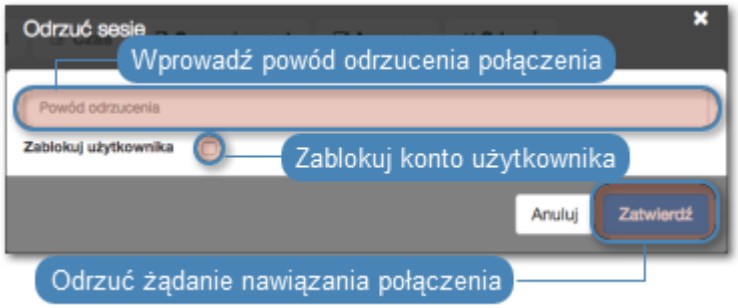


3. Opcjonalnie, wprowadź powdód odrzucenia żądania dostępu.

Informacja: Powód odrzucenia wyświetlany jest na liście sesji po najechaniu kursorem na ikonę 💬.

---

4. Opcjonalnie, zaznacz opcję zablokowania konta użytkownika, aby trwale uniemożliwić użytkownikowi nawiązywanie połączeń.
5. Kliknij *Zatwierdź*.



12.14.2 Fudo Mobile

1. Uruchom i zaloguj się do aplikacji *Fudo Mobile*.
2. Wybierz profil, z którego chcesz wyświetlić listę połączeń.
3. Wybierz połączenie oczekujące, a następnie opcję *Odrzuć* lub przesuń palcem w lewo na wybranej pozycji i wybierz opcję ✖.

4. Podaj powód odrzucenia połączenia.
5. Opcjonalnie, zaznacz opcję zablokowania użytkownika.
6. Wybierz *Odrzuć*, aby potwierdzić odrzucenie żądania połączenia.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Akceptowanie połączeń oczekujących*
- *Przerywanie połączenia*
- *Blokowanie użytkownika*
- *Sesje*

ROZDZIAŁ 13

Raporty

Usługa raportowania generuje szczegółową statystykę połączeń użytkowników w ramach określonych sesji dostępowych.

Pełne raporty generowane są cyklicznie przez system (dziennie, tygodniowo, miesięcznie, kwartalnie), i dostępne dla użytkowników o zdefiniowanej roli `superadmin`. Raporty generowane cyklicznie dla użytkowników o rolach `admin` lub `operator`, generowane są indywidualnie i zawierają jedynie dane sesji, do których określony użytkownik posiada uprawnienia.

Oprócz domyślnych raportów systemowych, raporty cykliczne mogą być także generowane na podstawie zapisanej *definicji filtrowania*. Raport może być również wygenerowany na żądanie, i zawierać dane dotyczące wskazanych sesji.

13.1 Subskrybowanie raportu cyklicznego

Aby włączyć usługę generowania raportów cyklicznych dla zalogowanego użytkownika, postępuj zgodnie z poniższą instrukcją.

Informacja: Raporty cykliczne, generowane na żądanie określonego użytkownika, zawierają dane sesji, do których użytkownik posiada uprawnienia.

---

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Kliknij *Zarządzaj subskrypcją*, aby wyświetlić dostępne opcje raportów cyklicznych.
3. Wybierz z listy rozwijalnej typ raportu.

Informacja: Lista zawiera opcje domyślne oraz zapisane przez użytkownika *definicje filtrowania*.

---

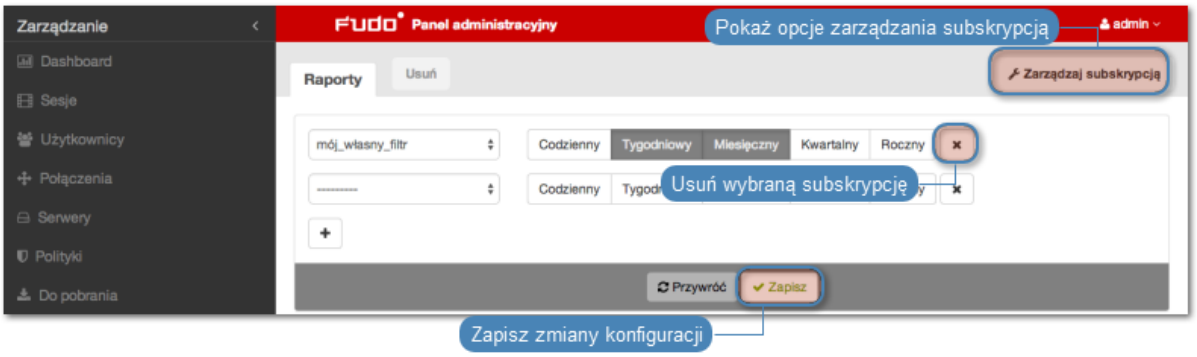
4. Zaznacz częstotliwość generowania wybranego raportu.

5. Kliknij *Zapisz*.

13.2 Rezygnacja z subskrypcji raportu cyklicznego

Aby zrezygnować z subskrypcji raportu cyklicznego, postępuj zgodnie z poniższą instrukcją.

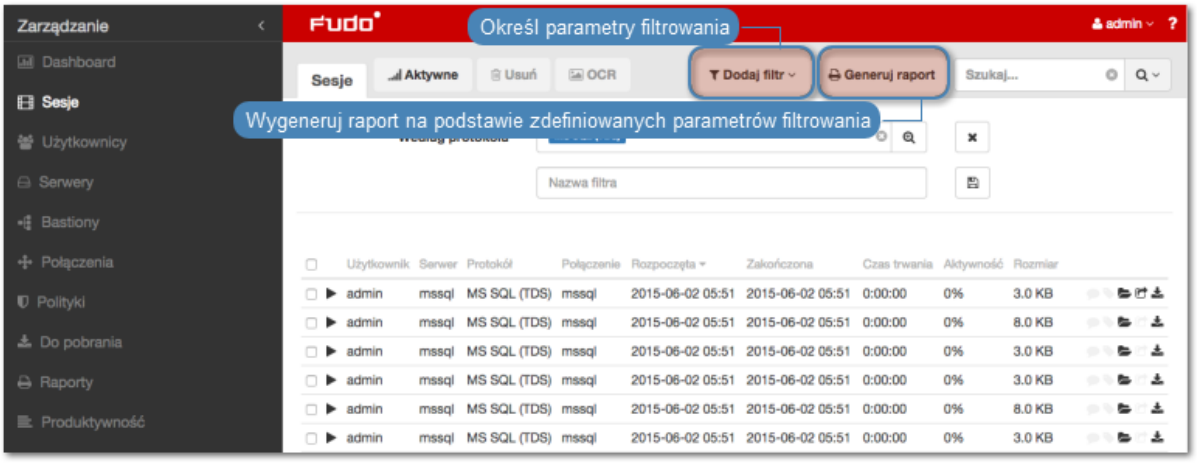
1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Kliknij *Zarządzaj subskrypcją*, aby wyświetlić dostępne opcje raportów cyklicznych.
3. Zaznacz opcję usunięcia przy wybranej definicji subskrypcji.
4. Kliknij *Zapisz*.



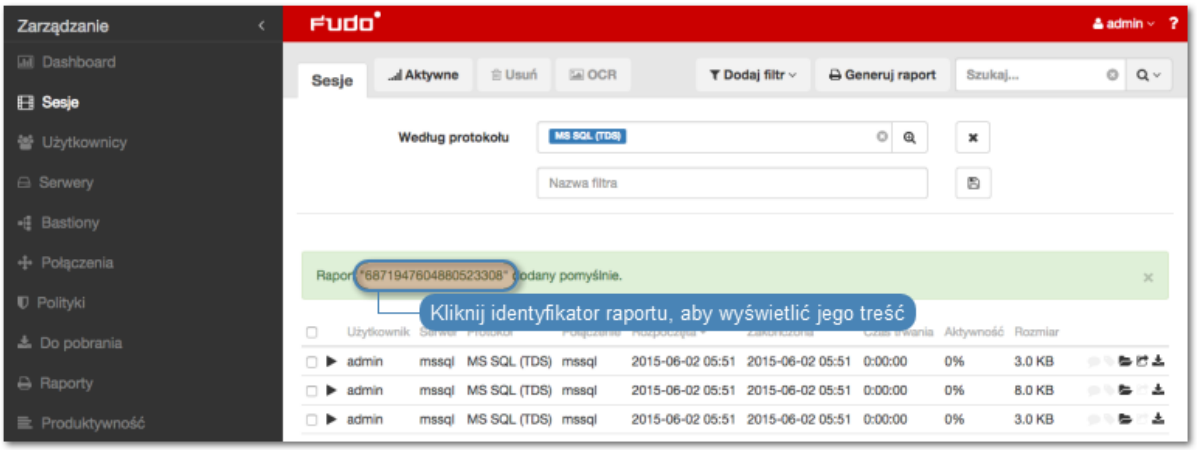
13.3 Generowanie raportu na żądanie

Raport może zostać wygenerowany dla określonego podzbioru sesji, zdefiniowanego parametrami filtrowania.

1. Wybierz z lewego menu‘Zarządzanie > Sesje‘.
2. Kliknij *Dodaj filtr* i zdefiniuj parametry filtrowania (więcej na temat filtrowania sesji, znajdziesz w rozdziale *Kontrola sesji zdalnego dostępu: Filtrowanie sesji*).
3. Kliknij *Generuj raport*.



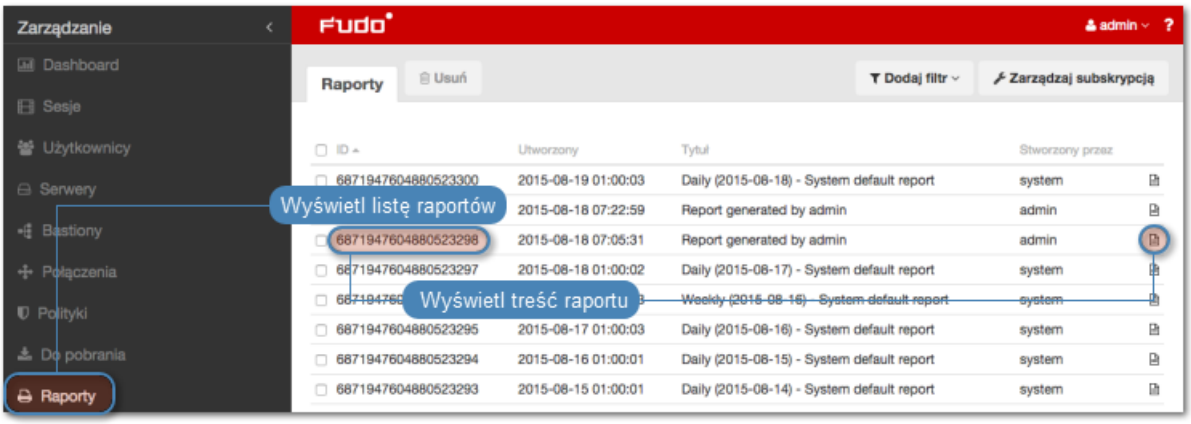
4. Kliknij identyfikator raportu, aby wyświetlić jego treść.



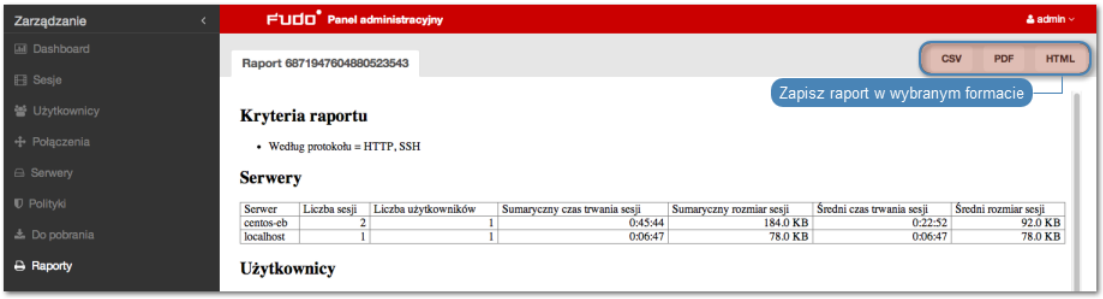
5. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
6. Kliknij ikonę podglądu raportu przy wybranym raporcie lub jego identyfikator, aby zobaczyć jego treść.
7. Kliknij *CSV*, *PDF*, *HTML*, aby zapisać raport w wybranym formacie.

13.4 Wyświetlanie i zapisywanie raportów

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Odszukaj i kliknij identyfikator lub ikonę podglądu treści wybranego raportu.



3. Kliknij *CSV*, *PDF*, *HTML*, aby zapisać raport w wybranym formacie.



13.5 Usuwanie raportów

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Zaznacz żądane raporty i kliknij *Usuń*.
3. Potwierdź usunięcie zaznaczonych raportów.

Tematy pokrewne:

- *Powiadomienia*
- *Filtrowanie sesji*

ROZDZIAŁ 14

Analiza produktywności

Wheel Fudo PAM dostarcza narzędzie wspomagające analizę produktywności użytkowników monitorowanych systemów. Urządzenie śledzi aktywność użytkownika i pozwala wykazać aktywny czas połączenia.

14.1 Zestawienie

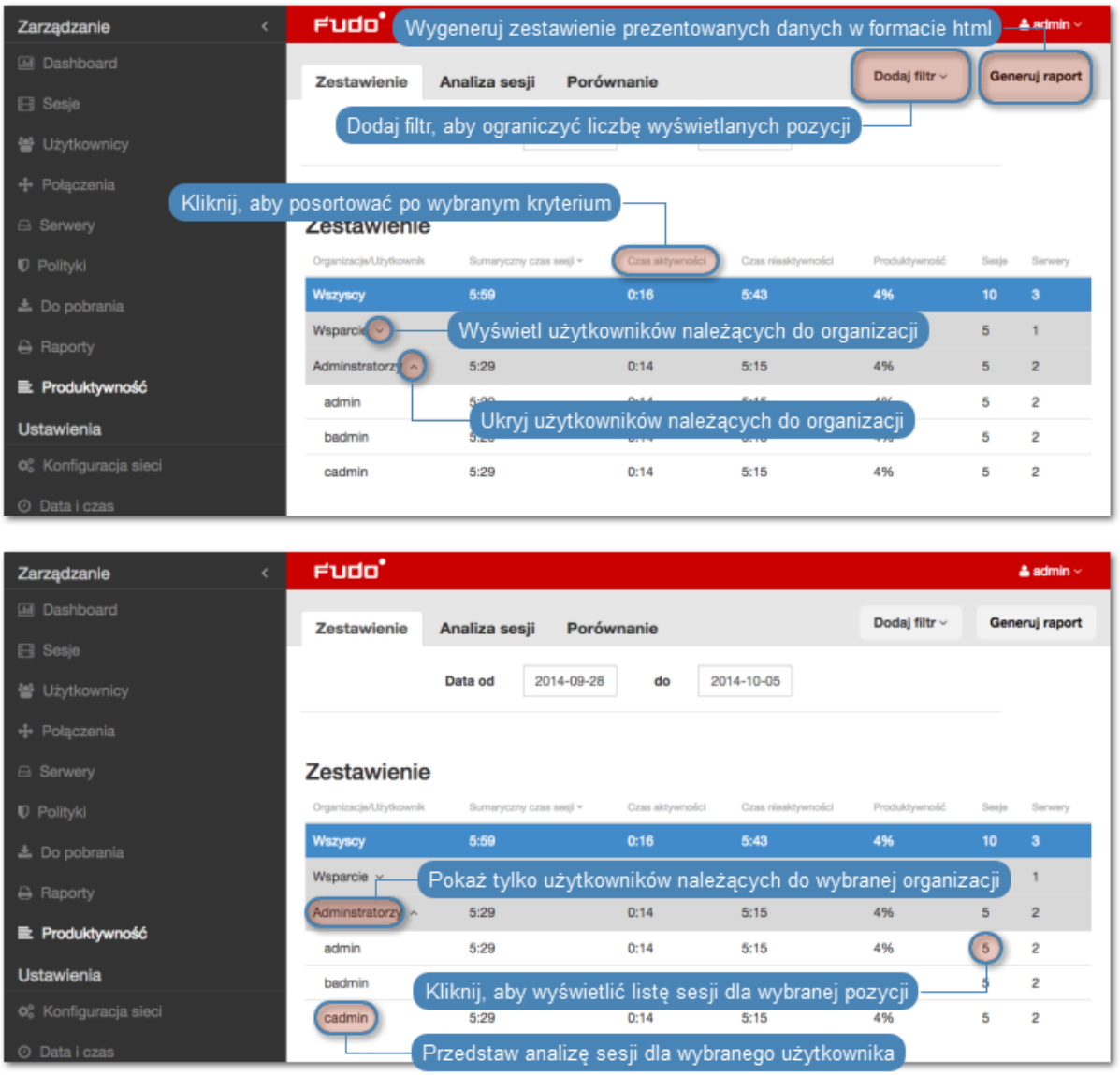
Zestawienie przedstawia dane o aktywności użytkowników i organizacji w wybranym przedziale czasu.

Informacja: Wskaźnik aktywności określany jest na podstawie interakcji użytkownika z systemem. Wheel Fudo PAM dzieli czas sesji na 60 sekundowe interwały. Brak akcji ze strony użytkownika przez czas trwania interwału powoduje zaliczenie danego przedziału do czasu bezczynności.

Aby wyświetlić zestawienie aktywności użytkowników, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Produktywność*.
2. Przejdź na zakładkę *Zestawienie*.
3. Zdefiniuj parametry filtrowania listy użytkowników.
4. Kliknij *Generuj raport*, aby wygenerować zestawienie prezentowanych danych w formacie HTML, CSV lub PDF.

Informacja: Zestawienie dostępne jest w sekcji *Raporty*.



Tematy pokrewne:

- *Analiza produktywności - Analiza sesji*
- *Analiza produktywności - Porównanie*
- *Sesje*

14.2 Analiza sesji

Analiza sesji przedstawia szczegółowo jak kształtowała się produktywność użytkowników/organizacji w zadanym przedziale czasu. Konfigurowalny parametr określający próg aktywności pozwala na szybkie identyfikowanie sesji, użytkowników oraz organizacji, które nie przekroczyły wymaganego poziomu aktywności oraz wspomaga ustalenie wartości progowej, przy której zadana liczba użytkowników lub sesji osiąga wymagany poziom aktywności.

Wykaz wskaźników aktywności użytkowników

Wskaźniki aktywności użytkowników umożliwia szybkie odnalezienie sesji, które nie przekraczają zdefiniowanego progu produktywności. Dalsze zapoznanie się z materiałem pozwala na ustalenie przyczyn niskiej aktywności w danej sesji i wyciągnięcie stosownych wniosków.

Informacja: Wykaz obejmuje przedział czasu nie dłuższy niż 31 dni. W przypadku zdefiniowania dłuższego interwału czasu, prezentowane zestawienie ograniczone jest do 31 dni.

Tematy pokrewne:

- *Analiza produktywności - Zestawienie*
- *Analiza produktywności - Porównanie*
- *Sesje*

14.3 Porównanie aktywności

Komponent analizy produktywności pozwala porównać aktywność organizacji lub użytkowników w zadanych przedziałach czasu.

Aby porównać organizacje/użytkowników, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Produktywność*.
2. Przejdź na zakładkę Porównanie.
3. Wybierz typ porównywanych obiektów.
4. Wybierz porównywany interwał czasu.
5. Dodaj obiekty do porównania, definiując czas początkowy indywidualnie dla każdego obiektu.
6. Kliknij *Zatwierdź*, aby wygenerować porównanie.

Tematy pokrewne:

- *Analiza produktywności - Zestawienie*
- *Analiza produktywności - Zestawienie*
- *Sesje*

ROZDZIAŁ 15

Administracja

Poniższy rozdział zawiera opisy czynności administracyjnych.

15.1 System

15.1.1 Data i czas

Wiele zdarzeń rejestrowanych przez Wheel Fudo PAM (sesje, wpisy dziennika zdarzeń) znakowanych jest czasem. Wheel Fudo PAM może pobierać czas z *serwera NTP* lub z zegara systemowego.

Ostrzeżenie:

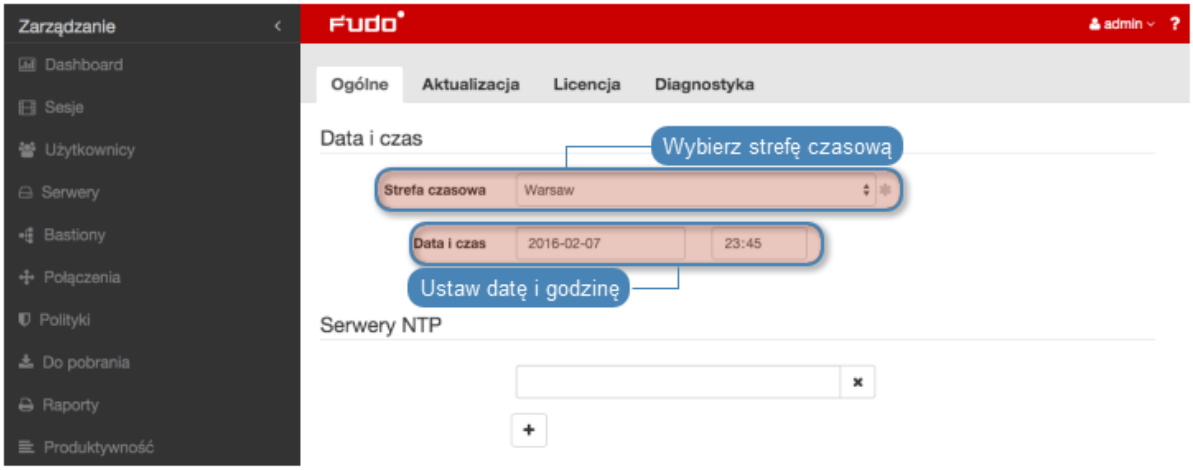
- Zaleca się, aby data i czas pobierane były z serwera NTP, będącego pewnym źródłem danych referencyjnych. Ręczna zmiana ustawień daty i czasu może spowodować nieprawidłowości w funkcjonowaniu urządzenia.
- Pobieranie czasu z serwera NTP jest wymagane w przypadku *konfiguracji klastrowych*.

Zmiana daty i czasu

Informacja: Opcja ręcznego ustawienia czasu nie jest dostępna, jeśli skonfigurowany jest serwer NTP.

Aby zmienić datę i czas serwera Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Zmień ustawienia daty i czasu w sekcji *Data i czas*.



3. Kliknij *Zapisz*.

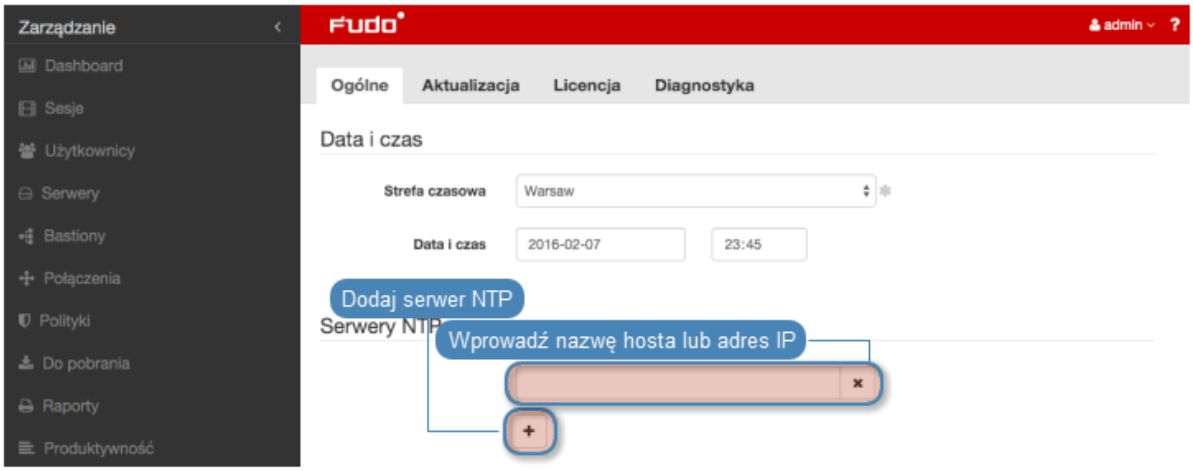
Konfiguracja serwerów czasu

Informacja: Serwer NTP pozwala na synchronizację czasu systemowego na urządzeniach będących częścią zakładowej infrastruktury IT. Zastosowanie serwera NTP zapewnia zgodność czasu rejestrowanej sesji, z czasem monitorowanego serwera.

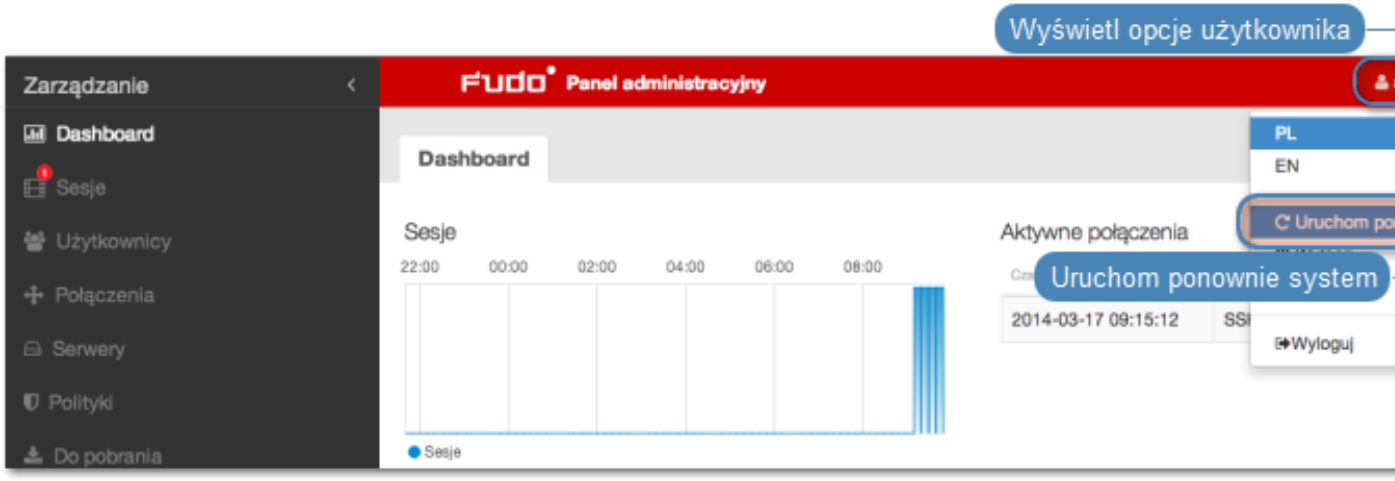
Dodawanie serwera NTP

Aby dodać serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Kliknij + w sekcji *Serwery NTP*, aby dodać definicję serwera czasu.
3. Wprowadź adres IP lub nazwę hosta serwera NTP.



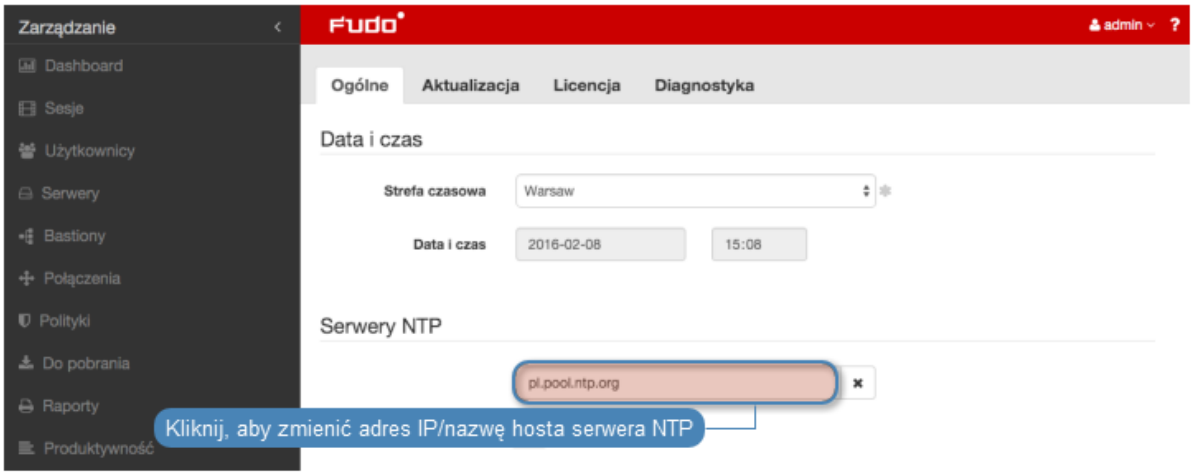
4. Kliknij *Zapisz*.
5. Wybierz z menu użyktownika opcję *Uruchom ponownie*.



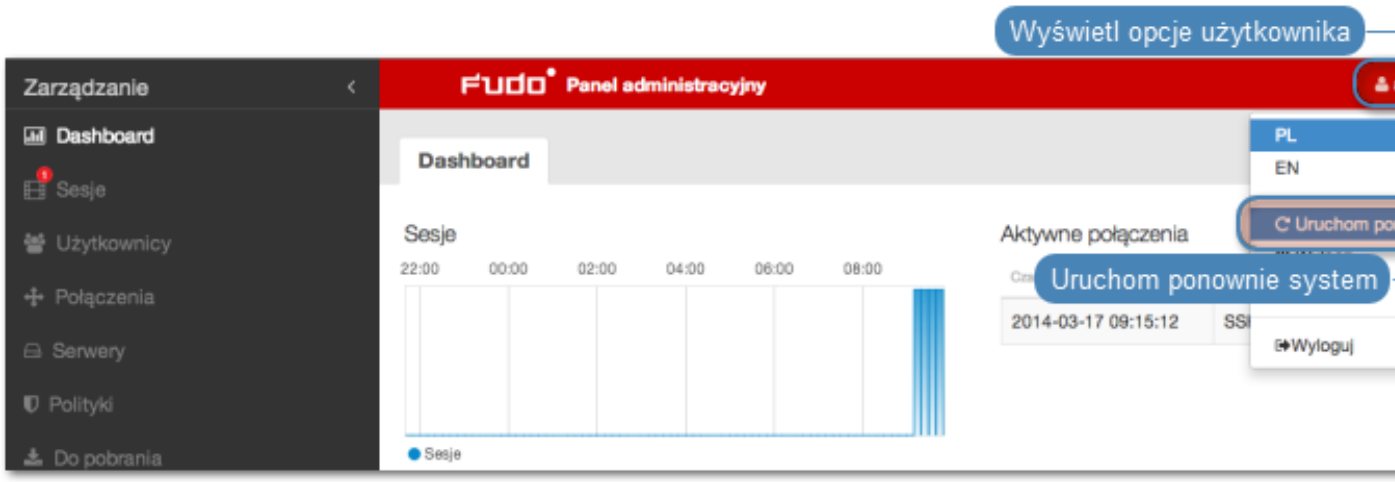
Modyfikowanie serwera NTP

Aby zmodyfikować serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wyszukaj i zmodyfikuj żądany wpis w sekcji *Serwery NTP*.



3. Kliknij *Zapisz*.
4. Wybierz z menu użyktownika opcję *Uruchom ponownie*.



Usuwanie serwera NTP

Aby usunąć serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. Zaznacz opcję *x* przy żądanej definicji serwera NTP i kliknij *Zapisz*.

Tematy pokrewne:

- *Znakowanie czasem*

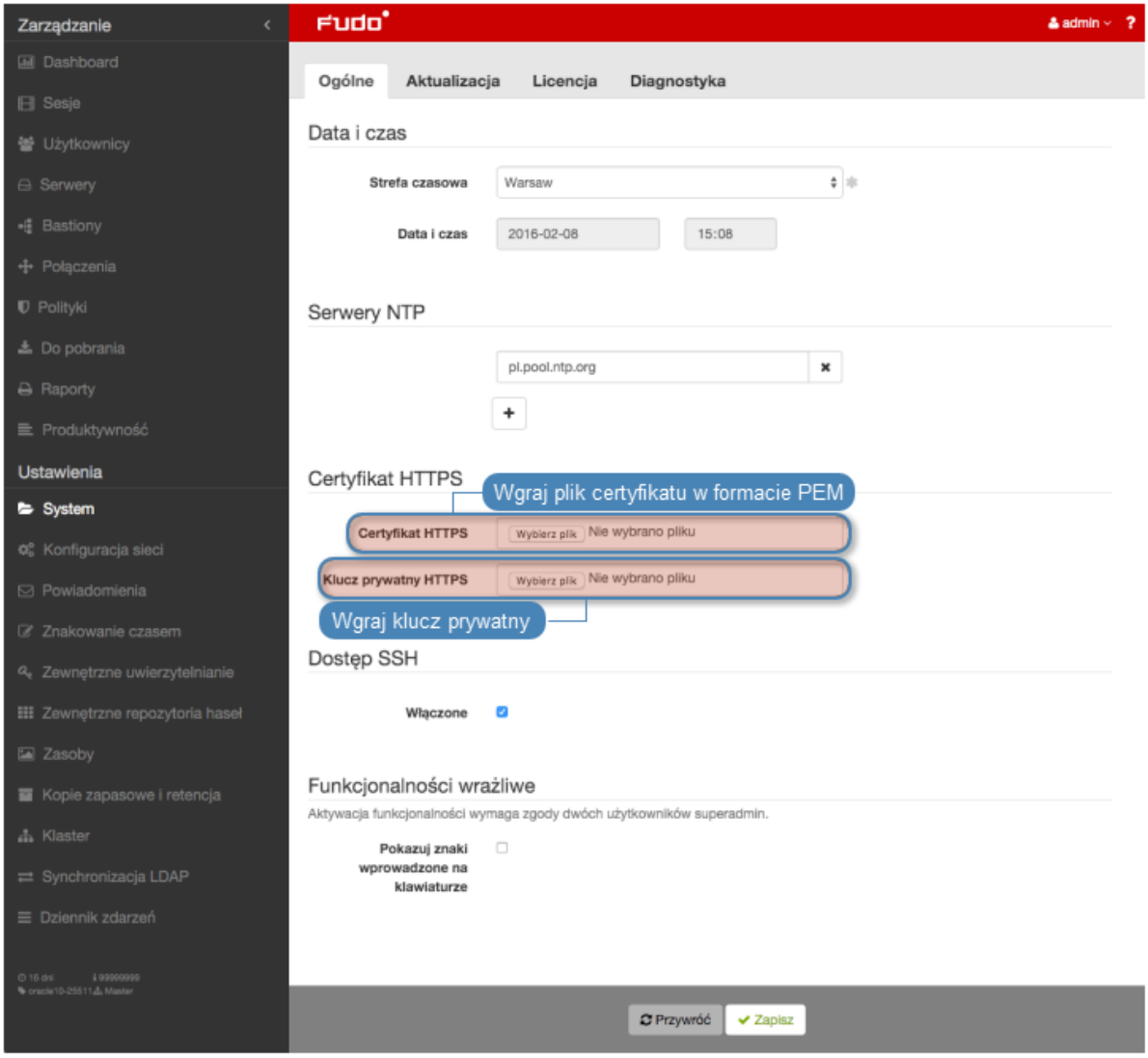
15.1.2 Certyfikat HTTPS

Certyfikat HTTPS pozwala administratorowi upewnić się, że nawiązał połączenie z panelem administracyjnym Wheel Fudo PAM a nie ze stroną próbującą podszyć pod panel administracyjny celem pozyskania danych logowania konta administratora.

Konfigurowanie certyfikatu SSL

Aby skonfigurować certyfikat SSL, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Kliknij przycisk *Wybierz plik* w polu *Certyfikat HTTPS* i wskaż w systemie plików definicję certyfikatu SSL w formacie PEM.
3. Kliknij przycisk *Przeglądaj* w polu *Klucz prywatny HTTPS* i wskaż w systemie plików definicję klucza prywatnego SSL.



4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

15.1.3 Blokowanie nowych połączeń

Opcja blokowania nowych połączeń umożliwia zablokowanie możliwości nawiązywania połączeń z monitorowanymi zasobami, np. w celu realizacji zaplanowanych prac serwisowych. |

Włączenie blokowania nowych połączeń |

Aby włączyć opcję blokowania nowych połączeń, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Sesje* zaznacz opcję *Blokuj nowe połączenia*.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

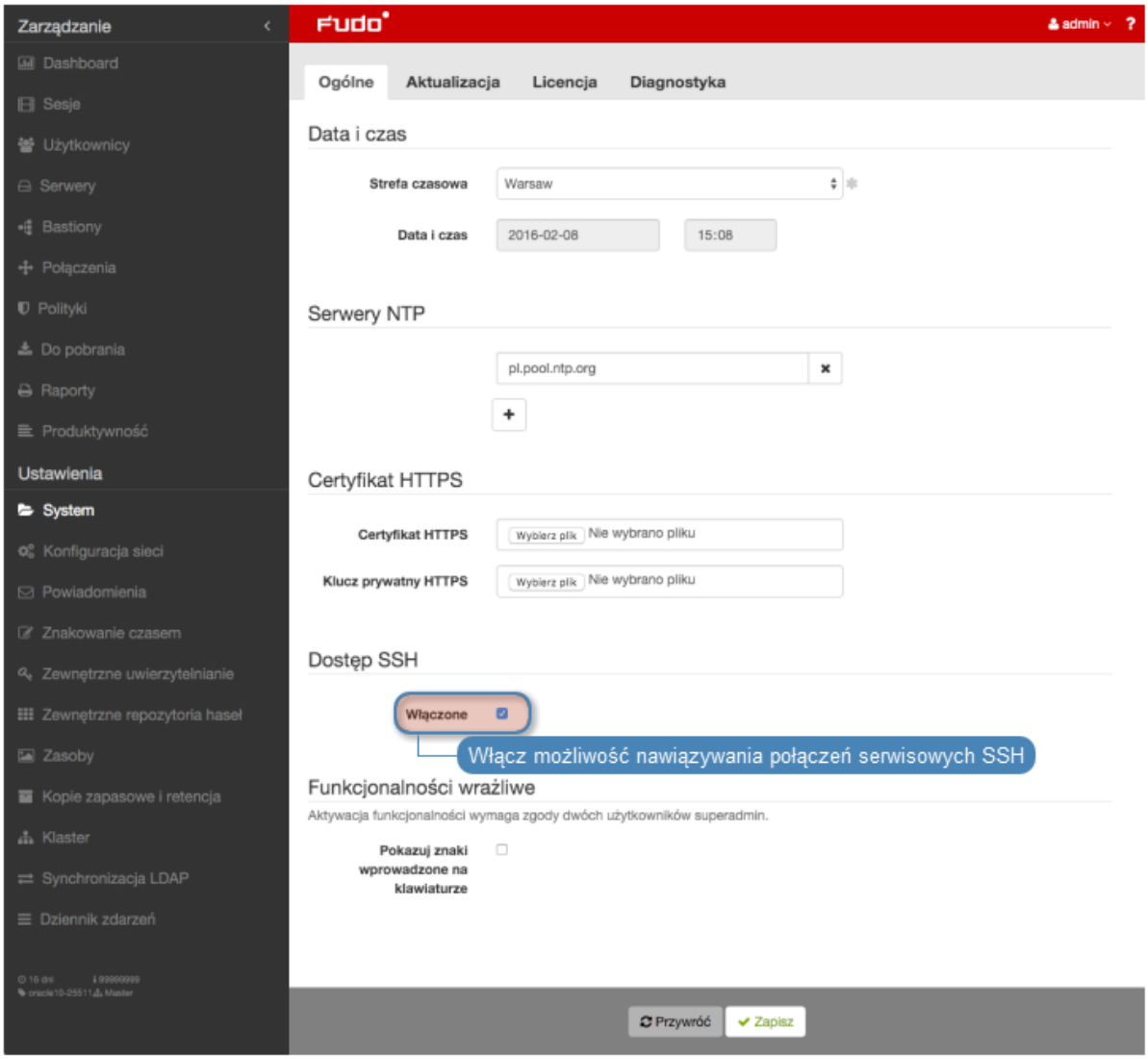
15.1.4 Dostęp SSH

Opcja umożliwia zdalny dostęp serwisowy do Wheel Fudo PAM za pośrednictwem protokołu SSH.

Włączanie dostępu SSH

Aby włączyć zdalny dostęp serwisowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Dostęp SSH* zaznacz opcję *Włączone*.



3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

15.1.5 Domyślna domena

Informacja: W przypadku gdy użytkownik nie ma określonej domeny, login użytkownika jest automatycznie uzupełniany o domenę domyślną.

Definiowanie domeny domyślnej

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnienie użytkowników*, wprowadź domenę domyślną.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

15.1.6 Konto reset

Konto reset umożliwia przywrócenie stanu fabrycznego urządzenia.

Włączanie konta reset

Aby włączyć możliwość zalogowania na konto reset, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Konto reset* zaznacz opcję *Włączone*.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

15.1.7 Funkcjonalności wrażliwe

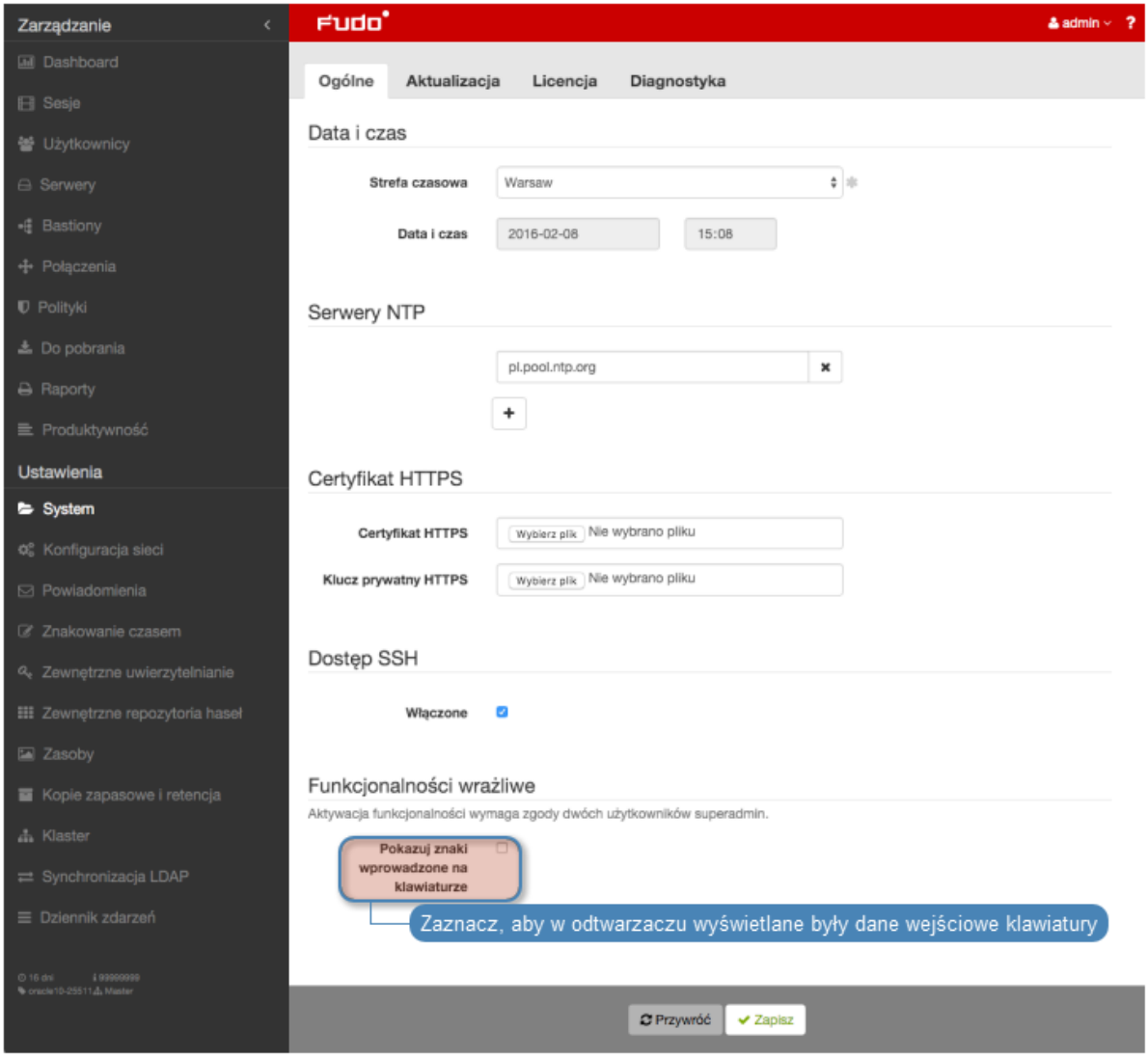
Funkcjonalności wrażliwe to zestaw opcji, których włączenie wymaga decyzji dwóch użytkowników o roli `superadmin`.

Włączanie pokazywania wejścia klawiatury

Informacja: Znaki wprowadzone na klawiaturze są domyślnie niepokazywane w odtwarzaczu. Włączenie podglądu znaków klawiatury wymaga zgody dwóch użytkowników `superadmin`.

Aby włączyć pokazywanie znaków wprowadzonych przez użytkownika na klawiaturze, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. Zaznacz opcję *Pokazuj znaki wprowadzone na klawiaturze* w sekcji *Funkcjonalności wrażliwe*, aby zainicjować włączenie funkcji.
3. Kliknij Zapisz.



4. Powiadom innego użytkownika `superadmin` o zainicjowaniu funkcjonalności, która wymaga potwierdzenia.

Tematy pokrewne:

- *Odtwarzanie sesji*

15.1.8 Aktualizacja systemu

Informacja:

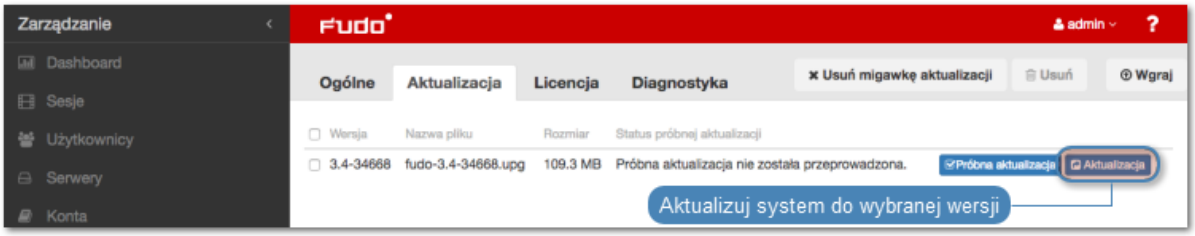
- Wheel Fudo PAM oprócz bieżącej wersji systemu, przechowuje jego poprzednią wersję, pozwalając na jej przywrócenie.
- Proces aktualizacji systemu nie dokonuje zmian w konfiguracji urządzenia ani nie narusza integralności zarejestrowanych sesji.
- Podczas aktualizacji systemu, zużycie wewnętrznej macierzy dyskowej może tymczasowo wzrosnąc.

15.1.8.1 Aktualizowanie systemu

Ostrzeżenie:

- Przed wykonaniem skryptów aktualizacyjnych, zaleca się dokonanie sprawdzenia wykonalności aktualizacji.
- W przypadku, gdy zajętość wewnętrznej macierzy danych przekracza 85%, przed wykonaniem aktulizacji systemu, skontaktuj się z działem wsparcia technicznego firmy Wheel Systems.
- W procesie aktualizacji, trwające połączenia użytkowników zostaną zerwane.
- Skorzystaj z opcji *Blokowanie nowych połączeń*, w sekcji *Sesja* ustawień systemowych, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Kliknij *Aktualizacja* przy wybranym pliku obrazu.



Ostrzeżenie: Po aktualizacji systemu, Wheel Fudo PAM zostanie uruchomione ponownie.

Ponowne uruchomienie wymaga obecności klucza szyfrującego. Włóż nośnik z kluczem szyfrującym do portu USB.

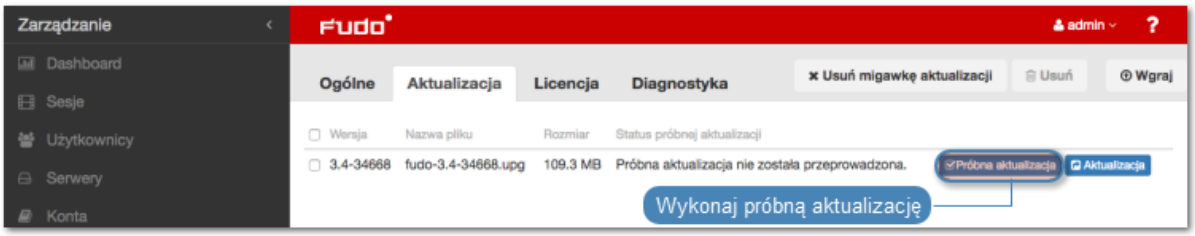
Informacja: W przypadku gdy uruchomienie systemu w nowej wersji nie powiedzie się, Wheel Fudo PAM wykryje problem i uruchomi system w poprzedniej wersji.

15.1.8.2 Weryfikacja wykonalności aktualizacji

Przed przystąpieniem do aktualizacji systemu, zaleca się zweryfikowanie czy bieżący stan konfiguracji pozwala na prawidłowe wykonanie skryptów aktualizacyjnych. Proces weryfikacyjny umożliwia też określenie przybliżonego czasu trwania aktualizacji.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.

3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Kliknij przycisk *Próbna aktualizacja*.



Informacja:

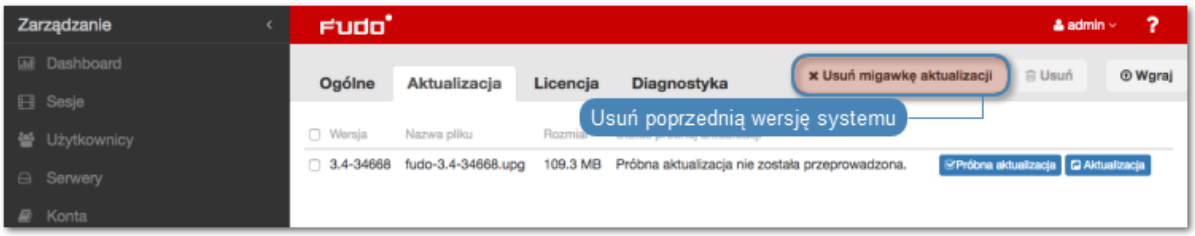
- Kliknij *Anuluj sprawdzanie*, aby przerwać działanie skryptów próbnej aktualizacji.
- Kliknij *Pobierz log*, aby pobrać plik z zapisem przebiegu aktualizacji próbnej i czasem wykonania skryptów aktualizacyjnych.

