FUDD

Wheel Fudo PAM 3.7 -Dokumentacja Systemu

Wydanie niewspierane

Wheel Systems

09.09.2021

Spis treści

1	Info 1.1	macje ogólne 1 O dokumentacji						
2	Opis	systemu 4						
	2.1	PSM (Privileged Sessions Management)						
		2.1.1 Citrix StoreFront (HTTP)						
		2.1.2 HTTP						
		2.1.3 ICA						
		2.1.4 Modbus						
		2.1.5 MS SQL (TDS)						
		2.1.6 MvSQL						
		2.1.7 Oracle						
		2.1.8 RDP						
		2.1.9 SSH						
		2.1.10 Telnet 3270						
		2.1.11 Telnet 5250						
		2.1.12 Telnet						
		2.1.13 VNC						
		2.1.14 X11						
		2.1.15 TCP 11						
	2.2	AAPM (Application to Application Password Manager)						
	2.3	Skarbiec hasel (Secret Manager)						
	2.4	Efficiency Analyzer						
	2.5	Portal użytkownika 12						
	2.6	Model danych						
	2.7	Scenariusze wdrożenia						
	2.8	Tryby połączenia						
	2.9	Metody i tryby uwierzytelniania użytkowników 17						
	2.10	Mechanizmy bezpieczeństwa						
		2.10.1 Szyfrowanie danych						
		2.10.2 Kopie zapasowe						
		2.10.3 Uprawnienia użytkowników 20						
		2.10.4 Sandboxing 21						
		2.10.5 Niezawodność						
		2.10.6 Konfiguracja klastrowa						
	2.11	Dashboard						

3	Insta	alacja i pierwsze uruchomienie 24
	3.1	Wymagania
	3.2	Urządzenie
	3.3	Pierwsze uruchomienie
	~ .	
4	Szyb	oki start 31
	4.1	SSH
		4.1.1 Załozenia
		$4.1.2 \text{Konfiguracja} \dots \dots$
		4.1.3 Nawiązanie połączenia $\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots 36$
		4.1.4 Podgląd sesji połączeniowej 37
	4.2	SSH w trybie bastionu
		4.2.1 Założenia
		4.2.2 Konfiguracja
		4.2.3 Nawiązanie połączenia 42
		4.2.4 Podgląd sesji połączeniowej 44
	4.3	RDP
		4.3.1 Broker połączeń RDP
		4.3.2 Założenia
		4.3.3 Konfiguracja
		4.3.4 Nawiazanie połaczenia
		4.3.5 Podglad sesij połaczeniowej
	4.4	Telnet
		4 4 1 Założenia 53
		4 4 2 Konfiguracia 53
		4 4 3 Nawiazanie połaczenia 57
		4 4 4 Podglad sesii połączeniowej 57
	4.5	Telnet 5250
	1.0	4.5.1 Założenia 59
		$4.5.1 \text{ZatoZellia} \qquad 50$
		$4.5.2 \text{Noninguracja} \qquad \qquad$
		4.5.5 Nawiązanie połączenia 02
	1 C	4.5.4 Podgiąd sesji połączeniowej 04
	4.0	MySQL
		4.0.1 Założenia 00
		$4.6.2 \text{Konfiguracja} \dots \dots \dots \dots \dots \dots \dots \dots \dots $
		4.6.3 Nawiązanie połączenia
		4.6.4 Podgląd sesji połączeniowej 70
	4.7	MS SQL
		4.7.1 Założenia
		4.7.2 Konfiguracja \ldots 72
		4.7.3 Nawiązanie połączenia 76
		4.7.4 Podgląd sesji połączeniowej 77
	4.8	HTTP
		4.8.1 Założenia
		4.8.2 Konfiguracja
		4.8.3 Nawiązanie połączenia 82
		4.8.4 Podgląd sesji połączeniowej 83
	4.9	Citrix
		4.9.1 ICA
		4.9.1.1 Plik konfiguracyjny połączenia ICA
		4.9.1.1.1 Plik ICA do połączeń bez TLS

		4.9.1.1.2 Plik ICA do połączeń TLS
		4.9.1.2 Założenia \ldots 85
		$4.9.1.3 \text{Konfiguracja} \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots $
		4.9.1.4 Zdefiniowanie połączenia w pliku .ica $\dots \dots \dots$
		4.9.1.5 Nawiązanie połączenia
		4.9.1.6 Podgląd sesji połączeniowej
		4.9.2 Citrix StoreFront
		$4.9.2.1 \text{Założenia} \dots \dots \dots \dots \dots \dots \dots \dots \dots $
		$4.9.2.2 \text{Konfiguracja} \dots \dots \dots \dots \dots \dots \dots \dots \dots $
	4.10	VNC
		4.10.1 Założenia
		4.10.2 Konfiguracja
		4.10.3 Nawiązanie połączenia
		4.10.4 Podgląd sesji połączeniowej 104
	4.11	Uwierzytelnienie użytkowników w katalogu LDAP 105
		4.11.1 Założenia
		4.11.2 Konfiguracja
-	тт• и	100
5	Uzyt	$\frac{108}{100}$
	0.1 E 0	Dodawanie uzytkownika 108 Madaffermenia 114
	0.Z	Modynkowanie użytkownika
	0.0 5 4	Diokowanie uzytkownika
	0.4 5 5	Ucumenia niuthermika
	5.6	Delitylia azagowa dostany do scifár
	5.0	Polityka czasowa dostępu do sejiow
	5.0	Kole uzytkownika
	5.0	Dodawania urządzenia mobilnoso
	5.10	Usuwanie urządzenia mobilnego
	0.10	Osuwanie powiązanego urządzenia mobilnego
6	Serw	130 nery
	6.1	Dodawanie serwera
		6.1.1 Serwery statyczne
		6.1.1.1 Dodawanie serwera Citrix
		6.1.1.2 Dodawanie serwera HTTP
		6.1.1.3 Dodawanie serwera ICA
		6.1.1.4 Dodawanie serwera Modbus
		6.1.1.5 Dodawanie serwera MS SQL
		6.1.1.6 Dodawanie serwera MySQL
		6.1.1.7 Dodawanie serwera Oracle
		6.1.1.8 Dodawanie serwera RDP
		6.1.1.9 Dodawanie serwera SSH
		6.1.1.10 Dodawanie serwera Telnet
		6.1.1.11 Dodawanie serwera Telnet 3270
		6.1.1.12 Dodawanie serwera Telnet 5250
		6.1.1.13 Dodawanie serwera VNC
		6.1.2 Serwery dynamiczne
		6.1.2.1 Definiowanie grupy serwerów
		6.1.2.2 Definiowanie pojedynczego hosta w ramach grupy serwerów 156
	6.2	Modyfikowanie serwera
	6.3	Blokowanie serwera
	6.4	Odblokowanie serwera

	6.5	Usuwar	ie serwera			•	•			160
		6.5.1	Usuwanie definicji serwera			•	• •			160
		6.5.2	Usuwanie wybranego hosta z grupy serwerów dynamicznych			•				161
7	Kont	a								162
	7.1	Dodawa	anie konta		•	•			•	162
		7.1.1	Dodawanie konta typu anonymous		•	•			•	162
		7.1.2	Dodawanie konta typu forward			•				165
		7.1.3	Dodawanie konta typu <i>regular</i>			•				168
	7.2	Edytow	vanie konta			•				173
	7.3	Blokow	anie konta							174
	7.4	Odblok	owanie konta							175
	7.5	Usuwar	nie konta							175
8	Sejfy	7								177
	8.1	Dodawa	anie sejfu		•	•				178
	8.2	Modyfil	kowanie sejfu			•				181
	8.3	Blokow	anie sejfu			•	• •			182
	8.4	Odblok	owanie sejfu							183
	8.5	Usuwar	nie sejfu							184
			•							
9	Gnia	zda nas	słuchiwania							186
	9.1	Dodawa	anie 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 MvSQL							195
		9.1.6	Dodawanie gniazda Oracle							197
		9.1.7	Dodawanie gniazda RDP							198
		918	Dodawanie gniazda SSH	•	•					201
		919	Dodawanie gniazda MS SOL	·	•	• •		•	•	204
		0.1.0	Dodawanie gniazda nasłuchiwania Telnet	·	•	• •		•	•	201
		0 1 11	Dodawanie gniazda nasłuchiwania Telnet 3270	•	•	• •	• •	•	•	200
		0.1.11	Dodawanie gniazda nasłuchiwania Tenet 5270	·	•	• •	• •		•	200
	0.9	9.1.12 Modufi	bouavanie gniazda nasłuchiwania VIVC	·	•	• •	• •	• •	•	210
	9.2	Dialaar	kowanie ginazua nasiuchiwania	·	•	• •		••	·	212
	9.5	Odblah	ame ginazua nasiucinwama	·	•	• •		••	·	210
	9.4		owanie gniazda nastucniwania	·	•	• •	• •	•	·	214
	9.5	Usuwar		·	•	• •		• •	·	210
10	Mod	vfikato	rv haseł							217
10	10.1	Polityki	i haseł							217
	10.1	10.1.1	Dodawania polituki zmiany hasał	·	•	• •		•	•	217
		10.1.1 10.1.2	Edutowanie polityki zmiany hasel	•	•	• •	• •	· •	•	217
		10.1.2 10.1.2	Uguwania polityki zmiany hasel	•	•	• •	• •	•	•	210
	10.9	IU.I.3	Jouwanie pontyki zinany nasei	·	•	• •		•	•	210 910
	10.2	Uniwers	Dadamania universalizaria mada flattaria haral	·	•	• •		• •	·	219
		10.2.1	Edutomonio universalinego modyfikatora naser	·	•	• •		• •	·	219
		10.2.2	Edytowanie uniwersaniego modyfikatora hasef	•	•	• •		• •	·	220
	10.2	10.2.3	Usuwanie modyfikatora hasef	·	•	•		• •	·	220
	10.3	Konfigu	irowanie modyfikatora haseł Unix poprzez SSH	·	•	• •		•	·	221
	10.4	Konfigu	irowanie modyfikatora haseł Windows WMI	•	•	•		• •	·	224

11 Polityki

12	Sesje	2	235
	12.1	Filtrowanie sesji	236
		12.1.1 Definiowanie filtrów	236
		12.1.2 Przeszukiwanie pełnotekstowe	238
		12.1.3 Zarzadzanie definicjami filtrowania	239
	12.2	Odtwarzanie sesji	240
	12.3	Podglad trwajacych sesji	242
	12.4	Wstrzymywanie połaczenia	242
	12.5	Przerywanie połaczenia	243
	12.6	Dołaczanie do sesii	245
	12.7	Udostepnianie sesii	246
	12.8	Komentowanie sesji	247
	12.0	Eksportowanie sesji	250
	12.0	Usuwanie sesii	251
	12.10	Przetwarzanie OCR sesii	251
	19.19	7 Znakowania czasem wybranych cesij	251
	12.12	Alcontowanie ozaceni wybranych sesji	250
	12.10	12.12.1. Interfeis administracyiny Fude	254
		12.12.2 Fudo Mobile	204
	19.14	12.15.2 Fudo Mobile	204
	12.14	12.14.1. Interfeis administración Euda	204
		12.14.1 Interiejs administracyjny Fudo	204
		12.14.2 Fudo Mobile	200
13	Rano	orty	257
10	13.1	Subskrybowania raportu cyklicznego	257
	12.1	Bozygnacja z subskrypcji raportu cyklicznogo	258
	13.2	Concrowania raportu na zadania	258
	12.0	Wyówiatlania i zapisywania raportów	200
	10.4		209
	19.0		200
14	Anal	liza produktywności 2	261
	14.1	Zestawienie	261
	14.2	Analiza sesii	262
	14.3	Porównanie aktywności	264
	11.0		-01
15	Adm	iinistracja 2	265
	15.1	System	265
		15.1.1 Data i czas	265
		15.1.2 Certyfikat HTTPS	268
		15.1.3 Blokowanie nowych połaczeń	269
		15.1.4 Dostep SSH	270
		15.1.5 Domyślna domena	271
		15.1.6 Konto reset	271
		15.1.7 Funkcionalności wrażliwe	271
		15.1.8 Aktualizacia systemu	272
		15.1.8.1 Aktualizowanie systemu	273
		15.1.8.2 Wervfikacja wykonalności aktualizacji	272
		15.1.8.3 Usuwanie migewki aktualizacji	274
		15.1.0. Liconcia	214 074
		15.1.10 Diagnostyle	214 075
			<u>- 10</u>

227

1	5.2	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
1	5.3	Powiadomienia	. 296
1	5.4	Znakowanie czasem	. 298
1	5.5	Zewnętrzne serwery uwierzytelniania	. 299
1	5.6	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
1	5.7	Zasoby	. 306
1	5.8	Przywracanie poprzedniej wersji systemu	. 308
1	5.9	Ponowne uruchomienie systemu	. 309
1	5.10	SNMP	. 310
		15.10.1 Odczytywanie informacji SNMP poprzez snmpwalk	. 311
		15.10.2 Rozszerzenia SNMP Wheel Fudo PAM	. 311
1	5.11	Kopie zapasowe i retencja	. 319
1	5.12	Zewnętrzna macierz dyskowa	. 321
		15.12.1 Konfigurowanie zewnętrznej macierzy dyskowej	. 322
		15.12.2 Rozszerzanie zewnętrznej macierzy dyskowej	. 322
1	5.13	Eksportowanie/importowanie konfiguracji systemu	. 323
		15.13.1 Eksportowanie konfiguracji	. 323
		15.13.2 Importowanie konfiguracji	. 323
1	5.14	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
1	5.15	Dziennik zdarzeń	. 335
1	5.16	Integracja z serwerem CERB	. 338
1	5.17	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 I	nfor	rmacje uzupełniające	355
1	6.1	Kody błędów	. 355
1	6.2	Mapowanie parametrów Fudo 2.2 na Fudo 3.0	. 359

		16.2.1 Połączenie	0
		16.2.2 Serwer	2
	16.3	Migracja modelu danych wersji 2.2 do 3.0	2
		16.3.1 Serwer	2
		16.3.2 Seif (dawniej <i>połaczenie</i>)	3
		16.3.3 Konto (dawniej <i>dane logowania</i>)	3
		16.3.4 Gniazdo nasłuchiwania (dawniej <i>bastion</i> lub cześć serwera)	3
		16.3.5 Sesie	4
	164	Obsługa wspieranych protokołów 36	4
	10.1	16.4.1 Citrix StoreFront (HTTP) 36	4
		16.4.2 HTTP 36	4
		16.4.3 ICA 36	5
		16.4.4 Modbus 36	5
		16.4.5 MS SOL (TDS) 36	5
		16.4.6 MySQL (1D5)	5
		16.4.7 Oracle 36	6
		16.4.8 BDP 36	6
		16.4.0 SSH 36	7
		16.4.0 Tolpot 36	7
		16.4.11 Telnet 2970 36	7
		16.4.12 Telnet 5250	0
		16.4.12 VNC 26	0
		10.4.15 VNO	0
		10.4.14 A11	0
17	AAP	2M (Application to Application Password Manager) 37	0
	17.1	Informacie ogólne	0
	17.2	fudonn 37	0
	17.3	Interfeis API	8
			Č
18	Serv	ice Now 37	9
	18.1	Konfiguracja	9
	18.2	Wnioskowanie o dostęp do serwerów	0
	18.3	Przyznawanie dostępu	2
19	Aplil	kacje klienckie 38	4
	19.1	PuTTY	4
	19.2	Microsoft Remote Desktop	6
	19.3	VNC Viewer	8
	19.4	SQL Server Management Studio	1
20	TIalas	an annual dhe anniourstalaisais 4 East	0
20	USIU	ga proxy dla uwierzyteinienia 4-Eyes 39	ა ე
	20.1	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	ა ე
	20.2	Inicjalizacja konfiguracji za pomocą whiproxyinit	3
	20.3	Zarządzanie klastrami za pomocą whiproxycti	5
		20.3.1 Dodawanie klastra	5
		20.3.2 Usuwanie klastra	5
		20.3.3 Wyświetlanie szczegółów klastra	5
		20.3.4 Wyświetlanie listy klastrów	5
	20.4	Zarządzanie węzłami za pomocą whlproxyctl	6
		20.4.1 Dodawanie węzła do klastra	6
		20.4.2 Usuwanie węzła klastra	6
		20 4 3 Wyświetlenie szczegółów wezłe 30	6

		20.4.4 Wyświetlanie listy węzłów	96
21 I	Rozv	viązywanie problemów 39	9 8
2	21.1	Uruchamianie Wheel Fudo PAM	98
2	21.2	Połączenia z serwerami	99
2	21.3	Logowanie do panelu administracyjnego	04
2	21.4	Odtwarzanie sesji	05
2	21.5	Konfiguracja klastrowa	05
2	21.6	Znakowanie czasem	06
22 (Częs	to zadawane pytania 40)7
23 \$	Słow	nik pojęć 41	LO
Ind	\mathbf{eks}	41	13

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 $2.\mathrm{x}$ a $3.\mathrm{x}.$

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

Wszystkie nazwy, grafiki i znaki firmowe lub towarowe, niebędące własnością firmy Wheel Systems, występujące w tym dokumencie, należą do ich właścicieli i zostały użyte wyłącznie w celach informacyjnych.

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 *ano-nymous* 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,
- $\bullet\,$ sqsh.

2.1.6 MySQL

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Oficjalny klient MySQL,
- Biblioteki PyMySQL dla Pythona.

Uwagi:

- $\bullet\,$ Brak w
sparcia 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:

- $\bullet\,$ 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,
- $\bullet\,$ 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 > Mody-fikatory 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, przezro-czysty) oraz protokół komunikacji.

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

🔁 1 serwer 👗 2 użytkownik 🔊 3 gniazdo nasłuchu 🖉 4 konto 🔳 5		1 serwer	4	2 użytkownik	۳	3 gniazdo nasłuchu		4 konto		5 sejt	F
--	--	------------	---	----------------	---	----------------------	--	-----------	--	----------	---

Ostrzeżenie: Obiekty modelu danych: *sejfy, użytkownicy, serwery, konta* i *gniazda na-słuchiwania* 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.

\mathbf{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.

	Minimalizuj panel opcji
Zarządzanie	Fudo [*]
Dashboard	Menu opcji użytkow
🖽 Sesje	Rozkład liczby połączeń Aktywne sesje użytkowników
볼 Użytkownicy	Sesje Aktywne sesje
🖴 Serwery	00:00 02:00 04:00 06:00 08:00 10:00 Czas Server Użytkownik
🛢 Konta	
Sejfy	
ন্ন Gniazda nasłuchiwania	• seoje
n- Modyfikatory hasel	
♥ Polityki	Aktywność dysku Wykorzystanie Status dysków 11:46 11:47 11:48 dysku
📥 Do pobrania	
🕀 Raporty	68%
≡ Produktywność	Zajęte: 24.4 GB Wolme: 11.4 GB
Ustawienia	Odczyt Ozapis
😂 System	Wykorzystanie pamięci i procesora
¢ Konfiguracja sieci	Pamięć i procesor Sieć
🖂 Powiadomienia	11:46 11:47 11:48 00:00 02:00 04:00 06:00 08:00
C Znakowanie czasem	
a, Zewnętrzne uwierzytelnianie	
III Zewnętrzne repozytoria haseł	
🔚 Zasoby	parties processor
Kopie zapasowe i retencja	Aktywność połączenia sieciowego
👍 Klaster	Dziennik zdarzeń
≓ Synchronizacja LDAP	Czas Typ Komunikat
≡ Dziennik zdarzeń	2016-06-10 11:44:36 user User admin authenticated using password logged in from IP address: 10.0.1.26.
0 28 dei i 12345678 9 pam-26485da Nie skonfigurgwane	2016-06-10 11:12:48 user User admin authenticated using password logged in from IP address: 10.0.1.26.
Status instancji FUD	O Bieżące wpisy z dziennika zd

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.

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:

2. Wprowadź hasło do konta administratora.



3. Wpisz 2 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
```

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):

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



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.

Host docelowy				
Adres	10.0.150.150	Port	22	*
Adres źródłowy	Dowolny			\$
Klucz publiczny serwera	ssh-rsa AAAAB3NzaC1yc2EAAAADAQA	ABAAAB	AQC6pbHklb/uemFNLobQ	
Pobie	erz klucz publiczny SS WEH/UVaSTOUAXTJ21Wx8d8Ri MQ5HIxOkq6TSkmE8WGLISos BGt0e/Q2M0zQFhkZGOgH55r7 KENtv2sb6Ppkm3700hxjH+p59 Odcisk palca	H hos kayonMc katWwE rCEHWZ iKaaoya iKaaoya	72:1c:6d:f0:cc:64:36	

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	×
Тур	Hasło
Hasło	john
Powtórz hasło	john

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.

Tryb połączenia	Pośrednik				¢ 1
Adres lokalny	10.0.150.151	\$	Port	1022	
Klucz publiczny FUDO	WJ Wygene gU Wygene 9SSh0ED9BGcw 2MckzjReQAAAI KH3oWBSSrTVN FOWIIvMoDY7N gkG/eGFDJbwYY UF1yZgBiwYVDy	eruj k e Wg MeFx6d0 GQqG0 DJGYBf4 ZAVBX	IUCZ p raj kli contkRo DwoC/62 wAAAC wAAAC wA+1H5L ndse6jAs	Drywatny SSH BAPA AM BAPA AM SERVICE Prywatny SSH SERVICE VSDRATYW1gnEY67JtOLMdUlJum 7L/MruL+0783ADnYSKgvaQlfdD AlGGYskAACMHEetWsSNDYTTa m+B308698RJ+5BrkRLgbEhBHo sm1afLnswMW2v/kDDmmqpx6n	A Contraction of the second se

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 ${\it Zarządzanie} > {\it Konta}.$
- 2. Kliknij + Dodaj.
- 3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	admin_ssh_server
Zablokowane	×
Тур	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 ha-	×
seł	
Modyfkator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	×
wany	
Hasło użytkownika uprzy-	X
wilejowanego	

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	X
Powód logowania	×
Powiadomienia	X
Polityki	×
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	¥
VNC	X
Uprawnienia	
Uprawniani użytkownicy	×
Powiązania obiektu	
admin_ssh_server	ssh_listener

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.

Management <	Fudo								≜ ad	min ~	?
Dashboard	Sessions	al Active 🕆 Delete	G OCR		¥ Add filter ∨	🕀 Generate repo	search		0	Q.~]
쑬 Users	User	Protocol Server	Account	Safe	Started at +	Finished at	Duration Activity	Size			
🖴 Servers	🗆 🕨 john_smith	SSH ssh_server	admin_ssh_server	ssh_safe	2016-10-17 22:02			10.0 KB	20	≥ ∵ al	
B A	Aktywne poła	aczenie użvtkowi	nika iohn smith	http_safe	2016-10-17 18:23	2016-10-17 18:39	0:16:07 0%	17.0 KB	221	2 ±	
M Accounts	- par cromanar	inter_ourier	and the second	http_safe	2016-10-17 18:21	2016-10-17 18:23	0:01:51 0%	1.8 MB	9.94	e ∷ 4	
Safes	ian_kowalski	ki HTTP http_server	admin_http_server	http_safe	2016-10-17 17:30	2016-10-17 17:46	0:15:47 0%	1.8 MB	(p, γ)	5 II A	

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

8	1 serwer	•	2 użytkownik	۲	3 gniazdo nasłuchu		4 konto		5 sejf
---	------------	---	----------------	---	----------------------	--	-----------	--	----------

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.

Host docelowy					
Adres IP	10.0.150.1	1	Port	22	*
Adres źródłowy	10.0.150.151				\$
Klucz publiczny serwera	ssh-rsa AAAAB3NzaC1yc2EAAAA	DAQABAA	ABAQDMFTQH	kwFfWcl	
Pobierz	klucz publiczny SS	SH host	a docelow	ego 🔭	F/rB IB9Ix
	1QULkQOv9V8lGbZjr/NL T8EhV0hJOlQqW1XDLMg N+utuaDDCmVitLgauQEt bhV4W38lN6zAHFjHR1FC	aDD9PKKn CIUKXn1X HLGXzzPtn Q9ZHND87/	mTia6z8ltBr+a0 H9iHrZZFhsN61 xklscD9itV+aFfn /kEYQpVZZrL3Z	BBgRzwW FWiufZGi B22oXDB ED04mihi	IW6J Fgn7o rcZ2u 03qG
	Odcisk palca —	1			
	a0:5f:e4:a3:31:b0:9f:f4:e8	:72:d9:d5:e	e:4d:5a:c7:d9:54	1:29:57	SHA1

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	X
Telefon	×
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	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.

Połączenie		
Tryb połączenia	Bastion	\$
Adres lokalny	10.0.150.152 ¢ Port	22 *
Klucz publiczny FUDO	Wygeneruj klucz prywatn Axfsgz4fRYU gmk2/1N7Si Wgraj klucz pry AA8L4uslQiT1qki0Qu5SFwphj2w9xTB4 NRjCy12oDV8tQ1NDxbU4Ljp8QdKm9 zSbEjM/+ttfFlkqDnMv5CRxnB/D4QaN d04VdFhkHZsbyyhTCBeazRkyaS1+gb Odcisk palca 53:ea:46:bf:c3:a8:o4:48:8f:f0:15:6b:33:	y SSH aBvmpuics/WeB watny SSH SdJ7)47K xJuEzFvG 4vH+j2doeWurC2yEI56v+esU BiYs9ipq9W86omZmiYXtHW pwJTNgw03v9TlahAdTI+2W ihg/ivHmtITukE7zXfE3OG+rL

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 \checkmark .

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	×
Тур	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 ha-	Statyczne, bez ograniczeń
seł	
Modyfkator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	X
wany	
Hasło użytkownika uprzy-	×
wilejowanego	

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	X
Powód logowania	×
Powiadomienia	×
Polityki	X
Funkcjonalność protokołów	
RDP	×
SSH	se a construction de la construc
VNC	X
Uprawnienia	
Uprawniani użytkownicy	×
Konta	
admin_ssh_server	ssh_listener

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.

🕵 PuTTY Configuration		? 🛛
Category:		
Session	Basic options for your PuTTY se	ssion
	Specify the destination you want to conne	ct to
	Host Name (or IP address)	Port
Bell	10.0.150.151	22
Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH	Connection type: ◎ Raw ◎ Telnet ◎ Rlogin ◎ SSH	H 🔘 Serial
	Load, save or delete a stored session Saved Sessions	
	Default Settings	Load Save
		Delete
i Serial	Close window on exit: Always Never	ean exit
About Help	Open	Cancel

- 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 użyt-kownik 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

8	1 serwer	-	2 użytkownik	۳	3 gniazdo nasłuchu		4 konto		5 sejf
---	------------	---	----------------	---	----------------------	--	-----------	--	----------

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:

	10/+
Parametr	vvartosc
Nazwa	rdp_server
Zablokowane	×
Protokół	RDP
Bezpieczeństwo	Standard RDP Security
Opis	Serwer RDP
U prawnienia	
Uprawnieni użytkownicy	×
Host docelowy	
Adres	10.0.35.10
Port	3389
Adres źródłowy	Dowolny

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

Adres	10.0.35.54 Port 3389	
Adres źródłowy	1 6.0.150 Podaj adres IP serwera oraz port u	sługi
Certyfikat serwera	BEGIN PUBLIC KEY MFwwDQYJKoZihvcNAQEBBQADSwAwSAJBANApps6+1WF1s Var/CNulwboAtX f5ZW3Z6Rab7Cpv VFUCAwEAAQ== END PUBLIC KEY	AGCB

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	X
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	×
Тур	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.

Połączenie		
Tryb połączenia	Pośrednik	¢ ==
Adres lokalny	10.0.150.151 ¢ Port 3389	
Klucz publiczny serwera	Wygeneruj klucz prywatny FUDO dA16xJeT1fno fuzwzcojsti CAWEAAQ== END PUBLIC KEY	*
	Odcisk palca d5:d2:b3:d3:9f:57:59:14:24:20:f4:07:43:29:0a:e4:68:33:ab:e6	IA1

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 menuZarządzanie > Konta.
- 2. Kliknij + Dodaj.
- 3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	admin_rdp_server
Zablokowane	X
Тур	regular
Nagrywanie sesji	wszystko
OCR sesji	4
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	×
Serwer	
Serwer	rdp_server
Dane uwierzytelniające	
Domena	X
Login	admin
Zastąp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora ha-	X
seł	
Modyfkator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	X
wany	
Hasło użytkownika uprzy-	X
wilejowanego	

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	X
Powiadomienia	X
Polityki	X
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	4
SSH	X
VNC	×
Uprawnienia	
Uprawniani użytkownicy	X
Konta	
admin_rdp_server	rdp_listener

4.3.4 Nawiązanie połączenia

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

🗧 😑 💿 🛛 Edit Re	mote Desktops - 10.0.150.151
General Session F	Redirection
Connection name	10.0.150.151
PC name	10.0.150.151
Gateway	No gateway configured
Credentials	
User name	Domain\user
Password	Password
Resolution	Native
Colors	True Color (24 bit)
Full screen mode	OS X native
	Start session in full screen
	Scale content
	Use all monitors

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



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	X
Uprawnienia	
Uprawnieni użytkownicy	X
Host docelowy	
Adres	10.0.35.137
Port	23
Adres źródłowy	Dowolny
Użyj bezpiecznych połą-	X
czeń 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	X
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	Hasło
Hasło	john
Powtórz hasło	john

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 połą- czeń 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:

Davamatu	\\/oxtoóó
Parametr	vvartosc
Og olne	
Nazwa	admin_telnet_server
Zablokowane	×
Тур	forward
Nagrywanie sesji	wszystko
OCR sesji	×
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	X
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	X
Powiadomienia	X
Polityki	X
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	X
VNC	×
Uprawnienia	
Uprawniani użytkownicy	X
Konta	
admin_telnet_server	telnet_listener

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.

Zarządzanie	¢	۴ı	lqo,											🕹 adi	min ~ 1	?
Dashboard			1. J.	Aktywne	i Ωsuń	I OCR			▼ Dodai filtr ~	A Gene	rui raport	Szukai		0	۹v	
💾 Sesje	r	505	sje E									ousingin		-	-	
管 Użytkownicy		_	Użytkownik	Protokół	Serwer	Konto		Sejf	Rozpoczęta +	Zakończona	Czas trwania	Aktywność	Rozmiar		_	
⊖ Serwery			john_smith	Telnet	teinet_server	admin_telnet	_server	teinet_safe	2016-10-18 00:47				10.0 KB		•)
🖻 Konta		A	ktywne p	połącze	enie użytł	kownika jo	hn_s	mith —								

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

8	1 serwer	-	2 użytkownik	۳	3 gniazdo nasłuchu		4 konto		5 sejf
---	------------	---	----------------	---	----------------------	--	-----------	--	----------

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 połą-	×					
czeń 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	X
Telefon	×
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	X
Тур	Hasło
Hasło	john
Powtórz hasło	john

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	telnet_listener					
Zablokowane	×					
Protokół	Telnet 5250					
Włącz obsługę SSLv2	×					
Włącz obsługę SSLv3	×					
U prawnienia						
Uprawnieni użytkownicy	×					
Połączenie						
Tryb połączenia	Pośrednik					
Adres lokalny	10.0.150.151					
Port	23					
Użyj bezpiecznych połą-	X					
czeń 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	X
Тур	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	X
Polityki	X
Użytkownicy	john_smith
$Funkcjonalność\ protokołów$	
RDP	×
SSH	×
VNC	×
Uprawnienia	
Uprawniani użytkownicy	×
Konta	
admin_telnet_server	telnet_listener

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.

2	9								Session A - [24 x 80]
	File	Edit View	Comn	nunication	Actio	ons V	Vindow	v Help	
(7	2	1	•		8	٠
	FUD	0 Auth	enti	catio	n . –				
l	Jse	ername:	_						
	as,	sword:							
	10	A							

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.
D Session A - [24 x 80]	
File Edit View Communication Actions Window Help	
MAIN IBM i Main Menu System:	
Select one of the following:	
1. User tasks	
2. Office tasks	
3. General system tasks	
4. Files, libraries, and folders	
5. Programming	
6. Communications	
7. Define or change the system	
8. Problem handling	
9. Display a menu	
IV. Information HSSIStant options	
II. IBM I HCCESS TASKS	
90. Sian off	
Selection or command	
===>	
F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assi	S
F23=Set initial menu	
(C) COPYRIGHT IBM CORP. 1980, 2015.	
MA A	

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.

						IBM	i Main Menu	9			
								Syst	em: PUB40	U	
				1. 0 2. 0 3. 0 4. 1 5. 1 6. 0 7. 1 8. 1 9. 1 10. 1 11. 2	User tasks Office tasks General system Files, librarie Programming Communications Define or chang Problem handlin Display a menu Information Ass EBM i Access ta	tasks s, and folde the system g istant optio sks	ns				
				90. 8	Sign off						
				Selection	or command						
				F3=Exit F23=Set i (C) COPYE	F4=Prompt F nitial menu RIGHT IBM CORP.	9=Retrieve 1980, 2015.					
	» »»	¢ N	0:00:22							N 0:00:22	Info
ĊТ	rminate	🕞 Join	Pause								

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

😑 1 serwer 🔺 2 użytkownik 💊 3 gniazdo nasłuchu 🧧 4 kon	onto 🔳 5 sejf
--	-----------------

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	X
Protokół	MySQL
Opis	X
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	X
Telefon	×
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	Hasło
Hasło	john
Powtórz hasło	john

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
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	×
Тур	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 ha-	X
seł	
Modyfkator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	X
wany	
Hasło użytkownika uprzy-	X
wilejowanego	

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	X
Polityki	X
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	X
VNC	×
Uprawnienia	
Uprawniani użytkownicy	X
Konta	
admin_mysql_server	mysql_listener

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.

Zarządzanie < Fudo [*]			admin 🗧 ?
Dashboard Secie Aktywne 🗟 Usuń 🖾 OCR 🕇 Dodaj filtr v 🔒 Generuj raport	Szukaj		0 Q~
Besje			
🔮 Użytkownicy 📃 Użytkownik Protokół Serwer Konto Sejf Rozpoczęta + Zakończona Czas trwania	i Aktywność R	Rozmiar	
Serwary	3	3.0 KB 🔗	· • ·)
Konta Aktywne połączenie użytkownika john_smith			
Selfy			
• • • Sesja 848388532111147061			
A https://10.0.150.151/sessions/84838853211114/061/?i=1&qi=on&qc=on&live=2016-10-18+03%3A17%3A59&qo=on			