15.1.8.3 Usuwanie migawki aktualizacji

Usunięcie migawki aktualizacji ma na celu zwolnienie przestrzeni dyskowej zajętej przez poprzednią wersję systemu.

Ostrzeżenie: Usunięcie migawki aktualizacji uniemożliwi przywrócenie poprzedniej wersji systemu.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Usuń migawkę aktualizacji*.



4. Potwierdź usunięcie migawki.

Tematy pokrewne:

- *Przywracanie poprzedniej wersji systemu*
- *Ponowne uruchomienie systemu*

15.1.9 Licencja

Wgrywanie licencji

Aby wgrać nowy plik licencji, postępuj zgodnie z poniższą instrukcją.

Informacja: Nowa licencja zastąpi istniejącą.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź na zakładkę *Licencja*.
3. Kliknij *Wgraj*.

4. Wskaż plik licencji i kliknij *OK*, aby zainicjować system nową definicją.

Tematy pokrewne:

- *Opis systemu*
- *Wymagania*

15.1.10 Diagnostyka

Moduł diagnostyczny pozwala na wykonanie podstawowych komend systemowych, tj. ping, netcat czy traceroute.

Aby uruchomić program narzędziowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź na zakładkę Diagnostyka.
3. Znajdź żądaną komendę, wprowadź parametry wykonania i kliknij przycisk wykonania komendy.

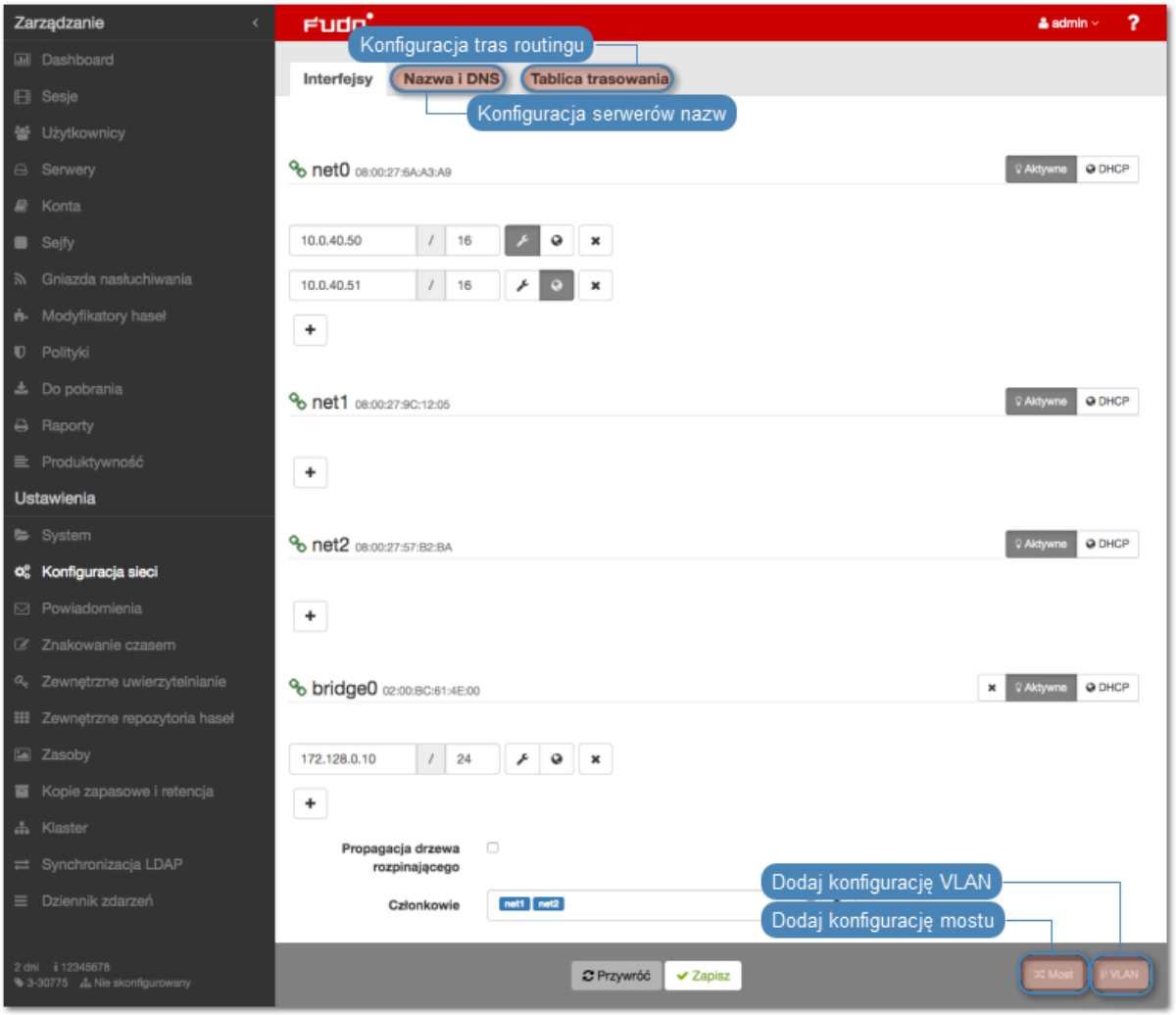
Komenda/ parametr	Opis
Ping	Ping wysyła sekwencję 10 pakietów icmp do wskazanego hosta.
Wyświetlaj adresy w formie numerycznej	Nie rozwiązuje adresu IP hosta do nazwy mnemonicznej.
Zapisz trasę	Umożliwia śledzenie trasy pakietów.
netcat	Netcat służy do nawiązywania połączeń ze zdalnym hostem na określonym numerze portu.
host	Polecenie host służy sprawdzeniu czy serwer DNS prawidłowo rozwiązuje nazwę maszyny docelowej.
traceroute	Komenda służy ustaleniu trasy, którą pokonują pakiety pomiędzy Wheel Fudo PAM i hostem docelowym.
Nie rozwiązuj nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do nazw mnemonicznych.
Uzyj protokołu ICMP zamiast UDP	Wymusza użycie pakietów UDP zamiast ICMP.
Tryb omijania firewall-a	Wymusza użycia niezmiennych numerów portu dla pakietów UDP i TCP. Port docelowy nie jest inkrementowany z każdym wysłanym pakietem.
Ustaw flagę „Nie fragmentuj”	Nie pozwala na fragmentację pakietów, w przypadku gdy przesyłany pakiet przekracza zdefiniowaną dla sieci wartość MTU (Maximum Transmission Unit). W przypadku przekroczenia MTU, zwrócony zostanie błąd.

Tematy pokrewne:

- *Rozwiązywanie problemów*

15.2 Konfiguracja sieci

Aby przejść do widoku zarządzania ustawieniami sieci, wybierz z lewego menu opcję *Ustawienia > Konfiguracja sieci*.



15.2.1 Konfiguracja ustawień sieciowych

W specyfikacji domyślnej, Wheel Fudo PAM wyposażone jest w dwa fizyczne interfejsy LAN, a opcje ustawień sieciowych umożliwiają:

- dodawanie aliasów IP interfejsów fizycznych, wykorzystywanych do konfigurowania zdalnych serwerów,
- konfigurowanie parametrów sieciowych wymaganych do komunikacji klastrowej,
- konfigurowanie adresacji IP do pracy w sieciach wirtualnych (VLAN),
- mostkowanie interfejsów fizycznych oraz sieci VLAN.

15.2.1.1 Zarządzanie interfejsami fizycznymi

Definiowanie adresu IP interfejsu

Definiowane adresy IP to aliasy interfejsu fizycznego, które wykorzystywane są w procedurach *konfiguracji serwerów* (pole *Adres lokalny* w sekcji *Pośrednik*).

Informacja: Jeśli lista adresów IP przypisanych do interfejsu sieciowego jest pusta i nie ma możliwości dodania adresu, sprawdź czy dany interfejs nie jest częścią mostu.

Aby dodać adres IP do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij + przy wybranym interfejsie i wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR.

Informacja: + będzie nieaktywny, jeśli włączona jest opcja pobierania adresu IP z serwera DHCP.

---

3. Zaznacz opcje dodatkowe dla definiowanego adresu IP.

Udostępnij panel administracyjny Wheel Fudo PAM pod wskazanym adresem IP. Adres zarządzający używany jest również do replikacji danych pomiędzy węzłami klastra.

Wirtualny adres IP, który zostanie automatycznie przejęty przez drugi węzeł klastra w przypadku awarii węzła głównego.

Informacja: Klastrowy adres IP należy dodać na każdym węźle klastra i aktywować dla niego opcję wirtualnego adresu IP  .

Udostępnij *Portal użytkownika* pod wskazanym adresem IP.

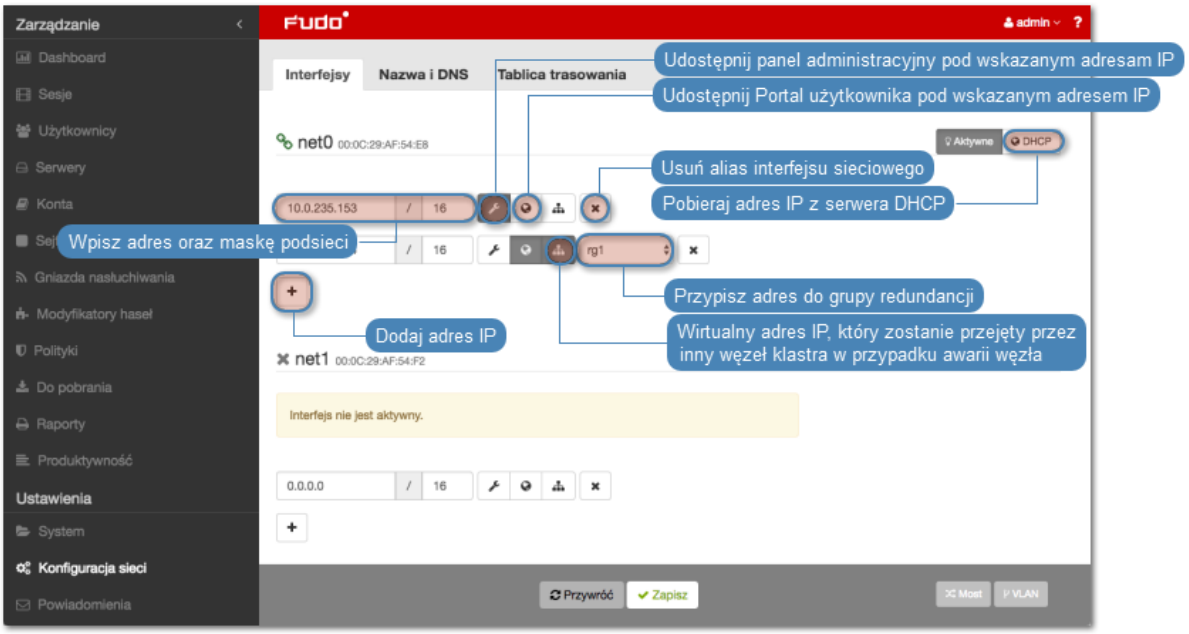
---

4. Określ grupę redundancji, do której zostanie przypisany adres IP (*dotyczy adresów klastrowych*).

Informacja: Grupy redundancji definiowane są w widoku *Klaster*, w zakładce *Grupy redundancji*.

---

5. Kliknij *Zapisz*.



Informacja: Każdy interfejs sieciowy opatrzony jest ikoną statusu.

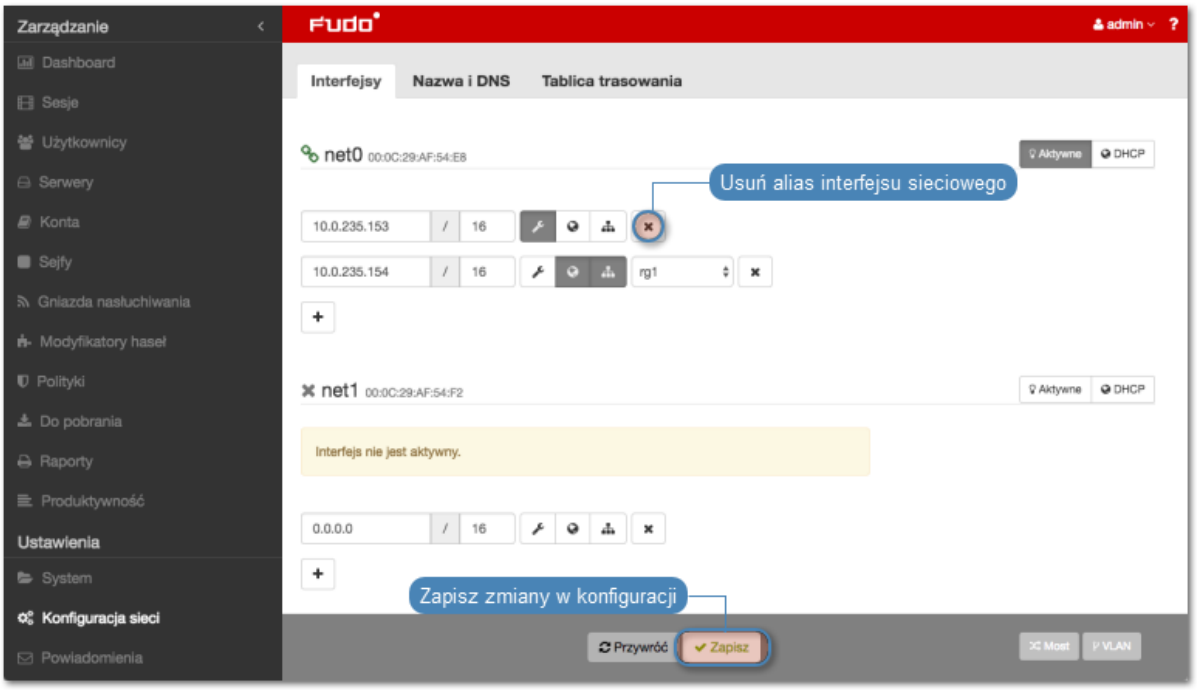
	Interfejs aktywny i podłączony.
	Interfejs aktywny ale odłączony.
	Interfejs wyłączony.

Usuwanie przypisanych adresów IP interfejsu

Ostrzeżenie: Usunięcie adresu IP uniemożliwi nawiązywanie połączeń z serwerami, które w polu *Adres lokalny* w sekcji *Pośrednik*, miały ustawiony usuwany adres IP.

Aby usunąć adres IP przypisany do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

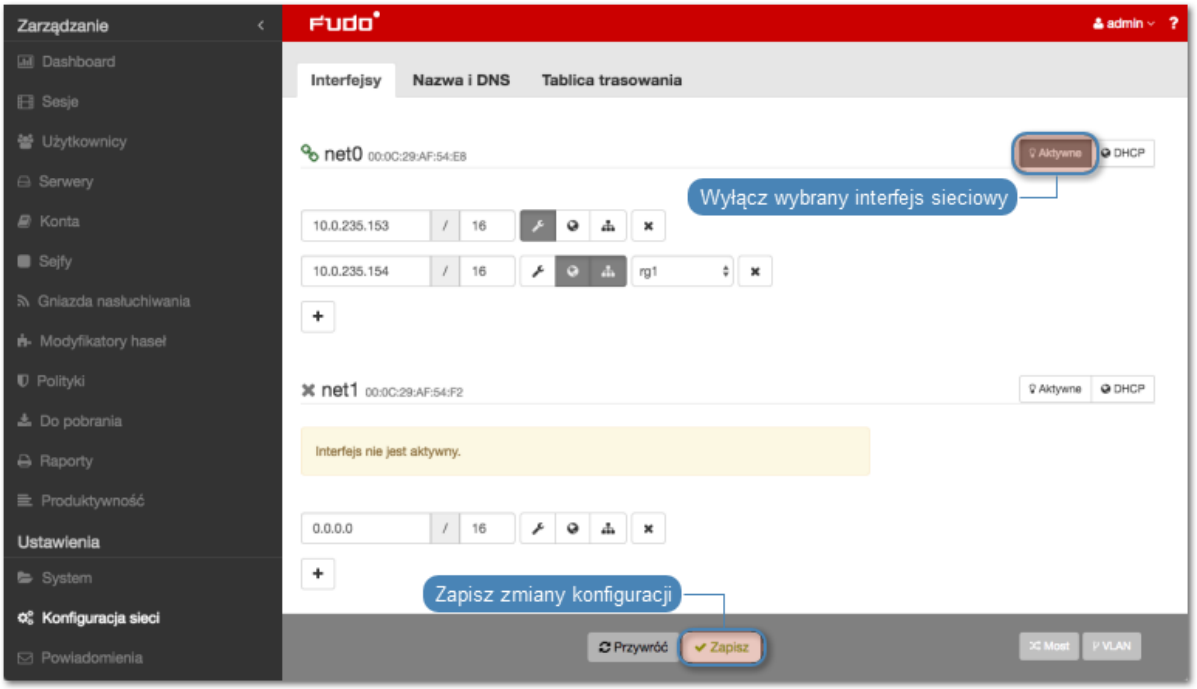
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Zaznacz opcję usunięcia wybranego interfejsu.
3. Kliknij *Zapisz*.



Wyłączanie interfejsu sieciowego

Aby wyłączyć adres IP przypisany do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

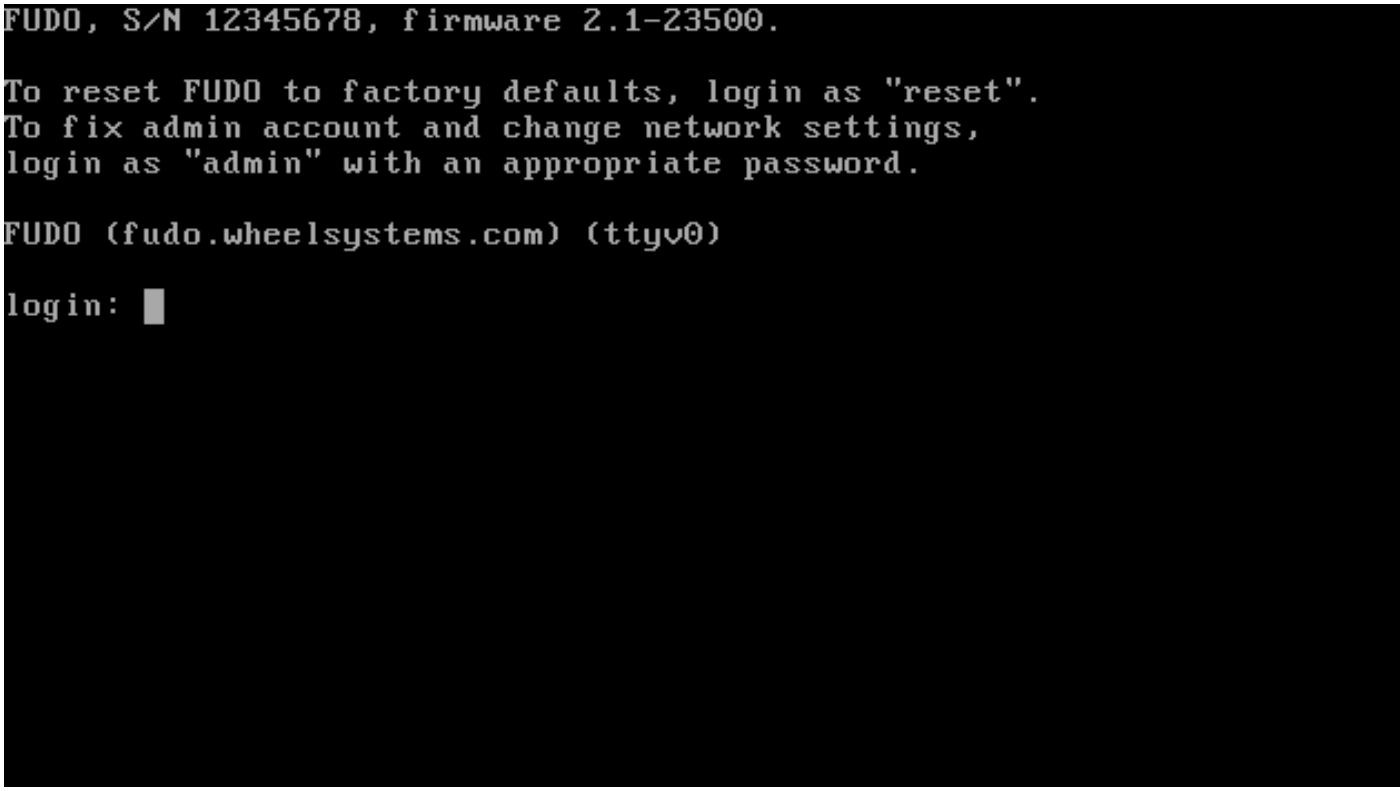
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *Aktywne*, aby wyłączyć wybrany interfejs.
3. Kliknij Zapisz.



15.2.1.2 Ustawianie adresu IP z konsoli

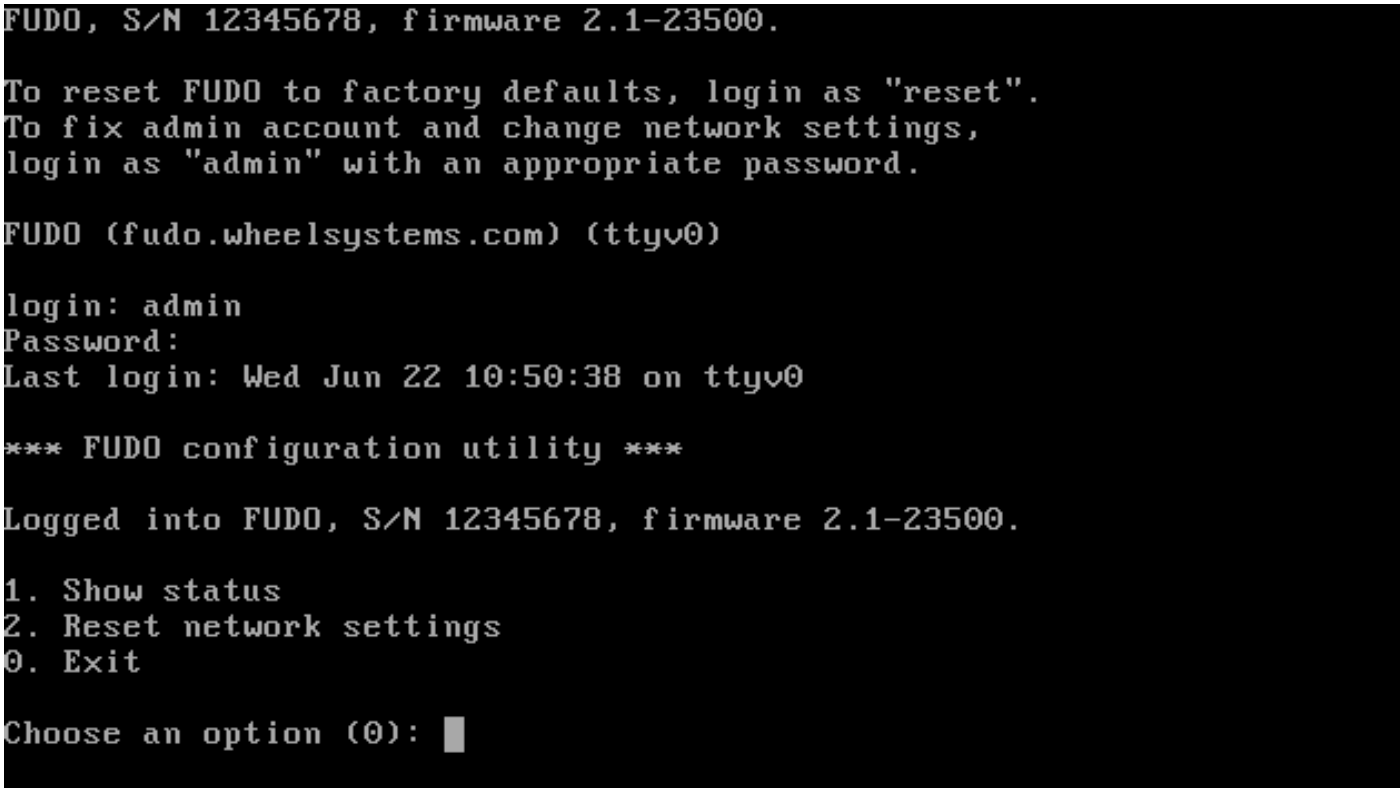
W sytuacji braku możliwości zalogowania się do zdalnego panelu administracyjnego, adres IP może zostać skonfigurowany z poziomu konsoli urządzenia.