Sesja: 848388532111147061, użytkownik: john_smith, serwer: mysql_server			ථ Zakończ
INIT	20)16-10-18 03:1	7:33.035478
Funkcjonalności: CULENT_IGNORE_SPACE, CLIENT_RESERVED, CLIENT_PLUGIN_AUTH, CLIENT_INTERACTIVE, CLIENT_SCOURE_CONNECTION, CLIENT_NULTI, CLIENT_NO_SCHEMA, CLIENT_TRANSACTIONS, CLIENT_IGNORE_SIGPIPE, CLIENT_LONG_FLAG, CLIENT_CONNECT_WITH_DB, CLIENT_FOUND_ROWS, CLIENT_PLUGIN_AUTH_LENENC_CLIENT_DATA, CLIENT_LOCAL_FILES, CLIENT_COMPRESS, CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_COMPRESS, CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_OK OK Zmienione wiersze: 0 Ostatnio wstawione ID: 0 Stan: 2 Ostrzeżenie: 0 Informacia:	_RESULTS, CLII	ENT_CONNEC	CT_ATTRS, RESULTS, 17:33.035478
Linenone wersze. U Ostauno watawione ibi U Otani z Osużeżenie. U miorinacja.			
COM_QUERY	20)16-10-18 03:1	7:33.037478
Zapytanie:			
select @@version_comment limit 1			
00:00:00	00:01:18	 Informacje Zakończ 	Udostępnij Wstrzymaj

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.*

Server Properties - MSEDGE	WIN10\FUDO	_		×
Select a page General	🖵 Script 🔻 😮 Help			
 Memory Security Connections Database Settings Advanced Permissions 	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Upewnij się, że opcja 'SQL Server and Windows Aut Cogin Vone Failed logins only Successful logins only Both failed and successful logins Server proxy account	henticatior jest w	n mode' łączona	
Connection	Enable server proxy account			
Server: MSEDGEWIN10\FUDO	Proxy account: Password:			
Connection: fudo	Options			
₩ <u>View connection properties</u>	 Enable C2 audit tracing Cross database ownership chaining 			
Progress				
Ready				
		ОК	Cano	el

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	X
Protokół	MS SQL (TDS)
Opis	X
Uprawnienia	
Uprawnieni użytkownicy	×
Host docelowy	
Adres	10.0.150.154
Port	1433
Adres źródłowy	Dowolny

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	X
Ważność konta	Bezterminowe
Rola	user
Preferowany język	polski
Pełna nazwa	John Smith
Email	×
Organizacja	X
Telefon	×
Domena AD	×
Baza LDAP	X
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	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	X
Połączenie	
Tryb połączenia	Pośrednik
Adres lokalny	10.0.150.150
Port	1433

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 menuZarządzanie > Konta.
- 2. Kliknij + Dodaj.
- 3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	admin_mssql_server
Zablokowane	×
Тур	regular
Nagrywanie sesji	wszystko
OCR sesji	X
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 ha-	X
seł	
Modyfikator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	X
wany	
Hasło użytkownika uprzy-	X
wilejowanego	

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	X
Powiadomienia	X
Polityki	X
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	X
VNC	X
Uprawnienia	
Uprawniani użytkownicy	×
Konta	
admin_mssql_server	MSSQL_proxy

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.

모 ^를 Connect to Server		×
	SQL Server	
Server type:	Database Engine	\sim
Server name:	10.0.150.150	~
<u>Authentication:</u>	SQL Server Authentication	~
<u>L</u> ogin:	john_smith	~
Password:		
	Remember password	
	Connect Cancel	Help <u>O</u> ptions >>
Incrosoft SQL Server Management Studio File Edit View Debug Tools Window Help Image: Second	☆ ☆ ☆ ☆ ☆ ☆ ☆ ☆ ↓ 2 - ℃ - 1 22	Quick Launch (Ctrl+Q) 🔎 – 🗖 🗙

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 \blacktriangleright .

Zarządzanie <	Fudo f			🛔 adr	nin ~	?
础 Dashboard ∯ Sesje	Sesje ⊜ Usuń ⊠ OCR		▼ Dodaj filtr ∨ Szuka	lj	0	۹v
Użytkownicy	🗆 Użytkownik Protokół Serwar Konto Sejf	Rozpoczęta • Zakończona	Czas trwania Aktywnoś	ó Rozmiar		_
B Serwerv	b john_smith MS SQL (TDS) mssql_server admin_mysql_server mss	sql_safe 2017-08-10 09:57		6.0 KB	• • •	· -)
R Konta	Aktywne połaczenie użytkownika john smith ^{ver m} s	sql_safe 2017-08-10 09:57		3.0 KB	-	- 4
er Konta		sql_safe 2017-08-10 09:57 2017-08-10 09:57	0:00:24	2.0 KB		±
ิ Gniazda nasłuchiwania	John_smith MS SQL (TDS) mssql_server admin_mysql_server mss bioba smith MS SQL (TDS) mssql_server admin_mysql_server it's	sql_safe 2017-08-10 09:57 2017-08-10 09:57	0:00:00	4.0 KB		- A-
Sejfy	 john_smith MS SQL (TDS) mssql_server admin_mysql_server it's john_smith MS SQL (TDS) mssql_server admin_mysql_server it's 	sare 2017-08-10 09:44 2017-08-10 09:51 safe 2017-08-10 09:44 2017-08-10 09:55	0:11:01	5.0 KB		- <u>-</u>
	Sesja 8483885321111	47120				
A Not Secure https://10.0.150.150/s	ssions/848388532111147120/?i=1					
Sesja: 8483885321	11147120, użytkownik: john_sm	hith, serwer: mssql	server		ΰZ	akończ
Pakiet SQL						
DECLARE @edition sysname; SET @e	lition = cast(SERVERPROPERTY(N'EDITION') as sysname);	lect case when @edition = N'SQL Az	ure' then 2 else 1 e	nd as 'Data	abaseE	ngineTy
SELECT SERVERPROPERTY('EngineEdi	ion') AS DatabaseEngineEdition					
select N'Windows' as host_platfo	m					
Wynik tabularyczny						
host_platform						
1						
04000000						
Windows						
Pakiet SQL						
			NI da com		- FCT	
IF((SELECT MAS_PERMS_BY_NAME(nu)	., null, 'view SERVER STATE')) = 1) BEGIN IF EXISTS(SELEC	ui * rkum sys.system_views WHERE na	ame = N'dm_server_re	gistry) SE	ELECT	value_
	SERVERPROPI	ERTY('ProductBuildType') AS [Produ	ctBuildType],			
	SERVERPROPI	ERTY('ProductLevel') AS [ProductLe	vel],			
	SERVERPROPI	ERTY('ProductUpdateLevel') AS [Pro	ductUpdateLevel],			
	6551/5555651			,		
₩ 00:00:00			00:01:10	Informacje	e u	dostępnij
				ථ Zakończ	Wstrzy	/maj

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

8	1 serwer	•	2 użytkownik	۳	3 gniazdo nasłuchu		4 konto		5 sejf
---	------------	---	----------------	---	----------------------	--	-----------	--	----------

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	X
Host docelowy	
Adres	www.wheelsystems.com
Port	80
Host HTTP	X
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	X
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	X
Тур	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	X
Połączenie	
Tryb połączenia	Pośrednik
Adres lokalny	10.0.150.151
Port	8080
Użyj bezpiecznych połą-	X
czeń (TLS)	

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	×
Тур	forward
Nagrywanie sesji	wszystko
OCR sesji	×
Usuń dane sesji po upływie	61 dni
U prawnienia	
Uprawnieni użytkownicy	×
Serwer	
Serwer	http_server
Dane uwierzytelniające	
Zastąp sekret	hasłem
Hasło	×
Powtórz hasło	X

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	X
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.

Zarządzanie <	Fud	io*			4	admin 🕤 🥐
Dashboard Sesje	Sesje	al Aktywne 🖹 Usuń 🖾 OCR		▼ Dodaj filtr ~ 🔒 Generuj raport	Szukaj	0 Q.~
🖆 Użytkownicy		izvíkownik Protokół Serwer Konto Seił	Rozpoc	zeta + Zakończona Czas trwania	Aktywność Rozmiar	
⊖ Serwery	ol 🔺 🗆	hn_smith HTTP http_server admin_http_server http.	safe 2016-1	0-18 03:56	17.0 KB	ः इ ः ज्य
🖉 Konta	Aktyv	vne połączenie użytkownika john_smith -				
Sejfy						
•••		Sesja 8483885321111	47064			
Sesja: 848388532111	14706	4, Użytkownik: john_smith		0 -11	101 - 6	ථ Zakońc
URL	Metoda	lyp	Hozmiar	GZas	UHL referencji	
/	GET	text/html; charset="UTF-8"	0 bajtów		http://10.0.150.151:8080)/
/webapi/entry.cgi? api=SYNO.Core.Desktop.SessionData&version	GET	application/javascript; charset="UTF-8" 0 bajtów			http://10.0.150.151:8080)/
/webman/security.cgi	GET	application/javascript; charset="UTF-8"	0 bajtów		http://10.0.150.151:8080)/
/webapi/query.cgi	POST	text/plain; charset="UTF-8"	0 bajtów		http://10.0.150.151:8080)/
/	GET	text/html; charset="UTF-8"	0 bajtów	2016-10-18 03:56:54.475365	http://10.0.150.151:8080)/
/webapi/entry.cgi? api=SYNO.Core.Desktop.SessionData&version	GET	application/javascript; charset="UTF-8"	0 bajtów	2016-10-18 03:56:55.442225	http://10.0.150.151:8080)/
/webman/security.cgi	GET	application/javascript; charset="UTF-8"	0 bajtów	2016-10-18 03:56:55.524982	http://10.0.150.151:8080)/
/webapi/query.cgi	POST	text/plain; charset="UTF-8"	0 bajtów	2016-10-18 03:56:57.442414	http://10.0.150.151:8080)/
/webapi/encryption.cgi	POST	None	0 bajtów	2016-10-18 03:57:32.865450	http://10.0.150.151:8080)/
/webman/login.cgi?enable_syno_token=yes	POST	None	0 bajtów	2016-10-18 03:57:33.042313	http://10.0.150.151:8080)/

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 używająć 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

₿	1 serwer	4	2 użytkownik	۳	3 gniazdo nasłuchu		4 konto		5 sejf
---	------------	---	----------------	---	----------------------	--	-----------	--	----------

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	10.0.21
Port	1494
Użyj TLS	X

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	X
Ważność konta	Bezterminowe
Rola	user
Preferowany język	polski
Pełna nazwa	John Smith
Email	×
Organizacja	×
Telefon	×
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	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 połą- czeń (TLS)	×

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	X
Тур	regular
Nagrywanie sesji	wszystko
OCR sesji	X
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	×
Serwer	
Serwer	ica_server
$Dane \ uwierzytelniające$	
Domena	X
Login	citrixuser
Zastąp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora ha-	Statyczne, bez ograniczeń
sła	
Modyfikator hasła	
Modyfikator hasła	Brak
Użytkownik uprzywilejo-	×
wany	
Hasło użytkownika uprzy-	X
wilejowanego	

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	X
Powiadomienia	X
Polityki	X
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	X
VNC	×
Uprawnienia	
Uprawniani użytkownicy	X
Powiązania obiektu	
admin_ica_server	ica_listener

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: Szczegółówe 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
- $\bullet \ ICA$

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

🔒 1 serwer	4	2 użytkownik	۳	3 gniazdo nasłuchu	4 konto	5 sejf
					·	

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	10.0.21
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	X
Połączenie	
Tryb połączenia	Pośrednik
Adres lokalny	10.0.150.151
Port	2494
Użyj bezpiecznych połą- czeń (TLS)	×

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:

Daramatr	Martoćć
Falameti	VVal LOSC
Ogólne	
Nazwa	ICA_forward
Zablokowane	×
Тур	forward
Nagrywanie sesji	wszystko
OCR sesji	×
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	×
Serwer	
Serwer	ica_server
Dane uwierzytelniające	
Zastąp sekret	X
Przekazuj domenę	4

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	X
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	×
Тур	regular
Nagrywanie sesji	wszystko
OCR sesji	×
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	X
Serwer	
Serwer	citrix_storefront
Dane uwierzytelniające	
Domena	tech.whl
Login	citrixuser
Zastąp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora ha-	Statyczne, bez ograniczeń
sła	
Modyfikator hasła	
Modyfikator hasła	brak
Użytkownik uprzywilejo-	×
wany	
Hasło użytkownika uprzy-	×
wilejowanego	

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	X
Domena AD	X
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	X
Тур	Hasło
Hasło	john
Powtórz hasło	john

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	X
Polityki	X
Użytkownicy	john_smith
$Funkcjonalność \ protokołów$	
RDP	×
SSH	×
VNC	×
Uprawnienia	
Uprawniani użytkownicy	X
Konta	
citrixuser_at_SF	citrix_storefront_listener
ICA_forward	ica_listener

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.

۴l	יםם.
	Authentication
Login	
Passw	ord
	Login
_	

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.

Za	rządzanie <	Fudo									
الل	Dashboard	Regio II	Usuń 🖼 OCR 🕜	Czas	🕀 Generuj rapo	ort			r Dodaj filtr v	Szukaj	
đ	Sesje	Sesje									
쓭	Użytkownicy	Użytkownik	Protokół	Serwer	r Konto	Seif	Rozpoczęta v	Zakończona	Czas trwania	Aktywność	
A	Serwery	🗆 🕨 admin	Citrix StoreFront (HTTP)	SF	citrixuser at SF	Citrix	2017-02-15 12:19			0%	1
		Aktywne po	łaczenie użytkow	nika i	iohn smith -	Citrix	2017-02-15 12:16	2017-02-15 12:17	0:00:35	0%	1
8	Konta	, anywhic po	iqezenie uzytkow	iiii.a j		Citrix	2017-02-15 11:48	2017-02-15 12:08	0:19:47	0%	1
2	Gniazda nasłuchiwania	🗆 🕨 admin	Citrix StoreFront (HTTP)	SF	citrixuser at SF	Citrix	2017-02-14 22:12	2017-02-14 22:31	0:19:36	0%	1
	Seifv	anonymou	s ICA	ICA	anonymous@ICA	Citrix ICA-ANONYMOUS	2017-02-14 18:37	2017-02-14 18:38	0:00:39	100%	
		Admin	ICA	ICA	citrixuserICA	Citrix-BASTION	2017-02-14 18:37	2017-02-14 18:37	0:00:13	100%	1
- 11-	Modyfikatory haseł	Admin	ICA	ICA	forward@ICA	Citrix	2017-02-14 18:35	2017-02-14 18:36	0:00:38	100%	1

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	X
Uprawnienia	
Uprawnieni użytkownicy	×
Host docelowy	
Adres	10.0.40.230
Port	5900
Adres źródłowy	Dowolny

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	X
Telefon	×
Domena AD	×
Baza LDAP	×
Uprawnienia	
Uprawnieni użytkownicy	×
Тур	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	vnc_listener
Zablokowane	×
Protokół	VNC
Uprawnienia	
Uprawnieni użytkownicy	×
Tryb połączenia	Pośrednik
Adres lokalny	10.0.150.151
Port	5900

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	×
Тур	regular
Nagrywanie sesji	wszystko
OCR sesji	4
Usuń dane sesji po upływie	61 dni
Uprawnienia	
Uprawnieni użytkownicy	×
Serwer	
Serwer	vnc_server
$Dane\ uwierzytelniające$	
Domena	X
Login	×
Zastąp sekret	hasłem
Hasło	root
Powtórz hasło	root
Polityka modyfikatora ha-	×
seł	
Modyfkator hasła	
Modyfikator hasła	brak
Użyj istniejące konto	×
Użytkownik uprzywilejo-	X
wany	
Hasło użytkownika uprzy-	×
wilejowanego	

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	X
Powód logowania	×
Powiadomienia	X
Polityki	×
Użytkownicy	john_smith
Funkcjonalność protokołów	
RDP	×
SSH	X
VNC	4
Uprawnienia	
Uprawnieni użytkownicy	X
Powiązania obiektu	
admin_vnc_server	vnc_listener

4.10.3 Nawiązanie połączenia

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

•••	VNC Viewer	
10.0.150.151		👤 Sign in 🗸

2. Wprowadź nazwę użytkownika, hasło i zatwier
dź klawiszem enter.

	10.0.150.151 (Fudo) - VNC Viewer	
	FIICO	
	. 888	
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.

Za	arządzanie	<	Fudo [®]									🚺 🛎 adr	nin ~	?
	Dashboard		Sesje	Usuń 🖾 OC	R Czas	🔒 Generuj rap	prt			▼ Dodaj filtr ∨	Szukaj		0	٤~
-			Użytkownik	Protokół	Serwer	Konto	Sejf	Rozpoczęta 🔻	Zakończona	Czas trwania	Aktywność	Rozmiar		
			▶ john_smith	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:28				258.0 KB		ы
			► test	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:10	2017-11-08 13:23	8 0:13:10	8%	1.8 MB		*
			► test	VNC	VNC_andrzej	VNC_anonim	vnc_safe	2017-11-08 13:00	2017-11-08 13:00	0 0:00:05	100%	345.0 KB		*
2			 test 	VNC	VNC_server	admin_vnc_server	VNC_safe_no_password	2017-11-08 12:59	2017-11-08 13:00	0:00:07	100%	139.0 KB		*

- 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.

			LDAP 1	0.0.0.2:389
DC	=co	m		
	DC	=example		
		CN=admin		

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
Тур	LDAP
Adres hosta	10.0.0.2
Port	389
Wysyłaj żądania z	10.0.10
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	×

Тур	LDAP +			\$	*	
Adres hosta	10.0.0.2	Port	389		*	
Wysyłaj żądania z	10.0.0.10 \$					
Bind DN	dc=example,dc=com					
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.

Uwierzytelnienie

Тур	Zewnętrzne uwierzytelnianie	\$
Zewnętrzne źródło uwierzytelnienia	LDAP 10.0.0.2:389 zbinduj do:dc=example,dc=com	\$ *
Usuń		

7. Kliknij Zapisz.

- 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 na-słuchiwania* 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.

Za	rządzanie	Dodaj uytkowni	ka			🛎 admin 🕤 💡 🤶	
		Uindkowniau	+ Dodaj O Blokuj	Odblokuj 🕾 Usuń	▼ Dodaj filtr ~	Szukaj O Q	
₿		Ozytkownicy					
쓭	Użytkownicy	🗆 Login 🔺	Rola Organizacja	Email Pelna nazwa	Metoda uwierzytelnienia	Ostatnie logowanie	
		admin	superadmin WHL_LAB	Imię Nazwisko	Hasło	8 minut temu	
		admin0	admin	email@email.aa	Hasło	3 miesiące temu	
₽		administrator	admin		Hasło	nigdy	
		 andrzej 	user		Hasło	2 lata, 5 miesięcy temu	
۳	Gniazda nasłuchiwania	anonymous	user			2 lata, 2 miesiące temu	

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.

Zarządzanie <	Fudo	ahu zdefiniować ututkownika na podobioństwo wokranaco obiał	🕹 admin 🗸 🧘
Jul Dashboard	Użytkownik 🖓 Kopiuj użytł	cownika	
🖽 Sesje			
Użytkownicy	Ogólne		
⊖ Serwery	ID	848388532111147009	
🛢 Konta	Synchronizacja z LDAP	0	
Sejfy	Login	admin	*
Siniazda nasłuchiwania			

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 utwo-rzeniu 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	\bullet 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).

$\operatorname{superadmin}$

- 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.

Zarzadzanie <	Fudo'	
Dashboard		
FI Sesie	Użytkownik	
 Użytkownicy 	Ogólne	Unikatowy login użytkownika
⊖ Serwery	Login	
🔊 Konta	1.0gm	
Sejfy	Zablokowane	Zablokuj konto po utworzeniu
niazda nasłuchiwania	Weine (6 kente	Okresi dalę ważności konta
n- Modyfikatory haseł	wazność konta	Zdefiniuj prawa dostepu u
🛡 Polityki	Rola	(user 🗘
📩 Do pobrania		Wybierz preferowany jęz
	Preferowany język	polski •
	Seifv	(Nada) uprawnienia dostę
E Produktywnosc		Imię i nazwisko użytkow
Ustawienia	Pełna nazwa	
System	Email	Adres email
¢6° Konfiguracja sieci	Organizacia	lednostka organizacyji
Powiadomienia	- Sauranda	
Znakowanie czasem	Telefon	- Numer telefonu
4 Zewnętrzne uwierzytelnianie	Domena AD	Domena Active Direct
III Zewnętrzne repozytoria haseł	Baza LDAP	Parametr BaseDN usł
🖾 Zasoby		
Kopie zapasowe i retencja	Uprawnienia	
å Klaster	Uprawnieni użytkownicy	० २
≓ Synchronizacja LDAP	Ilwierzutelnienie	Użytkownicy uprawnieni do zarządzania kontem
≡ Dziennik zdarzeń	Owierzyteinienie	
	Тур	÷
0 1 daleń i 12345678 % 3-30363 du Nie skonfigurowany	Usuń	Sposób uwierzytelnienia użytkownika
	API	-
	Dodaj źródłowy adres IP	+ Źródłowy adres IP wykorzystywany w dostępie poprzez interfejs API
		Zdefiniuj kolejną metodę ywierzyteln
		S Przywróć Zapisz Zapisz definicję obiektu +Dod

- 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.

Za	ırządzanle <	Fudo						
Jashboard		Użytkownicy	+ Dodaj	© Blokuj	© Odbiokuj	Usuń	₹ Dodaj fil	tr - Szukaj
₿	Sesje	CLYROWING						
쓭	Użytkownicy	🗆 Login 🔺	Rola	Organizacja	Email	Pelna nazwa	Metoda uwierzytelnienia	Ostatnie
	Serwerv	admin	superadmin	WHL_LAB		lmię Nazwisko	Haslo	8 minut
		admin0	admin		email@email.	aa	Hasło	3 miesia
₽	Konta	 administrator 	Edytuj ob	biekt			Haslo	nigdy
	Sejfy	 andrzej 	user				Haslo	2 lata, 5
2	Gniazda nasłuchiwania	anonymous	user					2 lata, 2

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.

Za	rządzanie <	Fudo			💄 admin 🗸	?
.11	Dashboard		街 Kopiu	j użytkownika		
⊞	Sesje	Uzytkownik				
*	Użytkownicy	Ogólne				
8	Serwery		ID	848388532111147082		
Ø	Konta					
	Sejfy	Synchronizacja z	LDAP			
٣	Gniazda nasłuchiwania	Login		john_smith	*	

• Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną $\ensuremath{\mathbb{Z}}$.

Ogólne		Niezapisane zmi	any w konfiguracji
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy	0	
	Opis	Opis	

Tematy pokrewne:

- Synchronizacja użytkowników
- Model danych
- Pierwsze uruchomienie
- Serwery
- \bullet 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.

Za	rządzanie <	Fudo					🚢 admin		?
M		Użytkownicy	+ Dodaj OBlokuj) © Od	Iblokuj 🔋 Usuń		▼ Dodaj filtr ~	Szukaj	0	۹
₿		797	acz obiekty						
쓭	Użytkownicy	D Login +		Email Pelna naz	wa Metoda uw	ierzytelnienia	Ostatnie logowanie		
_		admin	superadm. Zablokuj oblekty	Imię Naz	visko Hasło		8 minut temu		
		admin0	admin	email@email.aa	Hasło		3 miesiące temu		
₽		administrator	admin		Haslo		nigdy		
		 andrzej 	user		Hasio		2 lata, 5 miesięcy temu	4	
2		anonymous	user				2 lata, 2 miesiące temu	u	

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.

Za	rządzanie <	≓udo [•]	
.11	Dashboard	Lindsownik 🖓 Kopiuj	użytkownika
⊞	Sesje	Ozytkownik	
*	Użytkownicy	Ogólne	
8	Serwery	ID	848388532111147024
	Konta		
٣	Gniazda nasłuchiwania	Synchronizacja z LDAP	
	Sejfy	Login	john_smith #
÷	Modyfikatory haseł		_
U	Polityki	Zablokowane	Powód
	• Kliknij Zapisz.		

- 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.

Za	rządzanie <		Fudo'							
	Dashboard			+ Dodai	© Blokul	Odblokul	🛱 Usuń		T Dodai filtr v	Szuka
₿		P	Użytkownicy		e bionaj	(constant)			t boult int	GEGRA
*	Użytkownicy		🔘 Login 🔺	Zaznacz	z obiekty	Email	Peina nazwa	Metoda uwi	erzytelnienia	Ostatnie
	Serwenz		🛛 adm Odblok	kuj wybran	e obiekty		Imię Nazwisko	Hasło		0 minut
			admin0	admin		email@	email.aa	Haslo		3 miesi
			administrator	admin				Haslo		nigdy
			 andrzej 	user				Hasło		2 lata, 5
2	Gniazda nasłuchiwania		anonymous	user						2 lata, 2

4. Kliknij Zatwierdź, aby potwierdzić odblokowanie obiektu.

Odblokuj obiekty	×
Jesteś pewien że chcesz odbiokować 1 obiekt?	
	Anuluj Zatwierdź
	Odblokuj obiekt

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 użyt-kownika.

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.

Za	rządzanie <	Fudo					
æ	Dashboard		+ Dodei O Biokui	@ Odhiokui		T Dodai filtr v Sau	ikai
в		Użytkownicy	- Dodaj - Diokaj			t bouaj inu *	ina,
*	Użytkownicy	O Login Zaz	nacz obiekty _{anizacja}	Email Pelna naz	swa Metoda uw	ierzytelnienia Osta	stnie
	Servien	admin	Usuń wybrane obiekty	Imię Naz	wisko Hasło	8 mi	inut
		(B) admin0	admin	email@email.aa	Hasło	3 mi	iesi
₽		administrator	admin		Hasło	nigd	ły
		 andrzej 	user		Hasło	2 lat	ta, t
2	Gniazda nasłuchiwania	anonymous	user			2 lat	a, 2

4. Potwierdź operację usunięcia zaznaczonych obiektów.

Usuń obiekty	×
Jesteś pewien że chcesz usurąć 1 obiekt?	
	Anuluj
	Usuń obiekt

- 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.

Preferred language	English Kliknij, aby zdefiniować politykę czasową dla sejfu	\$⊪
Safes	RDP SSH portal © Q	
Full name		
Email		

- 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 Użyt-kownika*.
- 9. Kliknij kalendarz, aby zdefiniować przedziały czasowe, w których użytkownik będzie mógł się łączyć poprzez konta przypisane do wybranego sejfu.

Polityk	a cza	su dostęp	u do sej	jfu test dla	i użytkownika	john_smit	th X
	Zal	blokowane	0-	Zabloku	j dostęp do sej	jfu	
	Od	2017-11-23	13:21:43		Zdefiniuj int	terwał dost	ępu do sejfu
	Do	2017-11-26	13:21:45				
	_			Kliknij, aby	/ aktywować p	olitykę cza	isową dla sejfu
Włąca	z polityk	ę czasową	0		Pokaż hasło	O	
	00:0	0	Zez	walaj na po	odgląd haseł –	2	3:59
Poniedzi	iałek						
Wto	orek	\circ					
Śr	oda			(liknij, abv	zdefiniowanć p	orzedział c	zasowy
Czwar	rtek			<u>,</u> , ,	I		
Pia	ątek						
Sob	oota						
Niedz	tiela						
						An	uluj OK

- 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, 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).

$\operatorname{superadmin}$

- 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.

Zarządzanie <	ビロロ [®] Panel administracyjny
M Dashboard	
💾 Sesje	
🛎 Użytkownicy	Ogólne definicję użytkownika
🕂 Połączenia	Synchronizacja z LDAP
⊖ Serwery	Login def
🛡 Polityki	Zablokowane 🗌
📩 Do pobrania	Ważnośc konta Bezterminowe \$
🖨 Raporty	
Ustawienia	Rola user 0

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.

Synchronizacja LD	AP				
_	Włączone	٥			
Primary 🕕				AD (no controllers specified)	$\mathbf{\vee}$
	Nazwa	Primary			
	Priorytet	0	*		
		Wymuś pełną synchronizację			

- 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.
- 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).

Usługa katalogowa		
Rodzaj serwera	Active Directory	ale .
	· · · · · ·	-
Login	Administrator] •
Hasło		ale .
Domena	tech.whl	ale .
Podstawowy użytkownik	DC=tech,DC=whl	ste
Podstawowa grupa	DC=tech,DC=whl	ale .
Filtr użytkowników	(&(objectclass=user))	ale
Filtr grup	(&(objectclass=group))] 4 F

- 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 ocję *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.

Kontrolery LDAP				
Adres	10.0.0.4	Port	389	
Stronicuj wyniki LDAP				
Połączenie szyfrowane				
Usuń				
	+			

18. Zdefiniuj mapowanie pól atrybutów definicji użytkowników.

Mapowanie atrybutów		
Login	sAMAccountName	ak.
		- -
Email	mail	*
Przydział do grupy	memberOf	ale:
Telefon	telephoneNumber	a t
Organizacja	company	*
Pełna nazwa	displayName	*
Nazwa wyróżniająca (DN)	distinguishedName	ali:
GUID	objectGUID	ale

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.

Mapowanie grup		
Mapowanie	CN=t1,OU=testowa,DC=tech,DC	×
	CN=t1,OU=testowa,DC=tech,DC + Wybierz definicję z listy	×
	CN=Administratorzy,CN=Builtin,DC=tech,DC=whl	×
	CN=Administratorzy funkcji Hyper-V,CN=Builtin,DC=tech,DC=whi CN=Administratorzy funkcji Hyper-V,CN=Builtin,DC=tech,DC=whi	×
	CN=Administratorzy przedsiębiorstwa,CN=Users,DC=tech,DC=whl CN=Administratorzy schematu,CN=Users,DC=tech,DC=whl	×
L	Admini oracle \$ a _{t v}	×
	+	

- 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.

Group mappings

 ✓ CERB ✓ Radius △ AD Mapping ✓ Group A → Connection SSH ◆ ✓ × × 	Mapping 📝	Group B	∢	Connection	RDP	*	a, ~	×
✓ Radius AD Mapping ⊘ Group A → Connection SSH ♦ Q ₄ ∨ X					CEF	RB		
□ AD Mapping Group A → Connection SSH ♦ Q × ×					🗹 Rad	lius		
Mapping Group A Connection SSH Connection SSH					D AD			
	Mapping 🕝	Group A	→	Connection	SSH	\$	a. ~	×
		_				RB		
		T			Rad	lius		
Ø AD					🖸 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.

Za	rządzanie <		Fudo						
M	Dashboard			+ Dodaj	© Blokuj	Odblokuj	A Usuń	▼ Dodai	filtr v Szuka
₿		P	Uzytkownicy						
*	Użytkownicy		🗆 Login 🔺	Rola	Organizacja	Email	Pelna nazwa	Metoda uwierzytelnienia	Ostatnie
			admin	superadmin	WHL_LAB		Imię Nazwisko	Hasło	8 minut
			admin0	admin		email@en	nail.aa	Hasło	3 miesi
₽			administrator	Edvtuj ob	piekt			Haslo	nigdy
			 andrzej 	user				Haslo	2 lata, ŝ
۳	Gniazda nasłuchiwania		anonymous	user					2 lata, 2

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

4. W sekcji Fudo Mobile, kliknij Dodaj urządzenie.

Fudo Mobile	
	z tymoży Zainicjuj parowanie z aplikacją Fudo Mobile 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.

- 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.

Za	rządzanie <		Fudo [®]						
M	Dashboard			+ Dodaj	© Blokuj	© Odbiokuj	🕆 Usuń	T Do	odaj filtr v Szuka
₿		P	Uzytkownicy						
*	Użytkownicy		🗆 Login 🔺	Rola	Organizacja	Email	Peina nazwa	Metoda uwierzytelni	enia Ostatni
	Serwerv		admin	superadmin	WHL_LAB		Imię Nazwisko	Haslo	8 minu
			admin0	admin		email@en	nail.aa	Hasło	3 miesi
₽			administrator	Edytuj ob	viekt			Haslo	nigdy
			andrzej	user				Haslo	2 lata,
2	Gniazda nasłuchiwania		anonymous	user					2 lata, 3

4. W sekcji Fudo Mobile, kliknij Usuń urządzenie.

Fudo Mobile	
Enabled	0
Platform	iOS
Push ID	⁸⁴⁸³⁸ Usuń urządzenie
	Remove device

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

- 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.

			Zablo	okuj dostęp do z	zaznaczonych zasobów	
			Odbl	okuj dostęp do :	zaznaczonych zasobów	
Zarządzanie Dodaj defi	nicję serwera		Usur	i zaznaczone ol	biekty Przeszukaj liste	ę oł