1. Wprowadź login konta administratora.



2. Wprowadź hasło do konta administratora.

3. Wpisz 2 i naciśnij klawisz *Enter*.



4. Wpisz y i naciśnij klawisz *Enter*, aby potwierdź chęć zmiany ustawień sieciowych.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n):
```

5. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Wheel Fudo PAM) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

6. Wprowadź adres IP urządzenia wraz z maską podsieci oddzieloną znakiem / (np. `10.0.0.8/24`) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

7. Wprowadź bramę sieci i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

15.2.1.3 Konfigurowanie mostu sieciowego

Scenariusz wdrożeniowy *trybu pracy mostu*, wymaga wskazania interfejsów sieciowych przez które przekazywany będzie ruch pomiędzy administratorem i serwerem.

Aby stworzyć most sieciowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij Most.
3. Skonfiguruj przypisanie interfejsów fizycznych lub sieci VLAN do konfigurowanego mostu.

Informacja: Konfiguracja mostu wymaga usunięcia wszystkich adresów IP przypisanych bezpośrednio do interfejsów sieciowych będących członkami mostu.

---

4. Wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR, dla wirtualnego interfejsu definiowanego mostu.
5. Zaznacz opcję Propagacja drzewa rozpinającego, aby włączyć mechanizm wykrywania i zapobiegania zapętleń w sieci (STP - Spanning Tree Protocol).
6. Zaznacz opcję *Zarządzanie*, jeśli panel zarządzania ma być dostępny pod wybranym adresem IP, i kliknij *Aktywne*.
7. Kliknij *Zapisz*.

15.2.1.4 Konfigurowanie sieci wirtualnych (VLAN)

Sieci VLAN pozwalają na segmentację sieci w celu odseparowania domen rozgłoszeniowych.

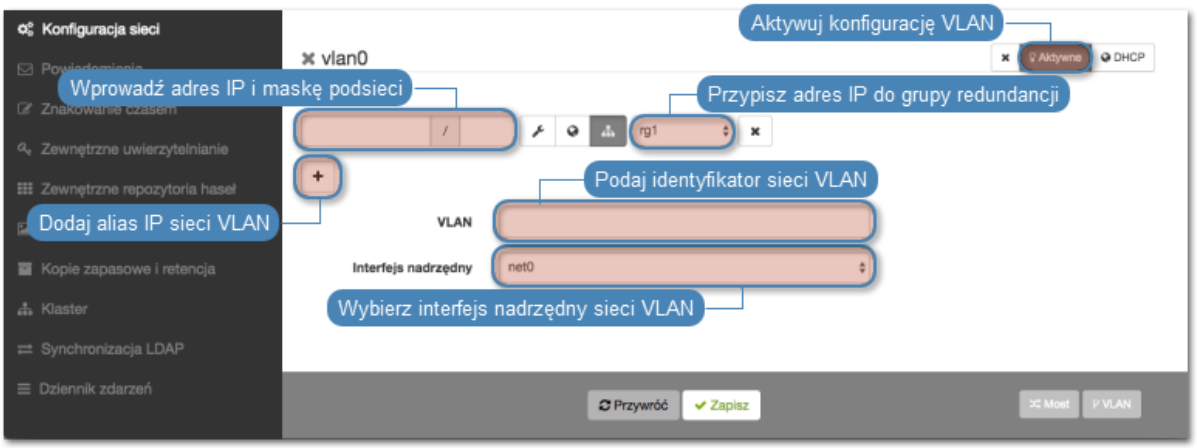
Aby skonfigurować Wheel Fudo PAM do pracy w sieci VLAN, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *VLAN*, aby dodać definicję sieci wirtualnej.
3. Wybierz nadrzędny interfejs sieciowy oraz nadaj identyfikator konfigurowanej sieci wirtualnej.
4. Dodaj adresy IP przynależne do konfigurowanej sieci VLAN lub kliknij DHCP, aby pobrać adres IP z serwera DHCP.

Informacja: Wprowadzone adresy IP będą dostępne jako adresy lokalne pośrednika w *konfiguracji serwerów*.

---

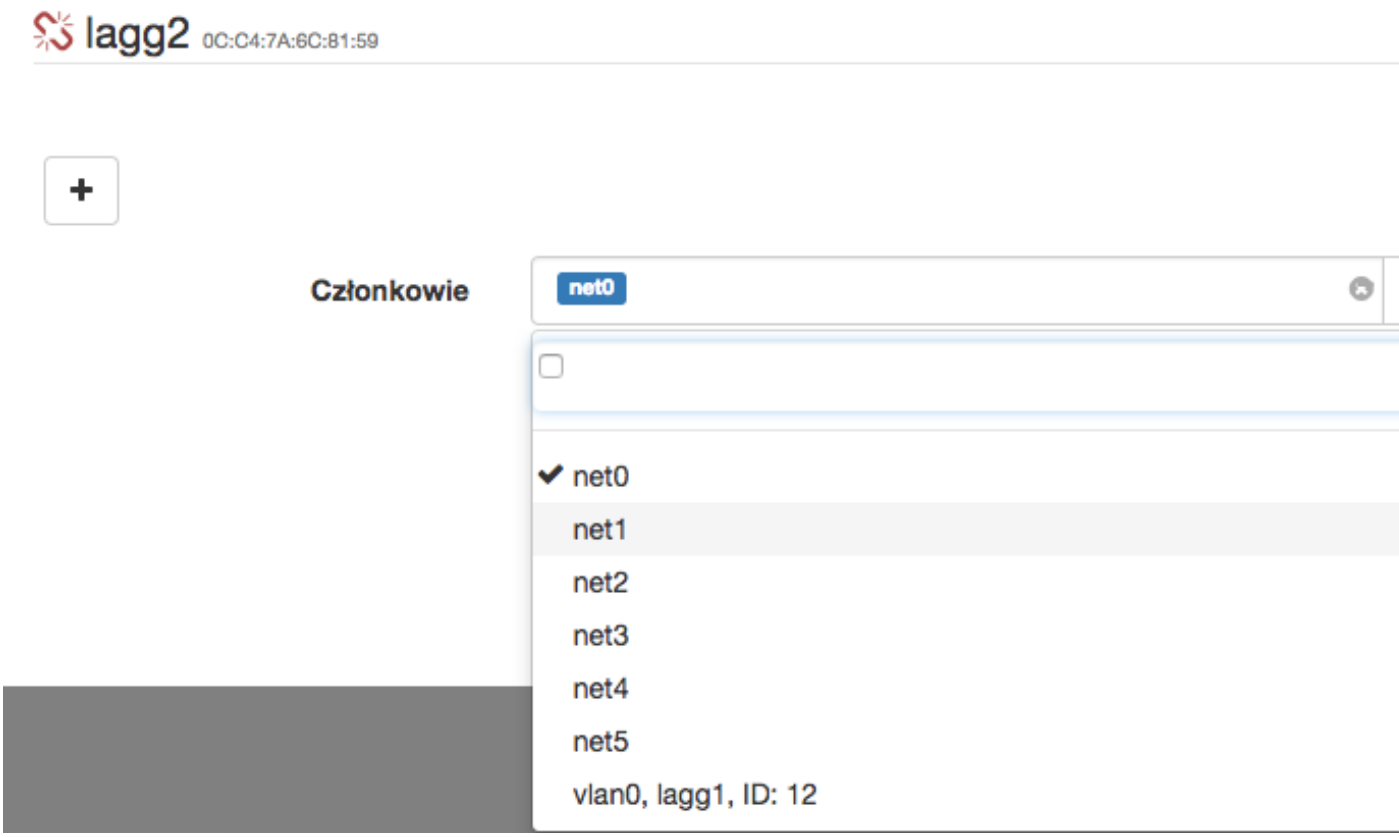
5. Kliknij *Aktywne*, aby aktywować VLAN.
6. Kliknij *Zapisz*.



15.2.1.5 Konfigurowanie agregacji połączeń LACP

Wheel Fudo PAM wspiera funkcję agregowania połączeń sieciowych, pozwalając na uzyskanie większej przepustowości transmisji danych lub implementację scenariusza umożliwiającego zapewnienie dostępności usług w przypadku awarii jednego z urządzeń sieciowych.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *Agregacja połączeń*.
3. Skonfiguruj przypisanie interfejsów fizycznych.



Informacja: Konfiguracja agregacji połączeń wymaga usunięcia wszystkich adresów IP przypisanych bezpośrednio do interfejsów sieciowych będących członkami zagregowanego interfejsu.

4. Wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR, dla tworzonej agregacji połączeń.
5. Zaznacz opcje dodatkowe dla definiowanego adresu IP.

	Udostępnij panel administracyjny Wheel Fudo PAM pod wskazanym adresem IP. Adres zarządzający używany jest również do replikacji danych pomiędzy węzłami klastra.
	Wirtualny adres IP, który zostanie automatycznie przejęty przez drugi węzeł klastra w przypadku awarii węzła głównego.
	Udostępnij *Portal użytkownika* pod wskazanym adresem IP.

6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zarządzanie serwerami*
- *Gniazda nasłuchiwania*

15.2.2 Etykiety adresów IP

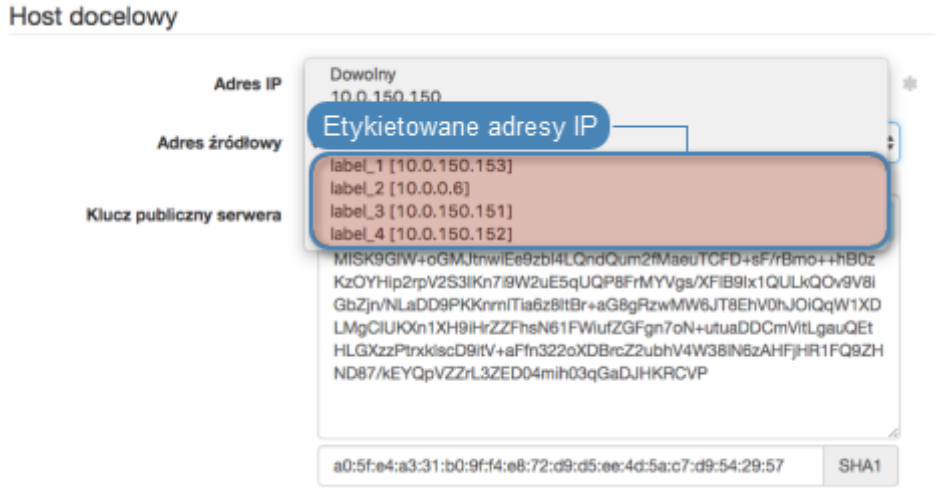
Etykiety adresów IP to parametry globalne konfiguracji. Objęte są procesem replikacji danych w obrębie klastra, ale ich przypisanie do adresów IP jest realizowane lokalnie na każdym z węzłów. Etykiety pozwalają na zachowania ciągłości dostępu do usługi uwierzytelnienia poprzez serwer LDAP w przypadku awarii węzła nadrzędnego a także implementację scenariusza balansowania obciążeniem węzłów klastra.

Definiowanie etykietowanego adresu IP

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Wybierz zakładkę *Etykiety IP*.
3. Kliknij +.
4. Wprowadź adres IP i nazwę etykiety.

Informacja: W nazwach etykiet dopuszczane są tylko małe litery, cyfry oraz znaki _ i -.

5. Kliknij *Zapisz*.
6. Użyj etykietowanego adresu IP w konfiguracji gniazda nasłuchiwania, serwera lub w konfiguracji zewnętrznych źródeł uwierzytelnienia.



Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Zewnętrzne serwery uwierzytelniania*
- *Serwery*
- *Gniazda nasłuchiwania*

15.2.3 Konfiguracja bajpasów

Bajpasy pozwalają na automatyczne przekierowanie ruchu sieciowego w przypadku awarii urządzenia.

Informacja: Opcje konfiguracjne bajpasów nie są dostępne w przypadku zainstalowania systemu Wheel Fudo PAM w środowisku wirtualnym.

1. Wybierz z lewego menu opcję *Ustawienia* > *Konfiguracja sieci*.
2. Wybierz zakładkę *Bajpasy*.
3. Wybierz tryb pracy interfejsu sieciowego.
   - Tryb bajpas stale włączony - opcja wymusza tryb bajpas, ruch sieciowy nie jest kierowany do systemu Wheel Fudo PAM. Ta opcja może być użyta przy pracach związanych z utrzymaniem systemu lub rozwiązywaniu problemów.
   - Tryb bajpas włączony tylko w przypadku awarii systemu - pakiety sieciowe zostają przekierowane do innego urządzenia tylko w przypadku awarii systemu lub gdy Wheel Fudo PAM jest wyłączony.
   - Bypass mode disabled - w przypadku awarii, ruch sieciowy nie będzie przekierowany do następnego urządzenia.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

15.2.4 Konfiguracja tras routingu

W konfiguracji domyślnej, Wheel Fudo PAM kieruje cały ruch przychodzący, do zdefiniowanej bramy. Routing statyczny pozwala na zdefiniowanie tras dla pakietów pochodzących ze wskazanych podsieci.

Informacja: Definiując domyślną trasę routowania pakietów, w polu *Sieć* wpisz `default`.

Dodawanie trasy routingu

Aby dodać trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Kliknij *+ Dodaj trasę*, aby zdefiniować nową trasę routingu.
4. Wprowadź adres sieci, maskę w notacji CIDR (np. `192.168.0.1/29`) oraz adres IP bramy (np. `10.0.0.1`).
5. Kliknij *Zapisz*.

Modyfikowanie trasy routingu

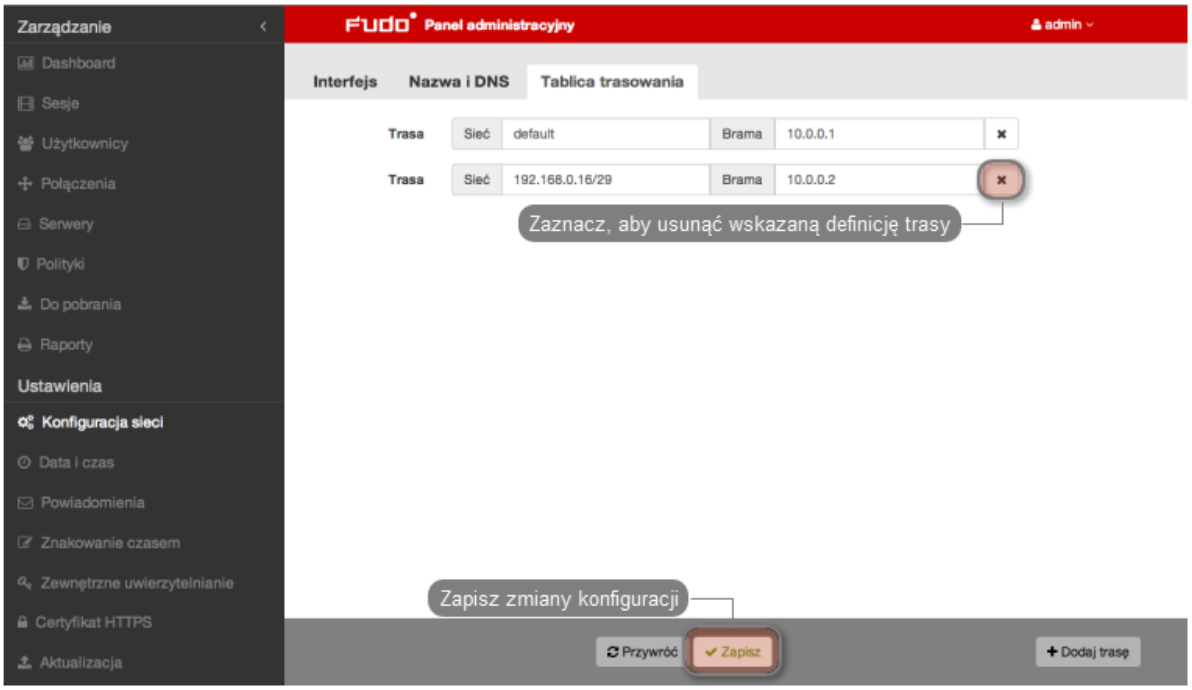
Aby zmodyfikować trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij *Zapisz*.

Usuwanie trasy routingu

Aby usunąć trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Zaznacz opcję usunięcia wybranej trasy routingu i kliknij *Zapisz*.

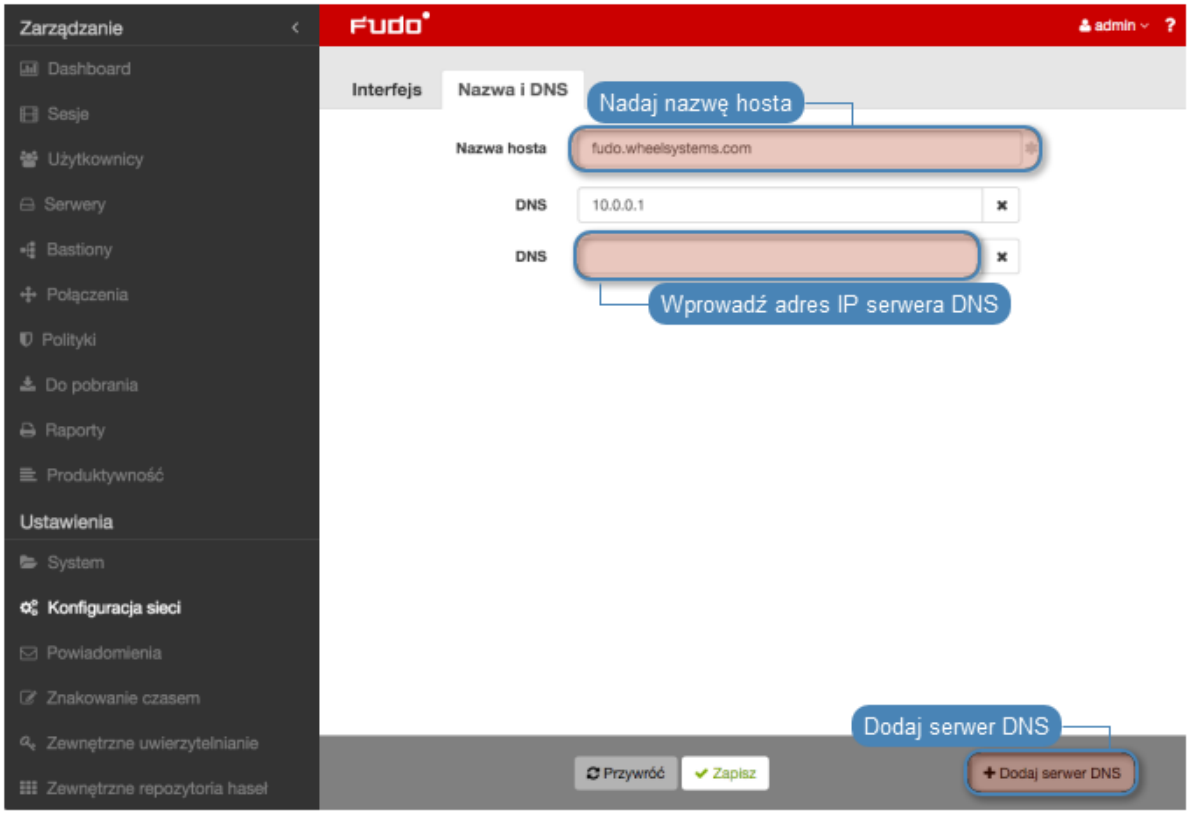


Tematy pokrewne:

- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*

15.2.5 Konfiguracja serwerów DNS

Informacja: Serwer DNS pozwala na używanie mnemonicznych nazw hostów zamiast adresów IP w konfiguracji zasobów.



Dodawanie serwera DNS

Aby dodać serwer DNS, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. Kliknij *+ Dodaj serwer DNS*, aby zdefiniować nowy serwer DNS.
4. Wprowadź adres IP serwera DNS.
5. Kliknij *Zapisz*.

Modyfikowanie serwera DNS

Aby zmodyfikować definicję serwera DNS, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki Nazwa i DNS.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij Zapisz.

Usuwanie serwera DNS

Aby usunąć definicję serwera DNS, postępuj zgodnie z poniższą instrukcją.

Informacja: Usunięcie definicji serwera DNS może spowodować zakłócenia w pracy urządzenia, jeśli w konfiguracji wykorzystywane były nazwy hostów zamiast adresów IP.

---

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.

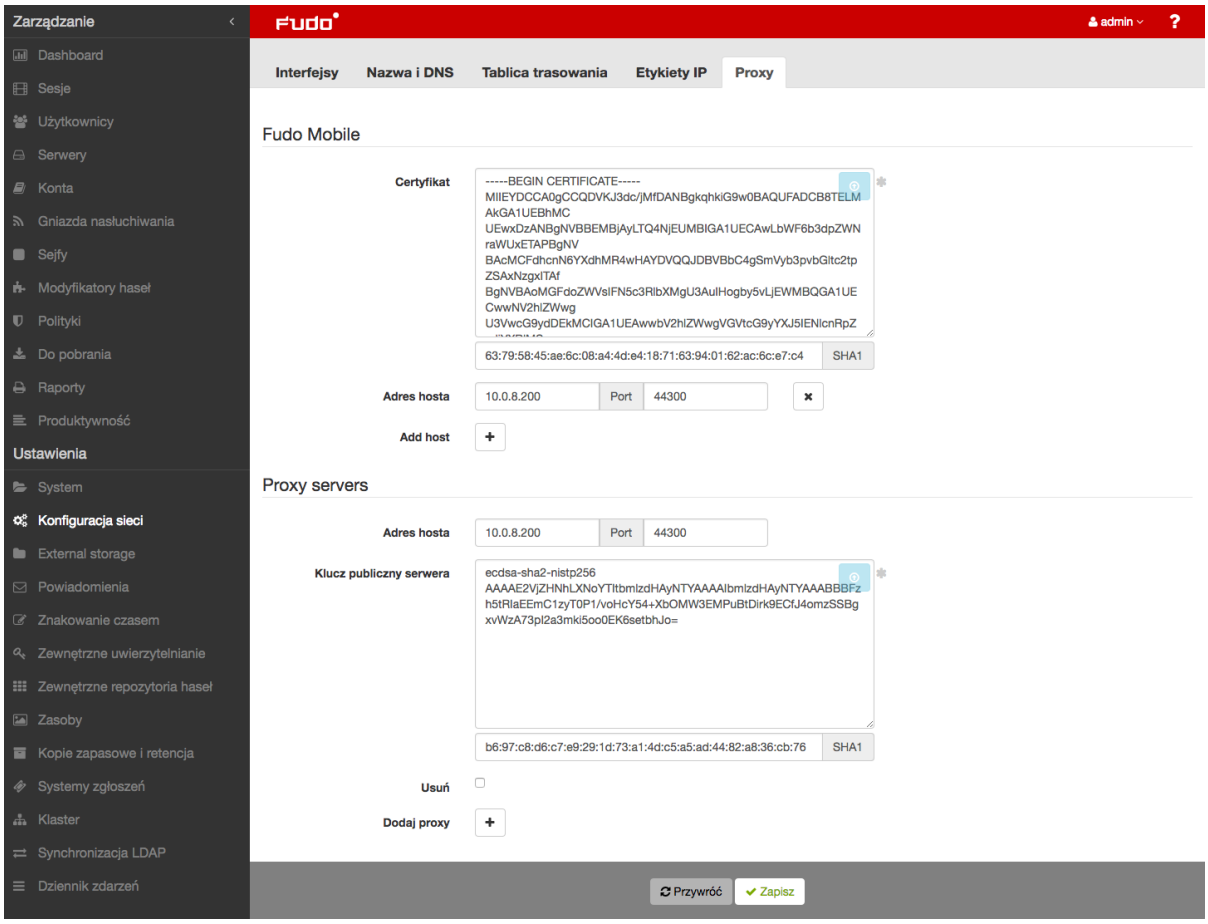
2. Przejdź do zakładki *Nazwa i DNS*.
3. Wyszukaj i kliknij opcję usunięcia wybranego wpisu.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*
- *Konfiguracja tras routingu*

15.2.6 Konfiguracja serwerów proxy

Informacja: Serwer proxy wymagany jest do zapewnienia komunikacji pomiędzy aplikacją *Fudo Mobile* a systemem Wheel Fudo PAM.



Dodawanie proxy

Aby dodać serwer proxy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Proxy*.

3. W sekcji *Fudo Mobile*, kliknij  , aby wgrać certyfikat komunikacji urządzeń mobilnych z serwerem proxy.
4. Wprowadź adres IP lub nazwę hosta, wraz z numerem portu, do komunikacji urządzeń mobilnych z API Fudo.

Informacja: Kliknij  , aby zdefiniować więcej hostów dla połączeń z API.

---

5. Wprowadź adres IP lub nazwę hosta serwera proxy, wraz z numerem portu połączeń SSH.
6. Kliknij  , aby pobrać klucz publiczny serwera proxy.

Informacja: Kliknij  , aby zdefiniować więcej hostów proxy dla połączeń SSH.

---

7. Kliknij *Zapisz*.

Informacja: Klucze SSH przedstawione w sekcji *Klucze SSH Fudo*, służą do skonfigurowania usługi proxy na wyznaczonym systemie. Więcej informacji znajdziesz w rozdziale *Usługa proxy dla uwierzytelnienia 4-Eyes*.

Modyfikowanie serwera proxy

Aby zmodyfikować definicję serwera proxy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Proxy*.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij *Zapisz*.

Usuwanie adresu IP komunikacji z Fudo Mobile

Aby usunąć adres IP do komunikacji proxy z aplikacją *Fudo Mobile*, postępuj zgodnie z poniższą instrukcją.

Informacja: Usunięcie adresu IP może spowodować zakłócenia w komunikacji pomiędzy instancjami aplikacji *Fudo Mobile* a systemem Wheel Fudo PAM.

---

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Proxy*.
3. W sekcji *Fudo Mobile*, wyszukaj żądany adres IP i zaznacz  .
4. Kliknij *Zapisz*.

Usuwanie serwera proxy

Aby usunąć definicję serwera proxy, postępuj zgodnie z poniższą instrukcją.

Informacja: Usunięcie definicji serwera proxy może spowodować zakłócenia w działaniu usług od niego zależnych.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Proxy*.
3. W sekcji *Serwery proxy*, wyszukaj i zaznacz opcję usunięcia wybranego wpisu.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*
- *Dodawanie urządzenia mobilnego*
- *Akceptowanie połączeń oczekujących*
- *Odrzucanie połączeń oczekujących*

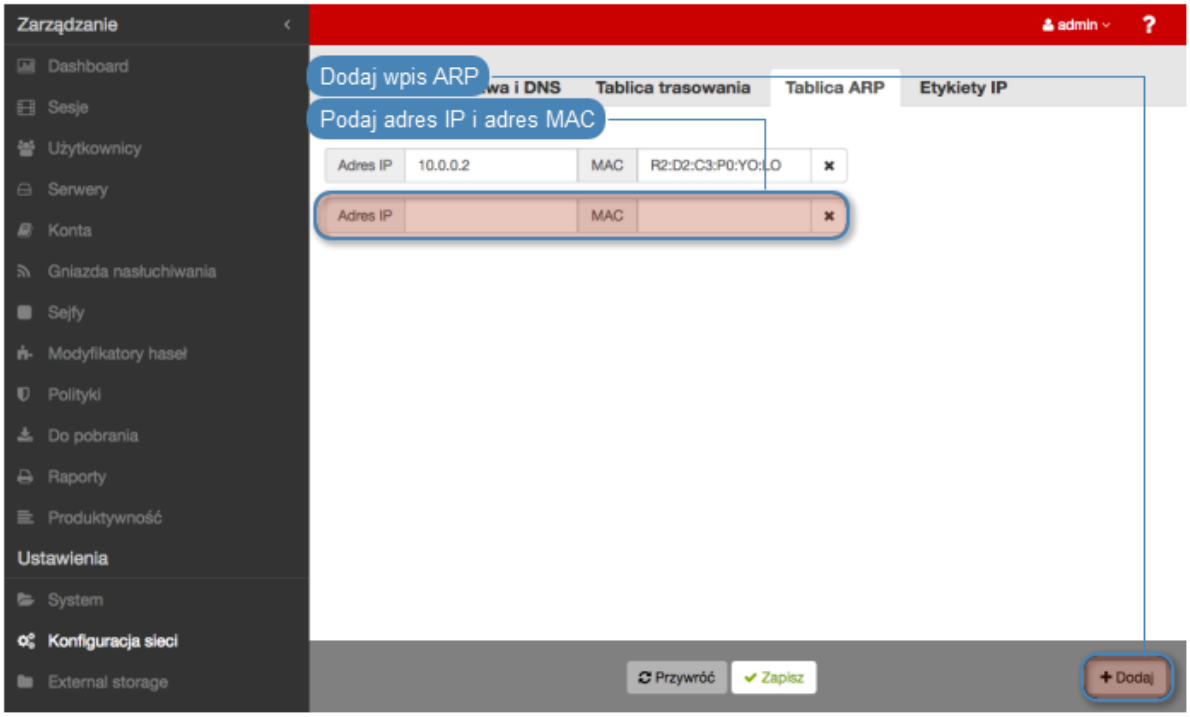
15.2.7 Konfiguracja tablicy ARP

Utworzenie wpisu w tablicy *ARP* pozwala rozwiązać problemy w komunikacji sieciowej.

Dodawanie wpisu ARP

Aby dodać wpis w tablicy ARP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica ARP*.
3. Kliknij *+ Dodaj*.
4. Wprowadź adres IP oraz adres MAC urządzenia sieciowego.
5. Kliknij *Zapisz*.



Modyfikowanie wpisu w tablicy ARP

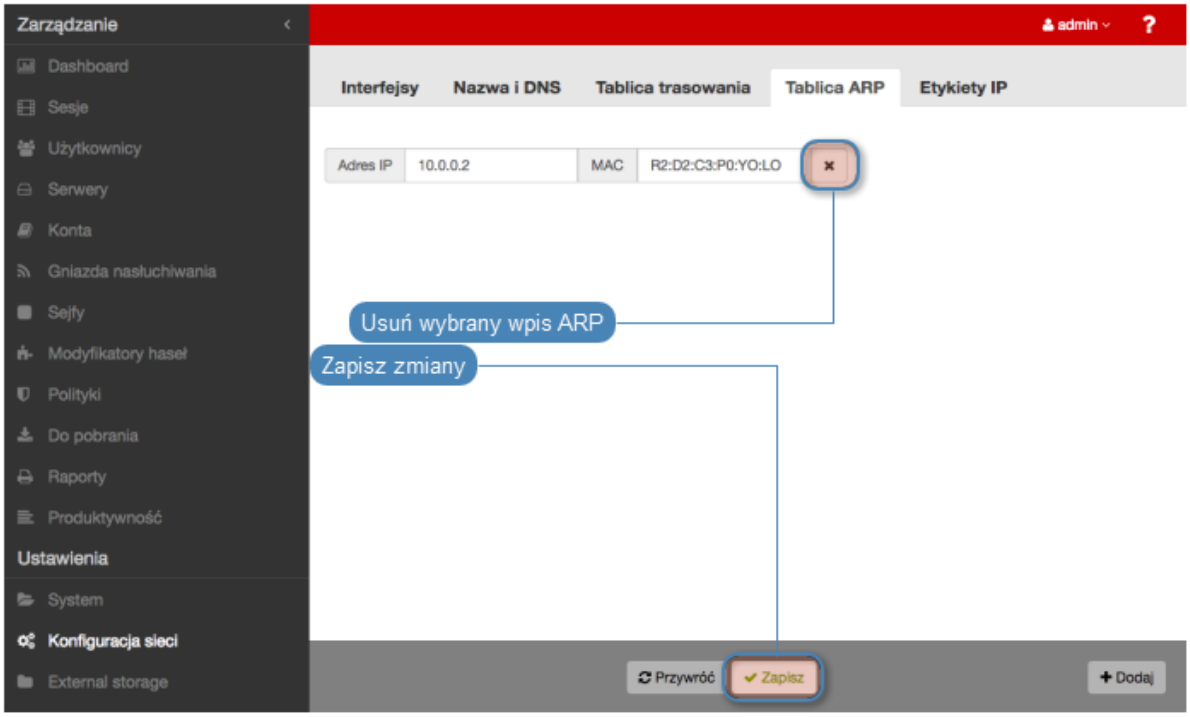
Aby zmodyfikować wpis ARP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica ARP*.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij *Zapisz*.

Usuwanie wpisu w tablicy ARP

Aby usunąć wpis ARP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica ARP*.
3. Zaznacz ikonę ✖ przy wybranym wpisie i kliknij *Zapisz*.



Tematy pokrewne:

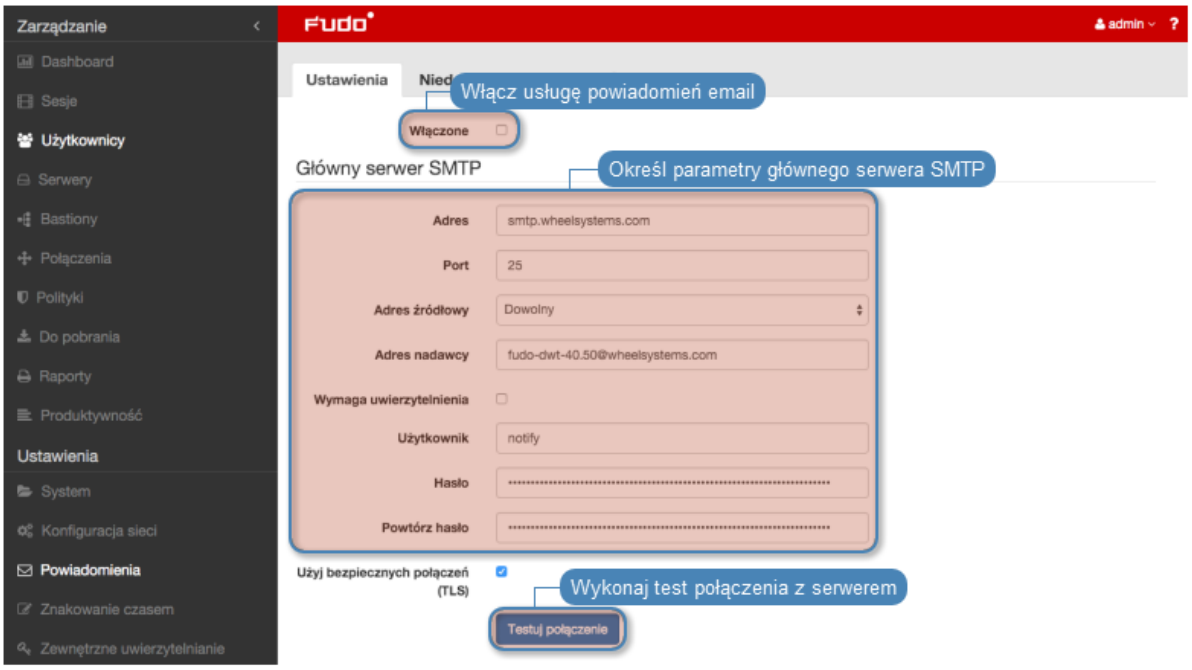
- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*

15.3 Powiadomienia

Wheel Fudo PAM może wysyłać powiadomienia email o zdarzeniach dotyczących zdefiniowanych połączeń (rozpoczęcie sesji, zakończenie sesji, otwarcie pomocy zdalnej, zakończenie pomocy zdalnej, wykrycie wzorca). Usługa powiadomień dla poszczególnych obiektów połączenia, definiowana jest przy tworzeniu nowego obiektu lub podczas edycji istniejącego połączenia. Wysyłanie powiadomień wymaga skonfigurowania serwera poczty SMTP.

Aby skonfigurować serwer SMTP, postępuj zgodnie z poniższą instrukcją.

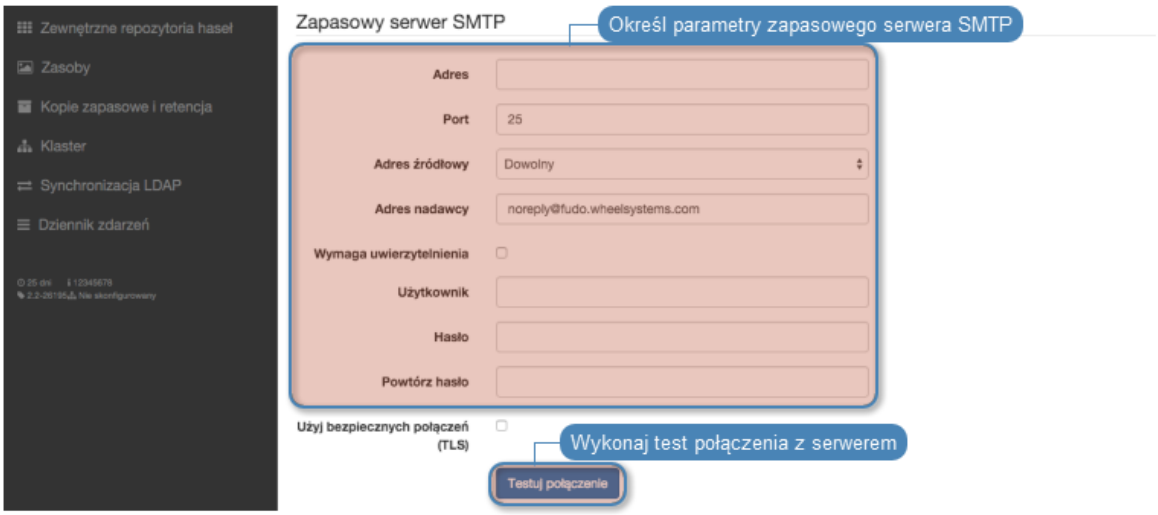
1. Wybierz z lewego menu *Ustawienia* > *Powiadomienia*.
2. Zaznacz opcję *Włączone*, aby system wysyłał powiadomienia.
3. Uzupełnij parametry konfiguracyjne głównego serwera SMTP.



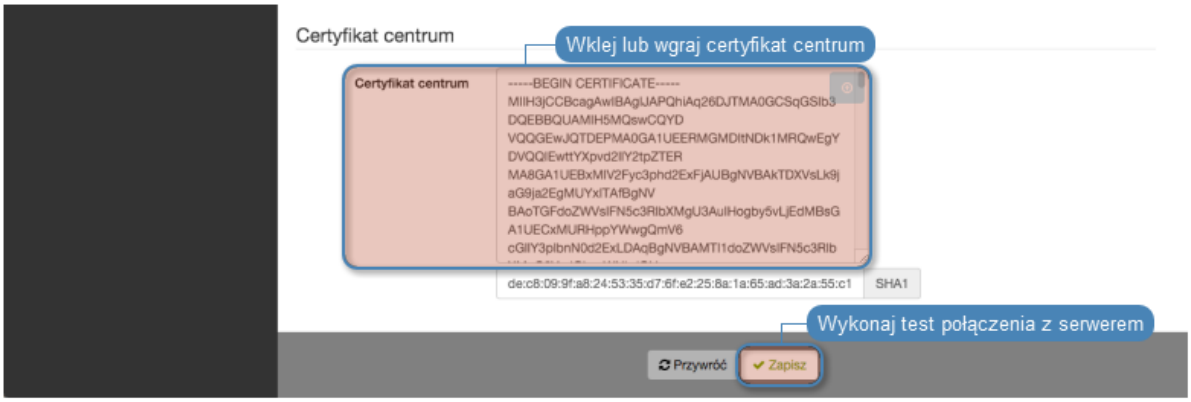
Parametr	Opis
Adres	Adres IP serwera SMTP.
Port	Numer portu, na którym działa usługa SMTP.
Adres nadawcy	Adres email, z którego wysyłane będą powiadomienia.
Wymaga uwierzytelnienia	Czy serwer SMTP wymaga uwierzytelniania.
Użytkownik	Nazwa użytkownika dla uwierzytelnienia usługi SMTP.
Hasło	Hasło użytkownika dla uwierzytelnienia usługi SMTP.
Użyj bezpiecznych połączeń (TLS)	Zaznacz, jeśli serwer pocztowy wykorzystuje protokół szyfrujący TLS.

Informacja: Kliknij *Testuj połączenie*, aby zweryfikować prawidłowość parametrów konfiguracyjnych.

4. Opcjonalnie, uzupełnij parametry konfiguracyjne dla zapasowego serwera SMTP.



5. Wprowadź treść certyfikatu urzędu certyfikacji, w formacie PEM.



6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konta*

15.4 Znakowanie czasem

Opatrzenie zarejestrowanej sesji znacznikiem czasu, czyni materiał bardziej wiarygodnym dowodem rzeczowym.

Informacja: Funkcjonalność znakowania sesji wymaga podpisania odrębnej umowy z instytucją świadczącą usługę znakowania czasem.

Konfigurowanie usługi znakowania czasem

Aby włączyć i skonfigurować usługę znakowania czasem, postępuj zgodnie z poniższą instrukcją.

Informacja: Znacznikiem czasu zostaną opatrzone również sesje, które zostały zarejestrowane przed włączeniem usługi.

---

1. Wybierz z lewego menu *Ustawienia* > *Znakowanie czasem*.
2. Zaznacz opcję *Włącz*, aby znakować znacznikiem czasu zarejestrowane sesje.
3. Wybierz z listy rozwijalnej dostawcę usługi.
4. Wskaż plik z certyfikatem i kluczem.

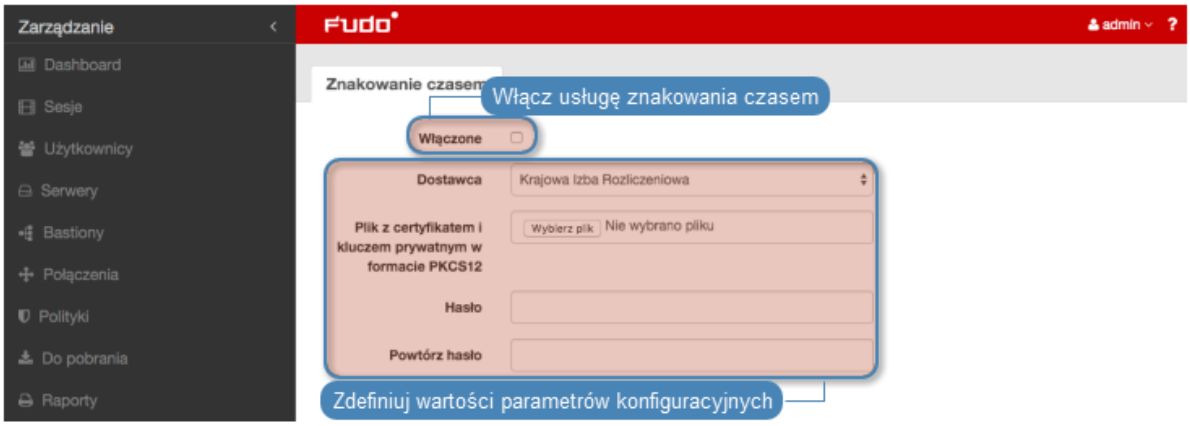
Informacja: Certyfikat oraz klucz prywatny otrzymasz od dostawcy usługi znakowania czasem.

---

5. Kliknij *Zapisz*.

Informacja: Prawidłowe działanie usługi znakowania czasem wymaga aby następujące serwery były osiągalne:

- `193.178.164.5` (w przypadku usługi snakowania czasem świadczonej przez PWPW)
- `http://www.ts.kir.com.pl/HttpTspServer` (w przypadku usługi snakowania czasem świadczonej przez KIR)



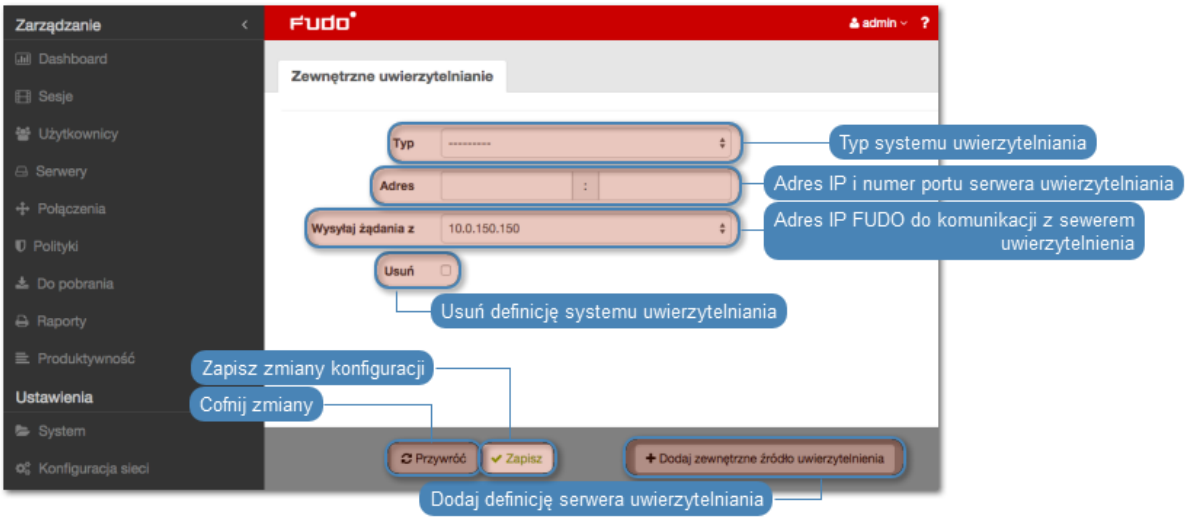
15.5 Zewnętrzne serwery uwierzytelniania

Uwierzytelnienie użytkowników za pomocą zewnętrznych serwerów uwierzytelniania (tj. *CERB*, *RADIUS*, *LDAP*, *Active Directory*) wymaga skonfigurowania połączeń z serwerami usług danego typu.

Widok zarządzania serwerami uwierzytelniania

Widok zarządzania zewnętrznymi serwerami uwierzytelniania pozwala na dodanie nowych oraz edycję istniejących serwerów.

Aby przejść do widoku zarządzania serwerami uwierzytelniania, wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.



Dodawanie definicji serwera zewnętrznego uwierzytelniania

Aby dodać serwer uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Kliknij + *Dodaj zewnętrzne źródło uwierzytelnienia*.
3. Z listy rozwijalnej *Typ*, wybierz rodzaj systemu uwierzytelnienia.
4. Uzupełnij parametry konfiguracyjne, zależne od typu wybranego systemu uwierzytelnienia.

Parametr	Opis
CERB	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa CERB.
Adres źródłowy	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelnienia.
Serwis	Serwis w systemie CERB w oparciu o który będzie uwierzytelniany użytkownik.
Sekret	Sekret wykorzystywany do połączeń z serwerem. Sekret odpowiada hasłu zdefiniowanemu podczas konfiguracji klienta RADIUS w systemie CERB.
Powtórz sekret	Sekret wykorzystywany do połączeń z serwerem.
RADIUS	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa RADIUS.
Adres źródłowy	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelniania.
NAS ID	Parametr, który zostanie przekazany w atrybucie NAS-Identifier do serwera RADIUS.
Sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowników.
Powtórz sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowników.
LDAP	
Host	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa LDAP.
Adres źródłowy	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelniania.
Bind DN	Miejsce w strukturze katalogowej, w której zawarte są definicje użytkowników uwierzytelnianych w usłudze LDAP. Np. `dc=example,dc=com`
Active Directory	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa AD.
Adres źródłowy	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelnienia.
Domena Active Directory	Domena, w oparciu o którą będzie wykonywane uwierzytelnienie w serwerze Active Directory.

Informacja: Etykietowane adresy IP

W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

6. Kliknij *Zapisz*.

Modyfikowanie definicji serwera zewnętrznego uwierzytelniania

Aby zmodyfikować serwer uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Zmień parametry konfiguracyjne żądanej definicji serwera.
3. Kliknij *Zapisz*.

Usuwanie definicji serwera zewnętrznego uwierzytelniania

Aby usunąć definicję serwera uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Zaznacz opcję *Usuń* przy żądanej definicji serwera uwierzytelniania.
3. Kliknij Zapisz.

Tematy pokrewne:

- *Metody uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

15.6 Zewnętrzne repozytoria haseł

Wheel Fudo PAM wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

15.6.1 CyberArk Enterprise Password Vault

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Z listy rozwijalnej *Typ* wybierz `CyberArk Enterprise Password Vault`.
4. Wprowadź nazwę obiektu.
5. W polu *URL*, wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

Przykład: `https://10.0.0.2/PWCWeb/`

---

6. Wprowadź identyfikator aplikacji.
7. Określ format konta.
8. Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.

2. Zmień parametry konfiguracyjne wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

Aby usunąć definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zaznacz opcję *Usuń* przy wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

15.6.2 Hitachi ID Privileged Access Manager

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Hitachi ID Privileged Access Manager`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

Przykład: `https://10.0.0.2/PWCWeb/`

---

7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.

Informacja: Konto użytkownika wskazane w konfiguracji musi być typu OTP (One Time Password).

---

8. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zmień parametry konfiguracyjne wybranej definicji repozytorium haseł.

3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

Aby usunąć definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zaznacz opcję *Usuń* przy wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

15.6.3 Lieberman Enterprise Random Password Manager

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Lieberman Enterprise Random Password Manager`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

Przykład: `https://10.0.0.2/PWCWeb/`

---

7. W polu *Uwierzytelnienie* określ moduł uwierzytelnienia przypisany do użytkownika uprawnionego do przeglądania zawartości repozytorium.
8. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
9. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
10. Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zmień parametry konfiguracyjne wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

Aby usunąć definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zaznacz opcję *Usuń* przy wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

15.6.4 Thycotic Secret Server

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Thycotic Secret Server`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

Przykład: `https://10.0.0.2/PWCWeb/`

---

7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
8. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. W polu *Format sekretu* wprowadź ciąg znaków definiujący format identyfikatorów obiektów w systemie Thycotic Secret Server.
10. Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zmień parametry konfiguracyjne wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

Aby usunąć definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zaznacz opcję *Usuń* przy wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

15.7 Zasoby

Wheel Fudo PAM pozwala na dostosowanie do własnych potrzeb ekranów logowania dla połączeń graficznych RDP i VNC.

Zmiana logo

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Kliknij *Wybierz Plik* i wskaż plik z nowym obrazem dla wybranego ekranu.

Informacja: Maksymalny rozmiar logo to 512 x 512 px.

4. Kliknij *Zapisz*.

Przywracanie domyślnego logo

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Zaznacz opcję *Przywróć domyślne*.
4. Kliknij *Zapisz*.

Definiowanie komunikatu globalnego

Komunikat globalny wyświetlany jest na ekranie logowania serwerów RDP i VNC.

Informacja: Oprócz komunikatu globalnego, możliwe jest zdefiniowanie komunikatu dla pojedynczego serwera w formularzu edycji obiektu.

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Uzpełnij treść w sekcji *Komunikat globalny*.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - RDP*

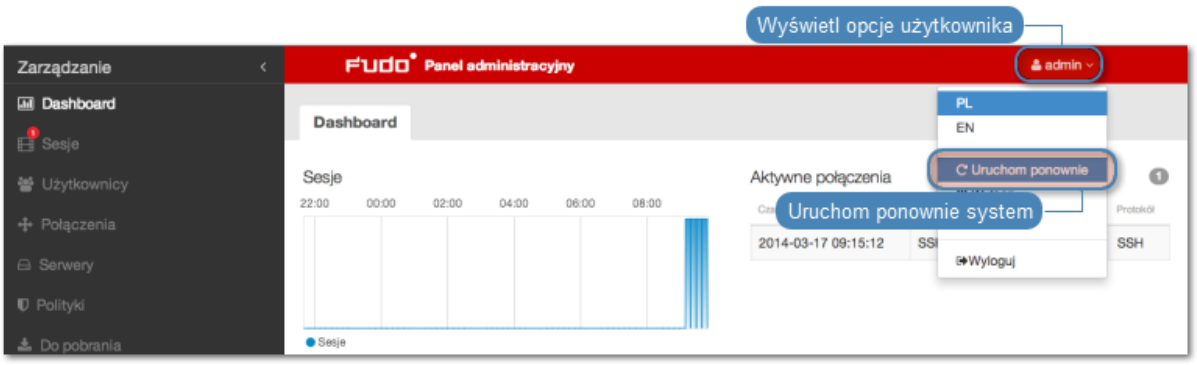
15.8 Przywracanie poprzedniej wersji systemu

W przypadku gdy wystąpił problem z bieżącą wersją oprogramowania, istnieje możliwość przywrócenia poprzedniej wersji oprogramowania.

Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. Dane sesji oraz zmiany w konfiguracji dokonane na nowej wersji systemu zostaną utracone.

Aby przywrócić poprzednią wersję systemu, postępuj zgodnie z poniższą instrukcją.

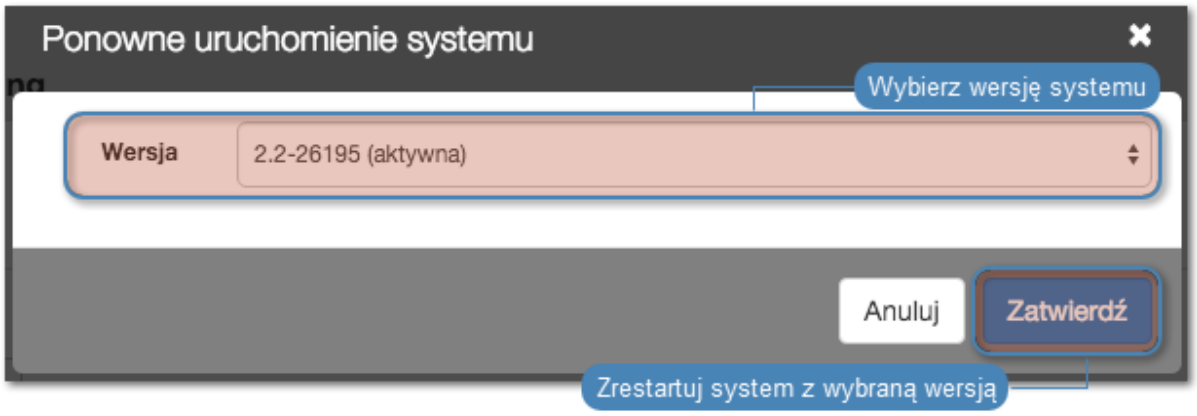
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



3. Wybierz wersję systemu, jaką chcesz załadować po zrestartowaniu urządzenia.

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

4. Kliknij *Zatwierdź*, aby potwierdzić operację ponownego uruchomienia, z wybraną wersją systemu.



Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Tematy pokrewne:

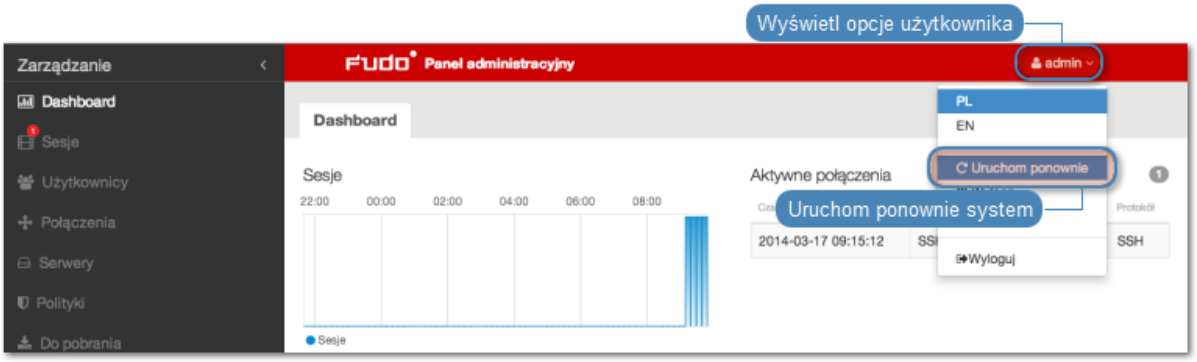
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

15.9 Ponowne uruchomienie systemu

Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Informacja: Skorzystaj z opcji *Blokowanie nowych połączeń* sekcji *Sesja* ustawień systemowych, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu.

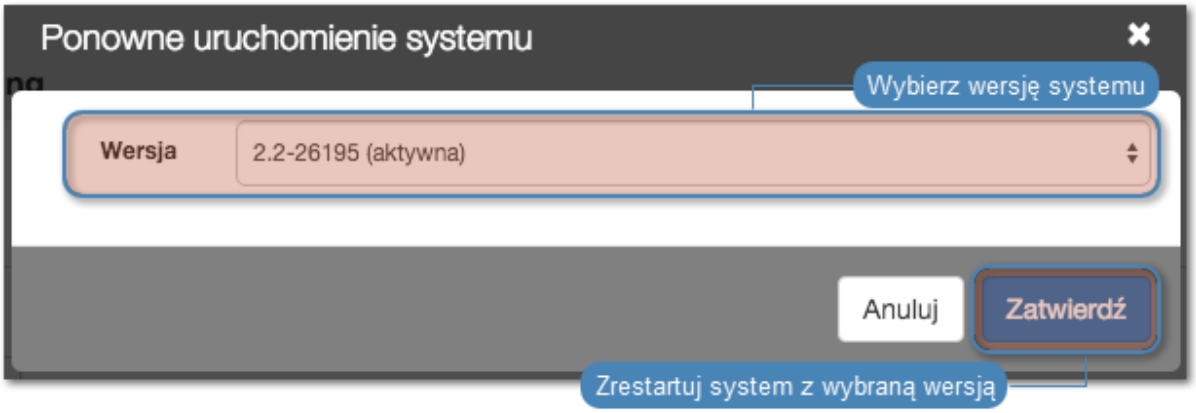
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



3. Wybierz wersję systemu, jaką chcesz załadować po zrestartowaniu urządzenia.

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

4. Kliknij *Zatwierdź*, aby potwierdzić operację ponownego uruchomienia, z wybraną wersją systemu.



Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Przywracanie poprzedniej wersji systemu*

15.10 SNMP

Wheel Fudo PAM wspiera funkcję monitorowania stanu systemu z wykorzystaniem protokołu SNMP.

Konfigurowanie SNMP

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *SNMPv3* zaznacz opcję *Włączone*.
3. Z listy rozwijalnej *Adres IP* wybierz adres IP, który będzie używany do komunikacji z innymi systemami poprzez protokół SNMP.
4. Kliknij *Zapisz*.
5. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
6. Kliknij + *Dodaj*.
7. Z listy rozwijalnej *Rola*, wybierz `service` i uzupełnij pozostałe parametry sekcji *Ogólne*.
8. W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `hasło` i wprowadź ciąg stanowiący hasło uwierzytelniające użytkownika technicznego.

Informacja:

- Ciąg definiujący hasło musi mieć co najmniej osiem znaków.
- Konto użytkownika serwisowego uwierzytelniane jest przez usługę SNMP pierwszym skonfigurowanym hasłem statycznym.

---

9. W sekcji *SNMP*, zaznacz opcję *Włączone*.
10. Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz metodę uwierzytelnienia.
11. Z listy rozwijalnej *Szyfrowanie*, wybierz algorytm szyfrujący komunikację SNMP.

12. Kliknij *Zapisz*.

SNMP MIBs

MIB wspierane przez Wheel Fudo PAM:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - częściowe wsparcie
- UCD-SNMP-MIB

15.10.1 Odczytywanie informacji SNMP poprzez `snmpwalk`

Informacja: Odczyt danych SNMP wymaga zainstalowania pakietu *Net-SNMP 5.7.3*.

Pobieranie wszystkich informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}" -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Pobieranie wybranych informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}" -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1.3.6.1.4.1.24410
```

Dane SNMP	Opis
.1.3.6.1.4.1.24410.1.1.1	Status dysków (status ZFS)
.1.3.6.1.4.1.24410.1.1.2	Stan zasilaczy **Informacja:** Ta funkcja nie jest wspierana przez wszystkie urządzenia Wheel Fudo PAM. Skontaktuj się z działem wsparcia technicznego Wheel Systems, aby uzyskać więcej informacji.
.1.3.6.1.4.1.24410.1.1.3	Temperatury procesora
.1.3.6.1.4.1.24410.1.1.4	Status S.M.A.R.T

15.10.2 Rozszerzenia SNMP Wheel Fudo PAM

Informacje ogólne

Rozszerzenia SNMP umożliwiają monitorowanie liczby sesji SNMP, status ZFS, status zasilaczy (jeśli jest dostępny), temperaturę rdzeni procesorów, status S.M.A.R.T dysków twardych (temperatura, realokacja sektorów, stan urządzeń).

Specyfikacja pliku MIB rozszerzeń SNMP

Poniższa definicja pliku MIB może zostać wczytana do managera SNMP w celu obsługi rozszerzeń specyficznych dla Wheel Fudo PAM.

```
WHEEL-SYSTEMS-MIB DEFINITIONS ::= BEGIN

--
-- MIB definition for Wheel Systems products
--

IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, Gauge32, Counter32, enterprises
                FROM SNMPv2-SMI;

wheel MODULE-IDENTITY
        LAST-UPDATED "201704240000Z"    -- 24 April 2017
        ORGANIZATION "www.wheelsystems.com"
        CONTACT-INFO
                 "Postal:   Wheel Systems Inc. (USA)
                                    31 N 2nd Street 370,
                                    San Jose, CA 95113
                  Phone:    +1 (415) 800 3230
                  email:    info@wheelsystems.com"
        DESCRIPTION
        "Top-level infrastructure of the Wheel Systems enterprise MIB tree"
        REVISION     "201704240000Z"
        DESCRIPTION
        "Moved common to .1, fudo to .2."
        REVISION     "201703270000Z"
        DESCRIPTION
        "Added objects for checking CPU temperature."
        REVISION     "201703150000Z"
        DESCRIPTION
        "Added objects describing status of power supply units."
        REVISION     "201703060000Z"
        DESCRIPTION
        "New objects to monitor disk status."
        REVISION     "201702140000Z"
        DESCRIPTION
        "First draft"
        ::= { enterprises 24410 }

products  OBJECT IDENTIFIER ::= { wheel 1 }

common OBJECT IDENTIFIER ::= { products 1 } -- Objects common to more than one␣
↪product.
fudo   OBJECT IDENTIFIER ::= { products 2 }

zpool OBJECT IDENTIFIER ::= { common 1 }

syncPercentage OBJECT-TYPE
        SYNTAX     Integer32 (0..100)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Percentage of vdev synchronization."
        ::= { zpool 1 }

syncTimeLeft OBJECT-TYPE
        SYNTAX     OCTET STRING
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Time left for synchronization or N/A if it cannot be determined."
        ::= { zpool 2 }

vdevTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF VdevEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of vdevs. The vdev is an element in ZFS pool"
        ::= { zpool 3 }

vdevEntry OBJECT-TYPE
        SYNTAX      VdevEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry for one vdev status in ZFS pool."
        INDEX { vdevIndex }
        ::= { vdevTable 1 }

VdevEntry ::= SEQUENCE {
        vdevIndex         Integer32,
        vdevStatus        OCTET STRING
}

vdevIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique value for each vdev in ZFS pool."
        ::= { vdevEntry 1 }

vdevStatus OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Status of the vdev in ZFS pool."
        ::= { vdevEntry 2 }

powerSupply OBJECT IDENTIFIER ::= { common 2 }

powerSupplyTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF PowerSupplyEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of power supply units status, such as which unit is
                 operating."
        ::= { powerSupply 1 }

powerSupplyEntry OBJECT-TYPE
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        SYNTAX      PowerSupplyEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in power supply table representing the status of the
                 associated power supply unit."
        INDEX { powerSupplyIndex }
        ::= { powerSupplyTable 1 }

PowerSupplyEntry ::= SEQUENCE {
        powerSupplyIndex   Integer32,
        powerSupplyStatus  INTEGER
}

powerSupplyIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each power supply unit."
        ::= { powerSupplyEntry 1 }

powerSupplyStatus OBJECT-TYPE
        SYNTAX     INTEGER {
                unknown(1),
                present(2),
                absent(3),
                configError(4),
                acLost(5),
                predictiveFailure(6),
                failed(7)
        }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The status of power supply unit. When everything is working, reported
                 status should be present(1). This information is gathered from IPMI
                 subsystem."
        ::= { powerSupplyEntry 2 }

cpu OBJECT IDENTIFIER ::= { common 3 }

cpuTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF CpuEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of CPUs statuses."
        ::= { cpu 1 }

cpuEntry OBJECT-TYPE
        SYNTAX      CpuEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in CPU table representing the status of the associated CPU."
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        INDEX { cpuIndex }
        ::= { cpuTable 1 }

CpuEntry ::= SEQUENCE {
        cpuIndex       Integer32,
        cpuTemperature Gauge32
}

cpuIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each CPU."
        ::= { cpuEntry 1 }

cpuTemperature OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The temperature of CPU in degree Celsius."
        ::= { cpuEntry 2 }

smart OBJECT IDENTIFIER ::= { common 4 }

smartTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF SmartEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table contains devices with enabled SMART and their statuses.␣
↪Note
                that interpretation all elements reported in this table are hard disk
                manufacturer dependent. Values are reported as raw value or as
                (normalized value - threshold). The lower is value of
                (normalized value - threshold) the worst. Keep in mind that every
                manufacturer uses their own algorithms for calculating 'normalized
                value'."
        ::= { smart 1 }

smartEntry OBJECT-TYPE
        SYNTAX      SmartEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry in SMART table representing the status of the associated
                device."
        INDEX { smartIndex }
        ::= { smartTable 1 }

SmartEntry ::= SEQUENCE {
        smartIndex              Integer32,
        smartModelFamily        OCTET STRING,
        smartDeviceModel        OCTET STRING,
        smartSerialNumber       OCTET STRING,
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        smartHealth             INTEGER,
        smartTemperature        Gauge32,
        smartReallocatedSectors Gauge32,
        smartPendingSectors     Gauge32,
        smartUncorrectable      Gauge32,
        smartUdmaCrcErrors      Gauge32,
        smartReadErrorRate      Gauge32,
        smartSeekErrorRate      Gauge32
}

smartIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique index for each SMART-enabled device."
        ::= { smartEntry 1 }

smartModelFamily OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Model family of device."
        ::= { smartEntry 2 }

smartDeviceModel OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Device model."
        ::= { smartEntry 3 }

smartSerialNumber OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Serial number of the device."
        ::= { smartEntry 4 }

smartHealth OBJECT-TYPE
        SYNTAX     INTEGER {
                unknown(1),
                ok(2),
                failed(3)
        }
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "Health of the device as reported by SMART system."
        ::= { smartEntry 5 }

smartTemperature OBJECT-TYPE
        SYNTAX     Gauge32
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The temperature of disk in degree Celsius."
        ::= { smartEntry 6 }

smartReallocatedSectors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of reallocated sectors: bad sectors found and then␣
↪remapped.
                Reported as raw value of 'Reallocated Sectors Count' SMART attribute."
        ::= { smartEntry 7 }

smartPendingSectors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of sectors waiting to be remapped. Reported as raw value␣
↪of
                'Current Pending Sector Count' SMART attribute."
        ::= { smartEntry 8 }

smartUncorrectable OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of uncorrectable errors when accessing sectors. Reported␣
↪as
                raw value of 'Offline Uncorrectable Sector Count' SMART attribute."
        ::= { smartEntry 9 }

smartUdmaCrcErrors OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The number of errors in data transfer determined by the means of␣
↪ICRC.
                Reported as raw value of 'UltraDMA CRC Error Count' SMART attribute."
        ::= { smartEntry 10 }

smartReadErrorRate OBJECT-TYPE
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The rate of hardware read errors. Reported as
                (normalized value - threshold) of 'Read Error Rate' SMART attribute."
        ::= { smartEntry 11 }

smartSeekErrorRate OBJECT-TYPE
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        SYNTAX     Gauge32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "The rate of seek errors. Reported as (normalized value - threshold)␣
↪of
                'Seek Error Rate'."
        ::= { smartEntry 12 }

sessionTable OBJECT-TYPE
        SYNTAX      SEQUENCE OF SessionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "The table of active sessions on Fudo."
        ::= { fudo 1 }

sessionEntry OBJECT-TYPE
        SYNTAX      SessionEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
                "An entry for one session type on Fudo. For example, information about
                active RDP sessions."
        INDEX { sessionIndex }
        ::= { sessionTable 1 }

SessionEntry ::= SEQUENCE {
        sessionIndex         Integer32,
        sessionName          OCTET STRING,
        sessionDescription   OCTET STRING,
        sessionActive        Counter32
}

sessionIndex OBJECT-TYPE
        SYNTAX     Integer32 (1..2147483647)
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A unique value for each supported sessions on Fudo."
        ::= { sessionEntry 1 }

sessionName OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A name of session type."
        ::= { sessionEntry 2 }

sessionDescription OBJECT-TYPE
        SYNTAX     OCTET STRING
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A description of session type."
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        ::= { sessionEntry 3 }

sessionActive OBJECT-TYPE
        SYNTAX     Counter32
        MAX-ACCESS read-only
        STATUS     current
        DESCRIPTION
                "A number of active sessions of this type."
        ::= { sessionEntry 4 }

END
```

Tematy pokrewne:

- *Bezpieczeństwo*
- *Rozwiązywanie problemów*

15.11 Kopie zapasowe i retencja

Retencja danych

Wheel Fudo PAM implementuje dwuetapowy mechanizm retencji danych. W pierwszym etapie, dane sesji przenoszone zostają na zewnętrzną macierz dyskową a po upływie zdefiniowanego przedziału czasowego zostają całkowicie usunięte. Więcej na temat konfigurowania zewnętrznej macierzy znajdziesz w rozdziale *Zewnętrzna macierz dyskowa*.

Aby włączyć retencję danych, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja*.
2. W sekcji *Retencja danych*, zaznacz opcję *Przenoszenie danych na zewnętrzną macierz włączone*, aby dane starsze niż zdefiniowana wartość, były automatycznie przenoszone na zewnętrzną macierz dyskową.
3. Wprowadź wartość w polu *Przenieś dane na zewnętrzną macierz po upływie*, aby określić po jakim czasie dane sesji zostaną przeniesione na zewnętrzną macierz dyskową.
4. Zaznacz opcję *Usuwanie danych sesji włączone*, aby dane sesji starsze niż zdefiniowana wartość były bezpowrotnie usuwane.
5. Wprowadź wartość w polu *Usuń dane sesji po upływie*, aby określić czas przechowywania danych sesji.

Informacja: Globalne wartości parametru retencji danych mają niższy priorytet niż wartość retencji zdefiniowana w *koncie*.

---

6. Kliknij *Zapisz*.

Kopia zapasowa systemu

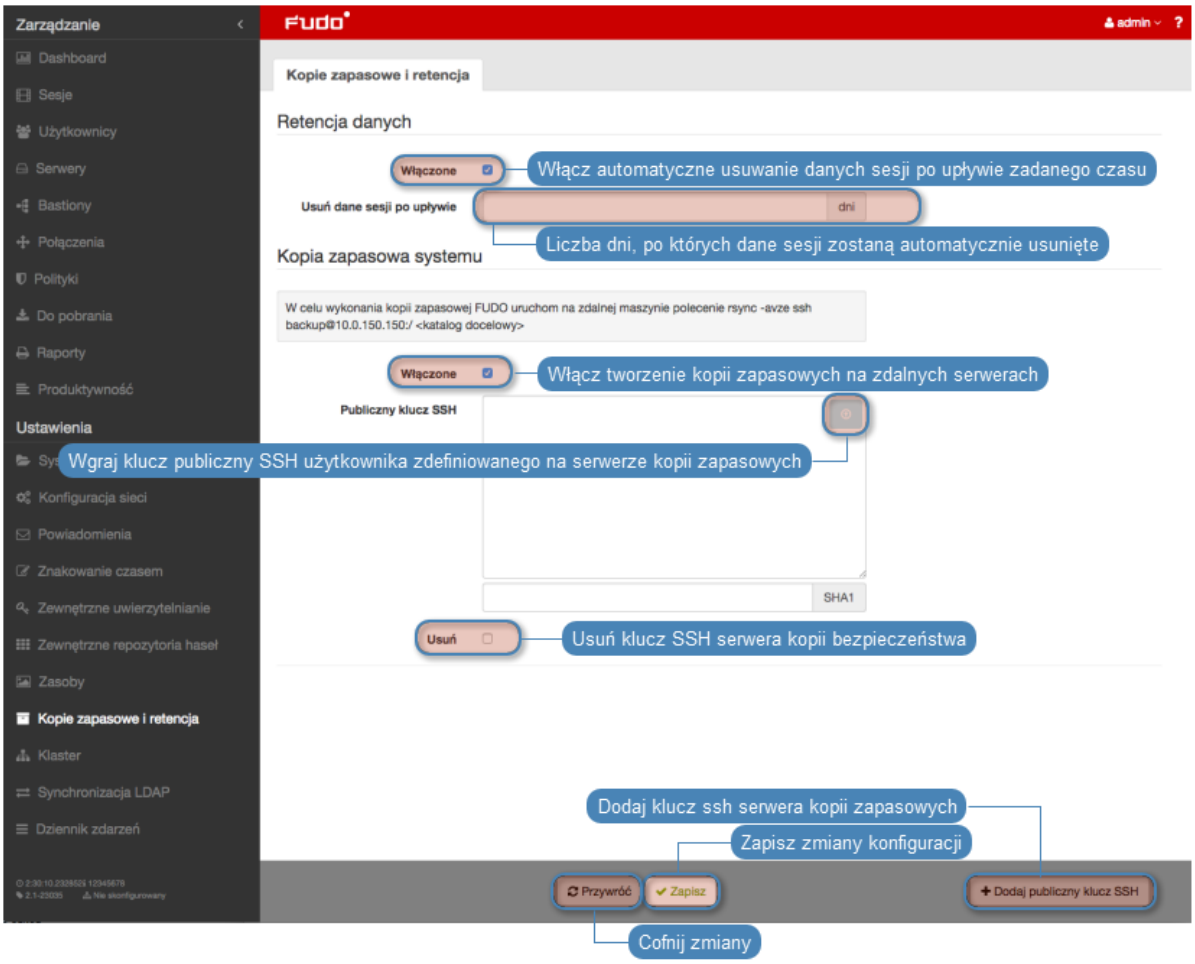
Ostrzeżenie: Kopia zapasowa systemu zawiera poufne informacje.

Automatyczne tworzenie kopii zapasowych danych przechowywanych na Wheel Fudo PAM wymaga skonfigurowania usługi `rsync` na zdalnym serwerze kopii zapasowych i przyznania prawa dostępu do danych przechowywanych na Wheel Fudo PAM, poprzez wgranie klucza publicznego serwera.

Informacja: Dane sesji przechowywane są w systemie plików z domyślnie włączoną kompresją o współczynniku sięgającym 12:1. Podczas kopiowania, dane podlegają dekompresji, stąd na serwerze kopii bezpieczeństwa mogą zajmować więcej miejsca niż wskazuje zajętość macierzy dyskowej Wheel Fudo PAM. Upewnij się, że serwer docelowy dysponuje odpowiednio dużą przestrzenią dyskową zdolną do przechowywania zdekompresowanych danych.

Aby włączyć usługę tworzenia kopii zapasowych, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja*.
2. W sekcji *Kopia zapasowa systemu*, zaznacz opcję *Włączone*.
3. Kliknij *Dodaj publiczny klucz SSH*.
4. Wprowadź lub wgraj klucz publiczny SSH użytkownika zdefiniowanego na serwerze kopii bezpieczeństwa.
5. Kliknij *Zapisz*.
6. Wykonaj na zdalnej maszynie polecenie: `rsync -avze ssh backup@adres_ip_fudo:/<katalog docelowy>`.



Odtwarzanie stanu systemu z kopii bezpieczeństwa

Usługa odtworzenia stanu systemu z kopii bezpieczeństwa świadczona jest przez dział wsparcia technicznego firmy Wheel Systems, na zasadach określonych w SLA.

Tematy pokrewne:

- *Mechanizmy bezpieczeństwa*
- *Eksportowanie/importowanie konfiguracji systemu*

15.12 Zewnętrzna macierz dyskowa

Wheel Fudo PAM umożliwia retencjonowanie danych sesji na zewnętrznej macierzy dyskowej.

Informacja: Zewnętrzna macierz dyskowa w konfiguracji klastrowej

- W konfiguracji klastrowej, każdy z węzłów musi mieć skonfigurowany własny obiekt *WWN*.
- Dane przechowywane na zewnętrznej macierzy dyskowej nie są replikowane pomiędzy węzłami klastra.

15.12.1 Konfigurowanie zewnętrznej macierzy dyskowej

Aby skonfigurować zewnętrzną macierz dyskową, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzna macierz dysków*.

Informacja: Status kart fiber channel przedstawiają ikony:

- - obie karty fiber channel pracują prawidłowo.
- - połączenie z macierzą dyskową jest zdegradowane - jedna z kart fiber channel nie działa prawidłowo.
- - obie karty fiber channel nie funkcjonują prawidłowo.

---

2. Z listy rozwijalnej «Tryb połączenia», wybierz tryb pracy kart Fiber Channel.
   - Failover - transmisja danych odbywa się przez jedną kartę fiber channel. Gdy ta ulegnie awarii, dane przesyłane są przez drugą kartę, co pozwala zachować ciągłość dostępu do zewnętrznej macierzy.
   - Load balancing - transmisja danych odbywa się z wykorzystaniem obu interfejsów fiber channel.
3. W sekcji *Zewnętrzne urządzenia przechowywania danych* wybierz WWN i kliknij ikonę .

Informacja: Kliknij ikonę , aby odświeżyć listę dostępnych obiektów WWN.

---

4. Kliknij *Zapisz* i przejdź do konfigurowania *retencji danych*.

15.12.2 Rozszerzanie zewnętrznej macierzy dyskowej

Po zmianie rozmiaru obiektu WWN, należy rozszerzyć dostępną powierzchnię przechowywania w panelu administracyjnym Wheel Fudo PAM.

Ostrzeżenie: Po powiększeniu przestrzeni przechowywania na zewnętrznej macierzy dyskowej nie jest możliwe jej pomniejszenie.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzna macierz dysków*.
2. W sekcji opisującej parametry zewnętrznego obiektu WWN, kliknij *Rozszerz*.
3. Potwierdź operację powiększenia przestrzeni przechowywania.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Kopie zapasowe i retencja*

15.13 Eksportowanie/importowanie konfiguracji systemu

Wheel Fudo PAM pozwala eksportować aktualny stan systemu, zdefiniowane obiekty jak i ustawienia konfiguracyjne, które później mogą zostać użyte do ponownego zainicjowania maszyny.

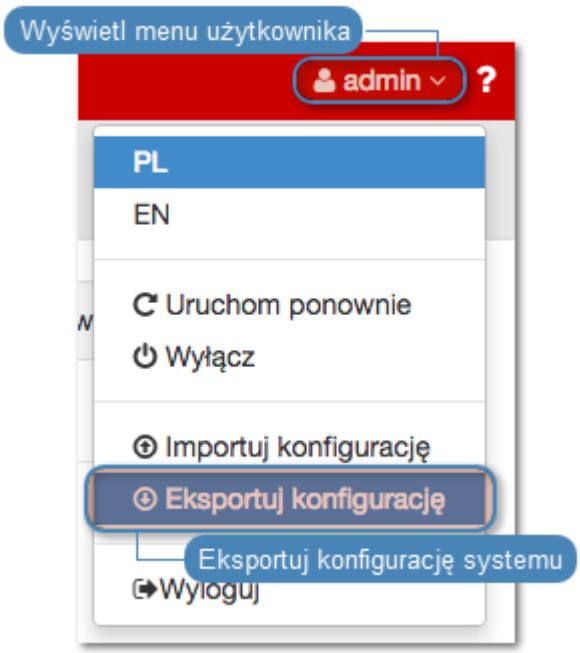
Ostrzeżenie: Wyeksportowana konfiguracja zawiera poufne informacje.

Informacja: Opcje importowania i eksportowania konfiguracji dostępne są dla użytkowników o przypisanej roli *superadmin*.

15.13.1 Eksportowanie konfiguracji

Aby wyeksportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z menu użytkownika opcję *Eksportuj konfigurację*.
2. Zapisz plik konfiguracji.

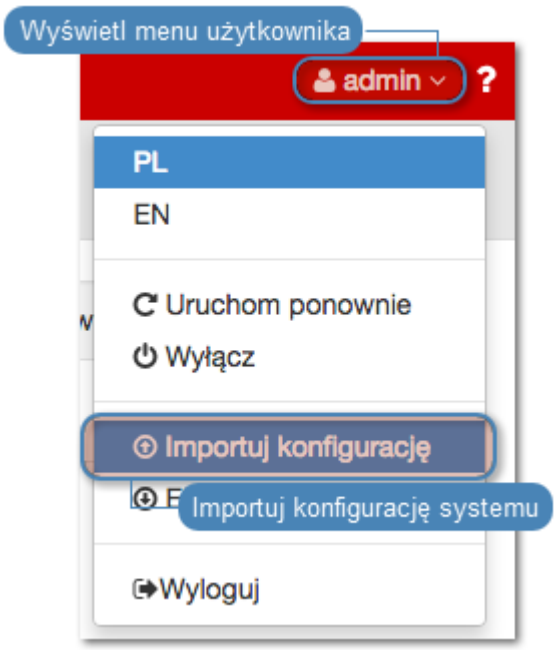


15.13.2 Importowanie konfiguracji

Ostrzeżenie: Zainicjowanie systemu wcześniej zapisaną konfiguracją spowoduje utratę wszystkich danych sesji.

Aby zaimportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z menu użytkownika opcję *Importuj konfigurację*.



2. Wskaż plik konfiguracji i kliknij *Zatwierdź*.
3. Zatwierdź zainicjowanie systemu danymi z pliku.

Tematy pokrewne:

- *Kopie zapasowe i retencja*
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

15.14 Konfiguracja klastrowa

Klaster Wheel Fudo PAM zapewnia nieprzerwany dostęp do serwerów, w przypadku awarii jednego z węzłów systemu, a także pozwala na implementację scenariuszy statycznego balansowania obciążeniem zapytaniami użytkowników.

Ostrzeżenie:

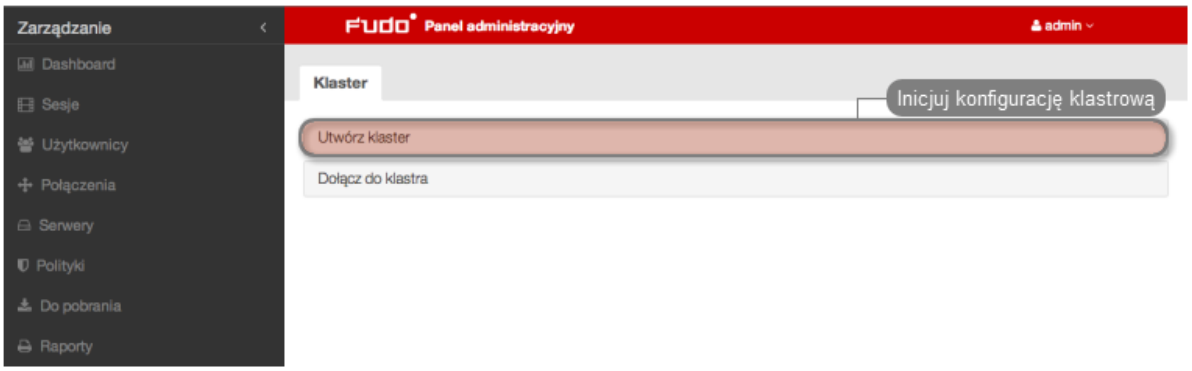
- Konfiguracja klastrowa nie jest mechanizmem tworzenia kopii zapasowych danych. Dane sesji usunięte z jednego węzła, zostaną również usunięte z pozostałych węzłów klastra.
- Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

15.14.1 Inicjowanie klastra

Ostrzeżenie: Prawidłowe funkcjonowanie klastra wymaga skonfigurowania *serwera czasu NTP* na wszystkich węzłach klastra.

Aby zainicjować klaster Wheel Fudo PAM postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Wybierz opcję *Utwórz klaster*, aby wyświetlić parametry inicjowania klastra.



3. Wprowadź nazwę węzła oraz opis ułatwiający identyfikację obiektu.
4. Z listy rozwijalnej *Adres* wybierz adres IP do komunikacji z innymi węzłami klastra.

5. Kliknij *Zatwierdź*, aby zainicjować klaster.

Informacja: Komunikat o konieczności skopiowania klucza może zostać pominięty przy inicjacji klastra.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Grupy redundancji*
- *Konfiguracja klastrowa*

15.14.2 Zarządzanie węzłami klastra

15.14.2.1 Dodawanie węzłów klastra

Ostrzeżenie:

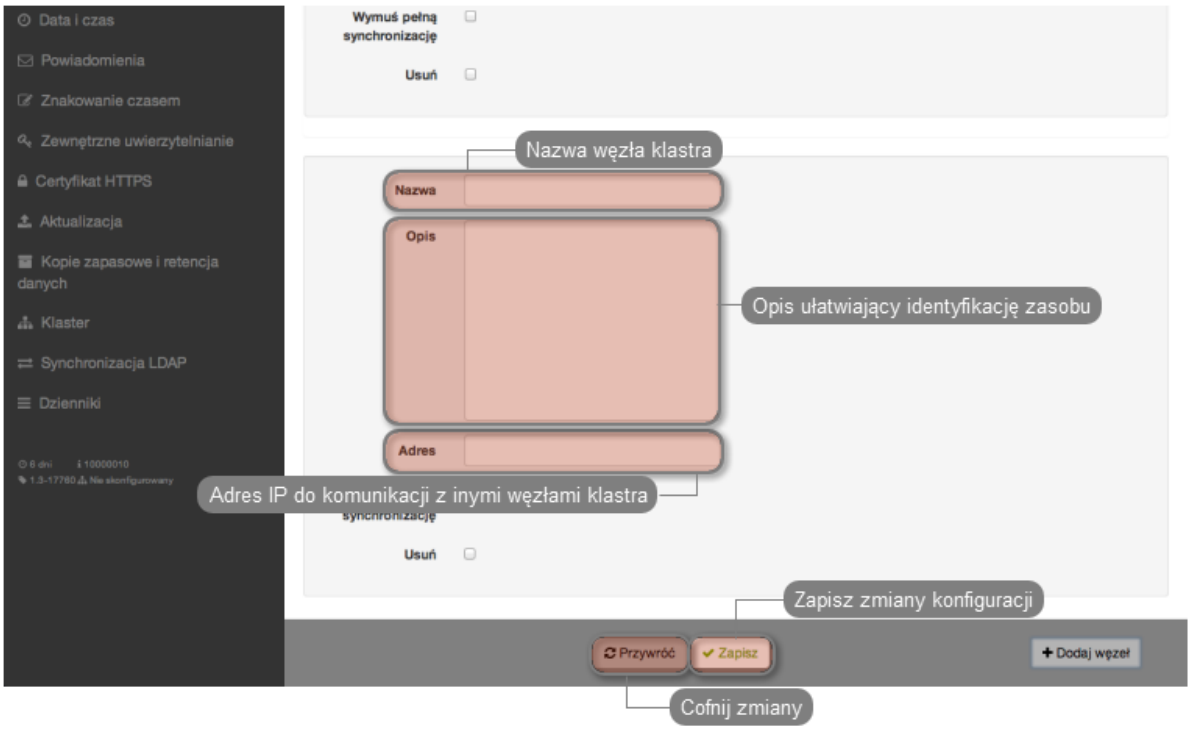
- Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.
- Dane sesji oraz parametry konfiguracyjne (*serwery*, *użytkownicy*, *konta*, *sejfy*, *gniazda nasłuchiwania*, *zewnętrzne serwery uwierzytelniania*) węzła dołączanego są usuwane i inicjowane na nowo danymi zreplikowanymi z klastra.

Aby dodać węzeł do klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM, na którym został *zainicjowany klaster*.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Kliknij *Dodaj węzeł*.

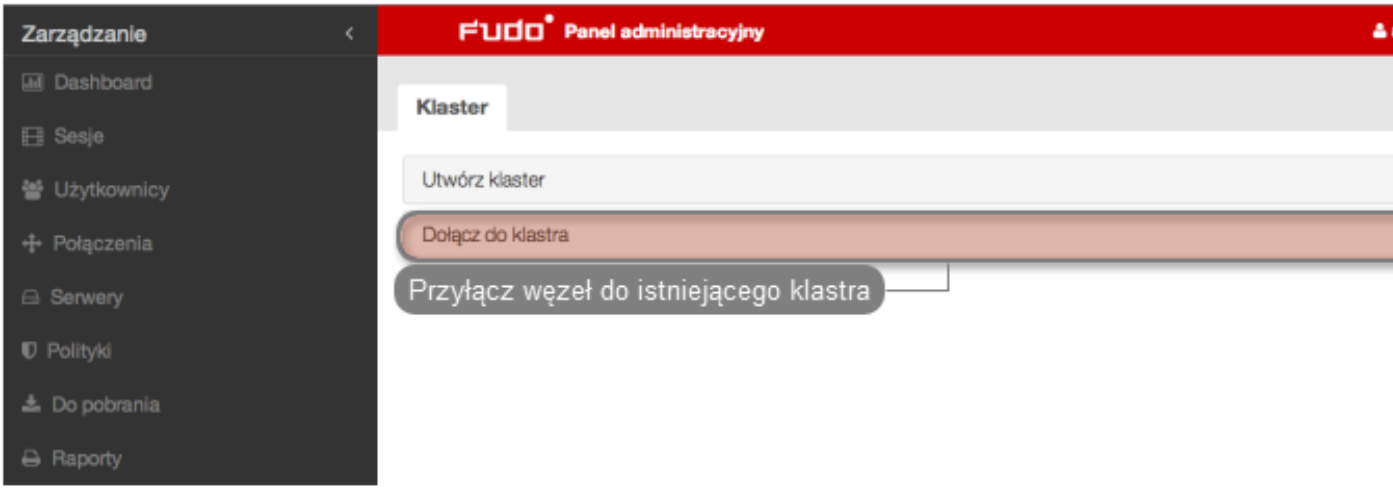
4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację obiektu.
5. Podaj adres IP węzła dołączanego.

Informacja: Na wskazanym interfejsie sieciowym dołączanego węzła musi być aktywna opcja zarządzania urządzeniem. Informacje na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.



6. Kliknij *Zapisz*, aby dodać definicję węzła i wygenerować klucz publiczny SSH.

7. Skopiuj wygenerowany klucz.
8. Zaloguj się do panelu administracyjnego węzła dołączanego.
9. Wybierz z lewego menu *Ustawienia* > *Klaster*.
10. Wybierz opcję *Dołącz do klastra*.

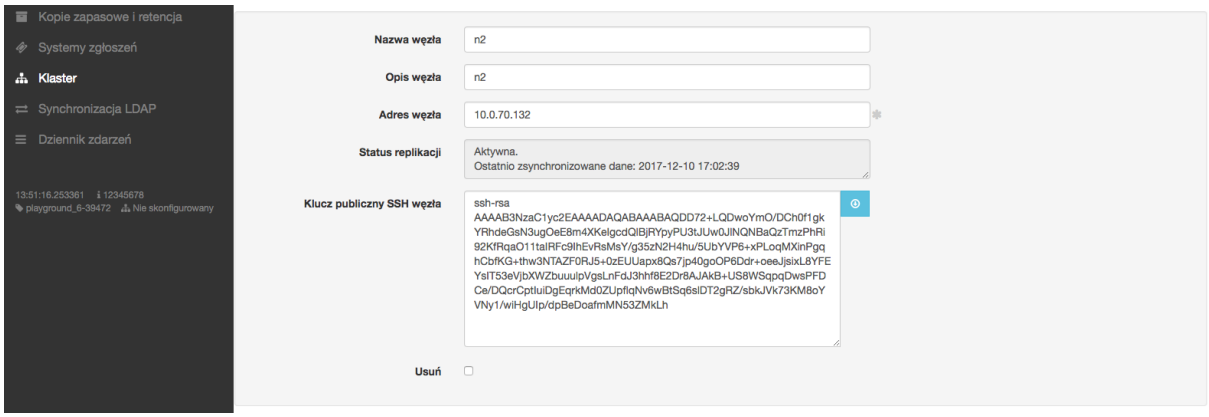


11. Wklej wygenerowany wcześniej klucz i kliknij *Zatwierdź*.

12. Kliknij przycisk *Rozumiem konsekwencje, kontynuuj.*

Informacja: Stan replikacji danych sesji oraz obiektów odczytasz z widoku głównego panelu administracyjnego Fudo lub menu konfiguracji klastra.

- *Dane sesji* - określa z którego dnia i godziny dane sesji zostały zreplikowane ze wskazanego węzła.
- *Obiekty* - wskazuje z którego dnia i godziny zostały zreplikowane obiekty modelu danych.



Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

15.14.2.2 Edytowanie węzłów klastra

Aby zmodyfikować konfigurację węzła klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Znajdź i zmodyfikuj dane żądanego węzła.
3. Kliknij *Zapisz*.

Tematy pokrewne:

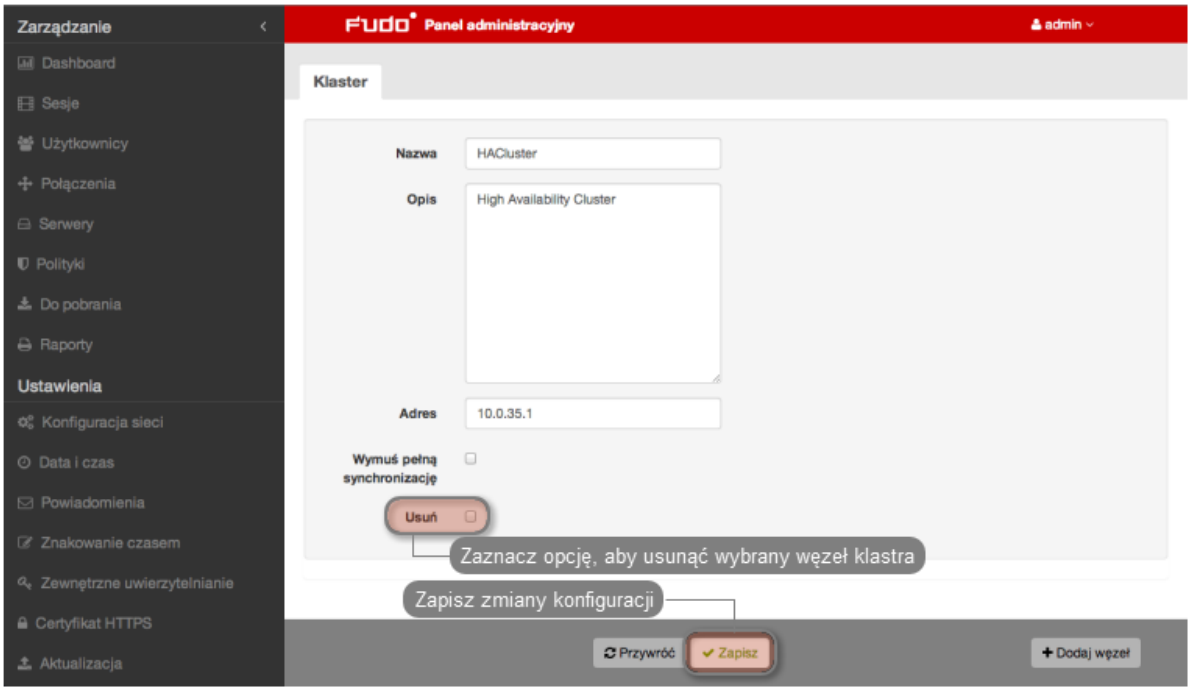
- *Dodawanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

15.14.2.3 Usuwanie węzłów klastra

Ostrzeżenie: Odłączenie węzła od klastra i ponowne jego przyłączenie może skutkować utratą danych.

Aby usunąć węzeł klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Zaznaczy opcję *Usuń* przy wybranym węźle klastra i kliknij *Zapisz*.



Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

15.14.3 Grupy redundancji

Grupy redundancji agregują adresy IP przypisane do interfejsów sieciowych. Nadanie różnym grupom odpowiednich priorytetów na poszczególnych węzłach klastra pozwala na statyczne balansowanie obciążeniem węzłów przy zachowaniu funkcjonalności klastra niezawodnościowego.

Informacja: Opcje konfigurowania grup redundancji dostępne są po zainicjowaniu klastra.

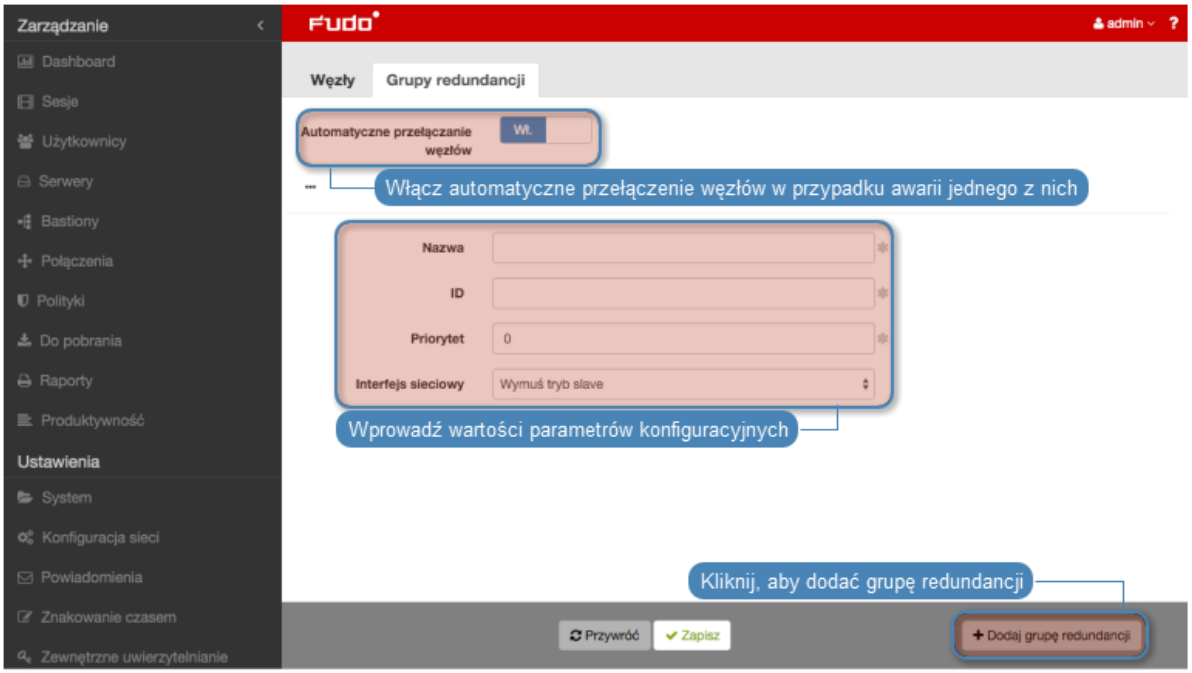
Dodawanie grup redundancji

Aby dodać grupę redundancji, postępuj zgodnie z poniższą instrukcją.

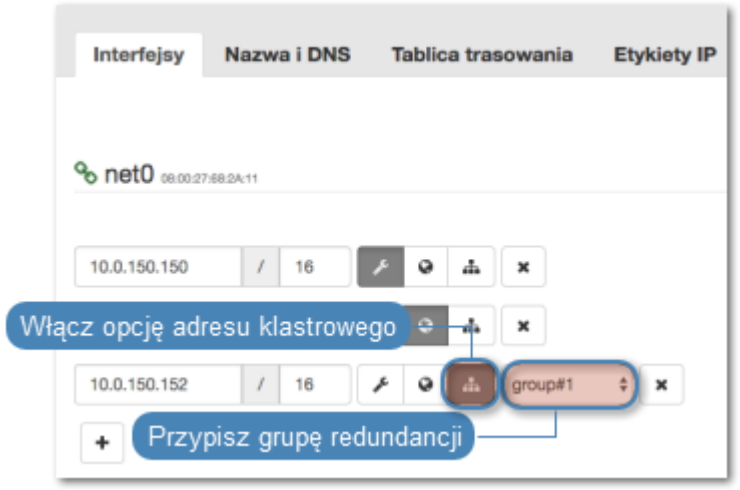
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.

2. Przejdź do zakładki *Grupy redundancji*.
3. Kliknij *+ Dodaj grupę redundancji*.
4. Zdefiniuj parametry grupy.

Parametr	Opis
Nazwa	Nazwa grupy redundancji.
ID	Identyfikator grupy redundancji (1-255).
Priorytet	Priorytet grupy redundancji (0-254), mniejsza wartość parametru oznacza wyższy priorytet.
	Grupa redundancji o wyższym priorytecie przyjmuje rolę *master* i obsługuje żądania dostępu do serwerów o adresach IP przypisanych do grupy. W przypadku awarii takiego węzła, zapytania kierowane są do węzła o najwyższym priorytecie wśród pozostałych.
Interfejs sieciowy	Interfejs sieciowy używany przez grupę redundancji do komunikacji z pozostałymi węzłami klastra.



5. Kliknij *Zapisz*.
6. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
7. Kliknij [+], aby dodać adres IP.
8. Wprowadź adres IP i kliknij [⚙], aby nadać mu atrybut klastrowy.
9. Z listy rozwijalnej wybierz wcześniej zdefiniowaną grupę redundancji.
10. Kliknij *Zapisz*.

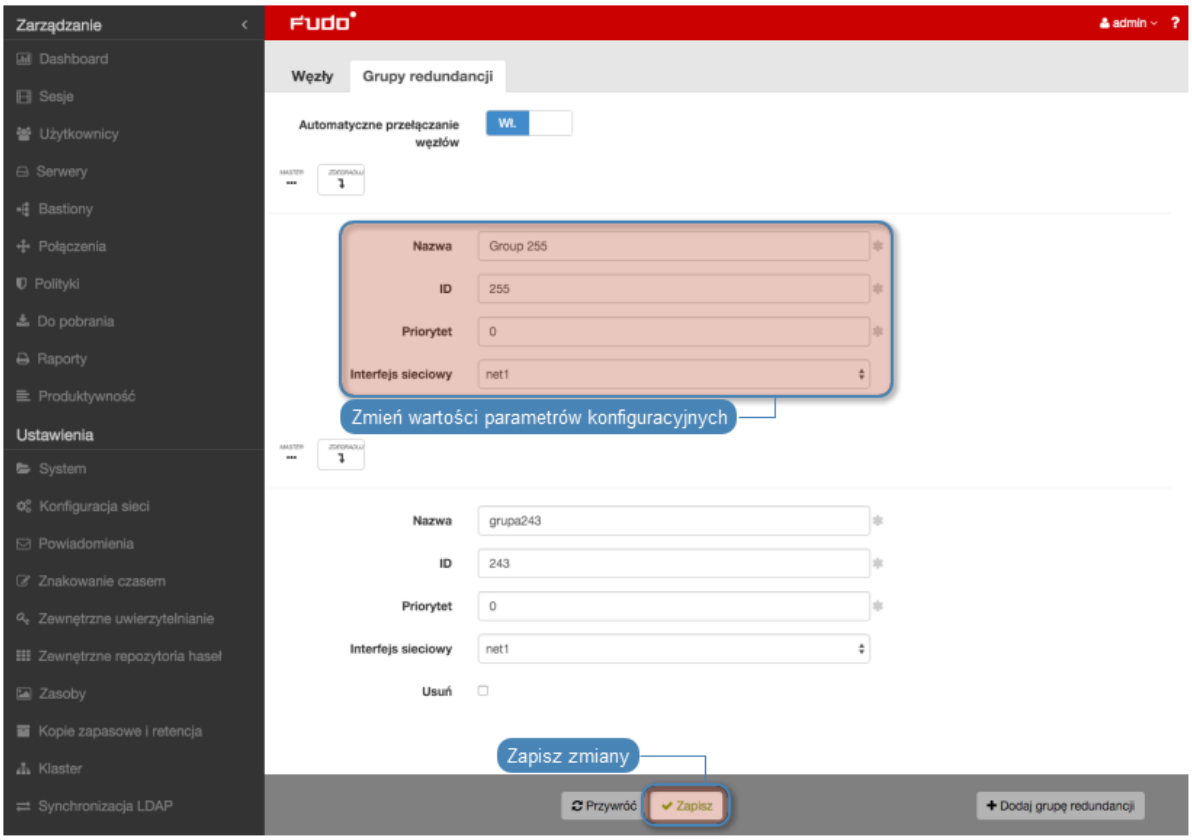


Informacja: Klastrowy adres IP należy zdefiniować na każdym z węzłów klastra.

Edytowanie grup redundancji

Aby zmodyfikować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

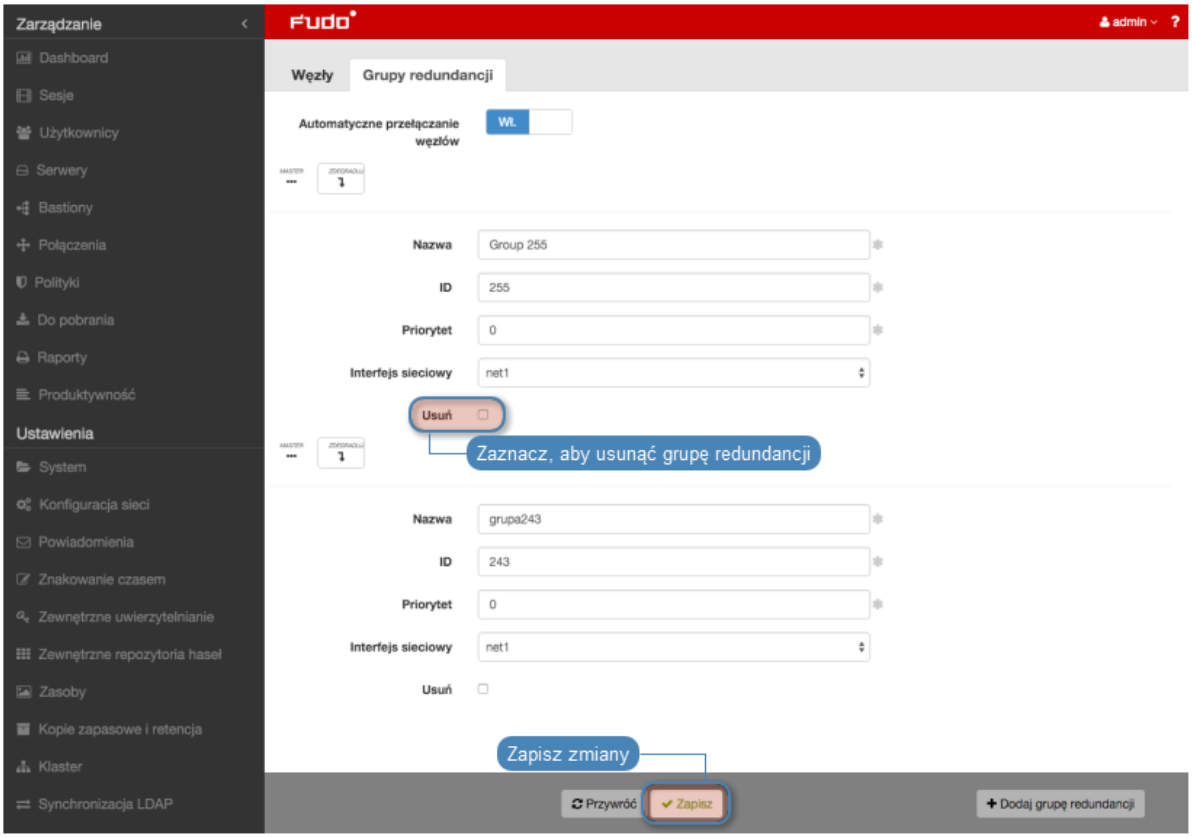
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zmień parametry wybranej grupy redundancji.
4. Kliknij *Zapisz*.



Usuwanie grup redundancji

Aby usunąć grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zaznacz opcję *Usuń* przy wybranej grupie redundancji.
4. Kliknij *Zapisz*.

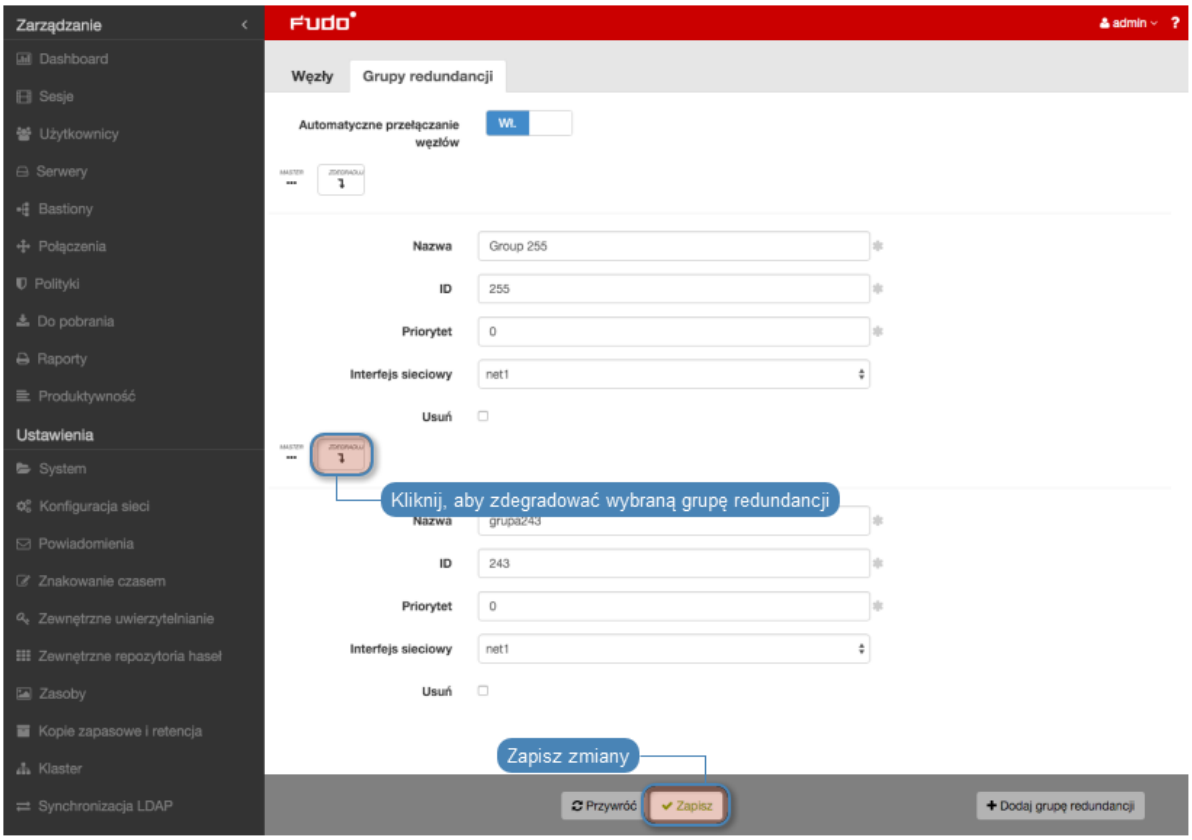


Degradowanie grupy redundancji

Informacja: Degradowanie grupy służy przełączeniu roli nadrzędnej dla danej grupy redundancji na inny węzeł klastra. Rolę nadrzędną dla grupy przejmie węzeł, na którym wybrana grupa redundancji ma najwyższy priorytet.

Aby zdegradować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Kliknij *Degraduj* przy wybranej grupie redundancji.
4. Kliknij *Zatwierdź*.



Informacja: Jeśli po zdegradowaniu grupy żaden z pozostałych węzłów nie przejmie dla niej roli nadrzędnej, ta zostanie przywrócona grupie redundancji na edytowanym węźle.

Wymuszanie roli podrzędnej

Informacja: Wymuszenie roli podrzędnej spowoduje, że grupa redundancji nigdy nie przejdzie w tryb nadrzędny, niezależnie od stanu pozostałych węzłów klastra. Wymuszanie roli podrzędnej zalecane jest przed wykonywaniem prac serwisowych, aby ruch sieciowy kierowany był do pozostałych węzłów klastra.

Aby wymusić rolę podrzędną wybranej grupy redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Odszukaj grupę redundancji i z listy rozwijalnej *Interfejs* wybierz `Wymuś tryb slave`.
4. Kliknij *Zapisz*.

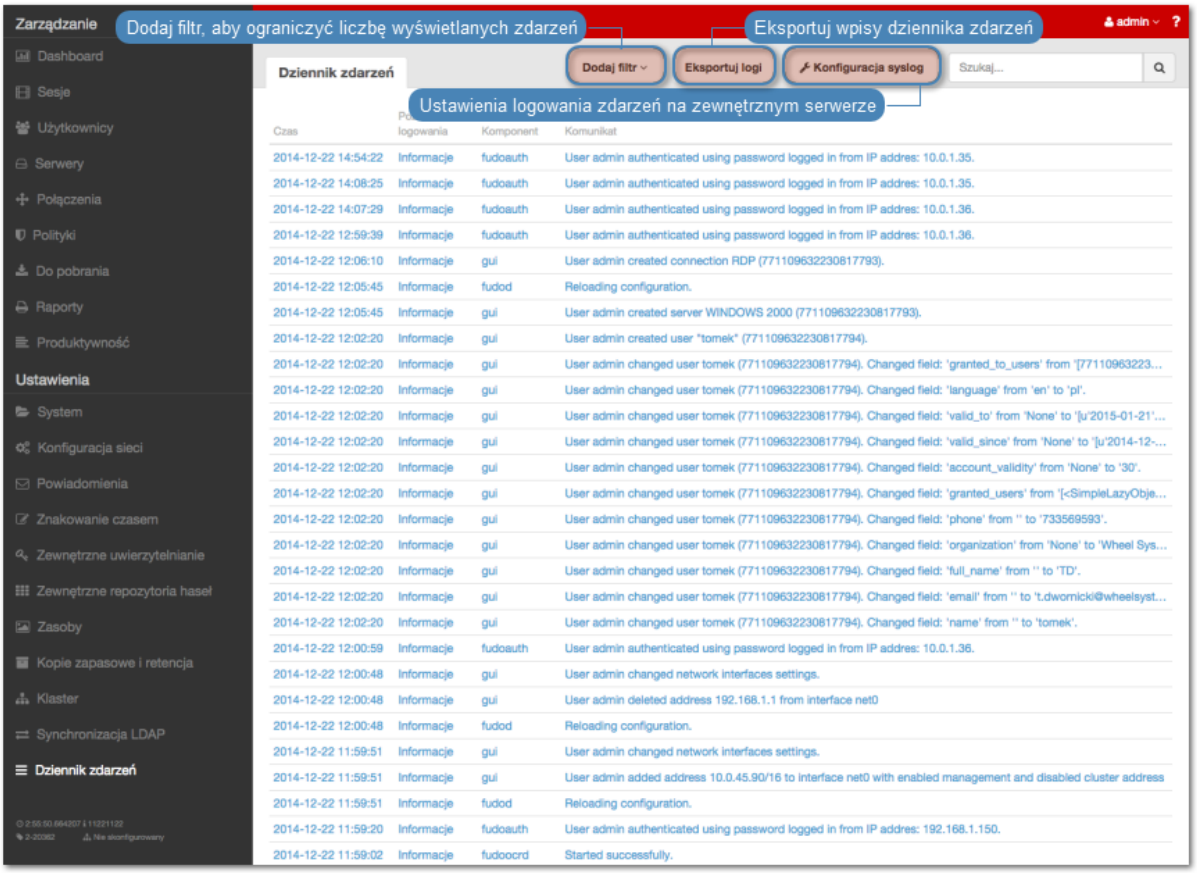
Tematy pokrewne:

- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Inicjowanie klastra*
- *Konfiguracja klastrowa*

15.15 Dziennik zdarzeń

Dziennik zdarzeń stanowi wewnętrzny zapis akcji użytkowników mających wpływ na stan systemu (logowanie użytkowników, czynności administracyjne, itp.).

W celu wyświetlenia listy zdarzeń, wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.



Zewnętrzne serwery syslog

Wheel Fudo PAM pozwala na przesyłanie rejestrowanych zdarzeń do zewnętrznych serwerów syslog.

Dodawanie serwera Syslog

Aby skonfigurować usługę rejestrowania zdarzeń na zewnętrznych serwerach *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić opcje konfiguracji rejestrowania zdarzeń na serwerach syslog.
3. Zaznacz opcję *Włącz logowanie zdarzeń na serwerach syslog*.
4. Kliknij *+*.
5. Wprowadź adres IP oraz numer portu serwera syslog.
6. Kliknij *Zapisz*.

Informacja: Wpisy dziennika zdarzeń przesyłane do serwerów syslog, przyjmują następującą

postać:

```
[<poziom_logowania>] (<nazwa_komponentu>) (nazwa_obiektu: id_obiektu)
<treść_komunikatu>
```

Na przykład:

```
[INFO] (fudordp) (fudo_server: 848388532111147015) (fudo_session:
848388532111147219) (fudo_user: 848388532111147012) (fudo_connection:
848388532111147014) User user0 authenticated using password logged in from IP
addres: 10.0.40.101.
```

Lista komponentów

Komponent
cfuploadcert
cluster
confapply
confget
confimport
confset
datasendd
dbconfd
dbrecvd
dbsendd
eventd
fudoauth
fudod
fudodump
fudogeneric
fudohttp
fudomail
fudomysql
fudoocrd
fudooracle
fudordp
fudoretention
fudossh
fudossl
fudotelnet
fudotn3270
fudovnc
license
notify
pmonitor
timestampd
upgrade

Lista obiektów

Obiekt
fudo_configuration
fudo_connection
fudo_connection_attribute
fudo_connection_grant
fudo_connection_network
fudo_erpm
fudo_external_authentication
fudo_http_request
fudo_ldap_address
fudo_ldap_connection
fudo_ldap_server
fudo_ldap_server_external_authentication_method
fudo_log_entry
fudo_log_object
fudo_node
fudo_node_replication
fudo_notification_filter
fudo_policy
fudo_regexp
fudo_regexp_policy
fudo_sensitive_feature_user
fudo_server
fudo_server_attribute
fudo_server_connection
fudo_server_grant
fudo_session
fudo_session_access
fudo_session_attribute
fudo_session_comment
fudo_session_event
fudo_session_share
fudo_session_text
fudo_user
fudo_user_attribute
fudo_user_authentication_method
fudo_user_connection
fudo_user_grant
reports_definedreport
reports_definedreportfilter
reports_definedreportsubscription
reports_report
reports_reportcriteria

Modyfikowanie serwera Syslog

Aby zmodyfikować definicję serwera *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.

2. Kliknij *Konfiguracja syslog*, aby wyświetlić opcje konfiguracji rejestrowania zdarzeń na serwerach syslog.
3. Wyszukaj żądaną definicję serwera syslog i zmień żądaną wartość parametru.
4. Kliknij *Zapisz*.

Usuwanie serwera Syslog

Aby usunąć serwer *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić listę zdefiniowanych serwerów Syslog.
3. Wyszukaj i zaznacz żądany wpis.
4. Kliknij *Zapisz*.

Eksportowanie dziennika zdarzeń

Aby wyeksportować zdarzenia zapisane w dzienniku zdarzeń, postepuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Eksportuj logi*, i wskaż miejsce, w którym zostanie zapisany plik z logami.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

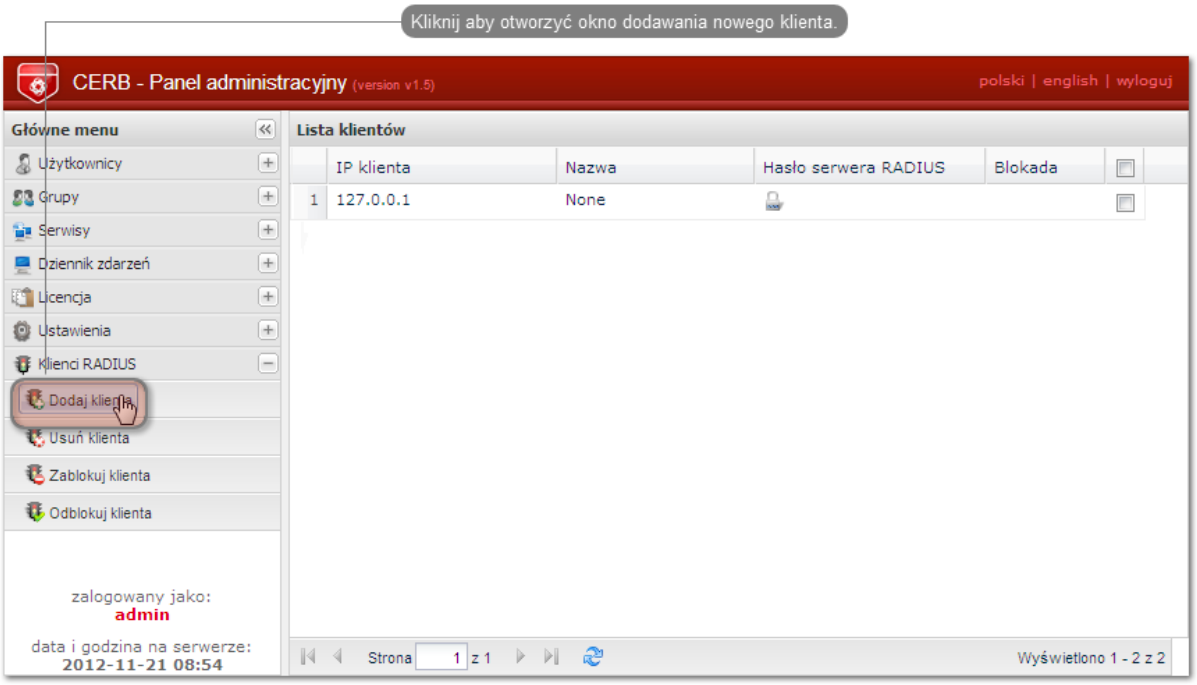
15.16 Integracja z serwerem CERB

CERB jest zewnętrznym serwerem uwierzytelniania wspierającym wiele mechanizmów weryfikacji tożsamości użytkowników (tj. token mobilny czasowy i zdarzeniowy, hasła jednorazowe, itp.). Poniższa instrukcja przestawia kroki konfiguracyjne jakie należy przeprowadzić aby użytkownicy nawiązujący połączenia zdalne za pośrednictwem Wheel Fudo PAM, uwierzytelniany byli przez zewnętrzny serwer CERB.

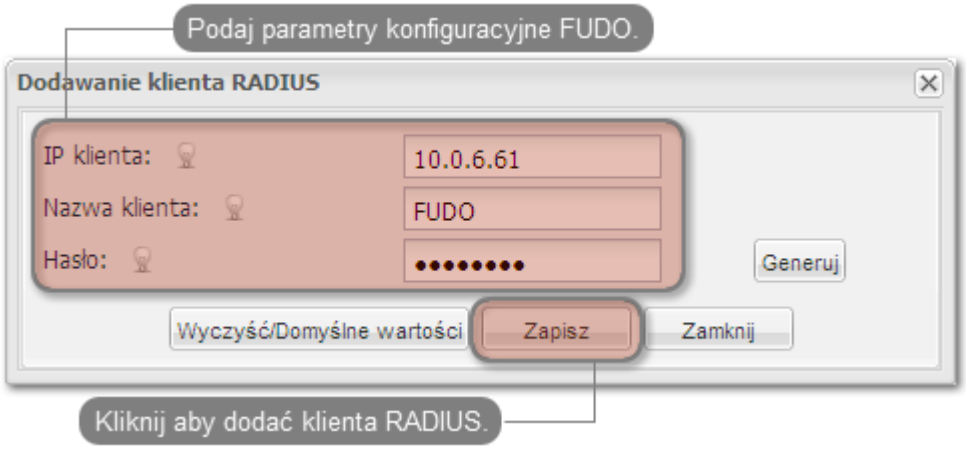
Konfiguracja serwera CERB

1. Dodanie klienta RADIUS.

- Wybierz z lewego menu *Klienci RADIUS* > *Dodaj klienta*, aby dodać Wheel Fudo PAM jako klienta RADIUS.



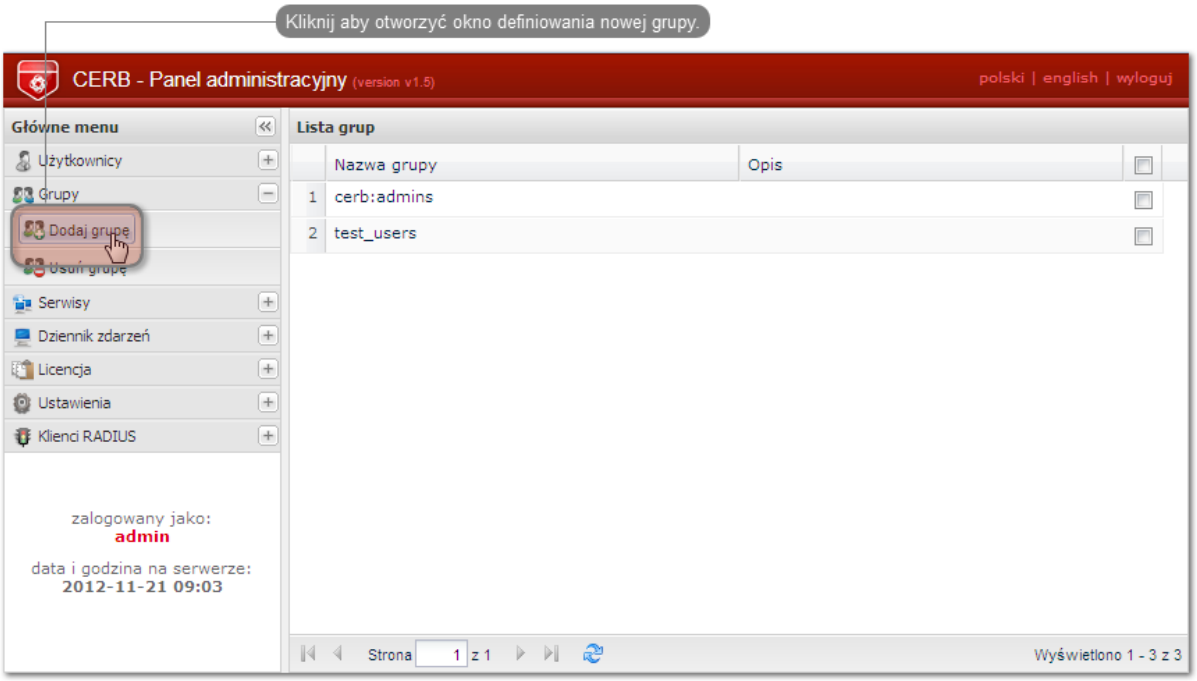
- Podaj adres IP serwera Wheel Fudo PAM, nazwę klienta oraz hasło i kliknij *Zapisz*.