M Dashboard	Serwery + Dodaj	O Blokuj	okuj 🔋 Usuń		T Dodaj filtr ~ Szukaj	
E Sesje			Zdefiniu	ui filtr dla listv ol	biektów	
Użytkownicy	🗆 Nazwa 🔺	Protokół	Adres	Port	Ostatnie logowanie	
⊖ Serwery	CentOS	SSH	10.0.7.11	22	1 miesiąc, 1 tydzień temu	
	FreeBSD10	SSH	10.0.45.4	22	1 tydzień, 6 dni temu	
🔊 Konta	FreeBSD2	SSH	10.0.35.52	22	1 miesiąc, 1 tydzień temu	
Sejfy	Windows2012	RDP	10.0.40.101	3389	1 miesiąc, 1 tydzień temu	
 Colezda peckuchkuania 	wine Edvtuj defini	cie serwera	10.0.8.106	3389	1 miesiac temu	
M Ghiazoa nasiuchiwania	asd	SSH	localhost	22 Zas	sób zablokowany	
n- Modyfikatory haseł	vnc	VNC	10.0.0.7	59102	1 miesiąc, 1 tydzień temu	
🛡 Polityki					Powód zablokov	vani
🛓 Do pobrania						
⊖ Raporty						

6.1 Dodawanie serwera

Ostrzeżenie: Obiekty modelu danych: *sejfy, użytkownicy, serwery, konta* i *gniazda na-słuchiwania* 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.

Za	ırządzanie	Dodaj serwer		
	Dashboard	Segurar + Dodaj O Biokuj O Odbiokuj 🔒 Usuń	▼ Dodaj filtr	 Szukaj
B	Sesje	Serwery		
*		Nazwa - Protokół Adres	Port O	statnie logowa
_	Senuery	0 10.0.35.1 SSH 10.0.35.1	22 4	miesiące, 1 ty
-	Golwely	MSSQL-10.0.35.1 MS SQL (TDS) 10.0.35.1	1433 ni	gdy
		MYSQL-0-10.0.35.52 MySQL 10.0.35.52	3306 2	lata, 5 miesię
		MYSQL-10.0.35.1 MySQL 10.0.35.1	3306 ni	gdy
	Gniazda nasłuchiwania	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521 2	lata, 5 miesię
		DP-0-10.0.35.54, RDP-0-10.0.35.54-A RDP 10.0.35.54	3389 1	rok temu
n-	Modyfikatory hasef	BDP-10.0.8.103- BDP 10.0.8.103	3389 1	rok temu

- 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.

- 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.

Za	rządzanie <	Fudo	
٥ı	Dashboard	0	
₿		Serwer	
*	Użytkownicy	Ogólne	Unikatowa nazwa zasobu
۵	Serwery	Nazwa	
•		Zablokowane	Cablokuj dostęp po utworzeniu Wybierz protokół połaczeni
2	Gniazda nasłuchiwania	Protokół	Ctrix StoreFront (HTTP)
ń-	Modyfikatory haseł		
U		Czas oczekiwania HTTP	900 Dopuszczalny cza
÷	Do pobrania	Opis	Dodaj opis ułatwia identyfikacje za
Ð		Uprawnienia	laontymaojų za
≡			Użytkownicy uprawnieni do zarządzania kontem
Us	stawienia	Uprawnieni użytkownicy	<u>०</u> २
		Host docelowy	
00	Konfiguracja sieci		
		Adres	Port 80 Adres IP I numer
œ		Adres źródłowy	Dowolny ¢ Źródłowy adres li
a,		URL	Bazowy URL Sto
===	Zewnętrzne repozytoria haseł		
1	Zasoby		
	Kopie zapasowe i retencja		Zapisz definicję obiektu

Tematy pokrewne:

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

6.1.1.2 Dodawanie serwera HTTP

- 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.

Za	rządzanie	Dodaj serwer				
M	Dashboard	Senueni (+ Dodaj O Blokuj O Odblokuj	🖹 Usuń		▼ Dodaj filtr ~	Szukaj
₿	Sesje	Serwery				
*		Nazwa A	Protokół	Adres	Port Osta	stnie logowa
-	Serviery	10.0.35.1	SSH	10.0.35.1	22 4 m	iesiące, 1 ty
-	Colwery	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 nigo	ty
8		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2 la	ta, 5 miesię
•		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 nigo	ty
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2 la	ta, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1 ro	k temu
- 11-	Modyfikatory haseł	BDP-10.0.8.103-	RDP	10.0.8.103	3389 1 ro	k temu

- 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.

- 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.

Zarządzanie <	Fudo	
Int Dashboard	Conver	
🖽 Sesje	Gerwei	
🔮 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
🖴 Serwery	Nazwa	
🔊 Konta		
Sejfy	Zablokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	4 qTTH S
n- Modyfikatory haseł	Czas oczekiwania HTTP	900 Wybierz tryb bezpiec
🛡 Polityki	Włącz obsługę SSLv2	D Zaznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
📥 Do pobrania	Włącz obsługę SSLv3	O-Zaznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
🖨 Raporty	Opis	Dodaj opis ułatwiaja
Produktywność	Uproupiopio	identyfikację zaso
Ustawienia	Oprawnienia	Użytkownicy uprawnieni do zarządzania kontem
🗁 System	Uprawnieni użytkownicy	ं ० ०
¢ ^e Konfiguracja sieci	Host docelowy	
🖂 Powiadomienia		
Znakowanie czasem	Adres	Port 80 Adres IP I numer por
a, Zewnętrzne uwierzytelnianie	Adres źródłowy	Dowolny Cródłowy adres IP
III Zewnętrzne repozytoria haseł	Host HTTP	
🖾 Zasoby		Użyj bezpiecznych połączeń (TLS)
Kopie zapasowe i retencja	Certyfikat serwera	
🚓 Klaster		Kliknij, aby pobrać certyfikat serwera
		Kliknij, aby wgrać certyfikat serwera
≡ Dziennik zdarzeń		
0 21-12-01 3754234 12344678		
♦ 3-30375		SHA1
		C Przywróć Zapisz Zapisz definicję obiektu

Tematy pokrewne:

- Model danych
- Modyfikowanie serwera
- $\bullet \ Blokowanie \ serwera$
- Odblokowanie serwera
- Usuwanie serwera

6.1.1.3 Dodawanie serwera ICA

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

Za	rządzanie	Dodaj serwer				
	Dashboard	Sonucri + Dodaj © Blokuj	© Odblokuj 🔒 Usuń		▼ Dodaj filtr ~	Szuka
₿	Sesje	Serwery				
쓭		Nazwa +	Protokół	Adres	Port Ost	atnie logowa
_	Senuen	0 10.0.35.1	SSH	10.0.35.1	22 4 m	niesiące, 1 t
	Colwory	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 nig	dy
₽		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2 la	ta, 5 miesię
•		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 nig	dy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2 la	ta, 5 miesie
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1 m	ok temu
- H-	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389 1 m	ok temu

- 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.

- 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.
| Zarządzanie < | Fudo | |
|---|------------------------|---|
| Jashboard | | |
| 🖽 Sesje | Serwer | |
| 🖶 Użytkownicy | Ogólne | Unikatowa nazwa zasobu |
| 🖴 Serwery | Nazwa | * |
| 🛢 Konta | | |
| Sejfy | Zablokowane | Zablokuj dostęp po utworzeniu |
| ふ Gniazda nasłuchiwania | Protokół | Wybierz protoko |
| Modyfikatory haseł | 0-1- | |
| 🛡 Polityki | Opis | Dodaj opis uł |
| 📥 Do pobrania | Uprawnienia | identyfikacj |
| 🕀 Raporty | Uprawniani uintkownieu | |
| Produktywność | oprawnen uzytkowney | |
| Ustawienia | Host docelowy | Uzytkownicy uprawnieni do zarządzania kontem |
| 🖕 System | Adres | Port 1494 Adres IP i nume |
| O ₆ Konfiguracja sieci | | |
| Powiadomienia | Adres Zrodłowy | Zrodrowy adres |
| Znakowanie czasem | | Zaznacz, aby włączyć obsługę połączeń szyfrowanych proto
(TLS) |
| e Zewnętrzne uwierzytelnianie | Włącz obsługę SSLv2 | |
| III Zewnętrzne repozytoria haseł | Włącz obsługe SSLv3 | |
| 🖿 Zasoby | Certyfikat serwera | Caznacz, aby wiączyć obsidgę połączen szynowanych prote |
| Kopie zapasowe i retencja | Contynikat och Hora | |
| 🖧 Klaster | K | liknij, aby pobrać certyfikat serwera |
| ≓ Synchronizacja LDAP | K | liknij, aby wgrać certyfikat serwera |
| E Dziennik zdarzeń | | |
| | | |
| 32 dni 🔹 12345678
🗣 3-31753 🚓 Nie skonfigurowany | | SHA1 |
| | | |
| | | C Przywróć Zapisz Zapisz definicję obiektu |

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

6.1.1.4 Dodawanie serwera Modbus

- 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.

Za	rządzanie	Dodaj serwer				
	Dashboard	Sepuent + Dodaj © Blokuj © Odblokuj	🔒 Usuń		▼ Dodaj filtr	v Szuka
₿	Sesje	Serwery				
*		Nazwa *	Protokół	Adres	Port C	statnie logowa
4	Servery	0 10.0.35.1	SSH	10.0.35.1	22 4	miesiące, 1 t
-	Connory	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 n	igdy
₽		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2	lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 n	igdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2	lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1	rok temu
ň-	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389 1	rok temu

- 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.

- 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.

Zarządzanie <	Fudo	
Jashboard		
🗄 Sesje	Serwer	
ở Użytkownicy	Ogólne	Unikatowa nazwa zasobu
🖴 Serwery	Nazwa	
🖉 Konta	Zablokowana	A Zablokuj dosten no utworzeniu
Sejfy	Zabiokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	2 Modbus +
n- Modyfikatory haseł	Opis	Dodaj opis ułatwiają identyfikacie zaso
🛡 Polityki	Uprawnienia	
📥 Do pobrania	opiannia	Użytkownicy uprawnieni do zarządzania kontem
🕀 Raporty	Uprawnieni użytkownicy	ं व
E Produktywność	Host docelowy	
Ustawienia	Adres	Port 502 Adres IP i numer por
🖨 System	Parez	
	Adres źródłowy	Dowolny 2rodłowy adres IP
🖂 Powiadomienia		
Znakowanie czasem		Zapisz definicję obiektu

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

6.1.1.5 Dodawanie serwera MS SQL

- 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.

Za	rządzanie	Dodaj serwer				
M	Dashboard	Segurani + Dodaj © Biokuj © Odbioki	uj 🖹 Usuń		▼ Dodaj filtr ~	Szuka
₿	Sesje	Serwery				
*		Nazwa +	Protokół	Adres	Port Ost	stnie logowa
_	Senuen	0 10.0.35.1	SSH	10.0.35.1	22 4 m	iesiące, 1 ty
-	Galwaly	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 nigo	ty
8		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2 la	ta, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 nigo	ty
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2 la	ta, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1 ro	k temu
- M-	Modyfikatory haseł	BDP-10.0.8.103-	RDP	10.0.8.103	3389 1 ro	k temu

- 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.

- 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.

Zarządzanie <	Fudo	
Ja Dashboard	Comuos	
🖽 Sesje	Serwer	
쯓 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
⊖ Serwery	Nazwa	
🖉 Konta	Zablokowana	7ablokui dosten no utworzeniu
Sejfy	Zablokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	WySQL ¢
n- Modyfikatory haseł	Opis	Dodaj opis ułatwiają identyfikacie zaso
🛡 Polityki	Uprawnienia	
📥 Do pobrania	opiannia	Użytkownicy uprawnieni do zarządzania kontem
🖨 Raporty	Uprawnieni użytkownicy	ं व
E Produktywność	Host docelowy	
Ustawienia	Adree	Port 3306 Adres IP i numer por
🖨 System	Hules	
¢.º Konfiguracja sieci	Adres źródłowy	Dowolny 2rodłowy adres IP
🖂 Powiadomienia		
Znakowanie czasem		Zapisz definicję obiektu

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

6.1.1.6 Dodawanie serwera MySQL

- 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.

Za	rządzanie	Dodaj serwer				
M	Dashboard	Segurani + Dodaj © Biokuj © Odbioki	uj 🖹 Usuń		▼ Dodaj filtr ~	Szuka
₿	Sesje	Serwery				
*		Nazwa +	Protokół	Adres	Port Ost	stnie logowa
_	Senuen	0 10.0.35.1	SSH	10.0.35.1	22 4 m	iesiące, 1 ty
-	Galwaly	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 nigo	ty
8		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2 la	ta, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 nigo	ty
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2 la	ta, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1 ro	k temu
- M-	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389 1 ro	k temu

- 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.

- 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.

Zarządzanie <	Fudo	
Ja Dashboard	Comuos	
🖽 Sesje	Serwer	
쯓 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
⊖ Serwery	Nazwa	
🖉 Konta	Zablokowana	7ablokui dosten no utworzeniu
Sejfy	Zablokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	WySQL ¢
n- Modyfikatory haseł	Opis	Dodaj opis ułatwiają identyfikacie zaso
🛡 Polityki	Uprawnienia	
📥 Do pobrania	opiannia	Użytkownicy uprawnieni do zarządzania kontem
🖨 Raporty	Uprawnieni użytkownicy	ं व
E Produktywność	Host docelowy	
Ustawienia	Adres	Port 3306 Adres IP i numer por
🖨 System	Hules	
¢.º Konfiguracja sieci	Adres źródłowy	Dowolny 2rodłowy adres IP
🖂 Powiadomienia		
Znakowanie czasem		Zapisz definicję obiektu

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

6.1.1.7 Dodawanie serwera Oracle

- 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.

Za	ırządzanie	Dodaj serwer				
M	Dashboard	Seguran + Dodaj © Biokuj © Odbiokuj	⊜ Usuń		▼ Dodaj filtr	~ Szuka
₿	Sesje	Serwery				
쓭		🗆 Nazwa 🔺	Protokół	Adres	Port O	statnie logowa
_	Senuery	0 10.0.35.1	SSH	10.0.35.1	22 4	miesiące, 1 ty
	Golwely	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 n	igdy
₽		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2	lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 n	igdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2	lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1	rok temu
- H-	Modyfikatory haseł	DP-10.0.8.103-	RDP	10.0.8.103	3389 1	rok temu

- 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.

- 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.

Zarządzanie <	Fudo [*]	
Jashboard	Conver	
🗄 Sesje	Serwer	
ở Użytkownicy	Ogólne	Unikatowa nazwa zasobu
⊖ Serwery	Nazwa	
🖉 Konta	Zablokowana	7ablakui dasten na utwarzeniu
Sejfy	Labrokowane	Wybierz protokół połączeniowy
か Gniazda nasłuchiwania	Protokół	Cracle +
 Modyfikatory haseł 	Opis	Dodaj opis ułatwiają identyfikacje zaso
🛡 Polityki	Uprawnienia	
📥 Do pobrania		Użytkownicy uprawnieni do zarządzania kontem
🕀 Raporty	Uprawnieni użytkownicy	ं २
🖹 Produktywność	Host docelowy	
Ustawienia	Adres	Ret 1521 Adres IP i numer por
🖨 System	Pulo	
¢ ^e Konfiguracja sieci	Adres źródłowy	Dowolny 2rodłowy adres IP
🖂 Powiadomienia		
C Znakowanie czasem		Zapisz definicję obiektu

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

6.1.1.8 Dodawanie serwera RDP

- 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.

Za	rządzanie	Dodaj serwer				