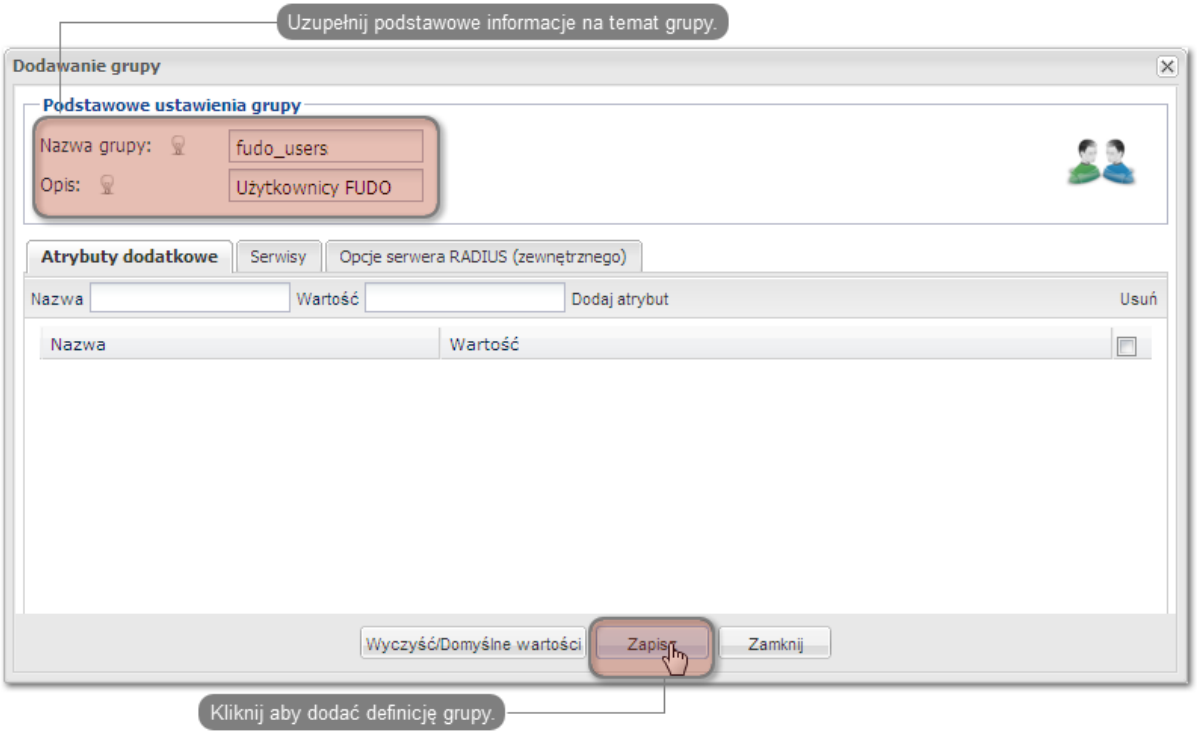
Informacja: Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelniania w panelu administracyjnym Wheel Fudo PAM.

2. Dodanie grupy użytkowników.

- Wybierz z lewego menu *Grupy* > *Dodaj grupę*, aby zdefiniować grupę użytkowników Wheel Fudo PAM, którzy będą autoryzowani poprzez serwer CERB.

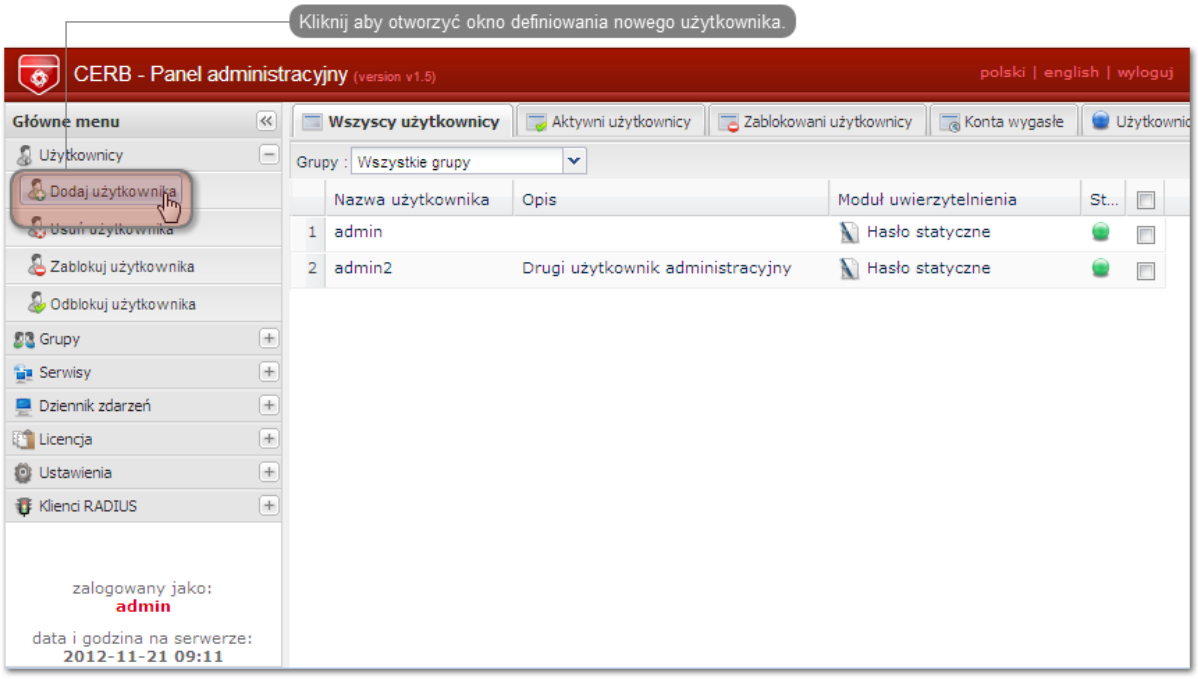


- Podaj nazwę grupy (`fudo_users`) i kliknij *Zapisz*.

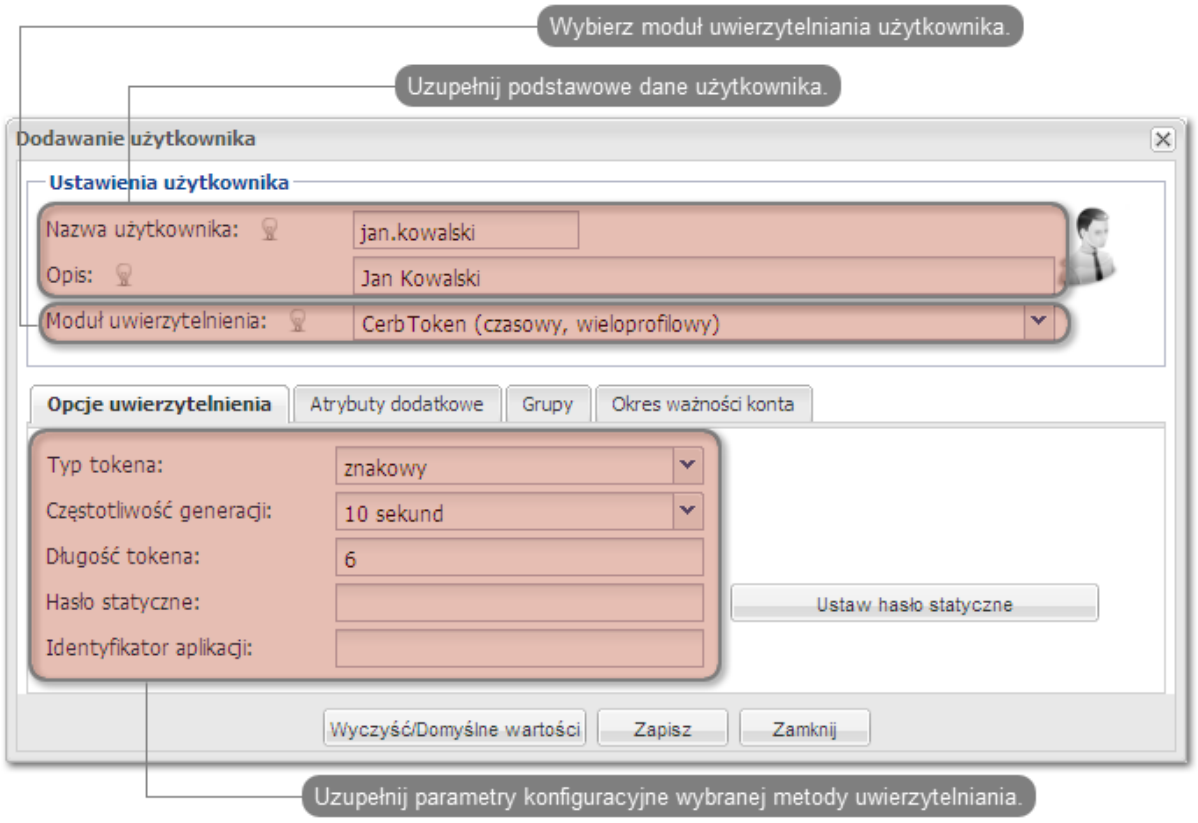


3. Dodanie użytkownika.

- Wybierz z lewego menu *Użytkownicy* > *Dodaj użytkownika*, aby otworzyć okno definiowania nowego użytkownika.

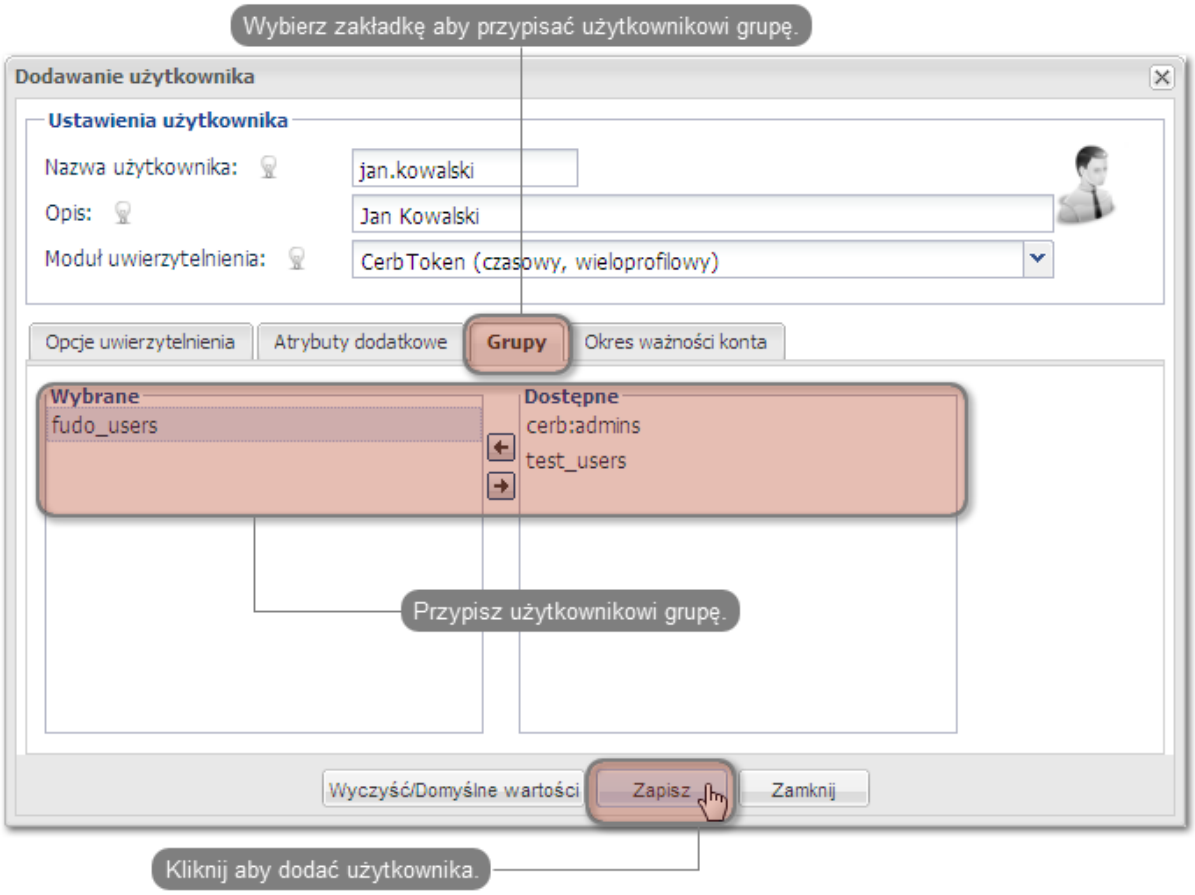


- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



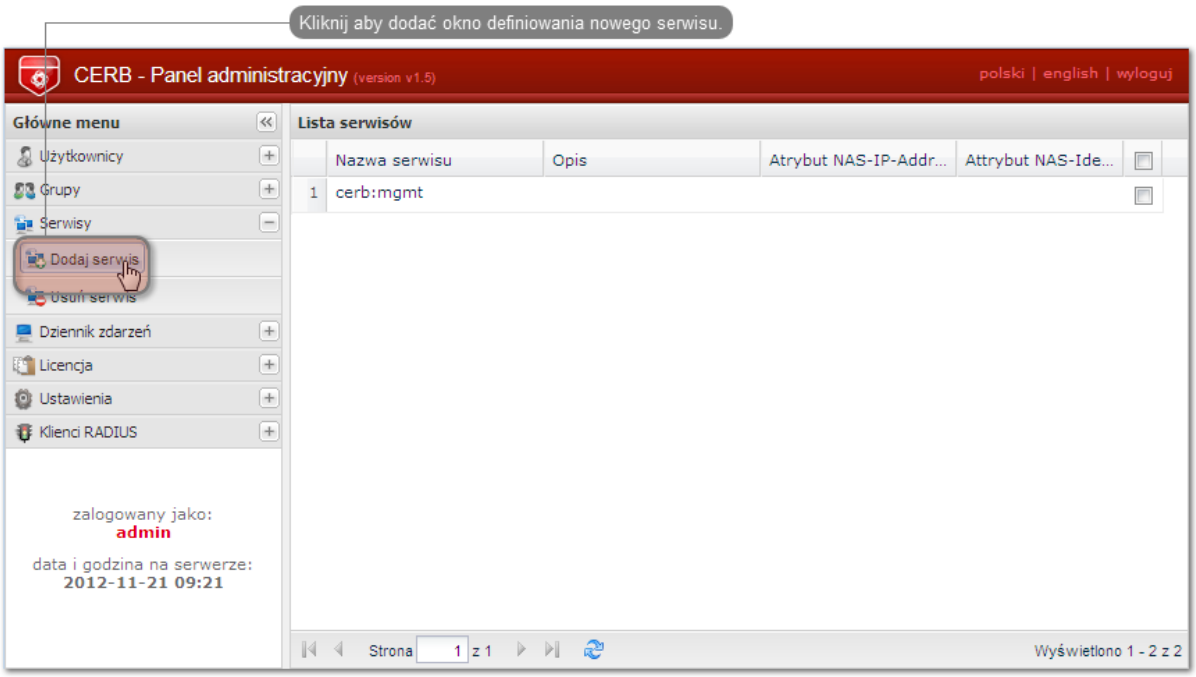
Informacja: Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkowników łączących się z Wheel Fudo PAM.

- Przypisz do użytkownika wcześniej dodaną grupę `fudo_users` i kliknij *Zapisz*.

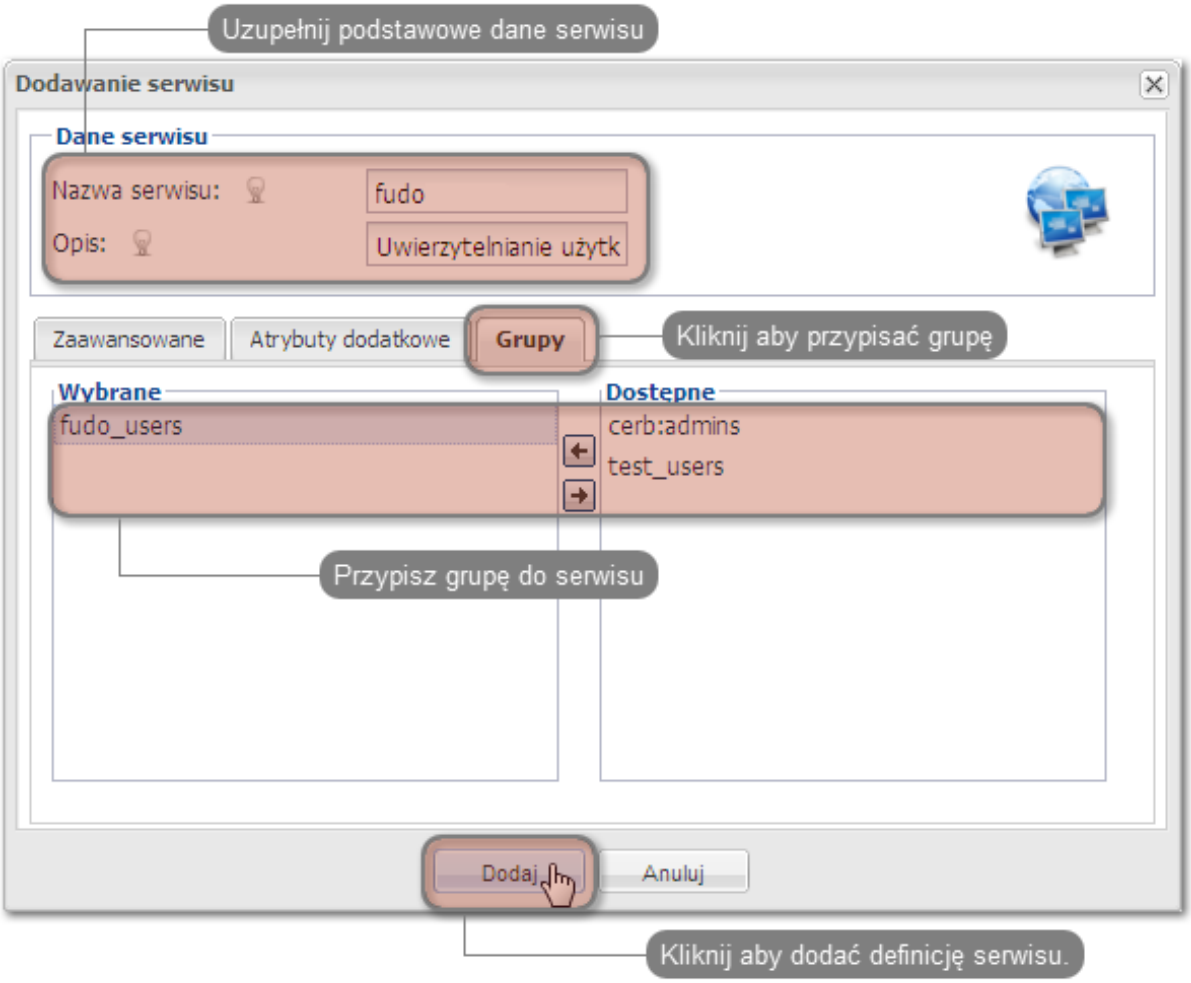


4. Skonfigurowanie serwisu.

- Wybierz z lewego menu *Serwisy* > *Dodaj serwis*, aby otworzyć okno definiowania nowego serwisu.



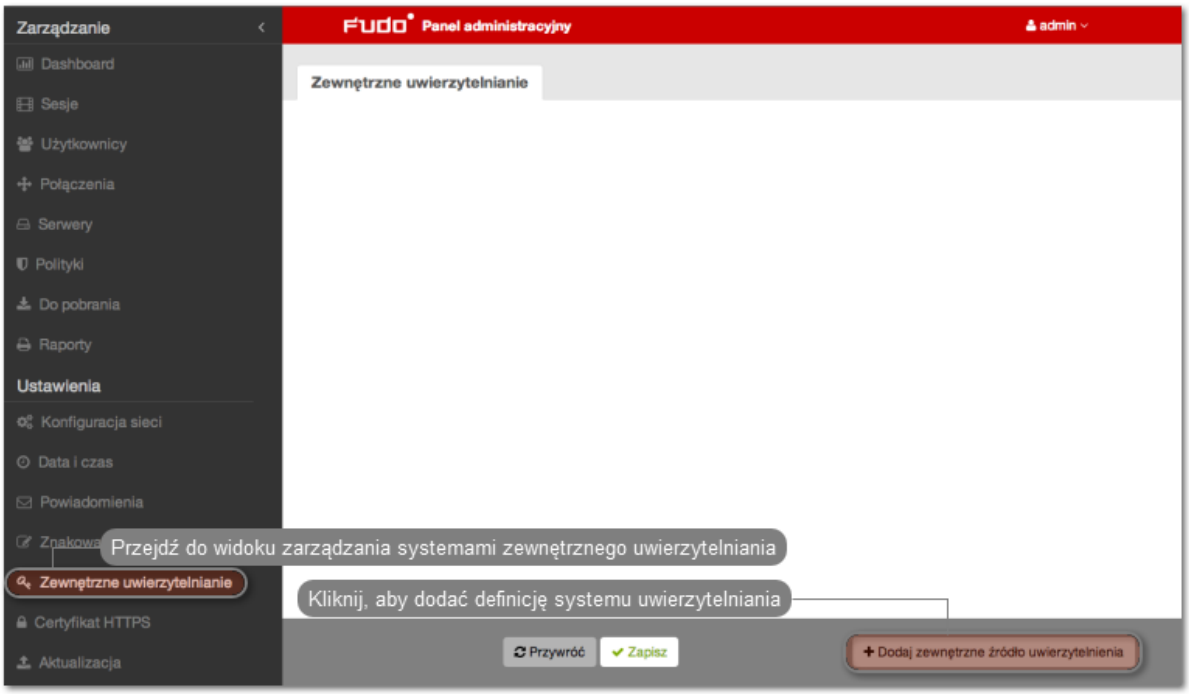
- Wpisz nazwę pod jaką identyfikowana będzie usługa uwierzytelniania (`cerb_fudo`) oraz opis serwisu.
- Dodaj do serwisu grupę `fudo_users` i kliknij *Dodaj*.



Konfiguracja serwera Wheel Fudo PAM

1. Dodanie serwera zewnętrznego uwierzytelniania CERB.

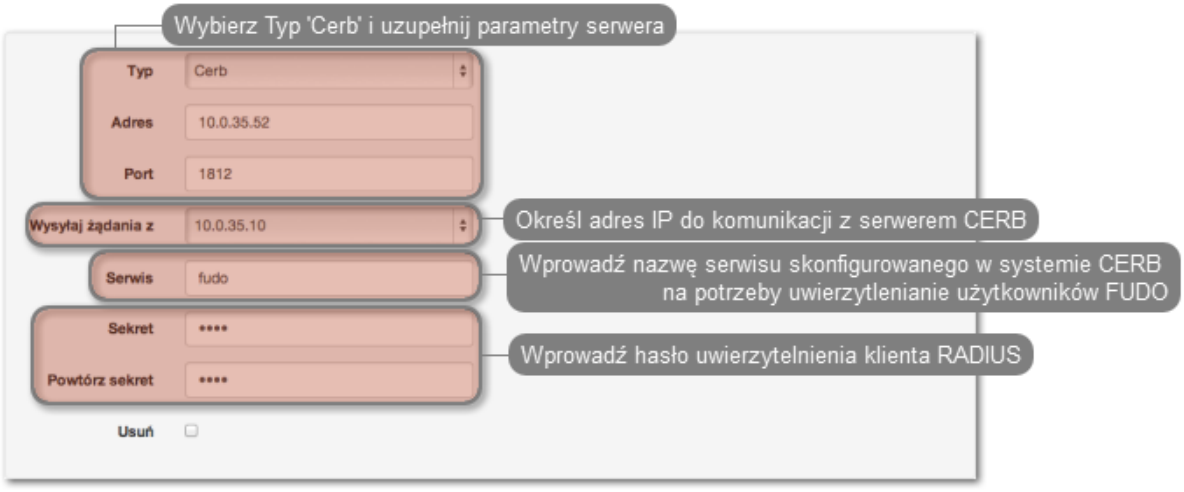
- Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
- Kliknij + *Dodaj zewnętrzne źródło uwierzytelnienia*, aby dodać definicję serwera CERB.



- Podaj adres IP serwera uwierzytelniania CERB, *sekret* oraz nazwę serwisu pod jaką identyfikowana będzie usługa uwierzytelniania.

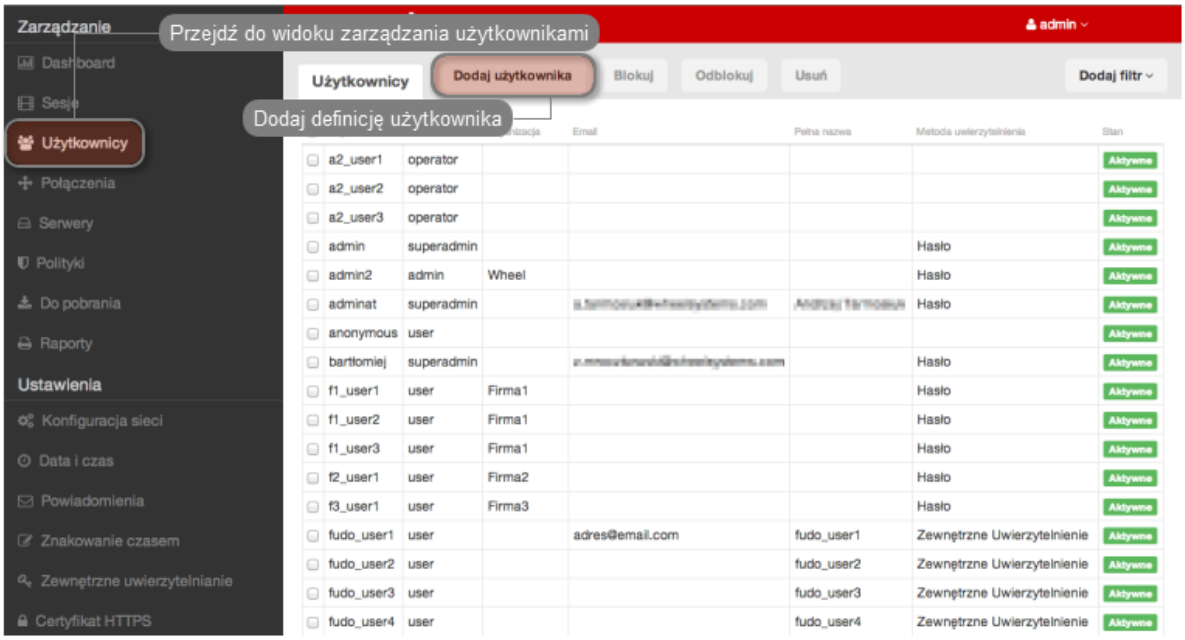
Informacja: Sekret odpowiada hasłu, które zostało podane przy konfigurowaniu klienta RADIUS na serwerze CERB. Nazwa serwisu musi być zgodna z nazwą nadaną przy konfigurowaniu serwisu na serwerze CERB.

- Kliknij *Zapisz*.



2. Dodanie użytkownika.

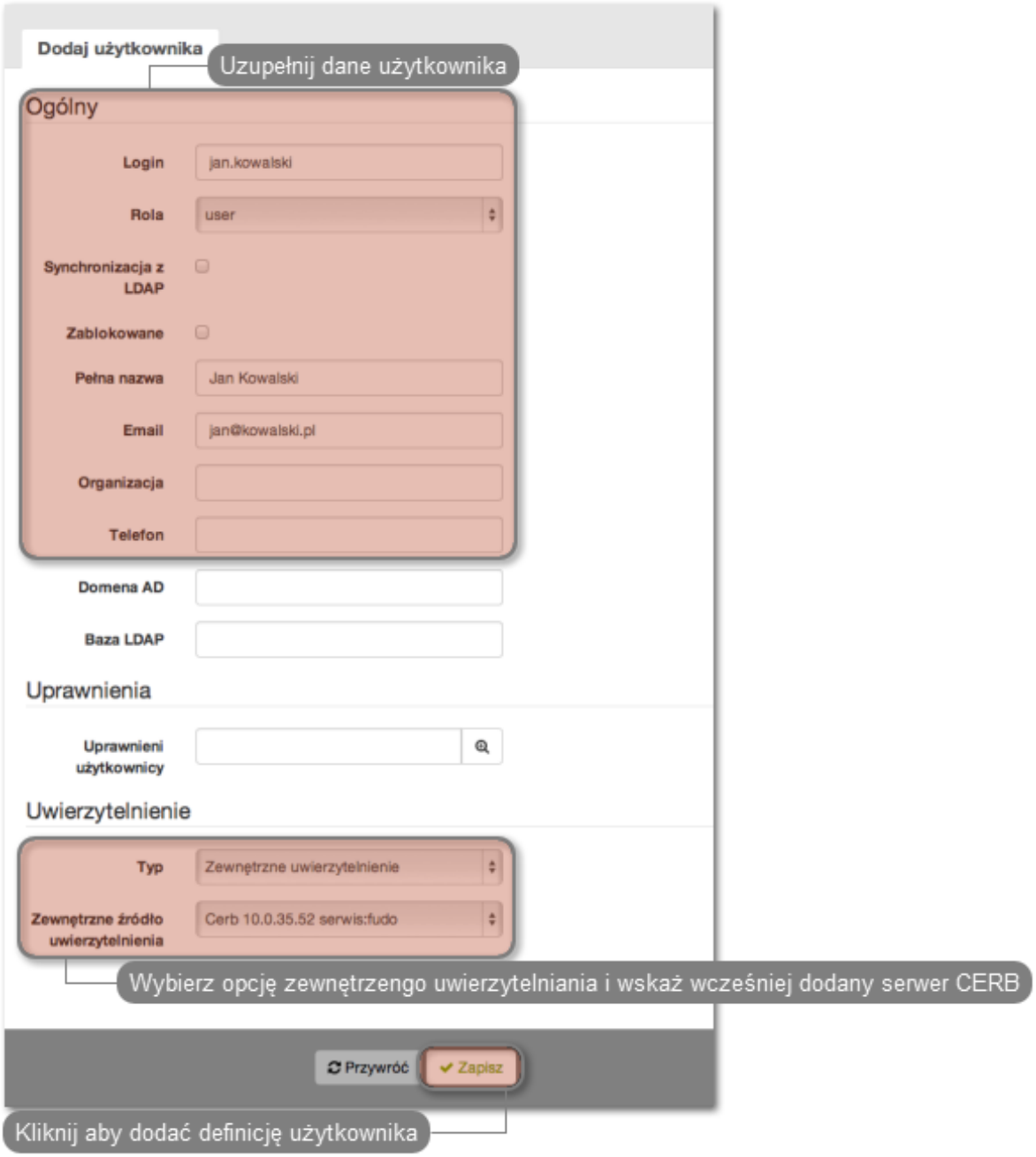
- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+ Dodaj*.



- Podaj podstawowe dane użytkownika.

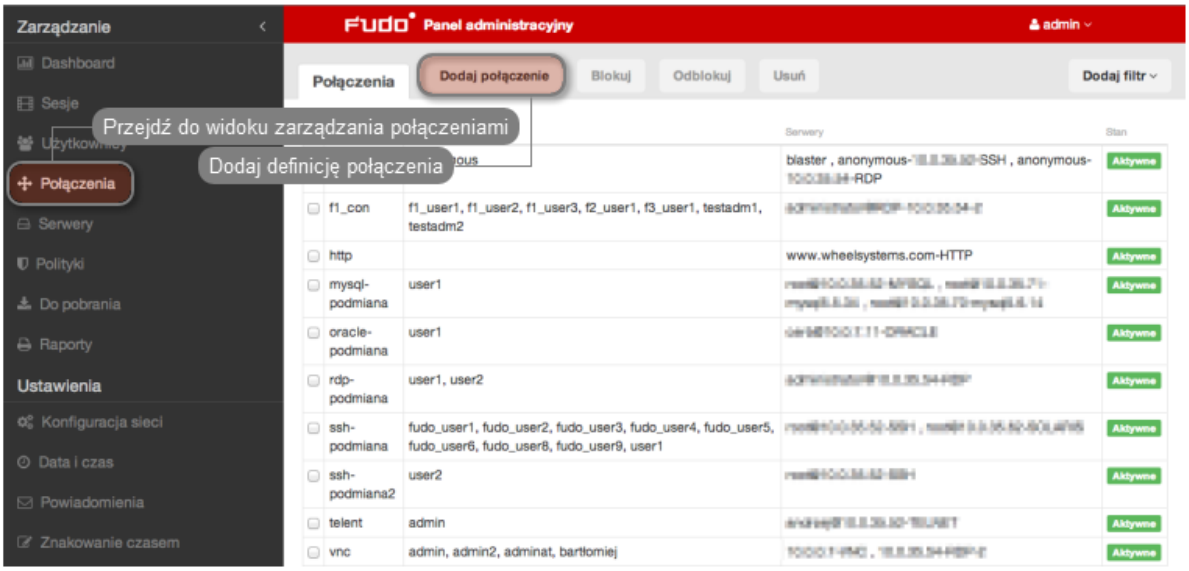
Informacja: Login użytkownika musi odpowiadać nazwie nadanej użytkownikowi na serwerze CERB.

- Z listy rozwijalnej wybierz `CERB` jako metodę uwierzytelniania i wskaż wcześniej dodany serwer uwierzytelniania.
- Kliknij *Zapisz*.

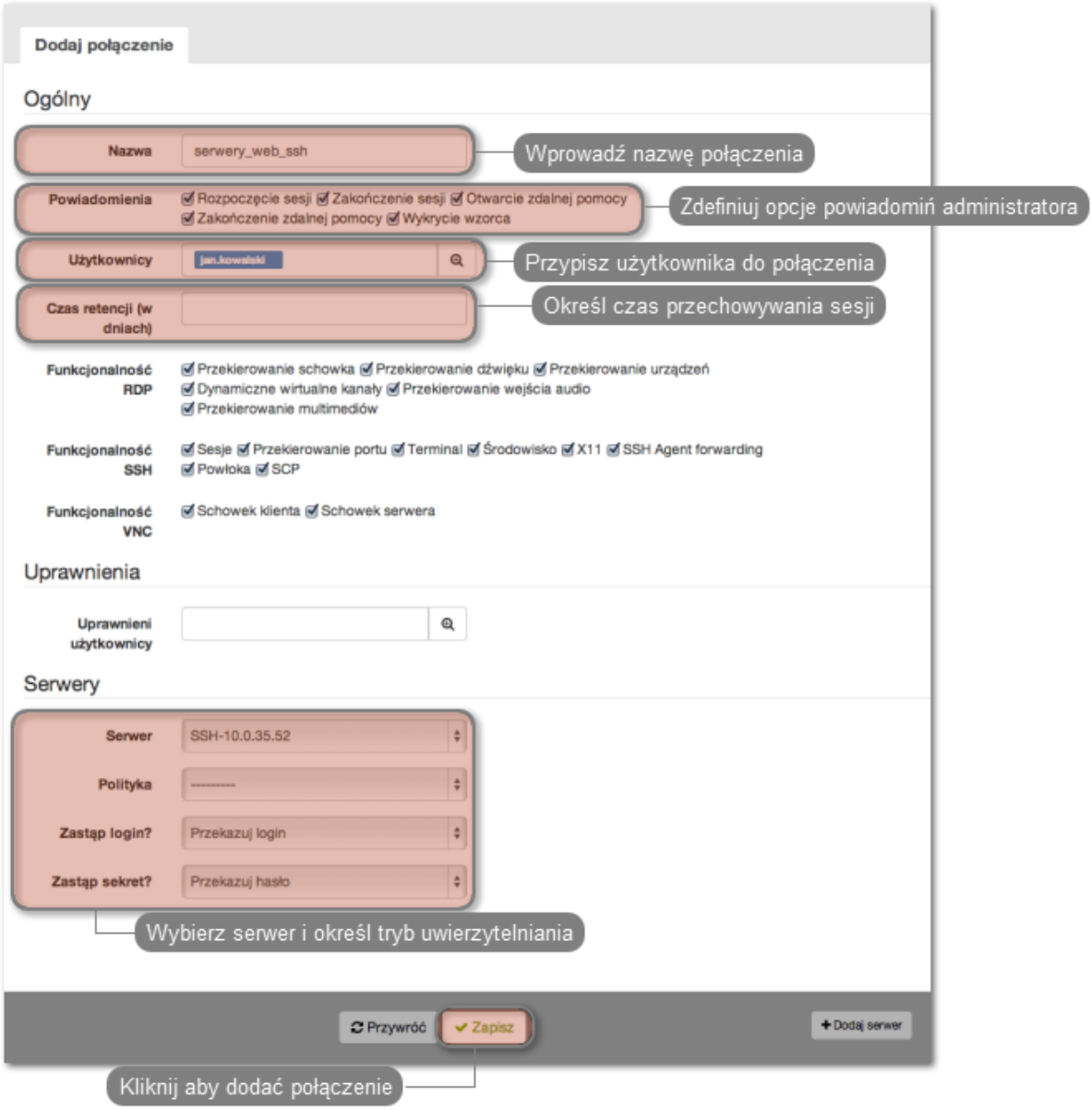


3. Dodanie połączenia.

- Wybierz z lewego menu *Zarządzanie* > *Połączenia*.
- Kliknij + *Dodaj*.



- Podaj podstawowe parametry połączenia.
- Wybierz z listy wcześniej dodanego użytkownika.
- Wybierz serwer, z którym użytkownik będzie się łączył w ramach tego połączenia.
- Wybierz tryb uwierzytelniania użytkownika (*Tryby uwierzytelniania*).
- Kliknij *Zapisz*.



Tematy pokrewne:

- *Zarządzanie użytkownikami*
- *Konfigurowanie serwerów uwierzytelniania*
- *Metody i tryby uwierzytelniania użytkowników*

15.17 Czynności serwisowe

Poniższy rozdział zawiera opisy czynności serwisowych.

15.17.1 Sporządzanie kopii zapasowej kluczy szyfrujących

Klucze szyfrujące wymagane są do zainicjowania systemu plików, na którym przechowywane są dane sesji. Uszkodzenie nośnika z kluczami szyfrującymi uniemożliwia poprawne uruchomienie

Wheel Fudo PAM.

Microsoft Windows

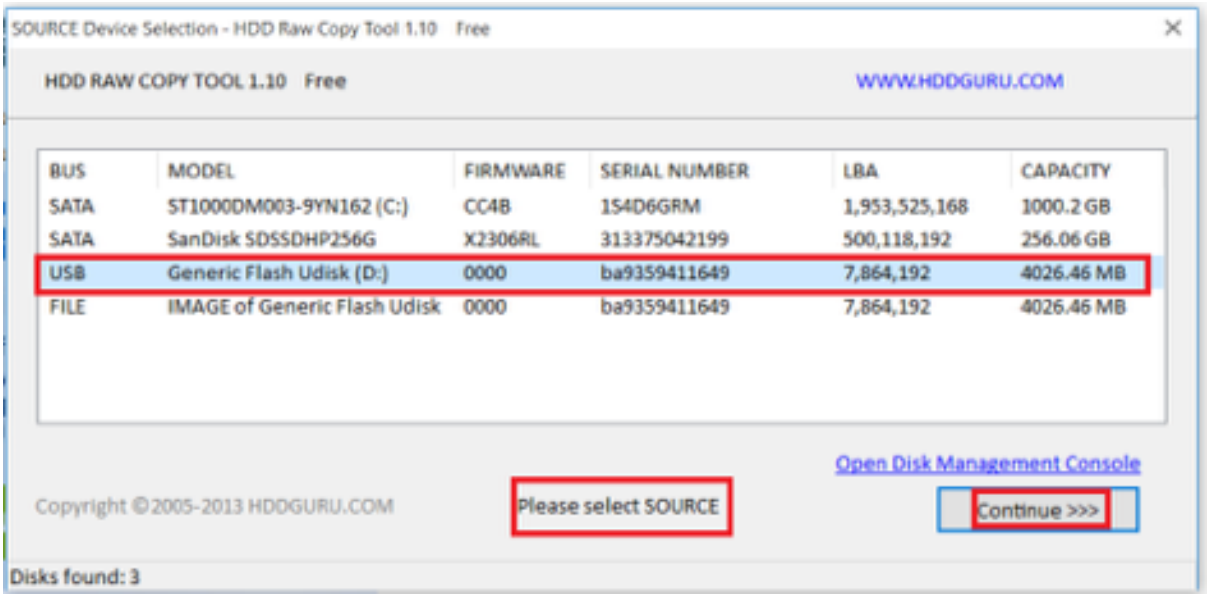
Ostrzeżenie: Po podłączeniu nośnika USB do komputera, pod żadnym pozorem nie należy wykonywać jego inicjowania/formatowania. Komunikat systemowy o braku możliwości odczytu danych należy zignorować i przystąpić do procedury tworzenia kopii zapasowej.

1. Pobierz i zainstaluj program *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (dostępna również wersja przenośna)

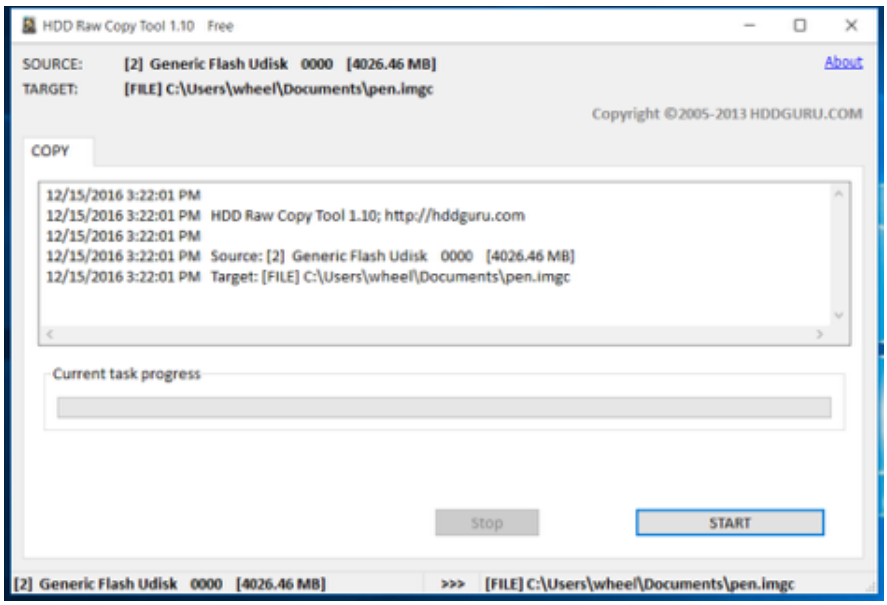
2. Uruchom program.

3. Na ekranie wyboru napędu źródłowego, zaznacz napęd USB z zapisanymi kluczami szyfrującymi i kliknij *Continue*.



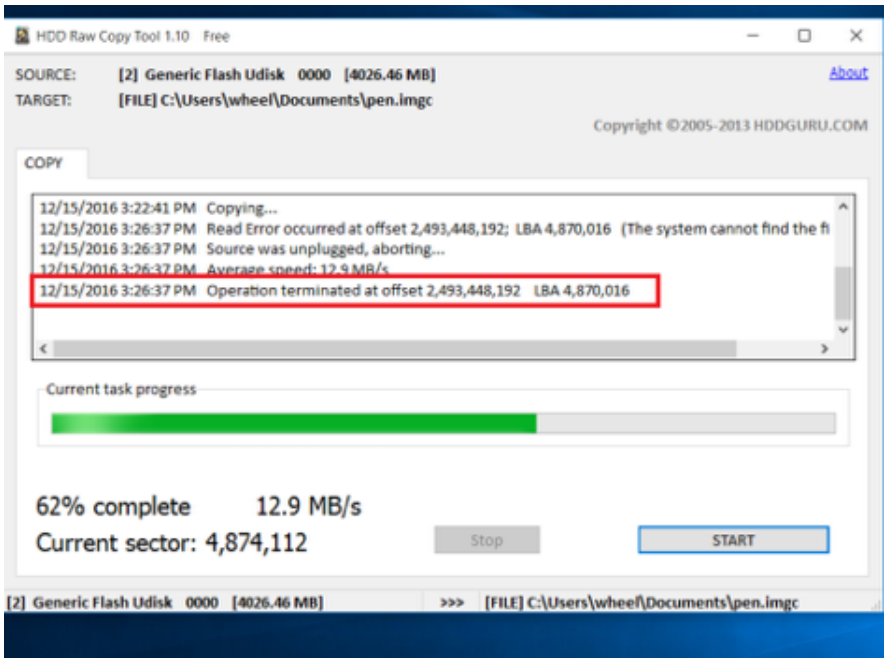
4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.

5. Kliknij *START*, aby rozpocząć procedurę kopiowania.

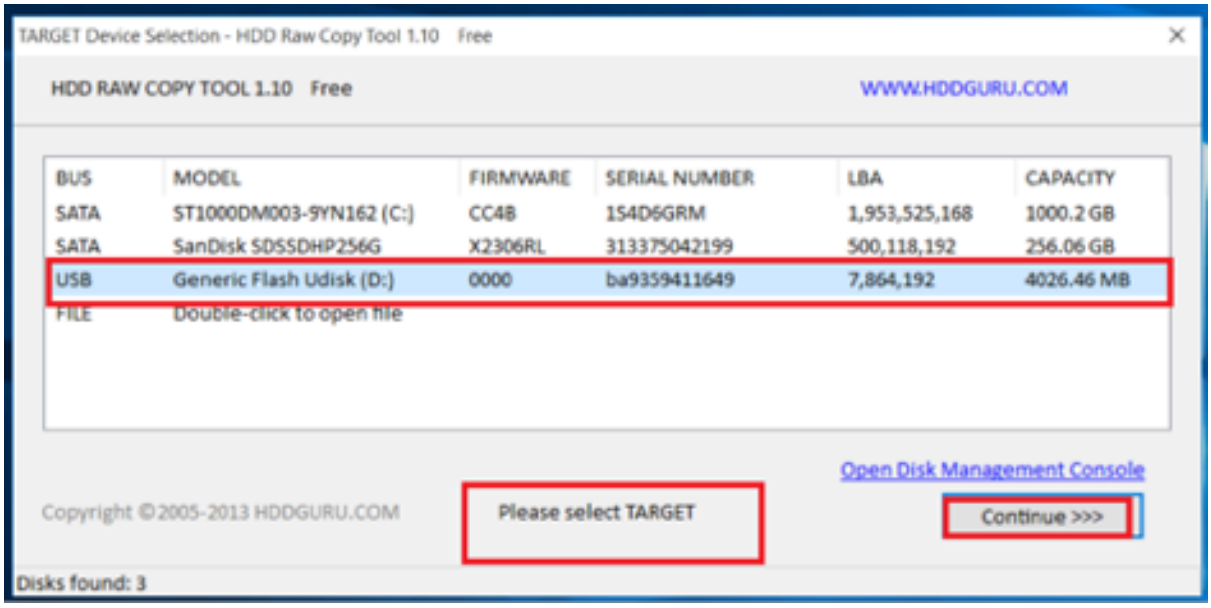


6. Z chwilą wystąpienia komunikatu

   `Operation terminated at offset...`, zamknij okno i odłącz napęd USB.

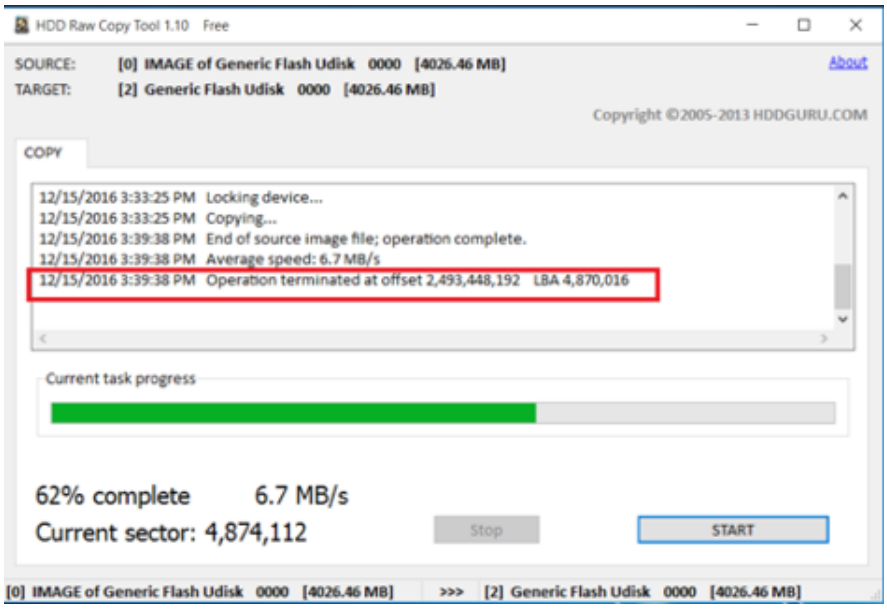


7. Podłącz nośnik pamięci flash i włącz program *HDD Raw Copy Tool*.
8. Na ekranie wyboru napędu źródłowego, zaznacz *FILE* i wskaż plik z obrazem kluczy szyfrujących.
9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij *Continue*.



10. Kliknij *Continue*.
11. Kliknij *START*.
12. Proces kopiowania obrazu zakończony jest z chwilą wystąpienia komunikatu:

    ```
    Operation terminated at offset....
    ```



13. Zamknij program i odłącz nośnik flash z zapisanym kluczem szyfrującym.

Mac OS X

1. Uruchom terminal.
2. Wykonaj komendę `sudo -s` i wprowadź hasło użytkownika.
3. Wykonaj komendę `diskutil list`, aby wyświetlić listę urządzeń.
4. Odszukaj napęd o następującym układzie partycji.

```
/dev/disk2 (external, physical):
#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *8.0 GB disk2
1: F649773F-1CD6-11E1-9AD2-00262DF29F0D 3.1 KB disk2s1
2: 2B163C2B-1FE5-11E1-8300-00262DF29F0D 1.0 KB disk2s2
```

5. Wykonaj obraz dysku komendą `dd if=/dev/disk2 of=fudo_pen.img bs=1m`, gdzie `if` wskazuje na napęd USB.
6. Odłącz nośnik pamięci flash z kluczem szyfrującym i podłącz nowy.
7. Wykonaj polecenie `dd if=fudo_pen.img of=/dev/disk2 bs=1m`.
8. Wykonaj komendę `sync`.
9. Odłącz nośnik pamięci flash z nowo zapisanym kluczem szyfrującym.

Linux

1. Uruchom terminal.
2. Wykonaj komendę `sudo -s` i wprowadź hasło użytkownika.
3. Wykonaj komendę `dmesg | less`, aby ustalić identyfikator nośnika danych.
4. Wykonaj obraz dysku komendą `dd if=/dev/disk2 of=fudo_pen.img bs=1m`, gdzie `if` wskazuje na napęd USB.
5. Odłącz nośnik pamięci flash z kluczem szyfrującym i podłącz nowy.
6. Wykonaj polecenie `dd if=fudo_pen.img of=/dev/disk2 bs=1m`.
7. Wykonaj komendę `sync`.
8. Odłącz nośnik pamięci flash z nowo zapisanym kluczem szyfrującym.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

15.17.2 Monitorowanie stanu systemu

Monitorowanie stanu Wheel Fudo PAM pozwala zapewnić prawidłową pracę systemu i zapobiegać przeciążeniom i awariom.

Monitorowanie aktywnych sesji

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź bieżącą liczbę aktualnie aktywnych połączeń użytkowników.

Informacja: Konfiguracja Wheel Fudo PAM pozwala na jednoczesną obsługę 300 połączeń RDP.

Monitorowanie przepustowości łącza sieciowego

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź bieżącą aktywność interfejsów sieciowych.

Informacja: Wheel Fudo PAM jest wyposażone w interfejsy sieciowe o przepustowości 1Gbps. W przypadku gdy bieżąca wartość transferu przekracza 500Mbps, użytkownicy mogą zauważyć spadek wydajności komunikacji z systemem.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

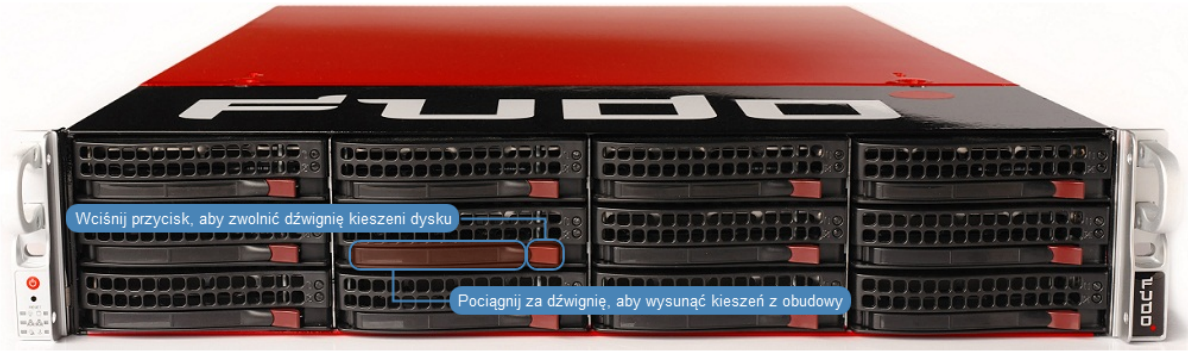
15.17.3 Wymiana dysku macierzy

W domyślnej konfiguracji, macierz dyskowa Wheel Fudo PAM składa się z 12 dysków twardych a zastosowany system plików pozwala na kontynuowanie świadczenia usług w przypadku awarii dwóch nośników.

Wymiana dysku macierzy

1. Przesuń w lewo dźwignię zwalniającą przedni panel, aby zdjąć go z obudowy.

2. Wciśnij przycisk zwalniający dźwignię kieszeni dysku twardego i pociągnij za dźwignię, aby wyjąć kieszeń z obudowy.



3. Odkręć śruby mocujące dysk twardy i wyjmij dysk z kieszeni.
4. Włóż nowy dysk twardy i wkręć śruby mocujące.
5. Włóż kieszeń z dyskiem twardym do serwera.

Informacja: System automatycznie wykryje zmianę stanu macierzy i przystąpi do odbudowywania struktury danych. Czas trwania procesu zależy od liczby danych przechowywanych w systemie.

Tematy pokrewne:

- *Urządzenie*
- *Często zadawane pytania*

ROZDZIAŁ 16

Informacje uzupełniające

16.1 Kody błędów

Kod błędu	Treść komunikatu i opis
FSE0001	*Internal system error*
FSE0002	*FUDO certificate error.*
FSE0003	*Unable to change configuration settings.*
FSE0004	*Configuration import error*
FSE0005	*Unable to initialize ${disk}.* Wymień dysk twardy, który sygnalizuje błąd. **Informacja:** Numeracja dysków zaczyna się od 0. Jeżeli błąd zgłasza dysk numer 1, fizycznie jest to drugi dysk w górnym rzędzie.
FSE0006	*Invalid license*
FSE0007	*Unable to find license file* System nie mógł zlokalizować licencji. Wgraj ponownie plik licencji zgodnie z procedurą opisaną w rozdziale *Administracja > System > Licencja*. Jeśli problem będzie się powtarzał skontaktuj się z działem wsparcia technicznego.
FSE0008	*Unable to attach hard drive ${disk}.*
FSE0009	*Upgrade failed.* Wystąpił błąd w procedurze aktualizacji systemu. Wgraj raz jeszcze plik z aktualizacją i ponownie wywołaj procedurę aktualizacji. Jeśli problem się powtórzy, skontaktuj się z działem wsparcia technicznego.
FSE0010	*License expired.* Skontaktuj się z działem wsparcia technicznego, aby otrzymać nową licencję.
FSE0020	*System backup error.*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FSE0024	*Hard drive belongs to another FUDO (${diskserial}) ${disk}.* Wskazany dysk twardy pochodzi z innej instancji Wheel Fudo PAM. Wymień dysk na właściwy. **Informacja:** Numeracja dysków zaczyna się od 0. Jeżeli błąd zgłasza dysk numer 1, fizycznie jest to drugi dysk w górnym rzędzie.
FSE0026	*Cluster communication error.*
FSE0028	*Unable to join node to cluster.*
FSE0031	*Timestamping service communication error*
FSE0032	*Unable to timestamp session.*
FSE0033	*Unknown timestamping service provider.*
FSE0040	*Cluster communication error. Local FUDO version is %s than %s FUDO version.*
FSE0046	*There is no filter called %s.*
FSE0048	*Error authenticating user over RADIUS.*
FUE0057	*Authentication method «password», required by MySQL, requested by the user %s, logging in from IP address %s, was not found.*
FUE0058	*Authentication method «password», required by MySQL, requested by the user %s, was not found.*
FSE0061	*Incorrect password repository configuration: login is empty.*
FSE0062	*Incorrect password repository configuration: password is empty.*
FSE0063	*Incorrect server configuration: ERPM namespace is empty.*
FSE0064	*Incorrect server configuration: ERPM name is empty.*
FSE0065	*License configuration error.*
FSE0066	*Unable to block user %jd.*
FSE0067	*Error connecting to Lieberman ERPM server %s: incorrect URL in configuration.*
FSE0068	*Error connecting to Lieberman ERPM server %s: incorrect protocol specified.*
FSE0069	*Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s.*
FSE0070	*Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server.*
FSE0076	*Unable to establish connection, could not find specified transparent server (tcp://%s:%u).*
FSE0077	*LDAP authentication error.*
FSE0078	*LDAP authentication error: unable to connect from %s to %s.*
FUE0079	*Authentication timeout after %ju key attempt%s and %ju password attempt%s.*
FUE0080	*Authentication timeout after %lu key attempt%s.*
FUE0081	*Authentication timeout after %lu password attempt%s.*
FSE0082	*Unable to establish connection to server %s (%s).*
FSE0083	*Unable to establish connection from %s to server %s (%s).*
FUE0089	*Authentication timeout.*
FSE0090	*Unable to connect to the passwords repository server %s.*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FSE0091	*Unable to add server %s.*
FSE0092	*Passwords repository server %s communication error.*
FSE0093	*Error connecting to Thycotic server %s: incorrect URL in configuration.*
FSE0094	*Error connecting to Thycotic server %s: incorrect protocol specified.*
FSE0095	*Error fetching password from Thycotic server %s: unable to get sessid for user %s.*
FSE0096	*Error fetching password from Thycotic server %s.*
FSE0097	*Error fetching password from Thycotic server %s: unable to get secretid for server %s.*
FSE0098	*Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server.*
FUE0099	*Connection terminated.*
FUE0101	*Unable to find matching HTTP connection.*
FUE0103	*HTTP connection error.*
FUE0106	*Authentication failed: %s.*
FUE0108	*MySQL connection error.*
FUE0110	*Oracle connection error.*
FUE0112	*RDP connection error.*
FUE0113	*TLS Security configured, but missing TLS private key.*
FUE0114	*TLS Security configured, but missing TLS certificate.*
FUE0115	*Standard RDP Security configured, but missing private key.*
FUE0116	*TLS certificate verification failed.*
FUE0117	*RSA key verification failed.*
FUE0124	*SSH connection error.*
FUE0125	*User %s failed to authenticate after %d attempts, disconnecting.*
FUE0127	*Invalid authentication method: expected passwordor sshkey, got %s.*
FUE0129	*Failed to authenticate against the server as user %s using %s.*
FUE0130	*Failed to authenticate against the server as user %s using %s (received %s).*
FUE0132	*Client requested incorrect terminal dimensions (%dx%d).*
FUE0133	*MSSQL connection error.*
FUE0134	*TN3270 connection error.*
FUE0135	*Unknown TN3270 command: %02x.*
FUE0136	*Telnet connection error.*
FSE0137	*Unable to read private key.*
FSE0138	*Server's certificate does not match configured certificate.*
FUE0139	*VNC connection error.*
FUE0140	*Client version: %s is higher than the client integrated in FUDO: %s.*
FUE0141	*VNC connection error. Client answered with unsupported security type: %hhu.*
FUE0142	*VNC connection error. Server version: %s is lower than client version: %s.*
FUE0144	*User %s failed to authorize logging in from IP address: %s.*
FUE0145	*User %s failed to authorize.*
FUE0146	*User %s failed to authenticate logging in from IP address: %s.*
FUE0147	*User %s failed to authenticate.*
FSE0148	*Listening on %s:%u failed while adding bastion %s.*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FAE0153	*Session indexing failure.*
FAE0154	*Session conversion failure for session %s.*
FAE0165	*Error authenticating user <user_name>.*
FAE0189	*Error saving NTP servers: <server_name>.*
FAE0232	*MySQL session playback error.*
FAE0267	*Error generating report %d: %s.*
FSE0283	*Unable to process pattern: %s.*
FSE0285	*Unable to read certificate.*
FSE0286	*No peer certificate received.*
FSE0290	*Unable to add server %s because %s is listening on same IP address and port.*
FUE0305	*Client connection closed: encryption is not available.*
FUE0306	*Client connection closed.*
FSE0307	*Error fetching password from HiPAM server %s: unable to get sessid for user %s.*
FSE0308	*HiPAM server internal error.*
FSE0309	*Error fetching password from HiPAM server %s: unable to get sessdat for user %s.*
FSE0310	*Incorrect server configuration: HiPAM name is empty.*
FSE0311	*Unable to fetch password from HiPAM.*
FSE0312	*Error connecting to HiPAM server %s: incorrect URL in configuration.*
FSE0313	*Error connecting to HiPAM server %s: incorrect protocol specified.*
FUE0314	*Invalid pixel format.*
FUE0315	*Unable to fetch standard RDP certificate.*
FUE0316	*Protocol security negotiation failure.*
FUE0317	*Unable to establish connection to server %s.*
FUE0318	*Unable to fetch SSL certificate.*
FSE0330	*Bad login field configured on server. Error while processing user %s.*
FSE0331	*Error while processing userAccountControl value of user %s.*
FUE0346	*Client sent a packet bigger than %d bytes.*
FSE0347	*Cluster communication error. Local FUDO version: ${lversion}, remote FUDO version: ${rversion}.*
FSE0348	*Unable to get configuration settings.*
FUE0351	*Client sent unsupported NTLM v1 response.*
FSE0352	*Bastion requires login and server delimited with one of «%s» (%s).*
FSE0355	*Inconsistent data, starting recovery replication to node ${name}.*
FUE0359	*Server rejected X11 connection: %.*s.*
FUE0360	*Server requires unsupported X11 authentication: %.*s.*
FSE0362	*Unable to propagate ARP.*
FUE0363	*User %s has no access to host %s:%u.*
FUE0365	*RDP server %s:%u has to listen on the default RDP port in order to redirect sessions.*
FSE0366	*Error connecting to CyberArk server %s: incorrect URL in configuration.*
FSE0367	*Error connecting to CyberArk server %s: incorrect protocol specified.*
FSE0368	*Error fetching password from CyberArk server %s.*
FSE0369	*Error fetching password from CyberArk server %s: unable to get password for user %s for server %s.*

Kontynuacja na następnej stronie

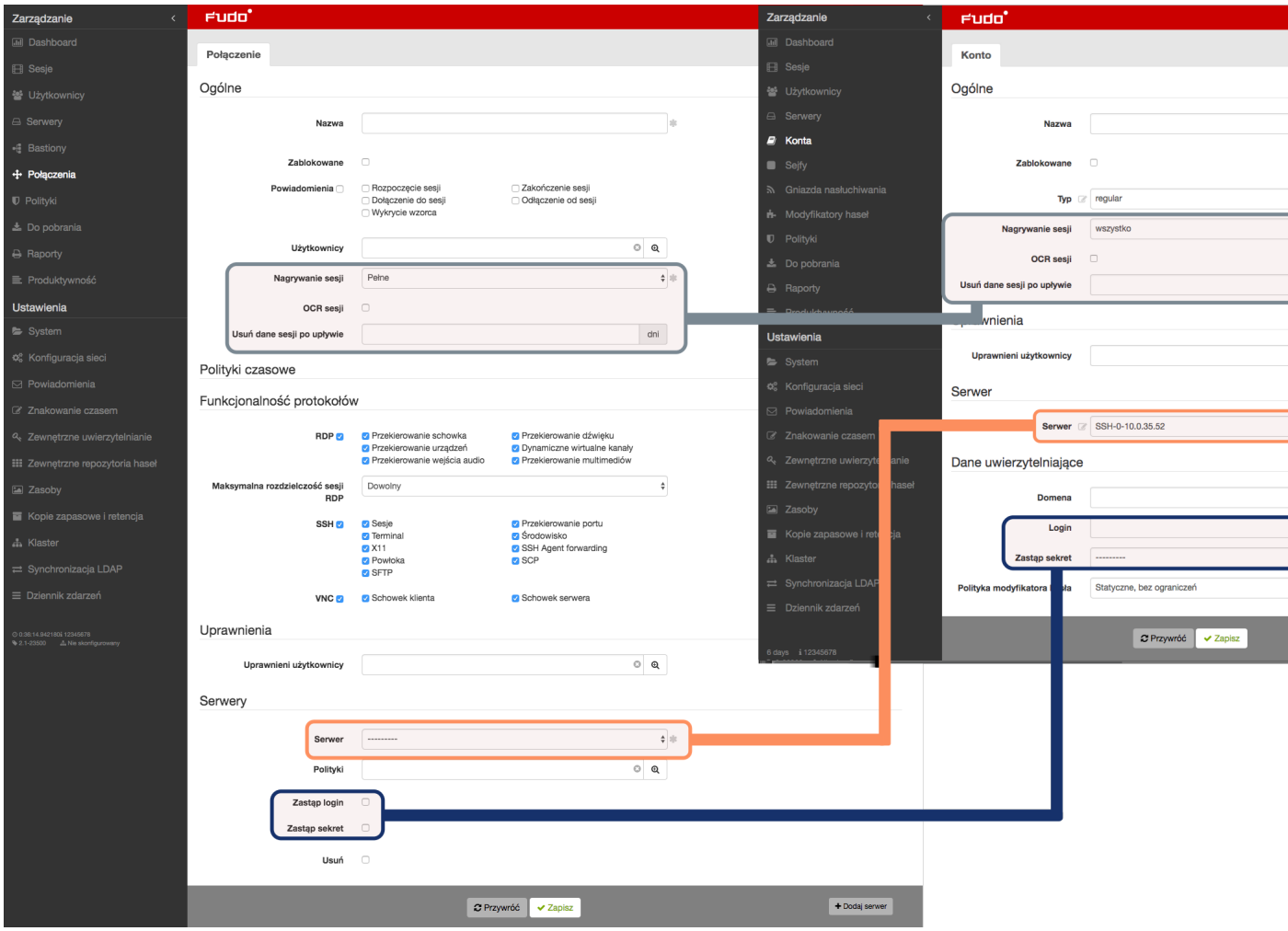
Tabela 1 – kontynuacja poprzedniej strony

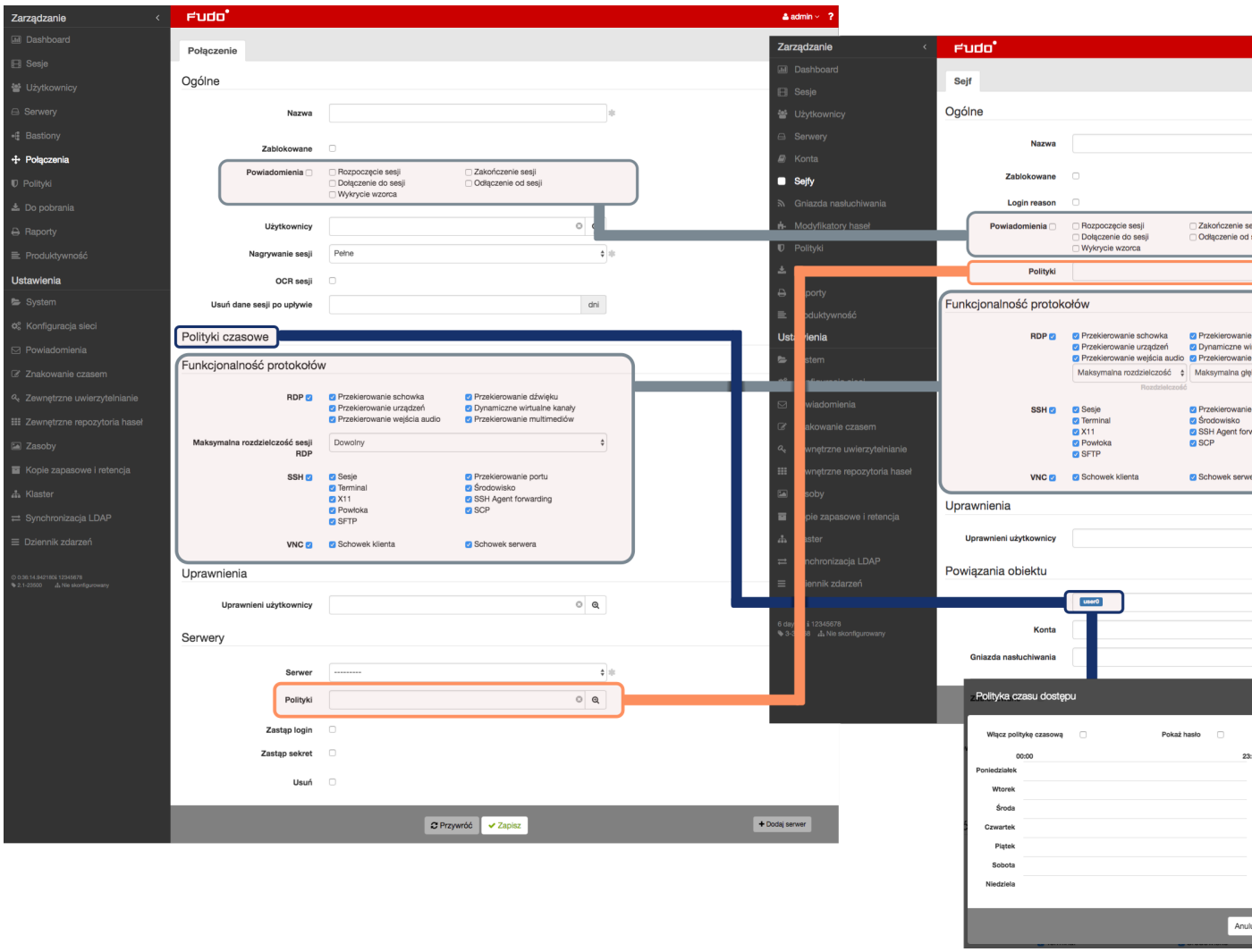
Kod błędu	Treść komunikatu i opis
FSE0372	*Unable to invalidate OTP password %jd.*
FSE0375	*Unable to add listener %s.*
FSE0376	*Unable to add listener %s because %s is listening on same IP address and port.*
FSE0377	*Bastion requires login and server delimited with a «%s» character (login: %s).*
FSE0378	*Unable to establish connection, could not find a server (login: %s).*
FSE0379	*Unable to establish connection, could not find specified transparent server (tcp://%s:%u) (login: %s).*
FSE0380	*Unable to authenticate user %s: server is blocked.*
FSE0381	*Unable to authenticate user %s: account not found.*
FSE0382	*Unable to authenticate user %s: account is blocked.*
FSE0383	*Unable to authenticate user %s: user not found.*
FSE0384	*Unable to authenticate user %s: user is blocked.*
FSE0385	*Unable to authenticate user %s: safe not found.*
FSE0386	*Unable to authenticate user %s: safe is blocked.*
FSE0420	*Unable to authenticate user %s against server %s.*
FSE0461	*Invalid data from AD server.*
FAE0464	*User %s is not allowed to login from address %s.*

16.2 Mapowanie parametrów Fudo 2.2 na Fudo 3.0

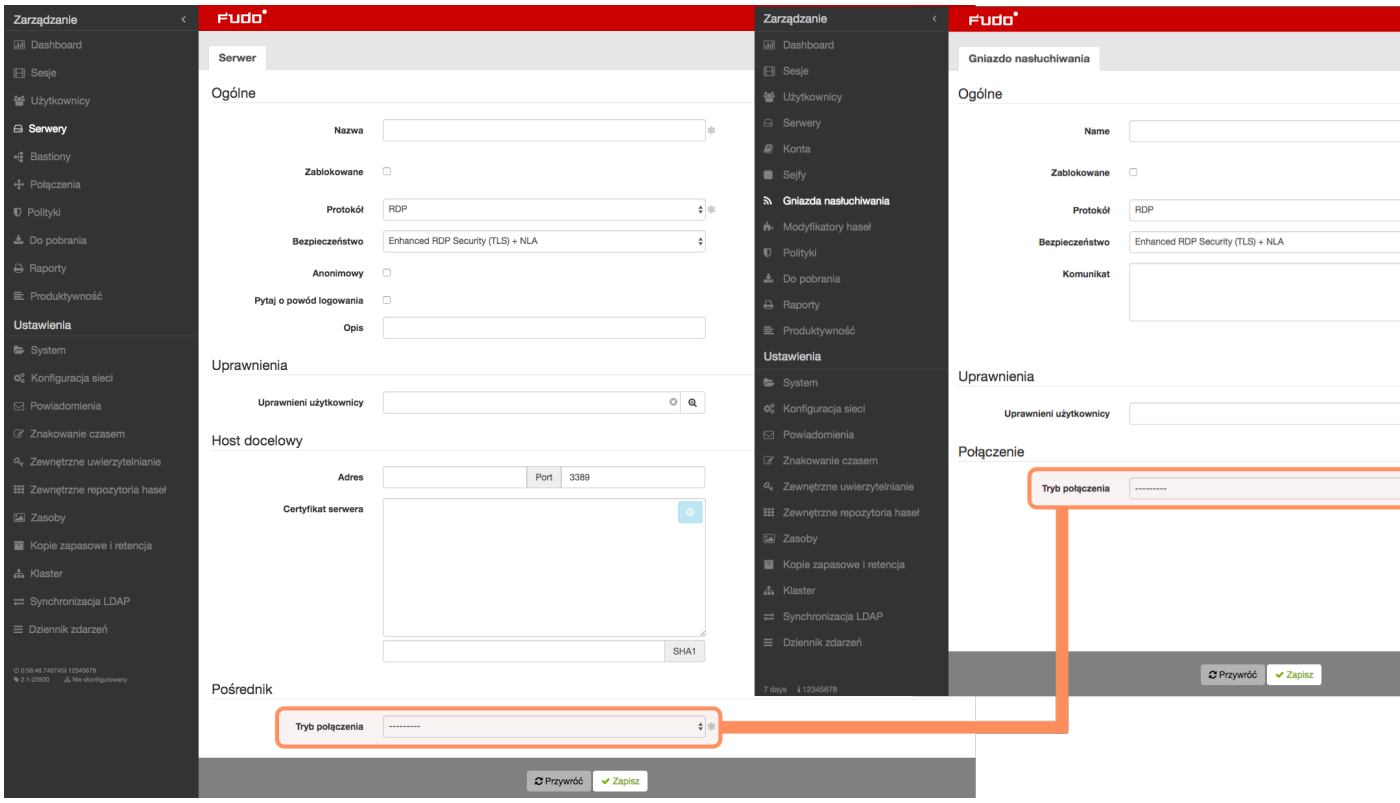
Ten rozdział zawiera opis odwzorowania parametrów obiektów w Fudo 2.2 na nowy model danych Fudo 3.0.

16.2.1 Połączenie




Zarządzanie
Dashboard
Sesje
Użytkownicy
Serwery
Bastiony
Połączenia
Polityki
Do pobrania
Raporty
Produktywność
Ustawienia
System
Konfiguracja sieci
Powiadomienia
Znakowanie czasem
Zewnętrzne uwierzytelnianie
Zewnętrzne repozytoria haseł
Zasoby
Kopie zapasowe i retencja
Klaster
Synchronizacja LDAP
Dziennik zdarzeń
admin
Połączenie
Ogólne
Nazwa
Zablokowane
Powiadomienia
Rozpoczęcie sesji
Zakończenie sesji
Dołączenie do sesji
Odłączenie od sesji
Wykrycie wzorca
Użytkownicy
Nagrywanie sesji
Pełne
OCR sesji
Usuń dane sesji po upływie
dni
Polityki czasowe
Funkcjonalność protokołów
RDP
Przekierowanie schowka
Przekierowanie urządzeń
Przekierowanie wejścia audio
Przekierowanie dźwięku
Dynamiczne wirtualne kanały
Przekierowanie multimediów
Maksymalna rozdzielczość sesji RDP
Dowolny
SSH
Sesje
Terminal
X11
Powłoka
SFTP
Przekierowanie portu
Środowisko
SSH Agent forwarding
SCP
VNC
Schowek klienta
Schowek serwera
Uprawnienia
Uprawnieni użytkownicy
Serwery
Serwer
Polityki
Zastąp login
Zastąp sekret
Usuń
Przywróć
Zapisz
Dodaj serwer
Konta
Sejfy
Gniazda nasłuchiwania
Modyfikatory haseł
Sejf
Login reason
Powiadomienia
Polityki
Funkcjonalność protokołów
Uprawnienia
Uprawnieni użytkownicy
Powiązania obiektu
user0
Konta
Gniazda nasłuchiwania
Polityka czasu dostępu
Włącz politykę czasową
Pokaż hasło
00:00
Poniedziałek
Wtorek
Środa
Czwartek
Piątek
Sobota
Niedziela

16.2.2 Serwer



16.3 Migracja modelu danych wersji 2.2 do 3.0

Ten rozdział opisuje mechanizmy migracji obiektów modelu danych Wheel Fudo PAM 2.2 do wersji 3.0.

Informacja: W przypadku niepowodzenia aktualizacji Wheel Fudo PAM do wersji 3.0, nieprawidłowości, które uniemożliwiły prawidłowe zakończenie migracji danych, zostaną zapisane w dzienniku zdarzeń.

16.3.1 Serwer

Serwery o tym samym adresie IP i numerze portu zostają zastąpione jednym obiektem. Nazwa powstałego obiektu stanowi konkatenację nazw serwerów, posortowanych rosnąco i oddzielonych przecinkiem.

Ostrzeżenie: Jeżeli dwa serwery o tym samym adresie docelowym i porcie mają przypisane różne protokoły, opisy, ustawienia zewnętrznego repozytorium haseł, poziom bezpieczeństwa RDP, ustawienia HTTP, ustawienia TLS, certyfikaty lub klucze publiczne, aktualizacja nie powiedzie się.

16.3.2 Sejf (dawniej *połączenie*)

- Połączenie anonimowe staje się obiektem typu sejf, który może zostać usunięty.
- Dla każdego bastionu (tj. grupy serwerów w trybie *bastion*, przypisanych do tego samego bastionu) z danego połączenia zostaje utworzony obiekt typu *sejf* o nazwie `<nazwa połączenia> > <nazwa bastionu>`.
- Dla każdego serwera w trybie *gateway*, *proxy* lub *transparent* z danego połączenia zostaje utworzony obiekt typu *sejf* o nazwie `<nazwa połączenia> > <nazwa serwera>`.
- Sejf utworzony na podstawie połączenia dziedziczy po nim jego prawa dostępu, uprawnienia, ustawienia powiadomień, ustawienia protokołów, a także mapowania LDAP.
- Ustawienia OCR, nagrywania sesji i retencji danych sesji nie są dziedziczone po połączeniu, ale znajdują swoje odzwierciedlenie w obiekcie typu *konto*.
- Polityki czasowe połączeń odwzorowane są na dostęp użytkownika do sejfu utworzonego na podstawie danego połączenia.
- Polityki danych logowania połączenia są odwzorowane na polityki sejfu.

16.3.3 Konto (dawniej *dane logowania*)

Dla każdych danych logowania z połączenia powstaje obiekt typu *konto*.

- Jeżeli dane logowania zawierają login to konto dostaje typ regular. Nazwa takiego konta to `<login> @ <ostateczna nazwa serwera>`.
- Jeżeli dane logowania nie zawierają loginu i dotyczą połączenia nieanonimowego, to konto dostaje typ forward. Nazwa takiego konta to `forward for <ostateczna nazwa serwera>`.
- Jeżeli dane logowania nie zawierają loginu i dotyczą połączenia anonimowego to konto będące wynikiem migracji danych będzie typu *anonymous*. Nazwa takiego konta to `anonymous for <ostateczna nazwa serwera>`.
- Zduplikowane dane logowania zostają zastąpione jednym kontem. Uprawnienia do zarządzania obiektem, ustawienia OCR, ustawienia nagrywania sesji, ustawienia retencji danych sesji konta zostają odziedziczone po połączeniu, z którego pochodziły dane logowania, na podstawie których konto zostało utworzone.

Ostrzeżenie: Jeżeli dane logowania zawierają login, ale nie zawierają sekretu, tzn. zastępują login, ale nie przekazują sekretu to aktualizacja zakończy się niepowodzeniem.

16.3.4 Gniazdo nasłuchiwania (dawniej *bastion* lub część serwera)

- Dla każdego serwera w trybie *proxy*, *transparent* lub *gateway* zostaje utworzone gniazdo nasłuchiwania z tym samym trybem.
- Obiekt dziedziczy po serwerze uprawnienia, ustawienia TLS i poziom bezpieczeństwa RDP.
- Komunikat i klucze prywatne przechodzą na gniazdo.

- Obiekt zostaje przypisany do wszystkich sejfów, które zostały utworzone na podstawie połączeń, do których należał serwer, z którego powstało gniazdo.
- Bastion staje się gniazdem nasłuchiwania w trybie *bastion*. Prawa dostępu i ustawienia bastionu przechodzą na gniazdo. Gniazdo zostaje dodane do wszystkich sejfów, które zostały utworzone na podstawie połączeń, do których należał przynajmniej jeden serwer z bastionu, z którego powstało gniazdo.

16.3.5 Sesje

- Dla każdej sesji zaktualizowany jest identyfikator sejfu, serwera i konta. Jeżeli sesja dotyczyła serwera, który nie działał w trybie bastion to również ustawiony jest identyfikator gniazda nasłuchiwania.

16.4 Obsługa wspieranych protokołów

Ten rozdział zawiera szczegółowy opis zakresu w jakim wspierane są obsługiwane protokoły.

16.4.1 Citrix StoreFront (HTTP)

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak wsparcia dla trybu bastion wynika z ograniczeń protokołu. Citrix StoreFront sam w sobie daje dostęp do bastionu maszyn. Użytkownik logując się do Citrix StoreFront może wybrać w swoim panelu maszynę, z którą chce się połączyć za pomocą protokołu ICA.

16.4.2 HTTP

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak monitorowania ściąganych zasobów z zewnętrznych.
- Brak śledzenia przekierowań.

16.4.3 ICA

Wspierane tryby połączenia:

- Bastion (możliwość wpisania konta lub serwera docelowego w pliku ICA),
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Citrix Receiver.

16.4.4 Modbus

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

16.4.5 MS SQL (TDS)

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqsh.

16.4.6 MySQL

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Oficjalny klient MySQL,

- Biblioteki PyMySQL dla Pythona.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.

16.4.7 Oracle

Protokół Oracle jest zamkniętym protokołem, którego implementacja wymaga reverse engineeringu, co ogranicza możliwości techniczne w zakresie rozbudowy i poprawy ewentualnych problemów.

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- SQLDeveloper 4.1.3.20.78,
- SQL*Plus: Release 11.2.0.4.0 Production.

Uwagi:

- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.
- Odtwarzacz uwzględnia tylko zapytania klientów (w podglądzie sesji nie wyświetlamy odpowiedzi serwera).
- Wspierane wersje 10 i 11.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

16.4.8 RDP

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Wszystkie oficjalne Microsoft – Windows, macOS,
- FreeRDP 2.0 i nowsze.

Uwagi:

- W przypadku uwierzytelnienia użytkowników Fudo przed AD (lub innym zewnętrznym źródłem) tryb bezpieczeństwa TLS+NLA (Network Level Authentication) nie jest obsługiwany; zamiast niego stosowany jest tryb TLS. Wsparcie dla trybu NLA po stronie serwera docelowego jest zapewnione.
- Trwają prace nad wsparciem dla mechanizmu RemoteApp.

16.4.9 SSH

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wybrane wspierane funkcje:

- Multipleksowanie połączeń,
- SCP,
- SFTP – brak podglądu sesji i plików SFTP w Fudo,
- Przekierowanie portów.

Uwagi:

- Brak możliwości przekazywania (forwardowania) klucza SSH.

16.4.10 Telnet

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

16.4.11 Telnet 3270

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- c3270.

16.4.12 Telnet 5250

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.
- Brak możliwości dołączenia do sesji.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- tn5250.

16.4.13 VNC

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- TightVNC,
- RealVNC.

16.4.14 X11

Protokół X11 wspierany jest w ramach protokołu SSH.

Wspierane serwery:

- Xorg,
- Xming,

- XQuartz.

ROZDZIAŁ 17

AAPM (Application to Application Password Manager)

17.1 Informacje ogólne

Moduł AAPM umożliwia bezpieczne przesyłanie haseł pomiędzy aplikacjami.

Kluczowym elementem modułu AAPM jest skrypt `fudopv`. Skrypt jest instalowany na serwerze aplikacyjnym i komunikuje się z modułem Secret Manager w celu pobrania haseł dostępu.

W komunikacji z Wheel Fudo PAM, skrypt `fudopv` jest uwierzytelniany na podstawie adresu IP oraz hasła jednorazowego/statycznego.

Moduł AAPM wspiera systemy operacyjne Microsoft Windows oraz rodziny systemów BSD i Linux.

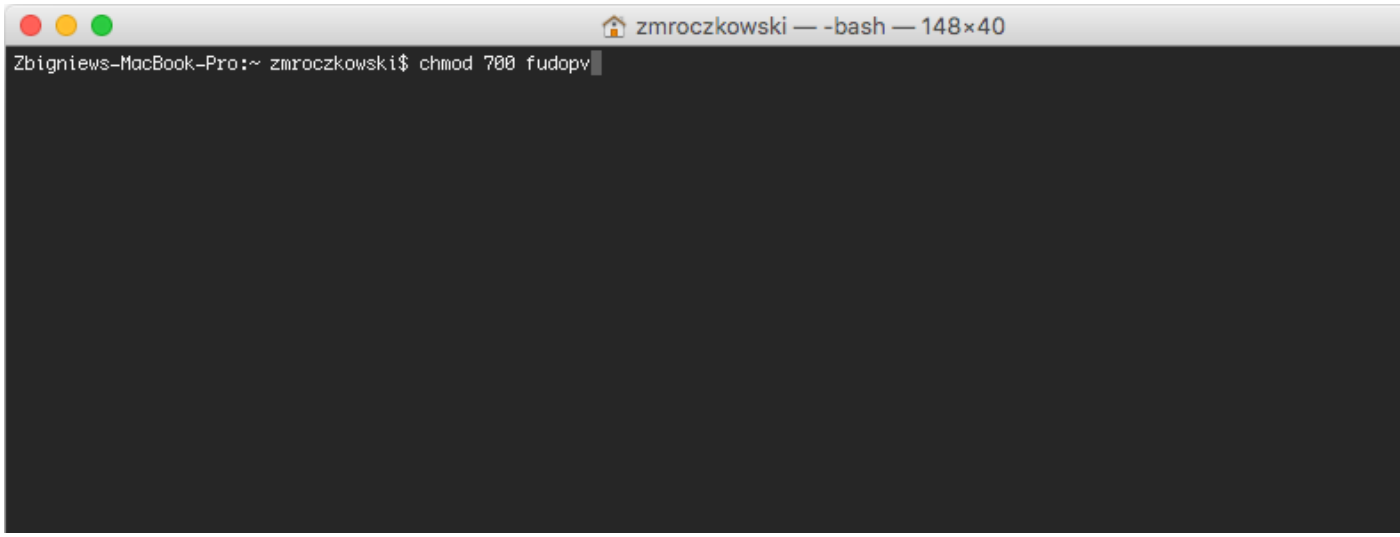
17.2 *fudopv*

Parametry wywołania

```
fudopv [<opcje>] <komenda> [<parametry>]
```

Komenda/opcja/parametr	Opis
Komendy	
`getcert`	Pobierz certyfikat SSL Wheel Fudo PAM.
`getpass` <typ> <konto>	Pobierz hasło do wybranego konta. typ: • `direct` - połączenie bezpośrednie, niemonitorowane; • `fudo` - połączenie monitorowane przez moduł PSM
Opcje	
`-c <ścieżka>`	Użyj pliku konfiguracyjnego znajdującego się we wskazanej lokalizacji.
`--cfg <ścieżka>`	
`-h, --help`	Wyświetl listę opcji i parametrów wywołania skryptu.

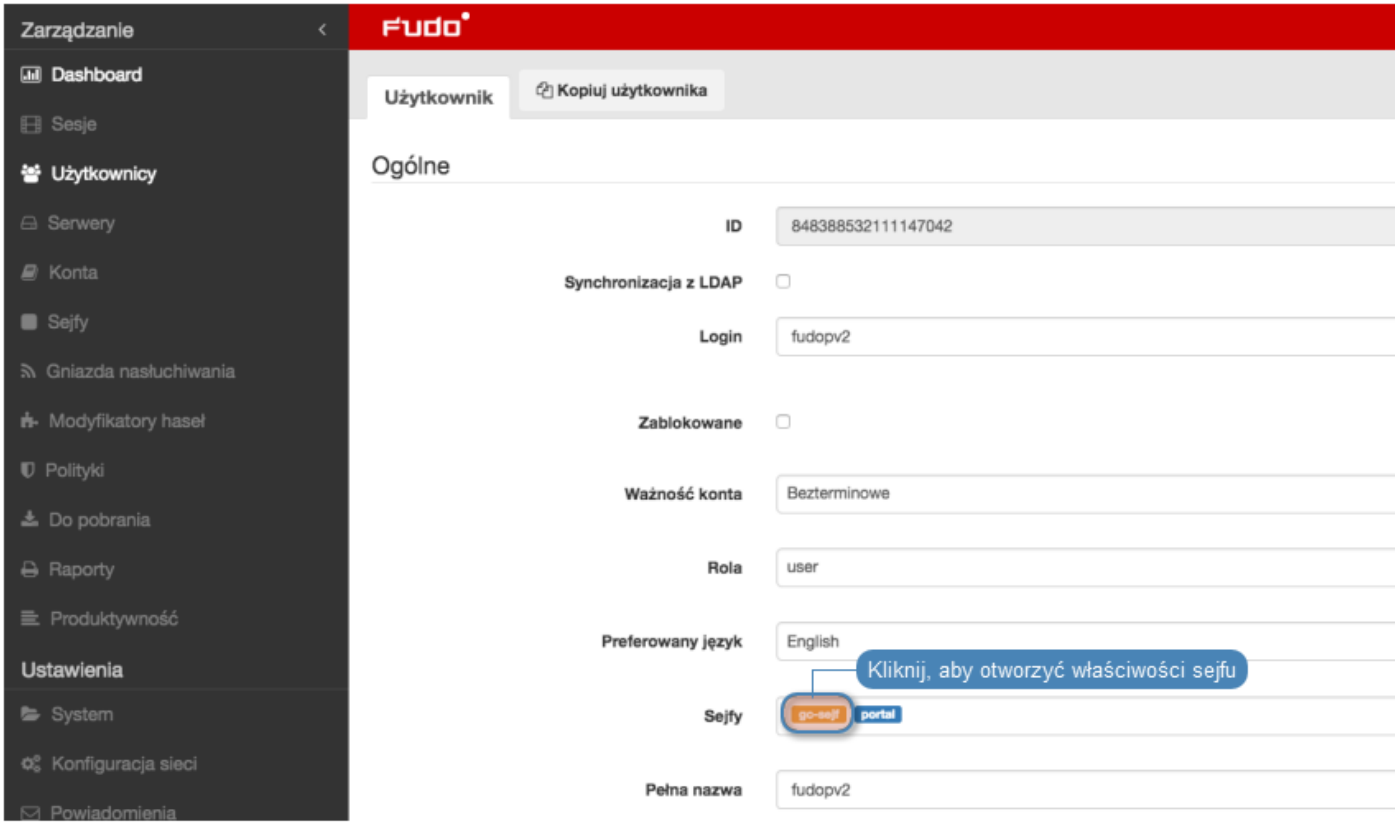
1. Umieść na serwerze skrypt `fudopv` i nadaj mu prawa wykonywalności.



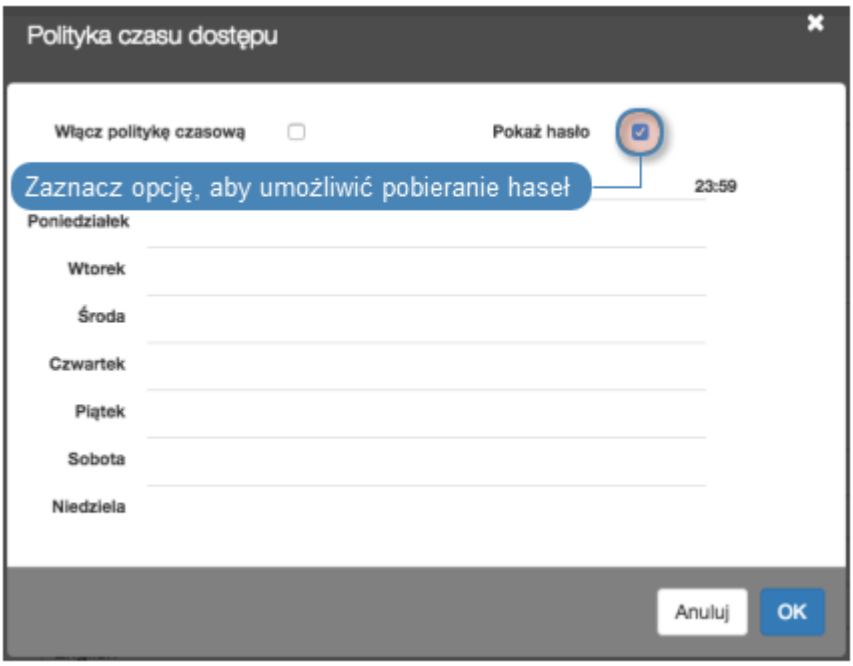
2. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
3. Stwórz konto użytkownika o roli `user`, uwierzytelnianego hasłem statycznym lub jednorazowym i dodanym adresem IP serwera w sekcji *API*.

Informacja:

- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+Dodaj*.
- Wprowadź nazwę użytkownika.
- Określ termin ważności konta.
- Z listy rozwijalnej *Rola*, wybierz `user`.
- Przypisz użytkownikowi sejf i kliknij obiekt, aby wywołać jego właściwości.

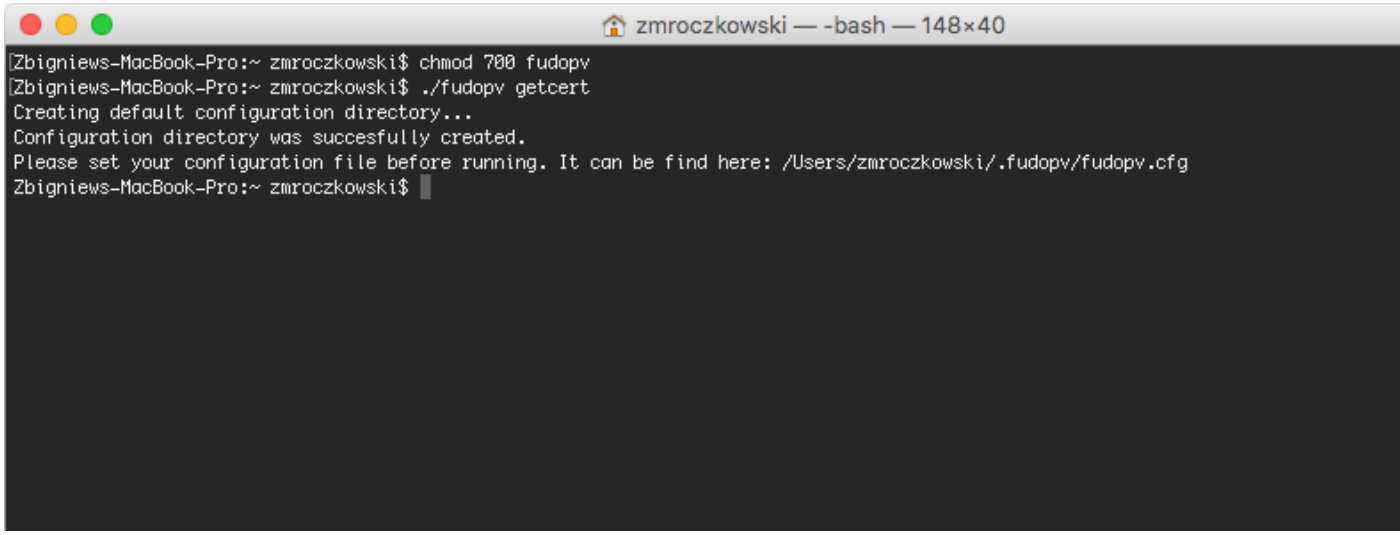


- Zaznacz opcję *Pokaż hasło*.



- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `Hasło` lub `Hasło jednorazowe`.
- Dla uwierzytelnienia hasłem, wprowadź hasło w polach *Hasło* i *Powtórz hasło*.
- W sekcji *API*, kliknij ikonę + i wpisz adres IP serwera, na którym uruchamiany będzie skrypt `fudopv`.
- Kliknij *Zapisz*.

4. Wykonaj komendę `fudopv getcert`, aby zainicjować konfigurację narzędzia.



5. Otwórz plik `fudopv.cfg`, aby skonfigurować skrypt pobierania haseł.

Sekcja	Opis
`[FUDO]`	
`address`	Adres IP Wheel Fudo PAM.
`cert_path`	Ścieżka pliku z certyfikatem SSL Wheel Fudo PAM.
`[CONN]`	
`bind_ip`	Adres IP serwera, na którym uruchamiany jest skrypt `fudopv`. Adres IP musi być taki sam jak podany w sekcji *API* w konfiguracji użytkownika.
`[AUTH]`	
`username`	Nazwa obiektu użytkownika zdefiniowanego w kroku 3.
`otp`	Ścieżka pliku z hasłem jednorazowym, w przypadku gdy użytkownik jest uwierzytelniany hasłem jednorazowym.
`secret`	Lokalizacja pliku z hasłem statycznym, w przypadku uwirzytelnienia hasłem.