	Dashboard	Segurani + Dodaj © Biokuj © Odbioki	uj 🖹 Usuń		▼ Dodaj filtr ~	Szuka
₿	Sesje	Serwery				
*		Nazwa +	Protokół	Adres	Port Ost	stnie logowa
_	Senuen	10.0.35.1	SSH	10.0.35.1	22 4 m	iesiące, 1 ty
-	Galwaly	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 nigo	ty
8		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2 la	ta, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 nigo	ty
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2 la	ta, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1 ro	k temu
- M-	Modyfikatory haseł	BDP-10.0.8.103-	RDP	10.0.8.103	3389 1 ro	k temu

- 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.

- 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.



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

6.1.1.9 Dodawanie serwera SSH

- 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.

Za	rządzanie	Dodaj serwer				
M	Dashboard	Sepuent + Dodaj Blokuj Odblokuj	⊟ Usuń		T Dodaj f	iltr v Szuka
₿	Sesje	Serwery				
*		Nazwa *	Protokół	Adres	Port	Ostatnie logowa
	Serwerv	0 10.0.35.1	SSH	10.0.35.1	22	4 miesiące, 1 t
_	Connorg	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	nigdy
-		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	nigdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389	1 rok temu
ñ-	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 rok temu

- 3. Wpisz nazwę obiektu serwera.
- 4. Zaznacz opcję Zablokowane, jeśli obiekt ma być niedostępny po utworzeniu.
- 5. Z listy rozwijalnej Protokół wybyierz 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.

- 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.

Zarządzanie <	Fudo		
M Dashboard	Convor		
🖽 Sesje	Serwer		
📽 Użytkownicy	Ogólne	Unikatowa nazwa zasobu	
⊖ Serwery	Nazwa		
📾 Konta	Zablatawana		
Sejfy	Zablokowane	Zabiokuj dostęp po utworzeniu	Wybierz protokół połączo
n Gniazda nasłuchiwania	Protokół	2 SSH	e ale
n- Modyfikatory haseł	Opis		Dodaj opis ułatwia
🛡 Polityki	Llorawnienia		
🕹 Do pobrania	oprawnienia		_
🔒 Raporty	Uprawnieni użytkownicy		• •
🖹 Produktywność	Host docelowy	Użytkownicy uprawnieni do zarz	ądzania kontem
Ustawienia	Adme	Post 22	Adres IP i numer
🖕 System		1.011 44	
¢° Konfiguracja sieci	Adres źródłowy	Dawolny	Zrodrowy adres in
Powiadomienia	Klucz publiczny serwera		
Znakowanie czasem	Klikn	ij, aby pobrać klucz publiczny serwera –	
۹ Zewnętrzne uwierzytelnianie			
III Zewnętrzne repozytoria haseł			
Zasoby			
Kopie zapasowe i retencja			SHA1
🚓 Klaster			Tentes definite attach
≓ Synchronizacja LDAP		Przywroc Zapsz	zapisz definicję obiektu

- 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.

Za	arządzanie	Dodaj serwer				
	Dashboard	Segurari + Dodaj © Blokuj ©	Odblokuj 🖹 Usuń		▼ Dodaj filtr	Szuka
B	Sesje	Serwery				
*		🗆 Nazwa 🔺	Protokół	Adres	Port O	statnie logowa
	Senuer	0 10.0.35.1	SSH	10.0.35.1	22 4	miesiące, 1 t
	Galwary	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433 ni	gdy
₽		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306 2	lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306 ni	gdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521 2	lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389 1	rok temu
÷.	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389 1	rok temu

- 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.

- 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.

Zarządzanie <	Fudo	
I Dashboard	Serwer	
🗎 Sesje		
쯀 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
🖴 Serwery	Nazwa	
📾 Konta	Tablekeware	Zahlakui daeten na utwarzeniu
Sejfy	Zabiokowane	Wybierz protokół połączeniowy
n Gniazda nasluchiwania	Protokół	Certeret Certeret
n- Modyfikatory haseł	Włącz obsługę SSLv2	O-Zaznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
🛡 Polityki	Włącz obsługę SSLv3	OHZaznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
📥 Do pobrania	Opis	
🖨 Raporty	Uprawnienia	Dodaj opis ułaty identyfikacje z
Produktywność	opianiona	Użytkownicy uprawnieni do zarządzania kontem
Ustawienia	Uprawnieni użytkownicy	े २
🖨 System	Host docelowy	
System ¢° Konfiguracja sieci	Host docelowy	Port 23 Adres IP i numer po
 ► System ♥\$ Konfiguracja sieci ☑ Powiadomienia 	Host docelowy	Port 23 Adres IP i numer po
 System Konfiguracja sieci Powiadomienia Znakowanie czasem 	Host docelowy Adres Adres źródłowy	Port 23 Adres IP i numer po Dowolny Żródłowy adres IP
 System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie 	Host docelowy Adres Adres źródłowy	Port 23 Adres IP i numer po Dowolny źródłowy adres IP 2 Użyj bezpiecznych połączeń (TLS)
 System Konfiguracja sleci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny - Źródłowy adres IP 2 Użyj bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby Kopie zapasowe i retencja 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny Źródłowy adres IP 2 Uży bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera Kliknij, aby wgrać certyfikat serwera
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby Kopie zapasowe i retencja Klaster 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny Żródłowy adres IP Vżyj bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera Kliknij, aby wgrać certyfikat serwera
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby Kopie zapasowe i retencja Klaster Synchronizacja LDAP 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny 2ródłowy adres IP 2 Użyj bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera Kliknij, aby wgrać certyfikat serwera
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby Kopie zapasowe i retencja Klaster Synchronizacja LDAP Dziennik zdarzeń 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny Źródłowy adres IP Vżyj bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera Kliknij, aby wgrać certyfikat serwera SHA1
 System System Konfiguracja sieci Powiadomienia Znakowanie czasem Zewnętrzne uwierzytelnianie Zewnętrzne repozytoria haseł Zasoby Kopie zapasowe i retencja Klaster Synchronizacja LDAP Dziennik zdarzeń 	Host docelowy Adres Adres źródłowy Certyfikat serwera	Port 23 Adres IP i numer po Dowolny Źródłowy adres IP * Użyj bezpiecznych połączeń (TLS) Kliknij, aby pobrać certyfikat serwera Kliknij, aby wgrać certyfikat serwera SHA1

- Model danych
- Modyfikowanie serwera
- $\bullet \ Blokowanie \ serwera$
- Odblokowanie serwera
- Usuwanie serwera

6.1.1.11 Dodawanie serwera Telnet 3270

- 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.

Za	ırządzanie	Dodaj serwer				
M	Dashboard	Senueny + Dodaj O Blokuj O Odblokuj	🔒 Usuń		▼ Dodaj f	iltr v Szukaj
₿	Sesje	Serwery				
쓭		Nazwa *	Protokół	Adres	Port	Ostatnie logowa
4	Serwerv	0 10.0.35.1	SSH	10.0.35.1	22	4 miesiące, 1 ty
_	Controlly	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	nigdy
-		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	nigdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389	1 rok temu
*	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 rok temu

- 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.

- 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.

Zarządzanie <	Fudo	
I Dashboard	Senver	
🖽 Sesje	0011101	
쓸 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
🖴 Serwery	Nazwa	
🔊 Konta		
Sejfy	Zabiokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	C Teinet 3270
n- Modyfikatory haseł	Włącz obsługę SSLv2	Caznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
0 Polityki	Włącz obsługę SSLv3	Zaznacz, aby włączyć obsługę połączeń szyfrowanych protokołem SSL
🕹 Do pobrania	Opis	
🔒 Raporty	Uprawnienia	identyfikację z
Produktywność		Uzytkownicy uprawnieni do zarządzania kontem
Ustawienia	Uprawnieni użytkownicy	<u> </u>
😂 System	Host docelowy	
¢º Konfiguracja sleci	Adres	Port 3270 Adres IP i numer por
Powiadomienia	Adres źródłowy	Drweley
Znakowanie czasem	Auto Louony	Contrast of the Contrast of th
e Zewnętrzne uwierzytelnianie		Uzyj bezpiecznych połączeń (TLS)
III Zewnętrzne repozytoria haseł	Certyfikat serwera	
Zasoby		Kliknij, aby pobrač certyfikat serwera
Kopie zapasowe i retencja		Kliknij, aby wgrac certyfikat serwera
🛔 Klaster		
≓ Synchronizacja LDAP		
≡ Dziennik zdarzeń		SHA1
0.3:09:42.1791123.12343678 \$-330429 Ne electrigurowany		₽rzywróć ✓ Zapisz Zapisz definicję obiektu

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

6.1.1.12 Dodawanie serwera Telnet 5250

Informacja:

- $\bullet\,$ 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.

Za	arządzanie	Dodaj serwer	
M	Dashboard	Serweny + Dodaj © Blokuj © Odblokuj 🔒 Usuń	▼ Dodaj filtr ~ Szukaj
₿	Sesje		
쓭		Nazwa * Protokół Adres	Port Ostatnie logowa
	Serwerv	□ 10.0.35.1 SSH 10.0.35.1	22 4 miesiące, 1 ty
	Controly	MSSQL-10.0.35.1 MS SQL (TDS) 10.0.35.1	1433 nigdy
₽		MYSQL-0-10.0.35.52 MySQL 10.0.35.52	3306 2 lata, 5 miesię
•		□ MYSQL-10.0.35.1 MySQL 10.0.35.1	3306 nigdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521 2 lata, 5 miesię
		□ RDP-0-10.0.35.54, RDP-0-10.0.35.54-A RDP 10.0.35.54	3389 1 rok temu
¹⁰⁻	Modyfikatory haseł	BDP-10.0.8.103- RDP 10.0.8.103	3389 1 rok temu

- 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.

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

6.1.1.13 Dodawanie serwera VNC

- 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.

Za	ırządzanie	Dodaj serwer		
M	Dashboard	Senueny + Dodaj	▼ Dodaj f	iltr - Szuka
₿	Sesje	Servery		
쓭		Nazwa A Protokół Adres	Port	Ostatnie logowa
	Servery	0 10.0.35.1 SSH 10.0.35.1	22	4 miesiące, 1 t
-	Connerg	MSSQL-10.0.35.1 MS SQL (TDS) 10.0.35.1	1433	nigdy
₽		MYSQL-0-10.0.35.52 MySQL 10.0.35.52	3306	2 lata, 5 miesie
•		MYSQL-10.0.35.1 MySQL 10.0.35.1	3306	nigdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521	2 lata, 5 miesi
		□ RDP-0-10.0.35.54, RDP-0-10.0.35.54-A RDP 10.0.35.54	3389	1 rok temu
10-	Modyfikatory hasel	BDP-10.0.8.103- RDP 10.0.8.103	3389	1 rok temu

- 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.

- 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.

	eta veles ^a	
Zarządzanie <	FUDD	
Dashboard	Serwer	
🖽 Sesje		
🗑 Użytkownicy	Ogólne	Unikatowa nazwa zasobu
⊖ Serwery	Nazwa	
🔊 Konta	Zablalauraa	
Sejfy	Zabiokowane	Wybierz protokół połączeniowy
n Gniazda nasłuchiwania	Protokół	VNC +
h- Modyfikatory haseł	Opis	Dodaj opis ułatwiaja identyfikacie zaso
Polityki	Llorawnienia	
📥 Do pobrania	oplawnienia	Użytkownicy uprawnieni do zarządzania kontem
🖨 Raporty	Uprawnieni użytkownicy	ं २
🖹 Produktywność	Host docelowy	
Ustawienia	Adree	Adres IP i numer po
🖙 System	Aures	
¢ ^e Konfiguracja sieci	Adres źródłowy	Dowolny - Zródłowy adres IP
🖂 Powiadomienia		
Znakowanie czasem		
a, Zewnętrzne uwierzytelnianie		
III Zewnętrzne repozytoria haseł		CPrzywróć 🗸 Zapisz – Zapisz definicję obiektu

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.

Za	arządzanie	Dodaj serwer				
	Dashboard	Senueny + Dodaj © Biokuj © Odbiokuj	🖹 Usuń		▼ Dodaj fi	ltr v Szukaj
B	Sesje	Serwery				
*		Nazwa +	Protokół	Adres	Port	Ostatnie logowa
-	Servery	□ 10.0.35.1	SSH	10.0.35.1	22	4 miesiące, 1 ty
-	Connory	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	nigdy
8		MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 lata, 5 miesię
		MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	nigdy
	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389	1 rok temu
ň-	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 rok temu

- 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.

intoi macja.	ODICKU	y grupuj	ace serwery	wyrozn	ione są ikolią				
Zarządzanie	<	Fudo'						💄 admin 🗸	?
In Dashboard		Serwery	+ Dodaj 🛛 🗢	0		▼ Dodaj fi	ltr v Szukaj	0	Q
🖽 Sesje		Serwery							
Użytkownicy		🗆 Nazwa 🔺		Protokół	Host(y)	Port	Ostatnie logowanie		
⊖ Serwerv		RDP1		RDP	10.0.70.235	3389	nigdy		
		servers_gro	up	SSH	10.0.150.0 🎄 24	22	nigdy		
Konta		servers_gro	up_2	RDP	10.0.150.0 🎄 24	3389	nigdy		
Gniazda nasłuchiwani	а								

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
- Servery 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.

Za	rządzanie <	Fudo	•						
M	Dashboard	Servery	+ Dodaj	O Blokuj	Odblokuj	🔒 Usuń		▼ Dodaj	filtr v Szukaj
₿	Sesje	Jerwery							
쓭		🗆 Nazwa 🔺				Protokół	Adres	Port	Ostatnie logowa
	Servery	0 10.0.35.1				SSH	10.0.35.1	22	4 miesiące, 1 tj
	Connery	D MISSQL-		orany obie	ĸŧ	MS SQL (TDS)	10.0.35.1	1433	nigdy
₽		MYSQL-0	-10.0.35.52			MySQL	10.0.35.52	3306	2 lata, 5 miesię
		MYSQL-1	0.0.35.1			MySQL	10.0.35.1	3306	nigdy
2	Gniazda nasłuchiwania	ORACLE-	10.0.40.149			Oracle	10.0.40.149	1521	2 lata, 5 miesię
		RDP-0-10).0.35.54, RDP-0	-10.0.35.54-A		RDP	10.0.35.54	3389	1 rok temu
- 11-	Modylikatory hasel	RDP-10.0	.8.103-			RDP	10.0.8.103	3389	1 rok temu

4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Ogólne		Niezapisane zn	niany w konfiguracji
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy		
	Opis	Opis	

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.

Za	rządzanie <	Fudo				4 a	dmin ~	?
		Septent + Dodaj OBlokuj OOdblokuj	🔒 Usuń		▼ Dodaj f	iltr - Szukaj	0	Q
	Sesje	Zaznacz objekt						
	Użytkownicy	Nazwa	Protokół	Adres	Port	Ostatnie logowanie		
	Server	10.0.35.1 Zablokuj zaznaczone obiekty	SSH	10.0.35.1	22	4 miesiące, 1 tydzień tem	u	
	Serwery	MSSQL-10.0.35.1	MS SQL (TDS)	10.0.35.1	1433	nigdy		
	Konta	MYSQL-0-10.0.35.52	MySQL	10.0.35.52	3306	2 lata, 5 miesięcy temu		
	Sejfy	MYSQL-10.0.35.1	MySQL	10.0.35.1	3306	nigdy		
	Gniazda nasłuchiwania	ORACLE-10.0.40.149	Oracle	10.0.40.149	1521	2 lata, 5 miesięcy temu		