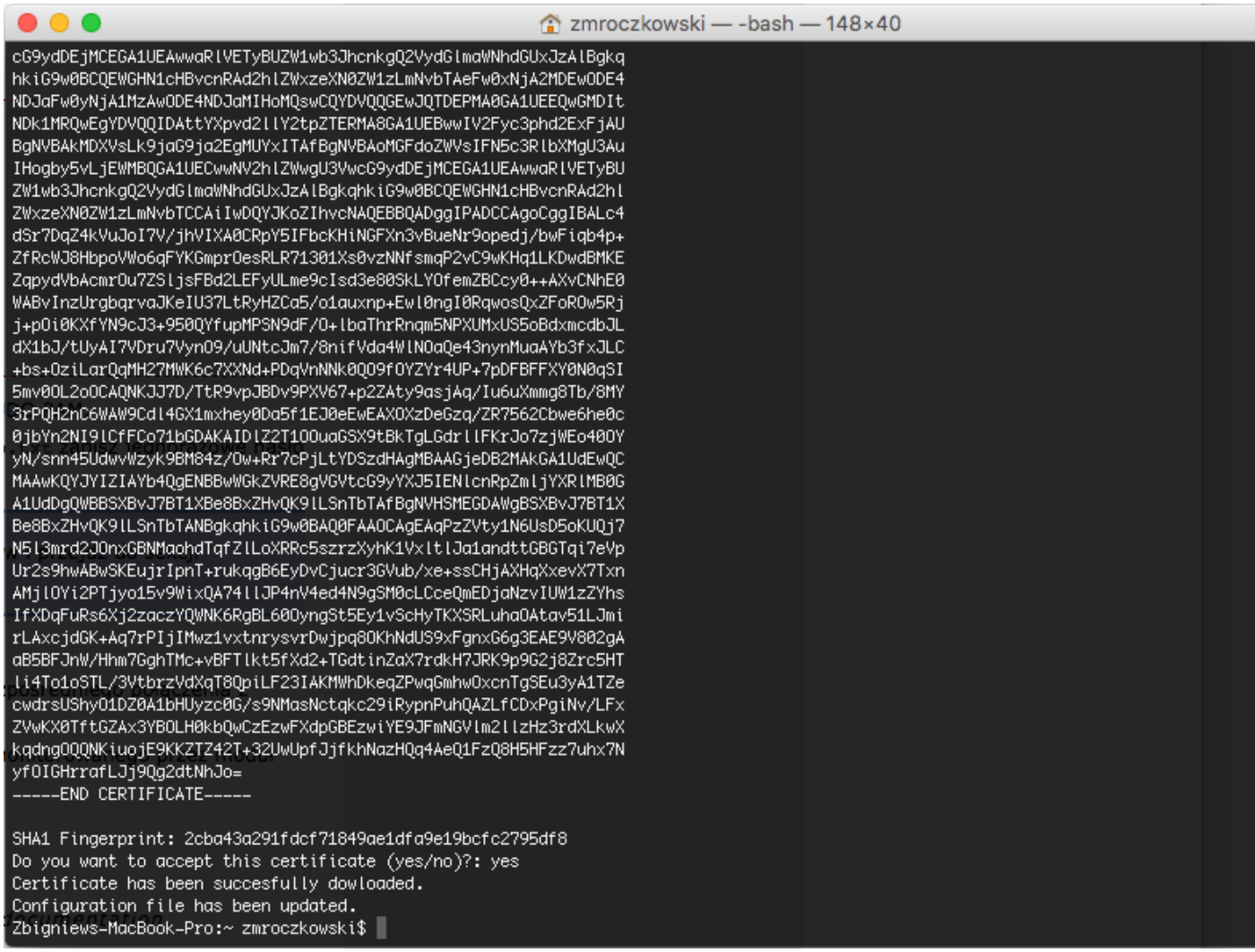
Informacja:

- W sekcji `[FUDO]`, w linii `address`, wprowadź adres IP Wheel Fudo PAM.
- Linię `cert_path` pozostaw bez zmian, zostanie ona uzupełniona automatycznie przy okazji poprawnego wykonania komendy `fudopv getcert`.
- W sekcji `[CONN]`, odkomentuj linię `bind_ip` i wprowadź adres IP serwera, na którym wykonywany jest skrypt `fudopv`.
- W sekcji `[AUTH]`, w linii `username`, uzupełnij nazwę konta obiektu użytkownik, stworzonego w kroku 3.
- W zależności od wybranego sposobu uwierzytelnienia, zakomentuj linię odpowiadającą wybranej metodzie.

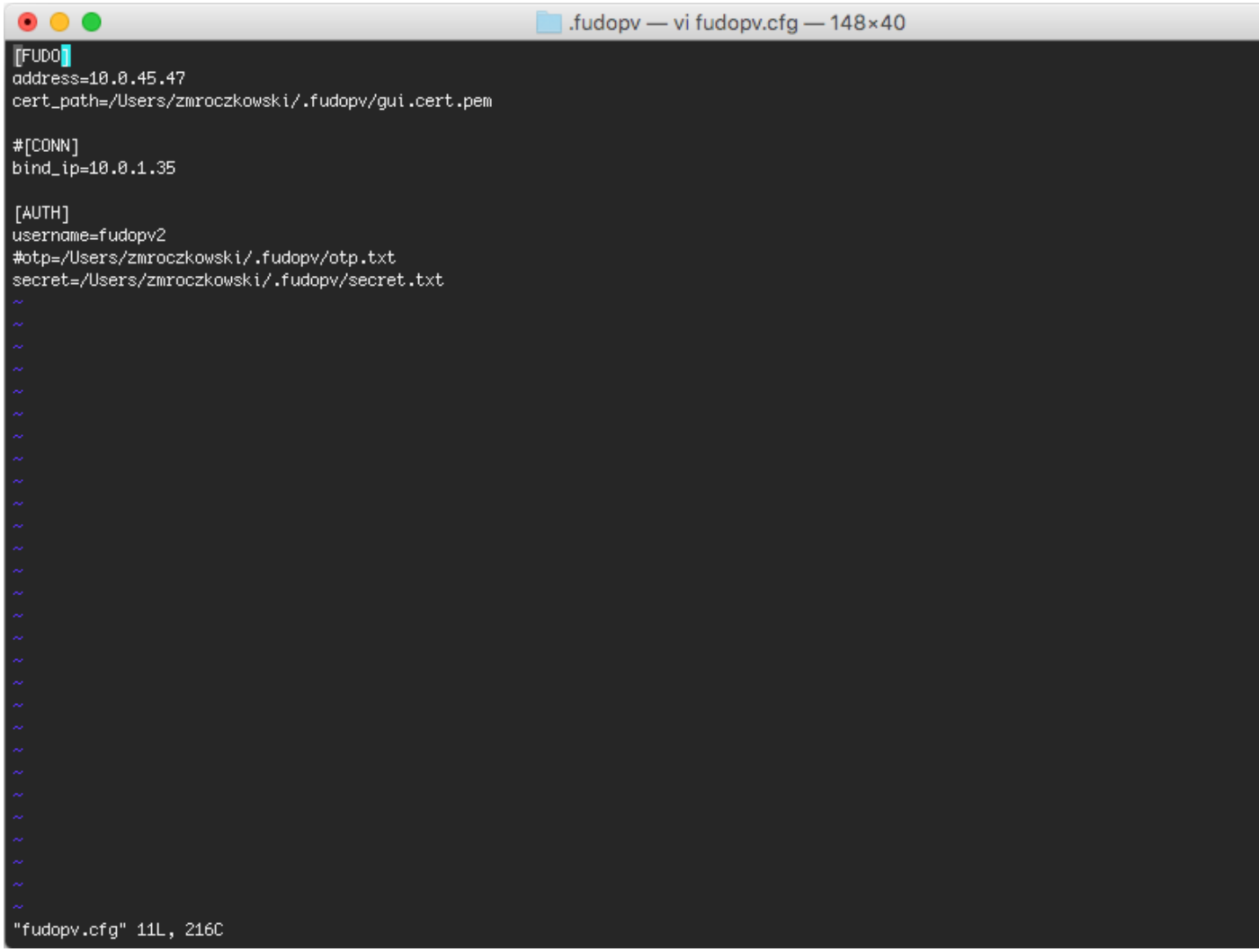
Na przykład:

```
[FUDO]
address=10.0.0.8.61
cert_path=<CERT_PATH>

#[CONN]
bind_ip=10.0.0.8.11

[AUTH]
username=fudopv
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
```

6. Wykonaj komendę `fudopv getcert`, aby pobrać certyfikat Wheel Fudo PAM.

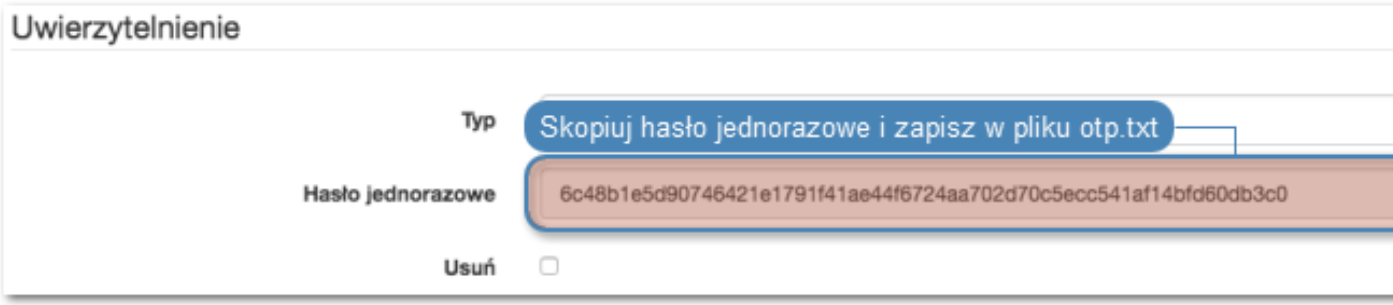


Informacja: Po prawidłowym wykonaniu komendy, ścieżka certyfikatu w pliku konfiguracyjnym zostanie automatycznie uzupełniona.



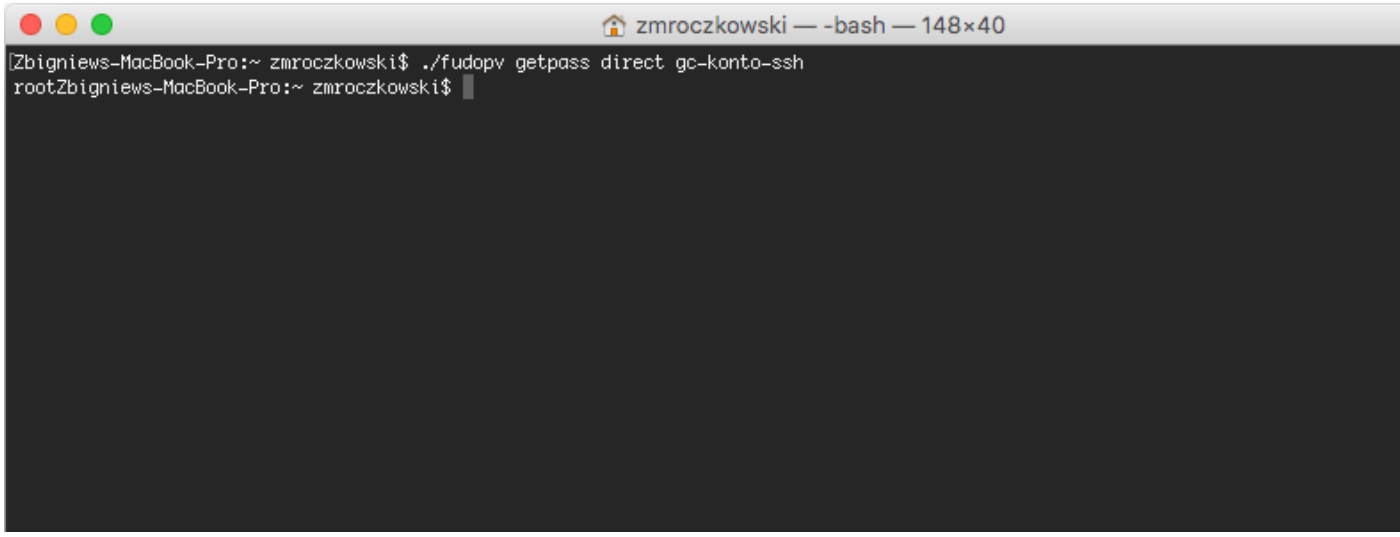
7. W pliku `secret.txt`, zapisz hasło konta użytkownika; lub w pliku `otp.txt` zapisz jednorazowe hasło dostępu.

Informacja: Aby uzyskać hasło jednorazowe, wybierz użytkownika z listy obiektów i przejdź do sekcji *Uwierzytelnienie*.

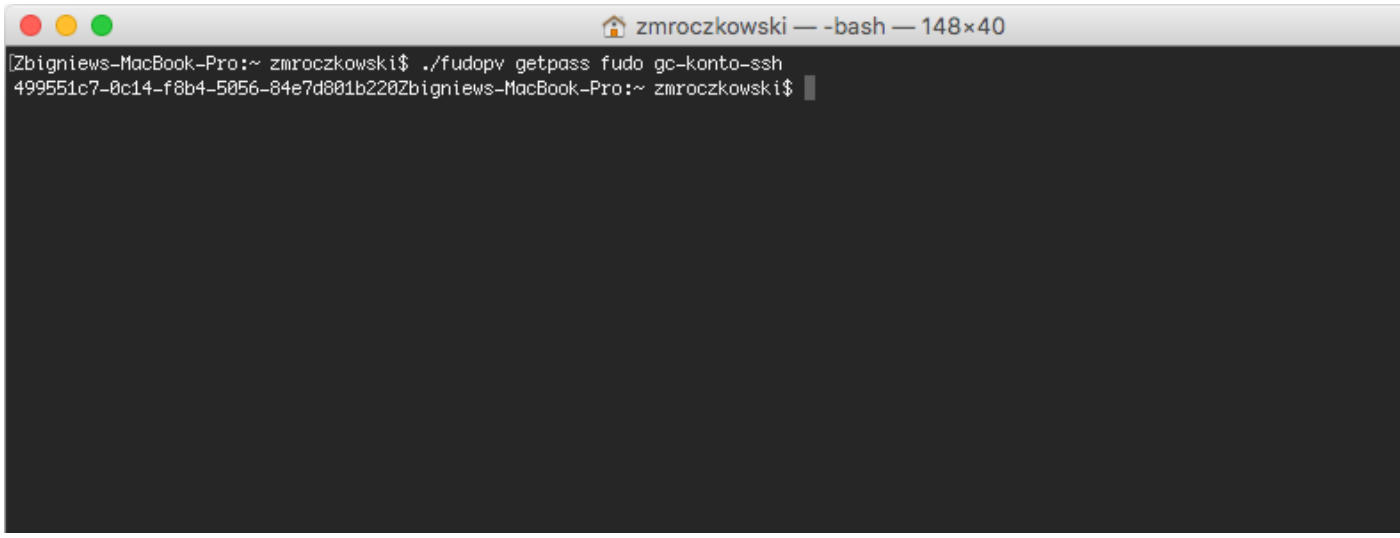


8. Wykonaj komendę:

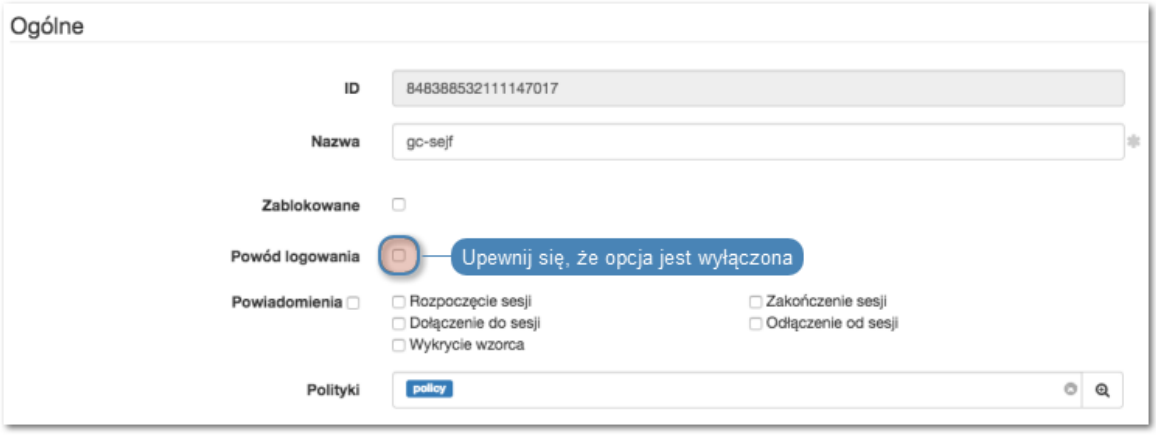
- `fudopv getpass direct <nazwa_konta>`, aby pobrać hasło do nawiązania bezpośredniego połączenia z serwerem.



- `fudopv getpass fudo <nazwa_konta>`, aby pobrać hasło do nawiązania połączenia monitorowanego przez moduł PSM.



Ostrzeżenie: Prawidłowe działanie skryptu `fudopv` wymaga wyłączenia we właściwościach sejfu, opcji wymuszania na użytkowniku podania powodu logowania przy nawiązywaniu połączenia z serwerem docelowym.



17.3 Interfejs API

Interfejs API modułu AAPM jest opisany w dokumencie *Wheel Fudo PAM - API documentation*.

Tematy pokrewne:

- *Model danych*
- *Opis systemu*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

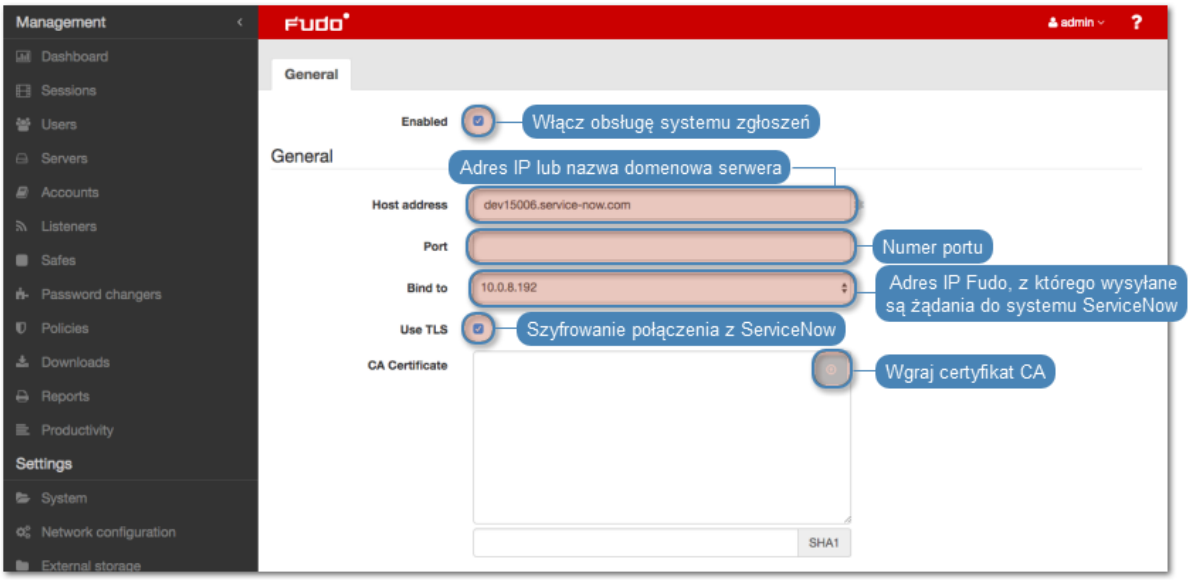
ROZDZIAŁ 18

Service Now

18.1 Konfiguracja

Aby skonfigurować system obsługi zgłoszeń *ServiceNow*, postępuj zgodnie z poniższą instrukcją.

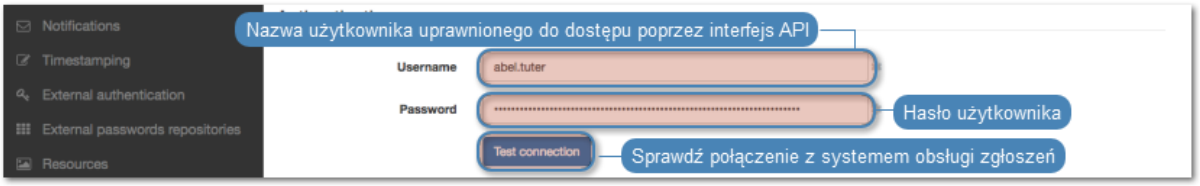
1. Wybierz z lewego menu *Ustawienia* > *System zgłoszeń*.
2. Zaznacz opcję *Włączone*.
3. W sekcji *Ogólne*, uzupełnij adres IP lub nazwę hosta oraz numer portu, na którym nasłuchuje interfejs API systemu *ServiceNow*.
4. Zaznacz opcję *Użyj szyfrowania TLS* i wgraj certyfikat CA, aby komunikacja z systemem zgłoszeń odbywała się w tunelu szyfrowanym.



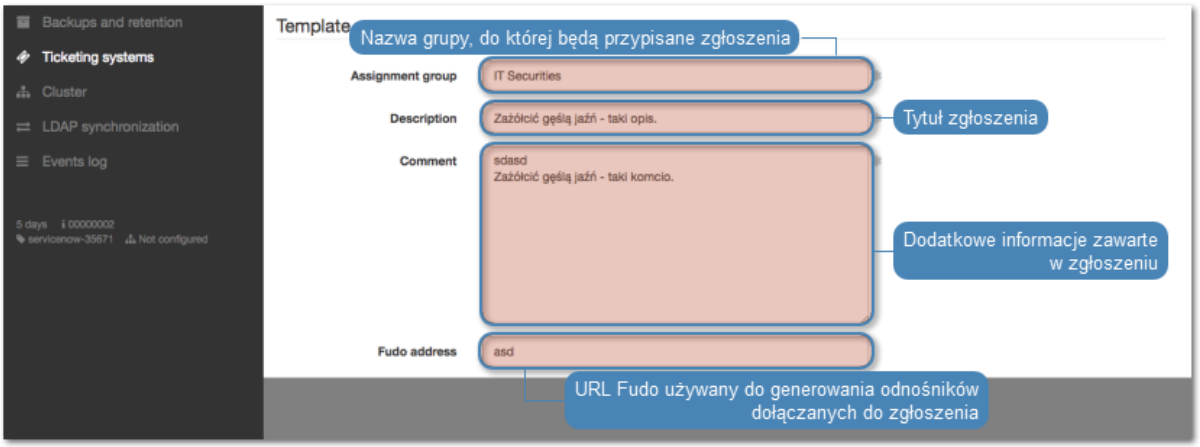
5. Określ z którego adresu IP wysyłane będą żądania do systemu *ServiceNow*.

6. W sekcji *Uwierzytelnienie*, wprowadź dane uwierzytelniające użytkownika uprawnionego do dostępu do systemu *ServiceNow* poprzez wskazany interfejs API.

Informacja: Kliknij *Testuj połączenie*, aby zweryfikować prawidłowość parametrów konfiguracyjnych. Rezultatem testu będzie utworzenie zgłoszenia w systemie *ServiceNow*, w którym szablon będzie wypełniony zdefiniowanymi wartościami prefiksowanymi ciągiem `test_`.



7. W sekcji *Szablon*, w polu *Grupa przypisania*, wskaż grupę do której przypisywane będą zgłoszenia wygenerowane w systemie *ServiceNow*.
8. W polu *Opis*, wprowadź szablon tytułu zgłoszenia w systemie *ServiceNow*.
9. W polu *Komentarz*, wprowadź dodatkowe informacje przekazywane w zgłoszeniu do systemu *ServiceNow*.
10. W polu *URL Fudo* wprowadź ciąg znaków, stanowiący pierwszy człon odnośnika dołączanego do zgłoszenia.



11. Kliknij *Zapisz*.

Tematy pokrewne:

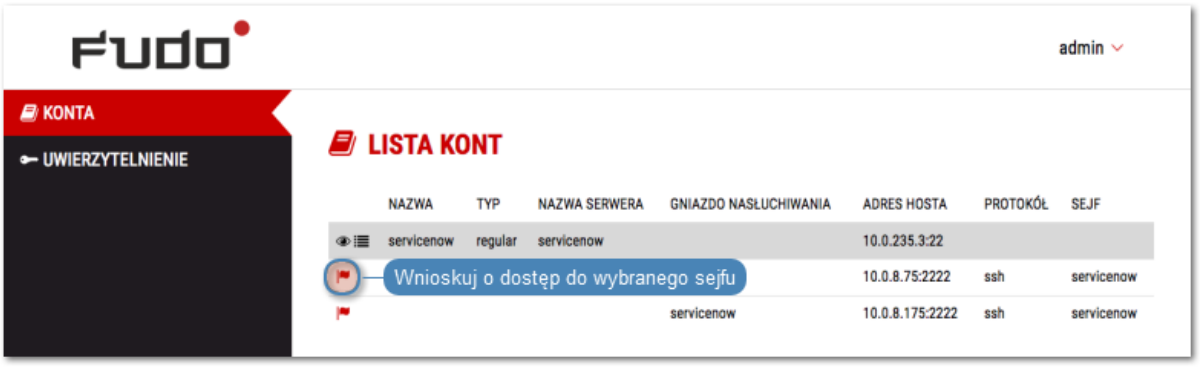
- *Wnioskowanie o dostęp do serwerów*
- *Przyznawanie dostępu*

18.2 Wnioskowanie o dostęp do serwerów

Informacja: Prawidłowe przetworzenie wniosku o przyznanie dostępu wymaga aby nazwy użytkowników w systemie Wheel Fudo PAM i *ServiceNow* były takie same.

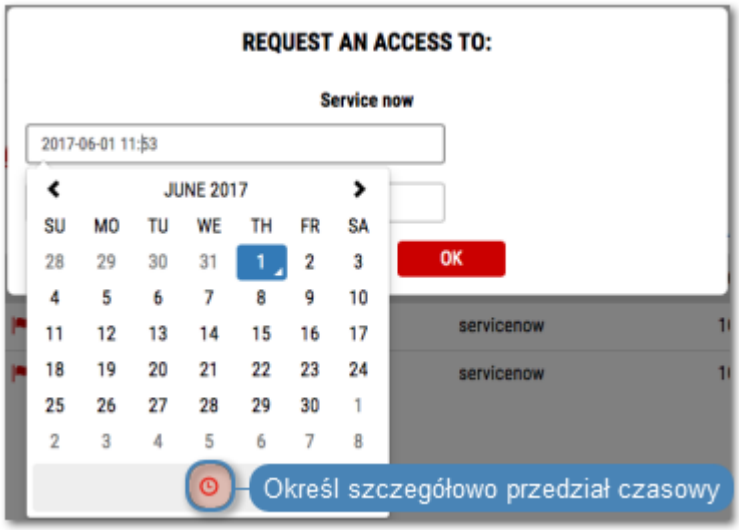
Aby stworzyć wniosek o dostęp do sejfu, postępuj zgodnie z poniższą instrukcją.

1. Zaloguj się do *Portalu Użytkownika*.
2. Odnajdź żądany sejf i kliknij .



3. Zdefiniuj przedział czasowy i kliknij *OK*.

Informacja: Kliknij ikonę , aby szczegółowo określić graniczne wartości ram czasowych.



Tematy pokrewne:

- *Konfiguracja*
- *Przyznawanie dostępu*

18.3 Przyznawanie dostępu

Aby przyznać użytkownikowi dostęp na podstawie zgłoszenia w systemie *ServiceNow*, postępuj zgodnie z poniższą instrukcją.

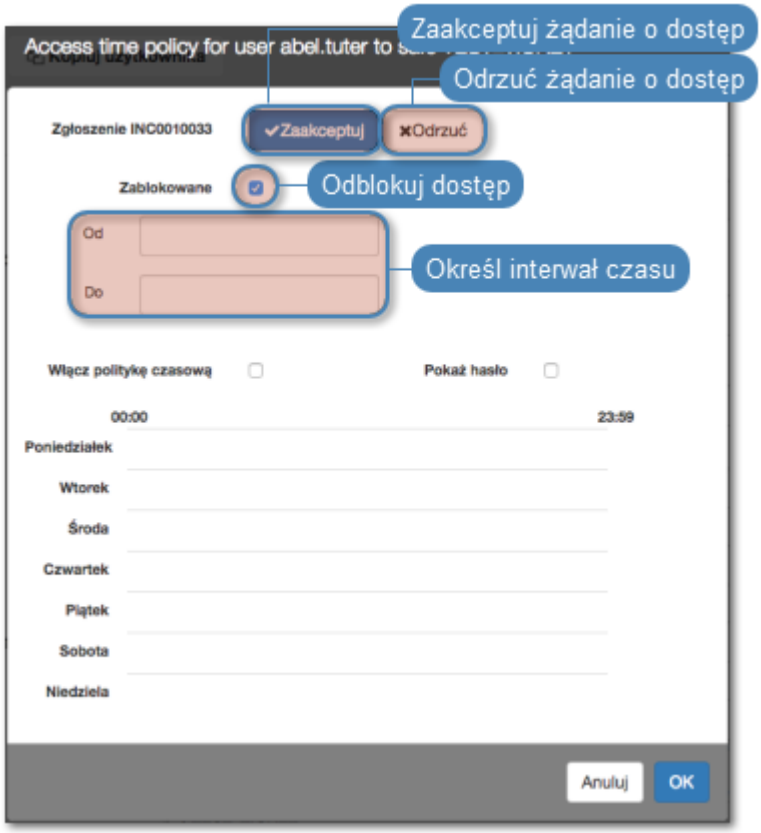
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj użytkownika, którego dotyczy zgłoszenie w systemie *ServiceNow* i kliknij jego definicję.

Informacja: Definicje użytkowników, którzy mają otwarte wnioski o dostęp, wyróżnione są ikoną  .

---

3. W polu *Sejfy*, odszukaj i kliknij obiekt, o dostęp do którego wnioskuje użytkownik.

4. Odznacz opcję *Zablokowane* i zdefiniuj przedział czasowy, w jakim użytkownik będzie mógł nawiązać połączenie z serwerami w ramach wybranego sejfu.
5. Kliknij *Zaakceptuj*.



Informacja: Okno zarządzania dostępem użytkownika do sejfu może być również wywołane z

poziomu widoku sejfu.

Tematy pokrewne:

- *Konfiguracja*
- *Wnioskowanie o dostęp do serwerów*

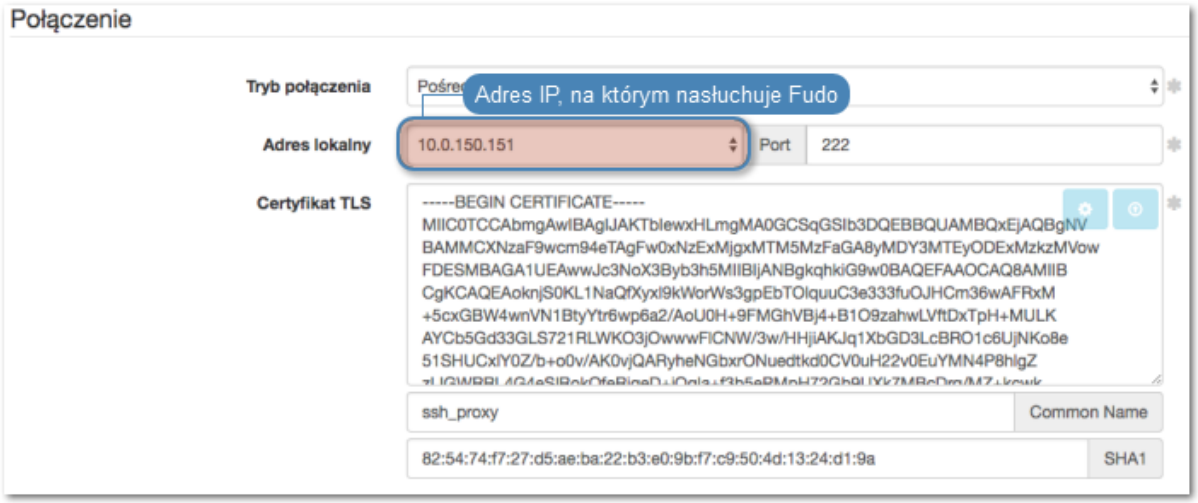
ROZDZIAŁ 19

Aplikacje klienckie

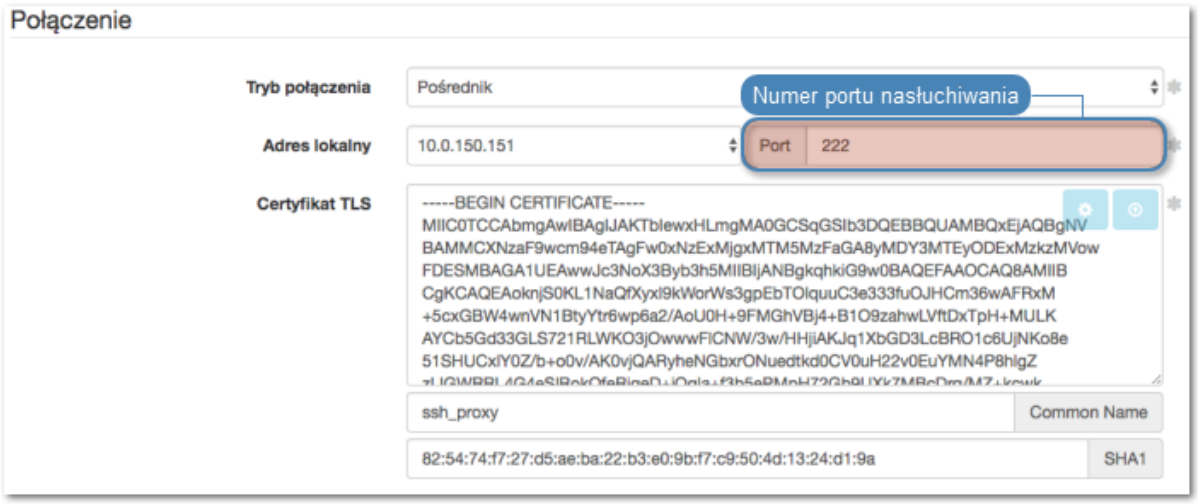
19.1 PuTTY

Połączenie *SSH* z serwerem monitorowanym poprzez gniazdo nasłuchiwania w trybie *proxy*.

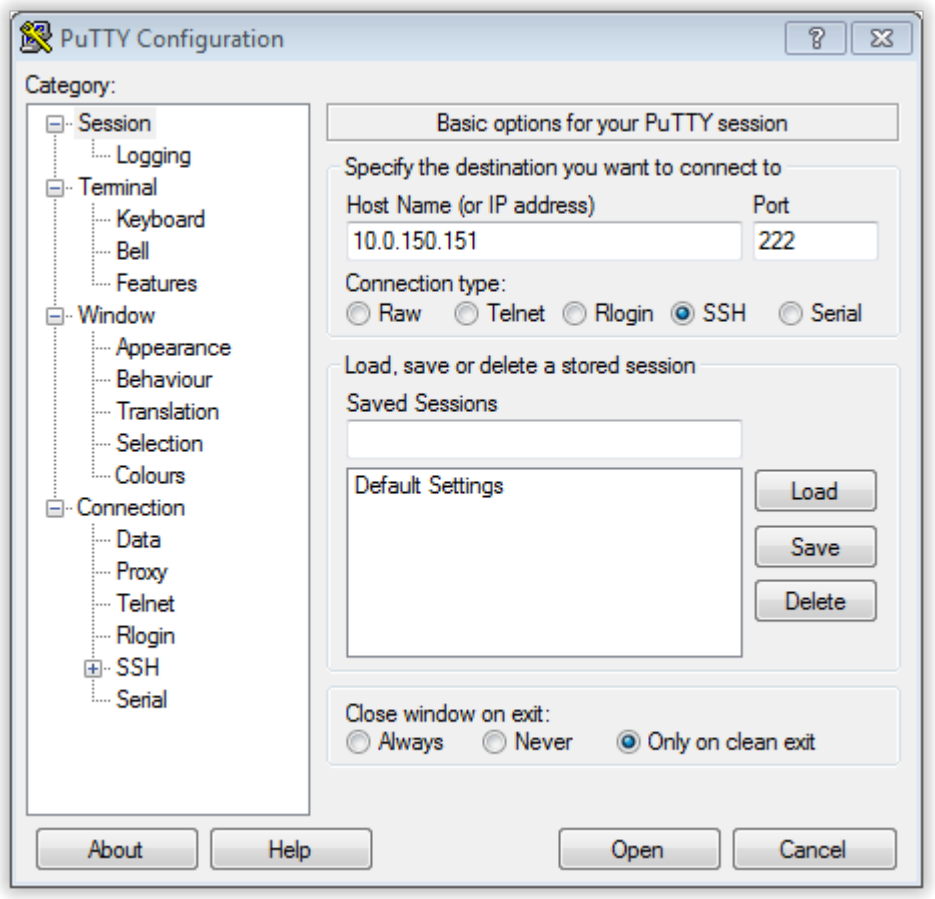
1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres IP zdefiniowany w sekcji *Połączenie*, w parametrze *Adres lokalny* gniazda nasłuchiwania.



3. Wprowadź numer portu zgodnie z definicją w obiekcie.

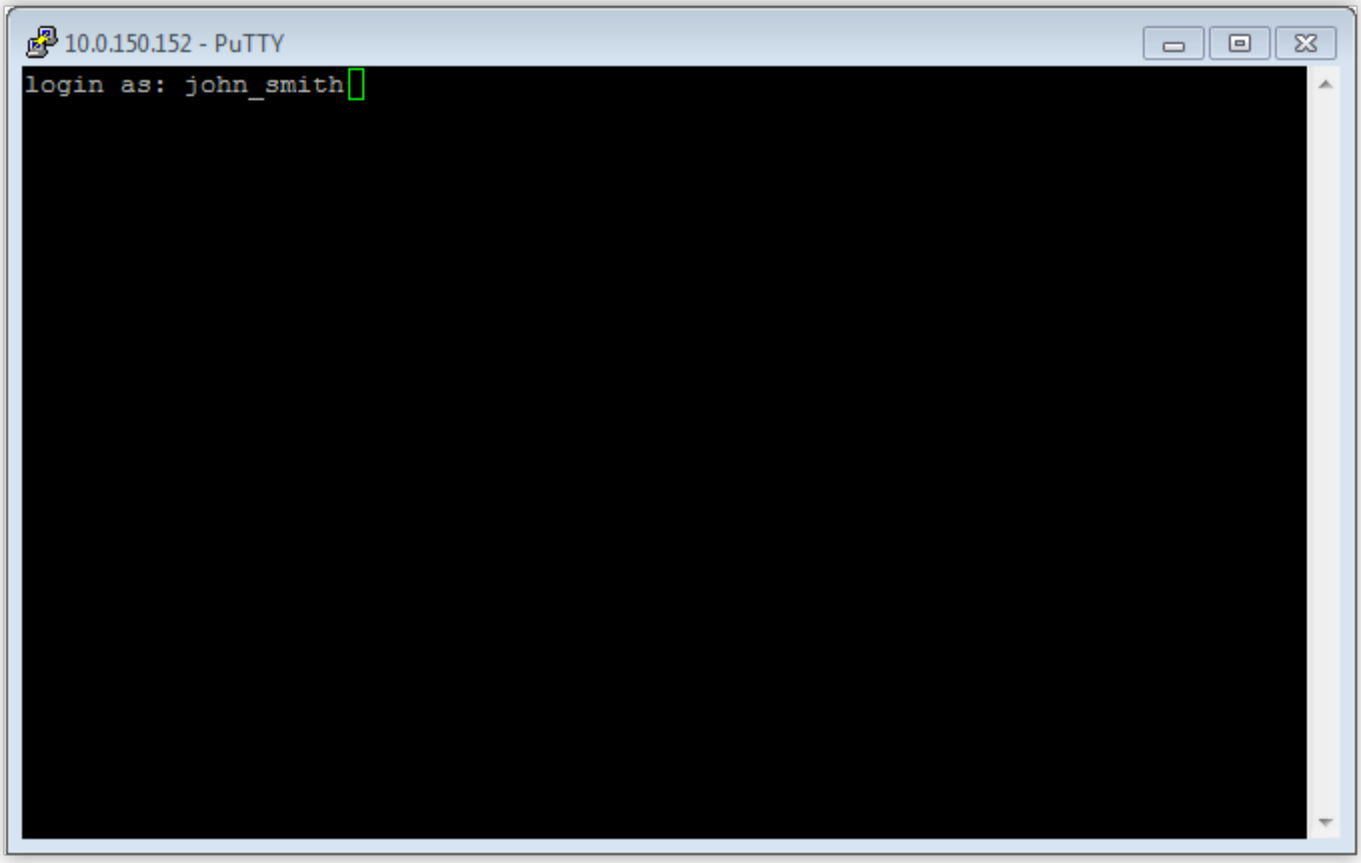


4. W polu wyboru typu połączenia (*Connection type*), wybierz `SSH`.



5. Kliknij *Open*.

6. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



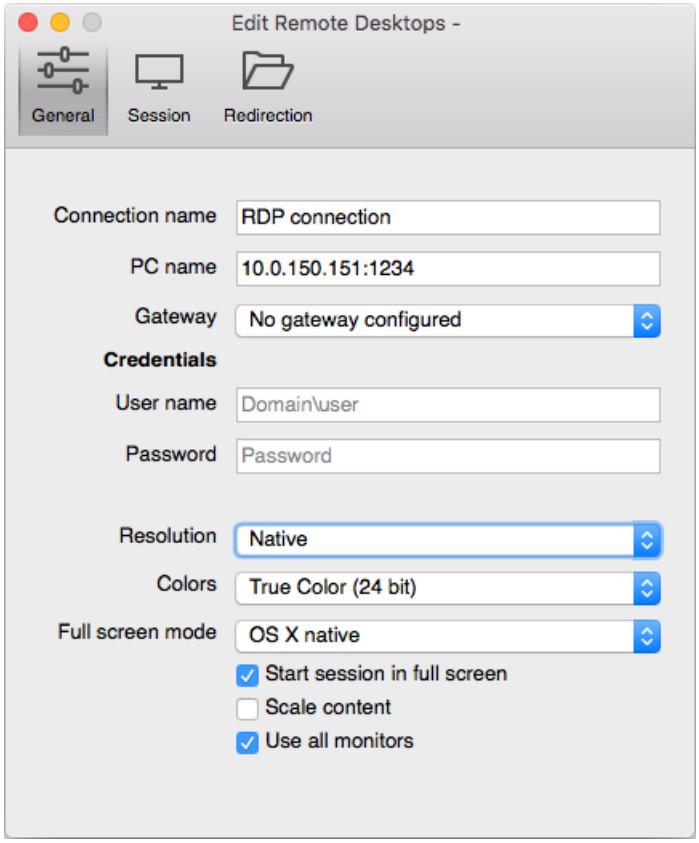
6. Wprowadź hasło użytkownika.

Tematy pokrewne:

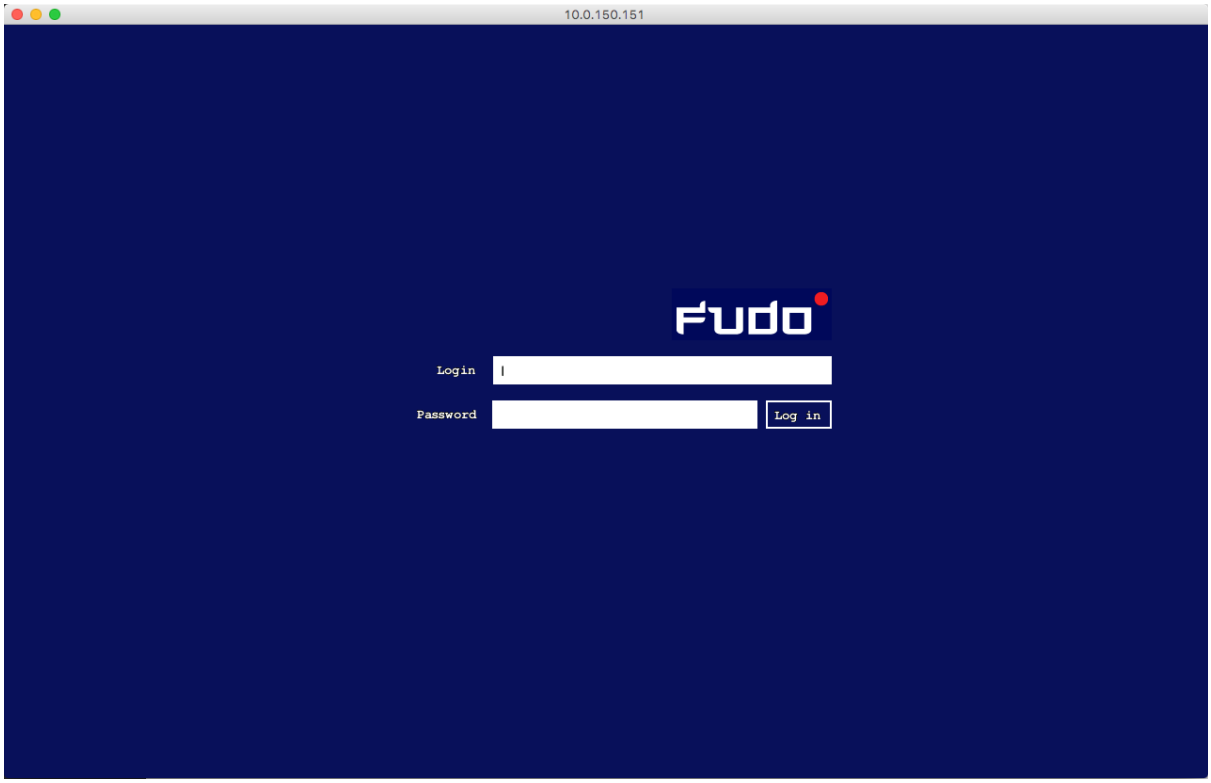
- *SSH*

19.2 Microsoft Remote Desktop

1. Uruchom klienta połączeń RDP.
2. W polu *PC name*, wprowadź adres IP oraz numer portu zdefiniowany w gnieździe nasłuchiwania.

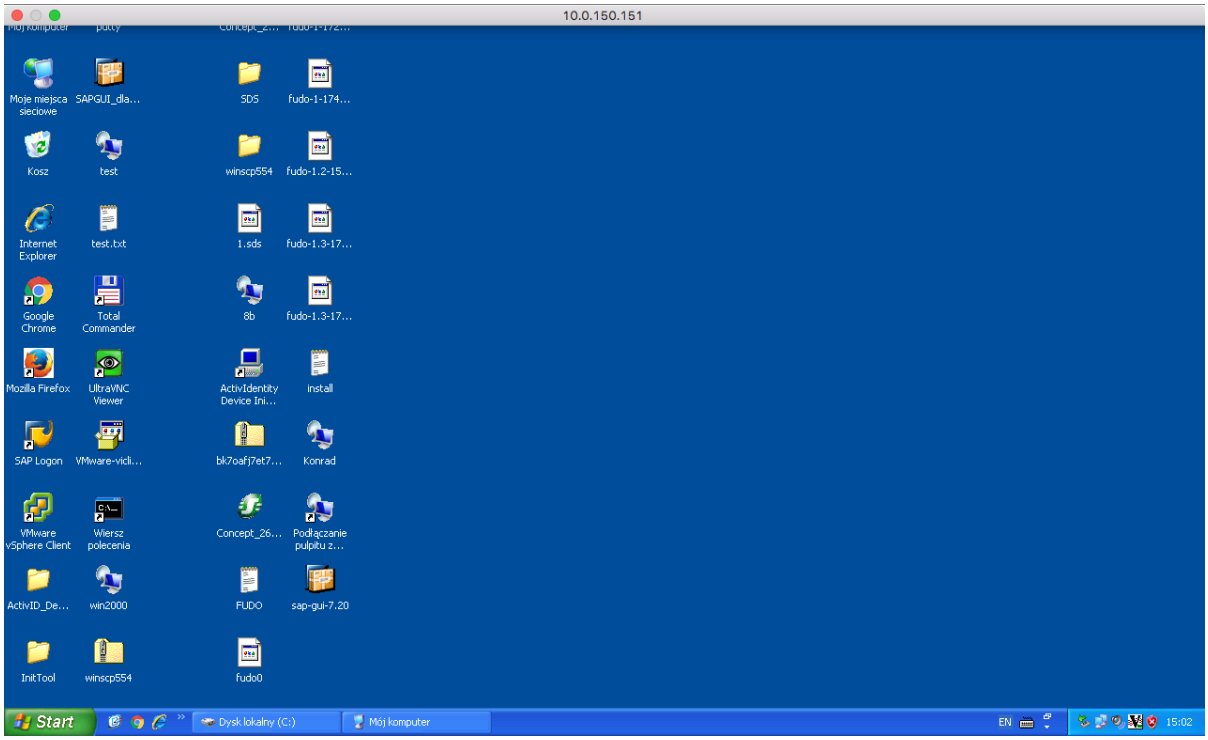


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: Wheel Fudo PAM pozwala na zastosowanie własnych ekranów logowania, braku dostępu i zakończenia sesji dla połączeń RDP i VNC. Więcej informacji na temat konfigurowania

własnych ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.

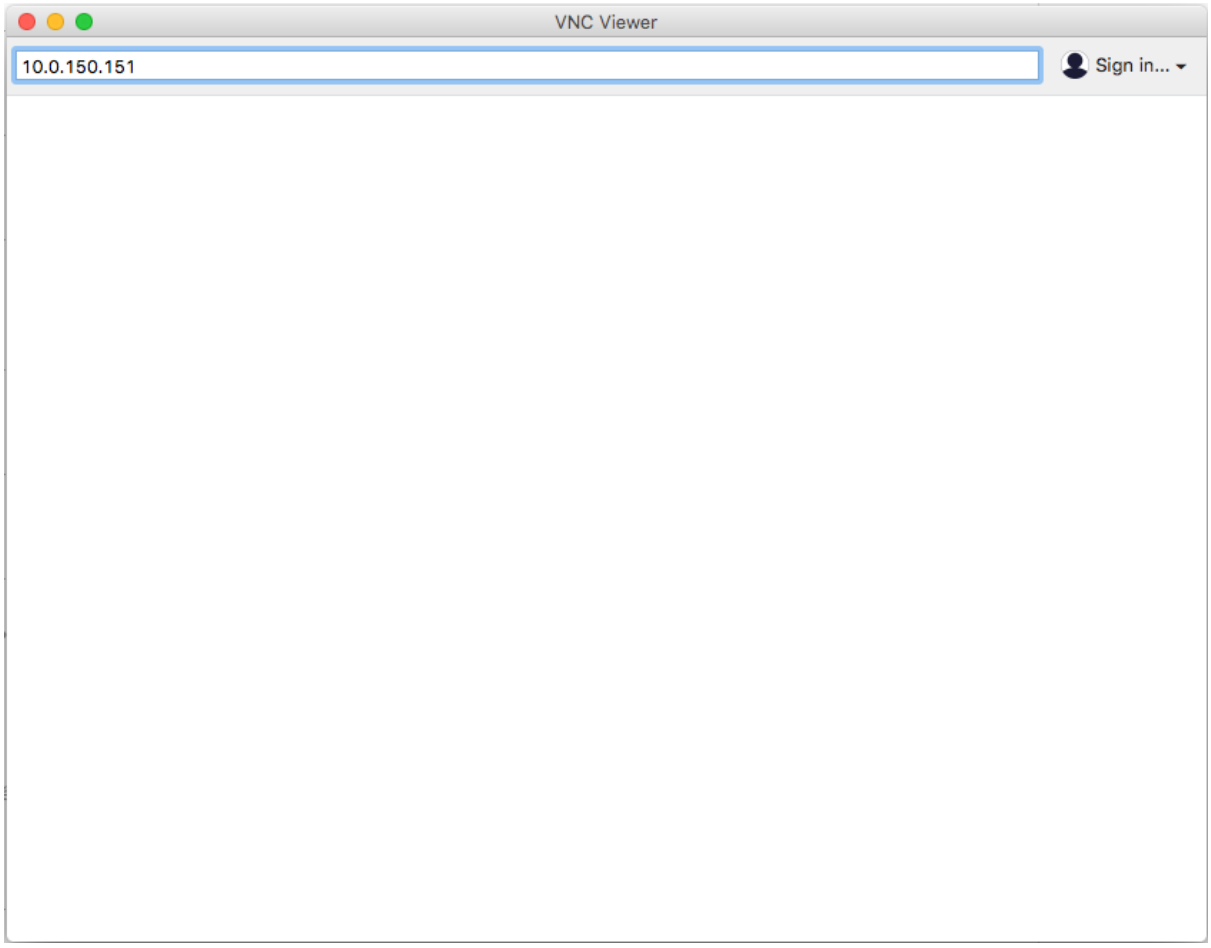


Tematy pokrewne:

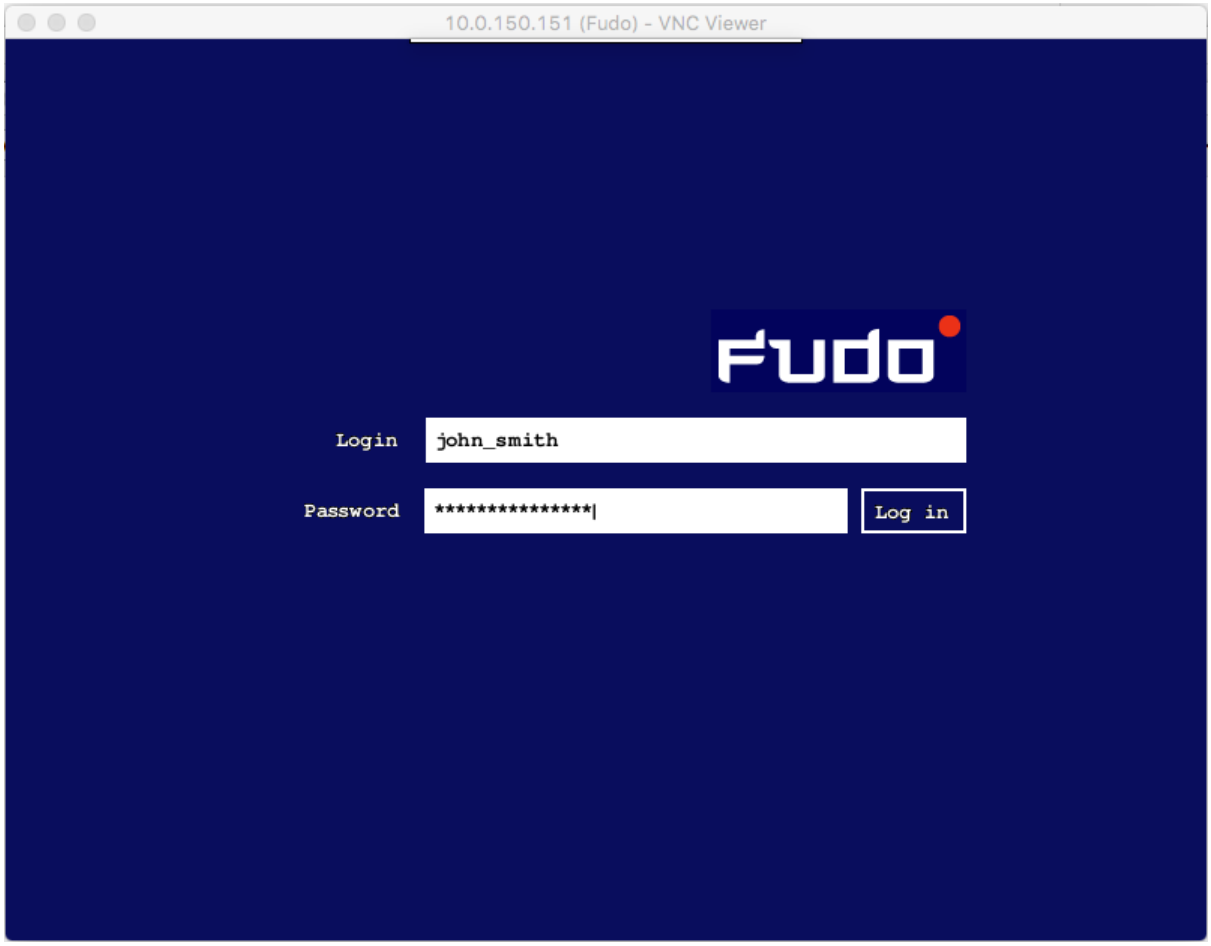
- *RDP*

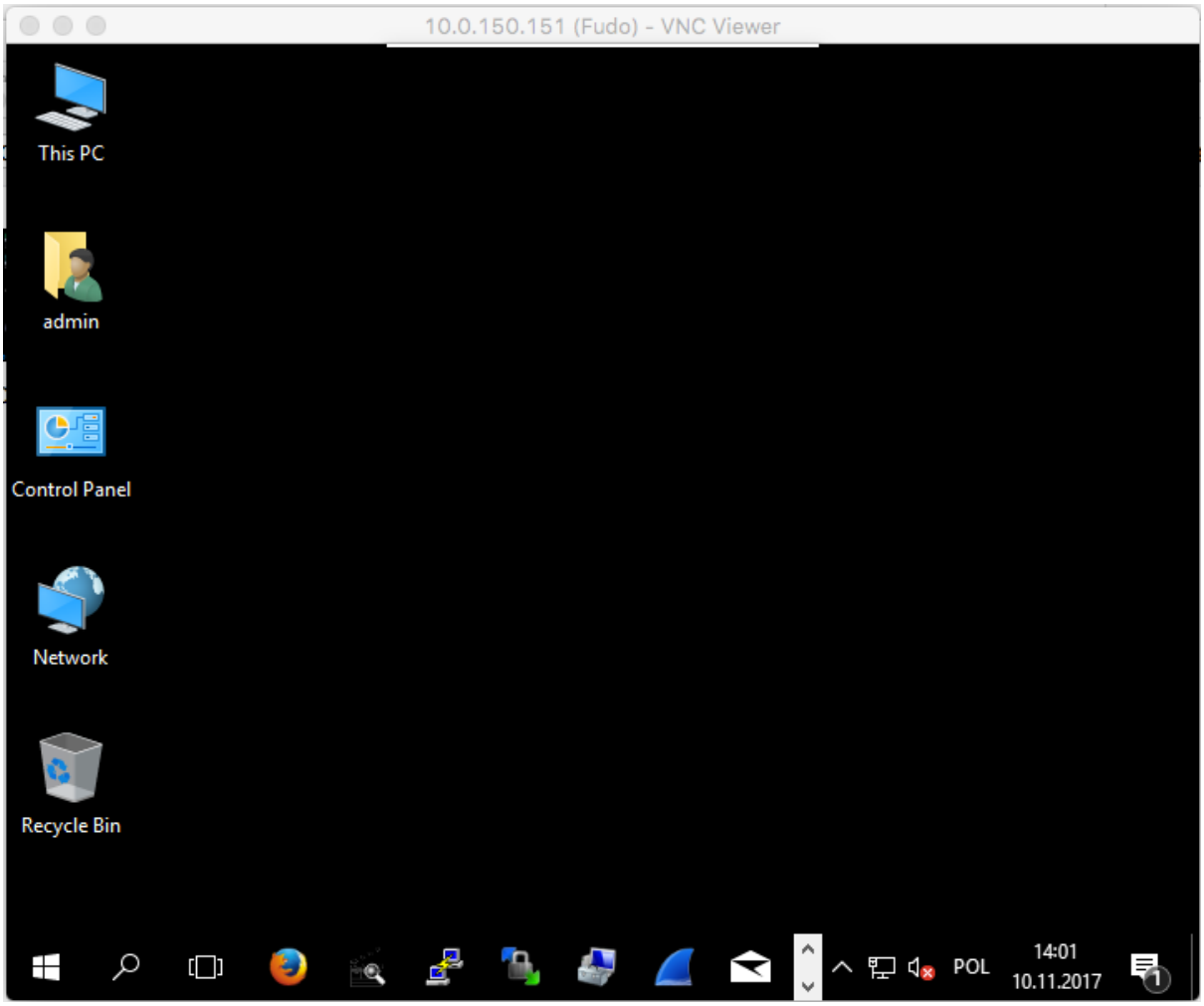
19.3 VNC Viewer

1. Uruchom aplikację kliencką *VNC Viewer* i w polu adresu wprowadź `10.0.150.151`.



2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in

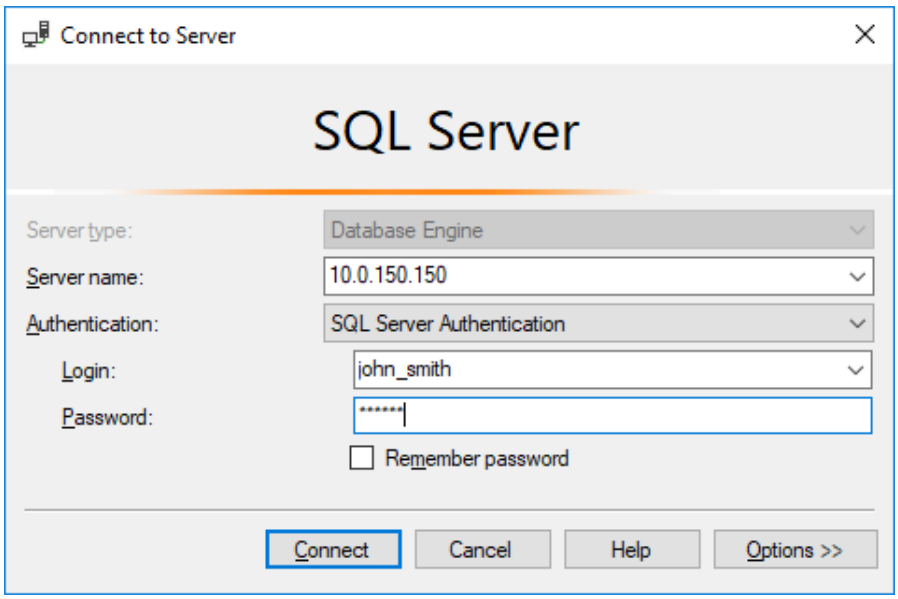


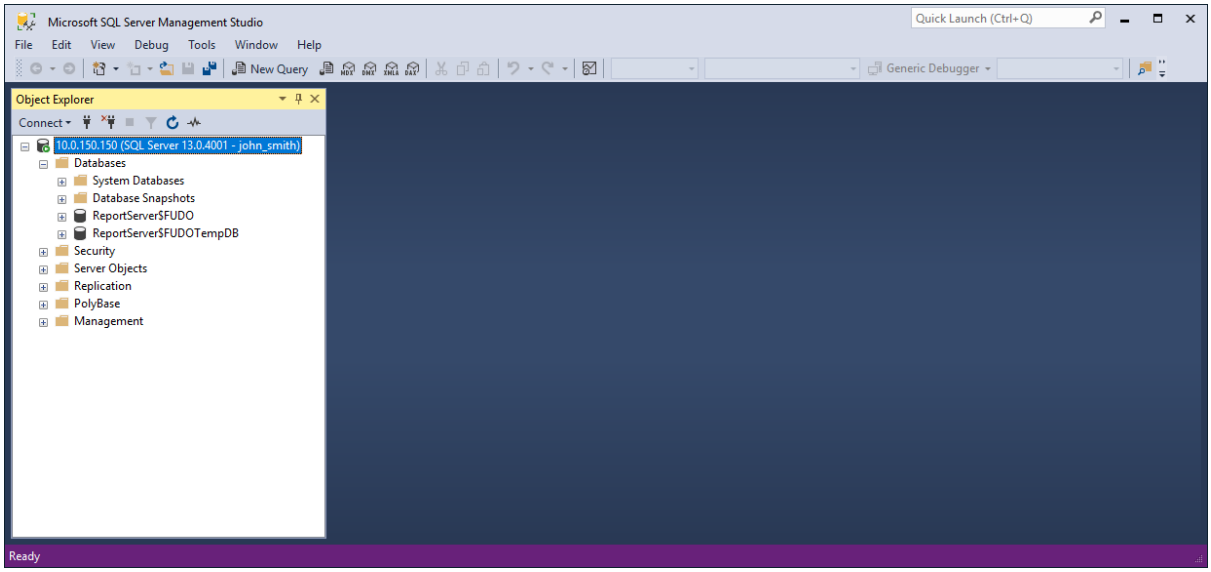
Tematy pokrewne:

- *Szybki start*

19.4 SQL Server Management Studio

1. Uruchom *SQL Server Management Studio*.
2. Wprowadź wcześniej skonfigurowany adres proxy, na którym Fudo oczekuje na połączenia z serwerem MS SQL (10.0.150.150).
3. Z listy rozwijalnej *Authentication*, wybierz *SQL Server Authentication*.
4. Wprowadź nazwę użytkownika oraz hasło.
5. Kliknij *Connect*.





Tematy pokrewne:

- *MS SQL*

ROZDZIAŁ 20

Usługa proxy dla uwierzytelnienia 4-Eyes

Usługa proxy dla uwierzytelnienia 4-Eyes pośredniczy w komunikacji Wheel Fudo PAM z aplikacją *Fudo Mobile*.

20.1 Instalacja usługi proxy

1. Zainstaluj system FreeBSD w wersji 10.x.
2. Do pliku `/boot/loader.conf` dodaj linię:

   ```
   pf_load="YES"
   ```

3. Wykonaj polecenie:

   ```
   kldload pf
   ```

Informacja: Alternatywnie, skompiluj kernel systemu ze wsparciem dla `pf`.

4. Wgraj paczkę `whlproxy` na serwer i wykonaj polecenie:

   ```
   pkg add /path/to/whlproxy.txz
   ```

20.2 Inicjalizacja konfiguracji za pomocą `whlproxyinit`

1. Wykonaj komendę `whlproxyinit`.
2. Nadaj nazwę DNS hosta, na którym usługa proxy.
3. Wskaż interfejs komunikacji z Wheel Fudo PAM.
4. Wprowadź adres IP wraz z maską sieci w notacji CIDR, np. `10.0.8.201/16`.
5. Wskaż interfejs komunikacji z siecią internet.

6. Wprowadź adres IP interfejsu komunikacji z siecią internet.
7. Wprowadź numer portu do połączeń z API.
8. Wprowadź domyślną trasę routingu.
9. Wprowadź nazwę klastra.
10. Wprowadź opis.
11. Podaj numer seryjny węzła.
12. Wprowadź klucz SSH węzła.

Informacja: Numery seryjne oraz klucze SSH węzłów klastra znajdziesz w panelu administracyjnym Fudo, w widoku *Ustawienia* > *Konfiguracja sieci*, zakładka *Proxy*, sekcja *Klucze Fudo SSH*.

---

13. Wybierz `Y`, aby wprowadzić dane kolejnego węzła klastra.
14. Wybierz `n`, aby zakończyć konfigurowanie usługi proxy.

Przykładowy przebieg konfiguracji:

```
System configuration.
You can modify configuration files after initialization.

Hostname: whlproxy1
Interface with an access to Fudo: em0
Internal IP address and netmask for em0: 10.0.8.201/16
Interface with an access to the Internet: em0
Public IP address and netmask for em0: 10.0.8.201/16
Public API port for 10.0.8.201: 44300
Default route: 10.0.0.1

TLS certificate for the proxy.

Now you will be asked to provide your Fudo cluster configuration.

Enter cluster details.
Name (only digits and uppercase letters): TEST
Description: Test
Enter nodes' details.
Serial: 12345678
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAA...
Add another node? [Y/n]: n

Your Fudo cluster configuration was successfully created.
In order to manage your clusters in the future run whlproxyctl tool.

Restarting services...

Wheel Systems Proxy is ready to use.
```

20.3 Zarządzanie klastrami za pomocą `whlproxyctl`

20.3.1 Dodawanie klastra

Aby dodać klaster, wykonaj komendę:

```
whlproxyctl cluster add <nazwa_klastra> <opis_klastra>
```

Informacja: Nazwa klastra musi zaczynać się literą `F` i może zawierać jedynie wielkie litery oraz cyfry, np. `FJMSBND007`.

Przykład:

```
whlproxyctl cluster add F007 "Opcjonalny opis"
```

20.3.2 Usuwanie klastra

Aby usunąć klaster, wykonaj komendę:

```
whlproxyctl cluster del <nazwa_klastra>
```

Przykład:

```
whlproxyctl cluster del F007
```

20.3.3 Wyświetlanie szczegółów klastra

Aby wyświetlić szczegółowe informacje na temat wybranego klastra, wykonaj komendę:

```
whlproxyctl cluster show <nazwa_klastra>
```

Przykład:

```
root@whlproxy1:~ # whlproxyctl cluster show F007
Name:           F007
GID:            1009
Description:    Opcjonalny opis
Token:
Nodes:          F23456789
```

20.3.4 Wyświetlanie listy klastrów

Aby wyświetlić listę klastrów, wykonaj komendę:

```
whlproxyctl cluster list
```

Przykład:

```
root@whlproxy1:~ # whlproxyctl cluster list
F007
FKW
FTEST
```

20.4 Zarządzanie węzłami za pomocą `whlproxyctl`

20.4.1 Dodawanie węzła do klastra

Aby dodać węzeł do klastra, wykonaj komendę:

```
whlproxyctl node add <nazwa_węzła> <nazwa_klastra> <klucz_ssh>
```

Informacja:

- Nazwa węzła przyjmuje postać `F<numer_seryjny>`, np. `F23456789`.
- Numery seryjne oraz klucze SSH węzłów klastra znajdziesz w panelu administracyjnym Fudo, w widoku *Ustawienia* > *Konfiguracja sieci*, zakładka *Proxy*, sekcja *Klucze Fudo SSH*.

Przykład:

```
whlproxyctl node add F23456789 F007 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA...
```

20.4.2 Usuwanie węzła klastra

Aby usunąć węzeł klastra, wykonaj komendę:

```
whlproxyctl node del <nazwa_węzła>
```

Przykład:

```
whlproxyctl node del F007
```

20.4.3 Wyświetlanie szczegółów węzła

Aby wyświetlić szczegółowe informacje na temat wybranego węzła, wykonaj komendę:

```
whlproxyctl node show name
```

Przykład:

```
root@whlproxy1:~ # whlproxyctl node show F12345678
Name:           F12345678
UID:            1007
Cluster:        FTEST
Key:            ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAA...
Rules:
```

20.4.4 Wyświetlanie listy węzłów

Aby wyświetlić listę węzłów, wykonaj komendę:

```
whlproxyctl node list
```

Przykład:

```
root@whlproxy1:~ # whlproxyctl node list
F00000005
F12345678
F23456789
```

Tematy pokrewne:

- *Dodawanie urządzenia mobilnego*
- *Usuwanie powiązanego urządzenia mobilnego*
- *Konfiguracja serwerów proxy*

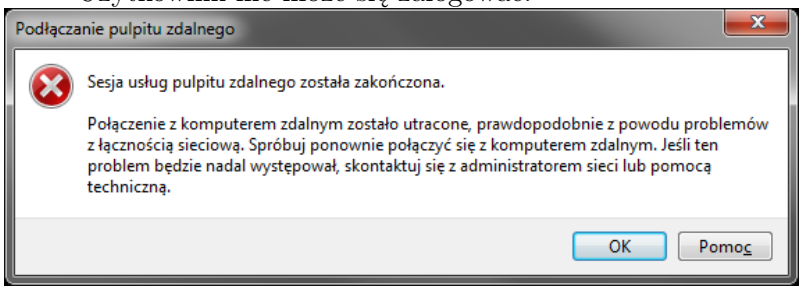
ROZDZIAŁ 21

Rozwiązywanie problemów

21.1 Uruchamianie Wheel Fudo PAM

Problem	Objawy i opis rozwiązania
Wheel Fudo PAM nie uruchamia się	• Sprawdź czy oba zasilacze są podłączone do instalacji elektrycznej 230V. Brak odpowiedniego podłączenia komunikowany jest sygnałem dźwiękowym. • Upewnij się czy podłączony został klucz szyfrujący. Brak klucza komunikowany jest sygnałem dźwiękowym. • W przypadku gdy problem wynika z nieudanej próby aktualizacji systemu, odczekaj kilka minut, podczas których urządzenie wykryje problem i uruchomi się ponownie przywracając poprzednią wersję systemu.

21.2 Połączenia z serwerami

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem	**Objawy:** • Użytkownik nie może się zalogować.  • Wpis w dzienniku zdarzeń: *Authentication failed: Invalid username kowalski or password.*
	Rozwiązanie: • Sprawdź czy definicja użytkownika istnieje w systemie Wheel Fudo PAM. • Zweryfikuj poprawność danych logowania użytkownika. • Upewnij się, że w kliencie za pośrednictwem którego realizowane jest połączenie z serwerem, nie są zapamiętane nieaktualne dane logowania.
	Objawy: komunikat w dzienniku zdarzeń: *Unable to establish connection to server zbigniew (10.0.35.53:3399).*
	Przyczyna: błędna konfiguracja serwera.
	Rozwiązanie: • Zweryfikuj poprawność definicji danego serwera (adres IP, numer portu). • Sprawdź, czy serwer osiągalny jest przez Wheel Fudo PAM: 1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM. 2. Wybierz *Ustawienia* > *System*, zakładka *Diagnostyka*. 3. Wprowadź adres serwera w sekcji *Ping* i wykonaj polecenie, żeby sprawdzić osiągalność hosta. • Sprawdź, czy serwer jest osiągalny pod wybranym numerem portu: 1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM. 2. Wybierz *Ustawienia* > *System*, zakładka *Diagnostyka*. 3. w sekcji *Netcat*, wprowadź adres IP serwera wraz z numerem portu wybranej usługi i wykonaj polecenie.

Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Wheel Fudo PAM (standardowy, z szarym tłem).	**Przyczyna:** • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Wheel Fudo PAM i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane poświadczenia w skrócie RDP, użytkownik używa poświadczeń lokalnych na Wheel Fudo PAM tak więc przed Wheel Fudo PAM jest poprawnie uwierzytelniany i nie pokazuje mu się ekran logowania. Następnie gdy Wheel Fudo PAM robi forward uwierzytelnień do docelowej maszyny to są one nie poprawne i użytkownikowi pokazuje się gina Windows gdzie sam się musi uwierzytelnić.
	Objawy: • Komunikat klienta: *Connection closed by remote host.* • Wpis w dzienniku zdarzeń: *Failed to authenticate against the server as user root using password.*
	Przyczyna: niepoprawne dane logowania do serwera docelowego.
	Rozwiązanie: zmień dane logowania w konfiguracji obiektu serwera.
	Objawy: • Komunikat klienta RDP: *Connection refused.* • Komunikat klienta SSH: *ssh: connect to host 10.0.1.111 port 10011: Connection refused*
	Przyczyna: serwer jest zablokowany.
	Rozwiązanie: odblokuj serwer w panelu administracyjnym Wheel Fudo PAM.

Problem	Objawy i opis rozwiązania
Połączenie jest zrywane	**Objawy:** • Użytkownik próbuje się połączyć z serwerem przez Wheel Fudo PAM, po wpisaniu nazwy użytkownika i hasła sesja od razu się zrywa. • Komunikat w dzienniku zdarzeń: *TLS certificate verification failed.*
	Rozwiązanie:
	Pobierz nowy certyfikat serwera docelowego w sekcji *Host docelowy.*
	
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje zerwanie połączenia. • Wpis w dzienniku zdarzeń: *RDP connection error.*
	Rozwiązanie: sprawdź czy w zakładce *General* we właściwościach TCP-Rdp, opcja *Encryption level* nie jest ustawiona na `FIPS Compliant`.
Brak połączenia z serwerem	**Objawy:** • Nie można zalogować się do serwera, komunikat *User user0 not allowed to connect to server.* • w dzienniku zdarzeń wpis: *Authentication failed: User user0 not allowed to connect to server.*
	Przyczyna: użytkownik nie jest dodany do połączenia.
	Rozwiązanie: dodaj użytkownika do odpowiedniego obiektu połączenia.

Problem	Objawy i opis rozwiązania
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje jakby zamrożenie ekranu logowania. • Wpis w dzienniku zdarzeń *Terminating session: User user0 (id=8483885321111147010) is blocked.*
	Przyczyna: użytkownik jest zablokowany w Wheel Fudo PAM.
	Rozwiązanie: odblokuj użytkownika.
Użytkownik musi logować się dwukrotnie	**Objawy:** użytkownik łącząc się poprzez protokół RDP wpisuje login i hasło po czym po chwili jest proszony o ponowne wprowadzenie danych autoryzujących.
	Przyczyna: serwer stanowi część infrastruktury zarządzanej przez broker połączeń, który wykrył istniejącą aktywną sesję użytkownika na innym serwerze.
	Objawy: użytkownik nawiązując połączenie SSH wprowadza dane logowania po czym ponownie proszony jest o ich podanie.
	Przyczyna: w obiekcie *połączenie* włączone są opcje zastępowania loginu i hasła, ale te pola ich definicji pozostawione są puste, co skutkuje podwójnym uwierzytelnieniem - w pierwszej kolejności przed Fudo, w drugiej przed serwerem docelowym.
Nie można nawiązać połączenia z serwerem RDP	**Objawy:** • użytkownik nawiązując połączenie RDP zostaje rozłączony chwilę po uwierzytelnieniu. • w dzienniku zdarzeń wpis: *RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.*
	Przyczyna: serwer docelowy, na który następuje przekierowanie, nie nasłuchuje na porcie 3389.
	Rozwiązanie: skonfiguruj serwer docelowy tak, by oczekiwał na połączenia użytkowników na porcie 3389.
	Objawy: • w dzienniku zdarzeń wpis: *User user0 has no access to host 192.168.0.1:3389*
	Przyczyna: broker stwierdza, że użytkownik ma aktywną sesję na innym serwerze i inicjuje przekierowanie, ale docelowy serwer nie jest skonfigurowany na Wheel Fudo PAM lub użytkownik nie jest uprawniony do nawiązywania połączeń z wybranym zasobem.
	Rozwiązanie: • Upewnij się, że obiekt serwera jest dodany do Fudo. • Dodaj użytkownika do odpowiedniego *sejfu*.

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem Telnet5250 poprzez aplikację PC5250 w wersji 20091005 S oraz 20111019 S	**Objawy:** próba nawiązania połączenia kończy się niepowodzeniem.
	Przyczyna: w przypadku wymienionych wersji aplikacji klienckiej, konieczne jest skonfigurowanie ruchu TCP na portach 449, 8470 i 8476, celem poprawnego zestawienia połączenia.
	Rozwiązanie: • Dodaj serwer Telnet TN5250, z domyślnym numerem portu, tj. 23. • Dodaj trzy obiekty typu serwer o protokole *TCP* i numerach portów odpowiednio 449, 8470 i 8476. • Dodaj gniazdo nasłuchiwania *TN5250*, w trybie *Pośrednik*, z domyślnym numerem portu. • Dodaj trzy gniazda nasłuchiwania *TCP*, w trybie *Pośrednik*, z numerami portów odpowiednio 449, 8470 i 8476. • Dodaj konto typu *regular*, określ parametry uwierzytelnienia i przypisz do głównej definicji serwera TN5250. • Dodaj trzy konta typu *anonymous* przypisując do kolejnych serwerów pomocniczych. • Dodaj sejf i przypisz konta wraz z odpowiadającymi gniazdami nasłuchiwania.

21.3 Logowanie do panelu administracyjnego

Problem	Objawi i opis rozwiązania
Nie można zalogować się do panelu administracyjnego	• Zweryfikuj czy wprowadzony adres Wheel Fudo PAM jest poprawny. • Ustaw adres IP Wheel Fudo PAM z poziomu konsoli, postępując zgodnie z instrukcją w rozdziale *Konfiguracja interfejsów sieciowych* w dokumentacji systemu Wheel Fudo PAM. • Upewnij się, że adres IP ma włączoną funkcję zarządzania Wheel Fudo PAM. 

21.4 Odtwarzanie sesji

Problem	Objawy i opis rozwiązania
Nie można odtworzyć wyeksportowanego materiału	**Przyczyna:** brak odpowiednich kodeków wideo.
	Rozwiązanie: zweryfikuj czy masz zainstalowane odpowiednie oprogramowanie.
Użytkownik administrator nie widzi sesji	**Objawy:** na liście sesji nie ma spodziewanych pozycji.
	Przyczyna: brak stosownych uprawnień.
	Rozwiązanie: nadaj użytkownikowi uprawnienia do określonego obiektu połączenia, serwera oraz użytkownika.
Nie można odtworzyć sesji w odtwarzaczu	**Objawy:** komunikat: `Nie można odnaleźć danych sesji.`
	Przyczyna: połączenie miało miejsce przy wyłączonej opcji rejestrowania sesji.
	Rozwiązanie: włącz opcję rejestrowania sesji, aby w przyszłości mieć możliwość odtworzenia materiału.

21.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na drugi węzeł	**Objawy:** Obiekty utworzone na jednym węźlę, nie pojawiają się automatycznie na pozostałych węzłach klastra. **Rozwiązanie:** Skontaktuj się z działem wspracia technicznego.

21.6 Znakowanie czasem

Problem	Objawy i opis rozwiązania
Sesje nie są znakowane znacznikiem czasu	**Objawy:** • Komunikat w dzienniku zdarzeń: *Timestamping service communication error.*
	Przyczyna: brak komunikacji z serwerem usługi znakowania czasem.
	Rozwiązanie: Upewnij się, że serwer usługi znakowania czasem jest osiągalny przez system Fudo. • adres IP serwera znakowania czasem PWPW: 193.178.164.5 • adres serwera znakowania czasem KIR: http://www.ts.kir.com.pl/HttpTspServer
	Objawy: • Komunikat w dzienniku zdarzeń: *Unable to timestamp session.* • Brak ikony przy wybranej sesji.
	Przyczyna: Problem z funkcjonowaniem usługi znakowania czasem.
	Rozwiązanie: Zweryfikuj poprawność *konfiguracji usługi znakowania czasem*.

ROZDZIAŁ 22

Często zadawane pytania

1. Jaka jest maksymalna ilość nagranych sesji na Wheel Fudo PAM dostępna z poziomu systemu?

2. W jaki sposób Wheel Fudo PAM obsługuje archiwizację sesji?

3. Jak wyliczyć wielkość przestrzeni dyskowej do archiwizacji?

4. W jaki sposób użytkownicy mogą ukrywać swoje działania na serwerach do których mają skonfigurowane połączenia na Wheel Fudo PAM?

5. W jaki sposób można stwierdzić próby uzyskania nieuprawionego dostępu do monitorowanych serwerów?

6. Czy możliwe jest ukrycie ekranu logowania podczas nawiązywania połączeń RDP?

7. Dlaczego lista użytkowników we właściwościach połączenia jest niekompletna?

8. Dlaczego użytkownik usunięty z serwera LDAP/AD w dalszym ciągu widoczny jest na Wheel Fudo PAM?

9. Jak często ma miejsce synchronizacja użytkowników z serwerem LDAP/AD?

*10. W odtwarzaczu sesji zamiast wprowadzonych znaków klawiatury wyświetlane są *. W jaki sposób zobaczyć dane wejścia klawiatury?*

11. Czy można unieważnić odnośnik do sesji?

1. Jaka jest maksymalna ilość nagranych sesji na Wheel Fudo PAM dostępna z poziomu systemu?

Urządzenia serii F1000 dysponują 24 TB przestrzeni dyskowej (18,2 TB przestrzeni użytkowej), a serii F3000 mają do dyspozycji macierz wewnętrzną o pojemności 96 TB (71,8 TB przestrzeni użytkowej) przeznaczoną do przechowywania danych sesji.

Rozmiar sesji determinowany jest aktywnością użytkownika. Średnie wartości dla jednej minuty zarejestrowanego połączenia wynoszą:

RDP	218 MB aktywnej sesji (brak aktywności ze strony użytkownika generuje pomijalnie niewielkie ilości danych). Ostateczny rozmiar sesji uzależniony jest od rozdzielczości ekranu, głębi kolorów i aktywności użytkownika w sesji.
SSH	41,5 MB aktywnej sesji.

Przy takich założeniach, wewnętrzna przestrzeń dyskowa pozwala na zarejestrowanie:

	RDP	SSH
F1000	28,6 lat	150,2 lat
F3000	112,8 lat	592,5 lat

Informacja:

- Informacja o zajętości przestrzeni dyskowej bierze pod uwagę obszar zarezerwowany przez mechanizm redundancji danych. Stąd wynika raportowana zajętość macierzy dyskowej po zainicjowaniu systemu.
- Wheel Fudo PAM pozwala określić, jak długo sesje mają być przechowywane i automatycznie usuwa dane sesji po upłynięciu czasu określonego *parametrem retencji*.

2. W jaki sposób Wheel Fudo PAM obsługuje archiwizację sesji?

Wszystkie sesje archiwizowane są na wewnętrznej macierzy dyskowej urządzenia, przeznaczonej na rejestrowanie zdalnych połączeń. Wheel Fudo PAM wspiera zewnętrzne macierze a także umożliwia eksport sesji w natywnym formacie lub w postaci nagrania video.

3. Jak wyliczyć wielkość przestrzeni dyskowej do archiwizacji?

Rozmiar plików w formacie natywnym jest zgodny z odpowiedzią z punktu 1. W przypadki eksportu do formatu video, rozmiar wynikowy pliku zależy od wybranego kodowania strumienia video oraz wybranej rozdzielczości nagrania.

4. W jaki sposób użytkownicy mogą ukrywać swoje działania na serwerach, do których mają skonfigurowane połączenia na Wheel Fudo PAM?

W przypadku protokołu SSH, obsługiwany jest kanał SCP przez co wszystkie pliki, w tym skrypty, również podlegają monitorowaniu. Dzięki temu można audytować daną sesję również pod kątem złośliwego kodu zamieszczanego w programach wysłanych na serwer, których zawartość nie jest wyświetlana na ekranie.

Ochrona innych kanałów komunikacji użytkownika z serwerem (np. przeglądarka internetowa lub inne programy) to zadanie dla rozwiązań innego rodzaju. Żadne rozwiązania jak Wheel Fudo PAM nie mogą monitorować tych kanałów, dlatego ważne jest stworzenie odpowiedniej konfiguracji serwera przez administratora systemu.

5. W jaki sposób można stwierdzić nieuprawnione próby uzyskania dostępu do monitorowanych serwerów?

Próby nadużyć (nieuprawniony dostęp, atak DoS), można stwierdzić na podstawie analizy wpisów w dzienniku zdarzeń. Wszelkie wpisy o poziomie logowania ERROR i WARNING powinny być dokładnie analizowane. Przypadki wystąpienia błędu przekroczenia limitu czasu logowania, mogą świadczyć o próbie dokonania ataku DoS.

6. Czy możliwe jest ukrycie ekranu logowania podczas nawiązywania połączeń RDP?

Ukrycie ekranu logowania wymaga zdefiniowania trybu bezpieczeństwa `Enhanced RDP Security (TLS) + NLA` monitorowanego serwera.

7. Dlaczego lista użytkowników we właściwościach połączenia jest niekompletna?

Lista użytkowników we właściwościach połączenia nie zawiera użytkowników synchronizowanych z serwerem usług katalogowych. Aby dodać takiego użytkownika do połączenia, zdefiniuj mapowanie grup we *właściwościach synchronizacji LDAP* lub wyłącz synchronizację LDAP dla wybranego użytkownika.

8. Dlaczego użytkownik usunięty z serwera LDAP/AD w dalszym ciągu widoczny jest na Wheel Fudo PAM?

Odwzorowanie zmiany polegającej na usunięciu użytkownika z serwera LDAP lub AD wymaga pełnej synchronizacji. Proces pełnej synchronizacji wyzwalany jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00, lub może zostać wyzwolony ręcznie z poziomu widoku ustawień *synchronizacji LDAP*.

9. Jak często ma miejsce synchronizacja użytkowników z serwerem LDAP/AD?

Definicje nowych użytkowników oraz zmiany w istniejących obiektach pobierane są okresowo w odstępie czasowym wynoszącym 5 minut. Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00.

10. W odtwarzaczu sesji zamiast wprowadzonych znaków klawiatury wyświetlane są *. W jaki sposób zobaczyć dane wejścia klawiatury?

Wejście klawiatury należy do grupy funkcjonalności wrażliwych i jest domyślnie ukryte. Włączenie pokazywania znaków wprowadzonych na klawiaturze wymaga decyzji dwóch użytkowników `superadmin`. Procedura aktywacji funkcjonalności opisana jest w rozdziale *Funkcjonalności wrażliwe*.

11. Czy można unieważnić odnośnik do sesji?

Aktywny odnośnik do sesji może zostać w każdej chwili unieważniony. Procedura unieważnienia odnośników opisana jest w rozdziale *Udostępnianie sesji*.

ROZDZIAŁ 23

Słownik pojęć

ARP Address Resolution Protocol - protokół mapujący adresy warstwy trzeciej (adresy IP) na fizyczne adresy warstwy łącza danych (adresy MAC).

DNS Domain Name Server - serwer nazw, tłumaczy mnemoniczne nazwy hostów na adresy IP.

SSH Secure Shell - protokół sieciowy do bezpiecznej komunikacji ze zdalnymi urządzeniami.

Syslog Standard logowania zdarzeń w systemach komputerowych. Serwer Syslog zbiera i przechowuje centralnie dane dzienników zdarzeń (log) urządzeń sieciowych, które mogą zostać wykorzystane w celach raportowania i analizowania.

Odcisk Palca Fingerprint - ciąg znaków będący działaniem funkcji skrótu na danych wejściowych, pozwalający jednoznacznie stwierdzić, czy dane nie zostały zmienione.

RDP Remote Desktop Protocol - protokół zdalnego dostępu do graficznych interfejsów użytkownika w systemach operacyjnych firmy Microsoft.

VNC Protokół graficznego dostępu do zdalnych zasobów komputerowych.

RADIUS Remote Authentication Dial In User Service - protokół sieciowy służący regulowaniu dostępu do określonych usług udostępnianych w sieci informatycznej.

Hasło statyczne Podstawowa metoda uwierzytelniania użytkowników, w której do potwierdzenia tożsamości używana jest kombinacja ciągów znakowych w postaci loginu i hasła.

Klucz publiczny Metoda uwierzytelniania, w której tożsamość użytkownika ustalana jest na podstawie pary kluczy - prywatny (będący tylko w posiadaniu użytkownika) i publiczny (udostępniany innym podmiotom).

CERB Kompleksowe rozwiązanie uwierzytelniania i autoryzacji użytkowników, wspierające metody uwierzytelniania tj. token mobilny (aplikacja na telefon komórkowy), hasło statyczne, hasła jednorazowe SMS.

LDAP Lightweight Directory Access Protocol - protokół dostępu i zarządzania rozproszonymi usługami katalogowymi w sieciach IP.

Active Directory Usługa uwierzytelniania i autoryzacji użytkowników w domenie Windows.

AD Active Directory - usługa uwierzytelnienia i autoryzacji użytkowników w domenie Windows.

notacja CIDR Skrócona notacja adresów sieciowych, w której adres IP zapisywany jest zgodnie z notacją IPv4, a maska podawana jest w postaci liczby wiodących cyfr «1» w zapisie bitowym (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

DoS (Denial of Service) Próba ataku na system polegająca na wysłaniu znacznej ilości zapytań do serwera, tak aby zaprzestał przetwarzać kolejne żądania użytkowników.

heartbeat Pakiet służący informowaniu innych węzłów klastra o stanie maszyny. W przypadku gdy drugi węzeł klastra nie otrzyma pakietu heartbeat przez określony czas, przejmuje rolę węzła głównego i przetwarza zapytania użytkowników.

PSM (Privileged Session Management) Moduł Wheel Fudo PAM służący rejestracji zdalnych sesji dostępowych.

sejf anonimowy Sejf anonimowy ma przypisane co najmniej jedno konto typu `anonymous` i może mieć przypisane jedynie konta tego typu. Do sejfów anonimowych nie można przypisać użytkowników.

AAPM Moduł AAPM (Application to Application Password Manager) umożliwiający bezpieczną wymianę haseł pomiędzy aplikacjami.

Efficiency Analyzer Moduł Efficiency Analyzer dostarcza danych statystycznych na temat aktywności użytkowników.

serwer

Serwery Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

gniazdo nasłuchiwania Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

użytkownik Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

konto Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

sejf Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

hot-swap Mechanizm umożliwiający wymianę komponentu bez wyłączania urządzenia.

polityka czasowa Mechanizm definiowania przedziałów czasu, w których użytkownicy mają dostęp do serwerów.

modyfikator haseł Narzędzie służące do zmiany hasła do konta na monitorowanym serwerze.

polityka Mechanizm pozwalający definiować wzorce i automatyczne akcje, które podejmie system w przypadku wykrycia danego wzorca.

sesja współdzielona Sesja użytkownika, do której dołączył inny użytkownik.

fudopv Skrypt modułu AAPM, rezydujący na serwerze, umożliwiający wymianę haseł pomiędzy aplikacjami.

dostęp SSH Dostęp serwisowy do Wheel Fudo PAM poprzez protokół SSH.

VLAN Mechanizm sieci wirtualnych, umożliwiający separację domen rozgłoszeniowych.

DHCP Mechanizm dynamicznego zarządzania adresacją w sieciach LAN.

znacznik czasu Znacznik będący skrótem danych, pozwalający zweryfikować czy dane nie zostały zmienione.

zewnętrzny serwer uwierzytelnienia Serwer przechowujący dane użytkowników, używany do weryfikacji tożsamości w procesie logowania do Wheel Fudo PAM lub nawiązywania połączenia z serwerami docelowymi.

repozytorium haseł Repozytorium haseł zarządza hasłami do serwerów docelowych, w dostępie do których, pośredniczy Wheel Fudo PAM.

retencja Retencja danych to mechanizm, który usuwa dane sesji po upływie zdefiniowanego czasu.

grupa redundancji Zdefiniowana grupa adresów IP, które w przypadku awarii jednego z węzłów, zostaną przypisane do drugiego serwera, dla zachowania ciągłości świadczenia usług.

broker połączeń RDP Mechanizm zarządzania sesjami dostępowymi do maszyn będących częścią farmy serwerów.

WWN World Wide Name - unikatowy identyfikator obiektów w rozwiązaniach macierzy dyskowych.

serwer dynamiczny Serwer dodawany automatycznie z chwilą nawiązywania połączenia, jeśli wcześniej zdefiniowany został obiekt opisujący zbiór serwerów w formie podsieci.

certyfikat CA Certyfikat urzędu certyfikacji.

Symbole

4 eyes
    proxy, 292

A

AAPM, **411**
Active Directory, **410**
Active Directory
    systemy zewnętrznego
        uwierzytelniania, 299
AD, **411**
administracja
    aktualizacja systemu, 272
    import/eksport konfiguracji, 323
    pierwsze uruchomienie, 25
    ponowne uruchomienie, 309
    przywracanie poprzedniej wersji, 308
API
    użytkownicy, 109
ARP, **410**

B

blokowanie
    serwery, 158
broker połączeń RDP, **412**
broker połączeń RDP, 45

C

CERB, **410**
CERB
    systemy zewnętrznego
        uwierzytelniania, 299
certyfikat CA, **412**
Citrix
    gniazda nasłuchiwania, 187
    serwery, 131
Citrix StoreFront
    protokoły, 4
    protokół, 4

D

DHCP, **412**
DNS, **410**
DNS
    konfiguracja, 290
dodawanie
    serwery, 131
DoS (*Denial of Service*), **411**
dostęp SSH, **412**
dynamiczne
    serwery, 156

E

Efficiency Analyzer, **411**
Efficiency Analyzer, 12

F

fudopv, **412**

G

gniazda nasłuchiwania
    Citrix, 187
    HTTP, 189
    ICA, 191
    konfiguracja, 186
    Modbus, 193
    MS SQL, 204
    MySQL, 195
    RDP, 198
    SSH, 201
    Telnet, 206
    Telnet 3270, 208
    VNC, 210
gniazdo nasłuchiwania, **411**
grupa redundancji, **412**

H

Hasło statyczne, **410**
heartbeat, **411**

hot-swap, **411**
HTTP
    gniazda nasłuchiwania, 189
    protokoły, 5
    protokół, 5
    serwery, 132

I

ICA
    gniazda nasłuchiwania, 191
    protokoły, 5
    protokół, 5
    serwery, 134

K

Klucz publiczny, **410**
konfiguracja
    gniazda nasłuchiwania, 186
    model danych, 12
    powiadomienia, 296
    serwery, 130
    synchronizacja użytkowników, 122
    ustawienia sieciowe, 277, 288, 289
    użytkownicy, 108
konto, **411**

L

LDAP, **410**
LDAP
    systemy zewnętrznego uwierzytelniania, 299

M

Modbus
    gniazda nasłuchiwania, 193
    protokoły, 6
    protokół, 6
    serwery, 136
model danych
    serwer, 13
    użytkownik, 13
moduł
    Efficiency Analyzer, 12
modyfikator haseł, **411**
modyfikowanie
    serwery, 157
MS SQL
    gniazda nasłuchiwania, 204
    serwery, 138
MS SQL (*TDS*)
    protokoły, 6
    protokół, 6
MySQL
    gniazda nasłuchiwania, 195
    protokoły, 6
    protokół, 6
    serwery, 140

N

notacja CIDR, **411**

O

odblokowanie
    serwery, 159
Odcisk Palca, **410**
Oracle
    protokoły, 7
    protokół, 7
    serwery, 142

P

polityka, **411**
polityka czasowa, **411**
protokoły
    Citrix StoreFront, 4
    HTTP, 5
    ICA, 5
    Modbus, 6
    MS SQL (*TDS*), 6
    MySQL, 6
    Oracle, 7
    RDP, 7
    SSH, 8
    TCP, 11
    Telnet, 9
    Telnet 3270, 8
    Telnet 5250, 9
    VNC, 9
    X11, 10
protokół
    Citrix StoreFront, 4
    HTTP, 5
    ICA, 5
    Modbus, 6
    MS SQL (*TDS*), 6
    MySQL, 6
    Oracle, 7
    RDP, 7
    SSH, 8
    TCP, 11
    Telnet, 9
    Telnet 3270, 8
    Telnet 5250, 9
    VNC, 9

X11, 10
proxy
konfiguracja, 292
PSM (*Privileged Session Management*), **411**

R

RADIUS, **410**
RADIUS
systemy zewnętrznego uwierzytelniania, 299
RDP, **410**
RDP
gniazda nasłuchiwania, 198
protokoły, 7
protokół, 7
serwery, 144
repozytorium haseł, **412**
retencja, **412**

S

scenariusze wdrożenia
bastion, 16
brama, 15
most, 14
pośrednik, 16
wymuszony routing, 14
sejf, **411**
sejf anonimowy, **411**
serwer, **411**
serwer dynamiczny, **412**
Serwery, **411**
serwery
blokowanie, 158
Citrix, 131
dodawanie, 131
dynamiczne, 156
HTTP, 132
ICA, 134
konfiguracja, 130
Modbus, 136
modyfikowanie, 157
MS SQL, 138
MySQL, 140
odblokowanie, 159
Oracle, 142
RDP, 144
ssh, 146
Telnet, 148
Telnet 3270, 150
Telnet 5250, 153
usuwanie, 160
VNC, 154
sesja współdzielona, **411**
sesje, 235
dołączanie do trwającej sesji, 245
eksportowanie, 250
filtrowanie, 236
komentowanie, 247
na żywo, 242
odtwarzanie i podgląd, 240
SSH, **410**
SSH
gniazda nasłuchiwania, 201
protokoły, 8
protokół, 8
ssh
serwery, 146
synchronizacja użytkowników, 122
konfiguracja, 122
Syslog, **410**
systemy zewnętrznego uwierzytelniania, 299
dodawanie serwera, 300
modyfikowanie serwera, 301
usuwanie serwera, 302

T

TCP
protokoły, 11
protokół, 11
Telnet
gniazda nasłuchiwania, 206
protokoły, 9
protokół, 9
serwery, 148
Telnet 3270
gniazda nasłuchiwania, 208
protokoły, 8
protokół, 8
serwery, 150
Telnet 5250
protokoły, 9
protokół, 9
serwery, 153
tryb połączenia
transparentny, 15

U

ustawienia sieciowe
ARP, 294
etykiety adresów IP, 288
konfiguracja bajpasów, 289
konfiguracja interfejsów, 277
proxy, 292

serwery DNS, 290
trasa routingu, 289
usuwanie
serwery, 160
użytkownicy, 108
API, 109
konfiguracja, 108
prawa dostępu, 109, 120
role, 109, 120
zewnętrzne uwierzytelnianie, 299
użytkownik, **411**

V

VLAN, **412**
VNC, **410**
VNC
gniazda nasłuchiwania, 210
protokoły, 9
protokół, 9
serwery, 154

W

WWN, **412**

X

X11
protokoły, 10
protokół, 10

Z

zewnętrzny serwer uwierzytelnienia, **412**
znacznik czasu, **412**