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A	RDP	10.0.35.54	3389	1 rok temu		
*	Modyfikatory haseł	RDP-10.0.8.103-	RDP	10.0.8.103	3389	1 rok temu		

4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij Zatwierdź.

Zablokuj obiekty	×
Powód	
Wprowadź powód zabokowania	Anuluj Zatwierdź
Zabloku	j obiekt

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

Tematy pokrewne:

- Model danych
- Pierwsze uruchomienie
- Użytkownicy
- Gniazda nasłuchiwania
- Sejfy
- $\bullet \ Konta$

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.

Za	rządzanie	< Fudo		
M	Dashboard	Samurar + Dodaj © Biokuj © Odbiokuj 🗟 Usuń	T Doda	j filtr v Szukaj
₿		Zaznacz obiekt		
*		Nazwa Protokół Adres	Port	Ostatnie logowanie
	Servery	0 10.0.35.1 SSH 10.0.35.1	22	4 miesiące, 1 tydz
	connony	Odblokuj zaznaczone objekty MS SQL (TDS) 10.0.35.1	1433	nigdy
₽		MySQL 10.035.52	3306	2 lata, 5 miesięcy
•		MYSQL-10.0.35.1 MySQL 10.0.35.1	3306	nigdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521	2 lata, 5 miesięcy
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A RDP 10.0.35.54	3389	1 rok temu
÷-	Modyfikatory haseł	BDP-10.0.8.103- BDP 10.0.8.103	3389	1 rok temu

4. Kliknij Zatwierdź, aby potwierdzić odblokowanie obiektów.

Odbiokuj obiekty	×
Jesteś pewien że chcesz odbiokować 1 obiekt	?
	Anuluj Zatwierdź
	Odblokuj obiekt

Tematy pokrewne:

- Model danych
- Pierwsze uruchomienie
- Użytkownicy
- Gniazda nasłuchiwania
- \bullet 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.

Za	arządzanie <	Fudo'		
M	Dashboard	Samuran + Dodaj O Blokuj O Odblokuj 🔒 Usuń	▼ Dodaj filtr	 Szukaj
₿		Zazpacz obiekt		
*		Nazwa Protokół Adres	Port C	statnie logowa
	Servery	10.0.35.1 Usun zaznaczone obiekty ssH 10.0.35.1	22 4	miesiące, 1 ty
	Controlly	MSSQL-10.0.35.1 MS SQL (TDS) 10.0.35.1	1433 n	igdy
₽		MYSQL-0-10.0.35.52 MySQL 10.0.35.52	3306 2	lata, 5 miesię
		MYSQL-10.0.35.1 MySQL 10.0.35.1	3306 n	igdy
2	Gniazda nasłuchiwania	ORACLE-10.0.40.149 Oracle 10.0.40.149	1521 2	lata, 5 miesię
		RDP-0-10.0.35.54, RDP-0-10.0.35.54-A RDP 10.0.35.54	3389 1	rok temu
- H-	Modyfikatory haseł	BDP-10.0.8.103- RDP 10.0.8.103	3389 1	rok temu

4. Potwierdź operację usunięcia zaznaczonych obiektów.

Usuń obiekty	×
Jesteś pewien że chcesz usunąć 1 obiekt?	
	Anuluj Zatwierdź
	Usuń obiekt

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 🗐.

Usta	wienia	Host docelowy								
🖨 S		Adres IP	10.0.150.150	/ 30		Port	22	*		
¢₿ K										
b 6		Adres źródłowy	Dowolny			Ŷ				
⊠ P		10.0.150.150 💼								~
₿ Z		Usuń wybrany host								
a, z										

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 na-słuchiwania* 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.

Za	rządzanie	Dodaj	konto					
M	Dashboard		(onto + Dodaj © Błokuj	© Odbiokuj ⊜ Usuń ⊠ Czas			▼ Dodaj filtr ~ Sa	ukaj
₿		111	Konta					
쓭		0	Nazwa *	Serwer -	Nagrywanie sesji v	Тур	Polityka modyfikatora hasla	Mo
8			admin@serwer3	serwer3	all	regular	Statyczne, bez ograniczeń	Br
-	Konta	0	administrator at RDP-0-10.0.35.54,	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Statyczne, bez	Br
			R				ograniczeń	
٣			administrator@serwer1	serwer1	all	regular	Statyczne, bez ograniczeń	Br
÷-	Modyfikatory haseł	•	administrator@serwer2	serwer2	all	regular	Statyczne, bez ograniczeń	Br
U	Polityki		anonymous	SSH-0-10.0.35.52	all	anonymous	None	No

- 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.

Ogólne		Niezapisane :	zmiany w konfiguracji
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy		
	Opis	Opis	

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.

Za	rządzanie	Dodaj	konto					
M	Dashboard		+ Dodaj O Blokuj	© Odblokuj 🔒 Usuń 🕼 Czas			▼ Dodaj filtr ~ Sz	ukaj
₿		11	Konta					
*		0	Nazwa 🔺	Serwer -	Nagrywanie sesji -	Тур	Polityka modyfikatora hasla	M
8			admin@serwer3	serwer3	all	regular	Statyczne, bez ograniczeń	Br
-	Konta	0	administrator at RDP-0-10.0.35.54,	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Statyczne, bez	Br
		_	R				ograniczeń	
2			administrator@serwer1	serwer1	all	regular	Statyczne, bez ograniczeń	Br
÷.	Modyfikatory haseł	0	administrator@serwer2	serwer2	all	regular	Statyczne, bez ograniczeń	Br
U	Polityki		anonymous	SSH-0-10.0.35.52	all	anonymous	None	No

- 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.

Dane uwierzytelniające

Zastąp sekret	 \$
Przekazuj domenę	
Uwierzytelnienie przez serwer	

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

Za	rządzanie	Fudo'	
M	Dashboard	Kanta	
₿		Konto	
쓭	Użytkownicy	Ogólne	Unikatowa nazwa obiektu
⊜	Serwery	Nazwa	*
۵	Konta		
٣	Gniazda nasłuchiwania	Zablokowane	Cablokuj dostęp po utworzeniu
•		Тур	forward
ń.	Modyfikatory haseł	Newsylawski	
U	Polityki	Nagrywanie sesji	• Opcje nagrywa
*	Do pobrania	OCR sesj	Indeksowanie materiałów sesji graficznych RDP i VNC
₽		Usuń dane sesji po upływie	dni)— Czas retencji dan
≡	Produktywność	Przenieś dane na zewnętrzną	dni
Us	tawienia	macierz po upływie	Pierwszy stopień retencji
		Uprawnienia	
¢°	Konfiguracja sieci	Uprawnieni użytkownicy	0 @
•	External storage		Użytkownicy uprawnieni do zarządzania obiektem
		Serwer	
ß	Znakowanie czasem	Serwer	(÷ •)
a _e	Zewnętrzne uwierzytelnianie	Describe delation	Przypisz konto do serwera
=	Zewnętrzne repozytoria haseł	Dane uwierzytelniając	e
	Zasoby	Zastąp sekret	+
	Kopie zapasowe i retencja	Przekazuj domenę	
å	Klaster		
≓	Synchronizacja LDAP		
≡	Dziennik zdarzeń		Przywróć ✓ Zapisz Zapisz definicję obiektu

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

7.1.3 Dodawanie konta typu regular

- 1. Wybierz z lewego menuZarządzanie > Konta.
- 2. Kliknij + Dodaj.

Za	rządzanie	Dodaj	konto					
M	Dashboard		+ Dodaj O Blokuj	© Odbiokuj ⊜ Usuń 🕼 Czas			▼ Dodaj filtr ~ S	zuka
₿		11	Konta					
*		0	Nazwa 🛎	Serwer -	Nagrywanie sesji v	Тур	Polityka modyfikatora hasla	M
⊖			admin@serwer3	serwer3	all	regular	Statyczne, bez ograniczeń	Br
-	Konta	0	administrator at RDP-0-10.0.35.54,	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Statyczne, bez	Br
			R				ograniczeń	
2			administrator@serwer1	serwer1	all	regular	Statyczne, bez ograniczeń	Br
÷-	Modyfikatory haseł	0	administrator@serwer2	serwer2	all	regular	Statyczne, bez ograniczeń	Br
U			anonymous	SSH-0-10.0.35.52	all	anonymous	None	N

- 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 hasel*, 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.
| Za | rządzanie < | Fudo [*] | ۵ : |
|-----------|------------------------------|-----------------------------|---|
| | Dashboard | Kanta | |
| ₿ | | Konto | |
| 쓭 | Użytkownicy | Ogólne | Unikatowa nazwa obiektu |
| ⊖ | | Nazwa | |
| ۵ | Konta | | |
| ٣ | Gniazda nasłuchiwania | Zablokowane | Zablokuj dostęp po utworzeniu |
| • | | Тур | regular two konta |
| ÷. | Modyfikatory haseł | Normaliania conii | |
| U | | Nagrywanie sesji | Opcje nagrywania s |
| * | Do pobrania | OCR sesji | Indeksowanie materiałów sesji graficznych RDP i VNC |
| Ð | | Usuń dane sesji po upływie | dni)— Czas retencji danych |
| ≡ | | Przenieś dane na zewnętrzną | dni) — Pierwszy stopień ret |
| Us | tawienia | macierz po upływie | |
| | | Uprawnienia | |
| ¢00 | Konfiguracja sieci | Uprawnieni użytkownicy | 0 0 |
| • | External storage | | Użytkownicy uprawnieni do zarządzania obiektem |
| | | Serwer | |
| Ø | | Serwer | (÷ •) |
| a, | Zewnętrzne uwierzytelnianie | D | Przypisz konto do serwera |
| = | Zewnętrzne repozytoria haseł | Dane uwierzytelniające | |
| | Zasoby | Domena | Domena konta |
| • | Kopie zapasowe i retencja | Login | Login konta |
| . | | Zecton celerat | |
| ≓ | Synchronizacja LDAP | Zastąp sekret | Dane autoryzujące d |
| ≡ | Dziennik zdarzeń | Polityka modyfikatora hasla | Statyczne, bez ograniczeń + Przypisanie typu mo |
| | | Modyfikator hasła | |
| 7:3
\$ | | | |
| | | Modyfikator hasla | Brak Charakterystyka Zmi |
| | | Użytkownik uprzywilejowany | Dane konta uprawnio
zmia |
| | | Haslo użytkownika | |
| | | uprzywiiejowanego | |
| | | | |
| | | | Zapisz definicję obiektu |

- 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.

z	arządzanie <	Fudo					
đ) Dashboard	Konta + Dodaj © B	Blokuj © Odbio	kuj 🖹 Usuń		T Dodaj filtr ∨	Szukaj
€	∄ Sesje						
-	Użytkownicy	🗆 Nazwa *	Serwar *	Nagrywanie sesji 💌	Тур	Polityka modyfikatora haslą	Modyfikator
8	Serwery	□ acc	CentOS	all	regular	Static, without restrictions	None
		admin@win2012	Windows2012	all	regular	Static, without restrictions	None
-	Konta	admin@windows7	Windows7	all	regular	Static, without restrictions	None
	I Sejfy	anonymo Edytuj konto	FreeBSD2	all	anonymous	None	None
	Gniazda naskuchiwania	asd	CentOS	all	regular	Static, without restrictions	None
•11		 joe@FreeBSD10 	FreeBSD10	all	regular	Random, 8 length, change 1 hour	Unix Accou
ń	 Modyfikatory haseł 	root@CentOS	CentOS	all	regular	Static, without restrictions	None
U	Polityki	 root@freebsd10 	FreeBSD10	all	regular	Static, without restrictions	None
	Provide a standard	vnc	vnc	all	regular	Static, without restrictions	None
2	Do pobrania						
€	Raporty						
=	: Produktywność						

4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną \mathbb{Z} .

Ogólne		Niezapisane zm	niany w konfiguracji
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy		
	Opis	Opis	

5. Kliknij Zapisz.

- 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.

Za	rządzanie <	Fudo'	Blokuj zaznaczone obiekty			📥 admin 🗸	?
	Dashboard	Konta + Dodaj OBlokuj	O Odblokuj 🗟 Usuń 🕼 Czas		▼ Dodaj filtr ~ Szu	ıkaj O	٩
	Sesje	Konta					
	Użytkownicy	Nazwa *	Serwer *	Nagrywanie sesji * Typ	Polityka modyfikatora hasla	Modyfikator hasla	
	Serwery	✓ admin@serwer3	serwer3	all regular	Statyczne, bez ograniczeń	Brak	
-	Konta	administrator at RDP-0-10.0.35.54,	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all regular	Statyczne, bez	Brak	
	Sejfy	R			ograniczeń		
	Gniazda nasłuchiwania	 administrator@serwer1 	serwer1	all regular	Statyczne, bez ograniczeń	Brak	
	Modyfikatory haseł	administrator@serwer2	serwer2	all regular	Statyczne, bez ograniczeń	Brak	

4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij Zatwierdź.

Zablokuj obiekty	×
Powód	
Wprowadź powód zabokowania	Anuluj Zatwierdź
Zabloku	j obiekt

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

- 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.

Odblokuj obiekty	×
Jesteś pewien że chcesz odbiokować 1 obiekt?	
	Anuluj Zatwierdź
Odblokuj	obiekt

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.

Za	ırządzanie	¢	Fudo'					
ad.	Dashboard		+ Dodaj © Blokuj	Odblokuj			▼ Dodaj filtr ~ Sz	ukaj
₿		г.	Zaznacz obiekt	—				
쓭			Nazwa Usuń zaznaczony	element	Nagrywanie sesji -	Тур	Polityka modyfikatora hasla	Mc
0			account_4	10.0.35.1	all	regular	Statyczne, bez ograniczeń	Bri
-	Konta	11	admin@serwer3	serwer3	all	regular	Statyczne, bez	Bra
							ograniczeń	
2			 administrator at RDP-0-10.0.35.54, R 	RDP-0-10.0.35.54, RDP-0-10.0.35.54-ANONYMOUS	all	regular	Statyczne, bez ograniczeń	Bri
ń	Modyfikatory haseł		administrator@serwer1	serwer1	all	regular	Statyczne, bez ograniczeń	Bri

4. Potwierdź operację usunięcia zaznaczonych obiektów.

Usuń obiekty	×
Jesteś pewien że chcesz usunąć 1 obiekt?	
	Anuluj Zatwierdź
	Usuń obiekt

- Dodawanie konta
- $\bullet \ Edy to wanie \ konta$
- 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.

Odblokuj zaznaczone	obiekty			
Blokuj zaznaczone	obiekty		Usuń zaznaczone	sejfy
Zarządzanie <	Dodaj sejf			Zdefiniuj filtr dla lis
Jashboard	Soify + Doda	Blokuj Odblokuj 🕆 Usuń		T Dodaj filtr v Szukaj
🖽 Sesje	Selly			
🖶 Użytkownicy	🗆 Nazwa 🔺	Użytkownicy	Konta	G
🖴 Serwery	 adusers 	jdoe, kwitaszczyk, mborysiak, mzaborski, tdwornicki		F
🔊 Konta	api-robot-safe1			
■ Sejfy	portal Edvt	ui seif pdawidek, test-fudo		
A Gniazda nasłuchiwania	□ safe -	anonymous	anonymous@FreeBSD2	s
n- Modyfikatory haseł	anonymous	pdawidek	joe@FreeBSD10	Sejf zabloko
Polityki	testsafe			
🕹 Do pobrania	 whisys 	admin1, pdawidek	admin@windows7, vnc, root@C	CentOS, root@free Powód zablokow
A Raporty				

8.1 Dodawanie sejfu

Ostrzeżenie: Obiekty modelu danych: *sejfy, użytkownicy, serwery, konta* i *gniazda na-słuchiwania* 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 $\mathit{Zarzqdzanie} > \mathit{Sejfy}.$
- 2. Kliknij + Dodaj.

Za	arządzanie	Dodaj seji P		
M	Dashboard	Polity + Dodaj O Blokuj © Odblokuj ⊕ Usuń	▼ Dodaj filtr ~	Szukaj
₿		Sejry		
*		Nazwa A Użytkownicy Kont	a	Gniazda nas
8		anonymous > RDP-0-10.0.35.54- anonymous anon ANONYMOUS 10.0	tymous for RDP-0-10.0.35.54, RDP-0- .35.54-ANONYMOUS	RDP-0-10.0
-		anonymous > RDP-0-TLS- anonymous anon 10.0.40.100-AN RDP	tymous for RDP-0-TLS-10.0.40.100, 2-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS ANONYMO
	Sejfy	anonymous > RDP-0-TLS-NLA- anonymous anon	tymous for RDP-0-TLS-NLA-	RDP-0-TLS
۳		10.0.40.10 10.0	.40.101, RDP-0-TLS-NLA- .40.101-ANONYMOUS	ANONYMO
ń-	Modyfikatory haseł	anonymous > RDP-10.0.8.103- anon	tymous for RDP-10.0.8.103-	RDP-10.0.8
U	Politvki	anonymous > TELNET-0- anonymous anonymous	tymous for TELNET-0-10.0.35.52,	TELNET-0-1

- 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.

Zar	ządzanie <	Fudo	
	Dashboard	Soif	
⊟		30)1	
*	Użytkownicy	Ogólne	Unikatowa nazwa obiektu
⊜		Nazwa	*
2		Zabiokowane	O-Zabokuj obiekt po utworzeniu
•	Sejfy	Powód logowania	Pytaj użytkownika o powód logowania
÷-	Modyfikatory haseł	Wymagaj akceptacji	O-Wymagaj akceptacji połączeń przez administratora
U		Powiadomienia 🗆	Rozpoczęcie sesji Rozpoczęcie sesji (push)
÷	Do pobrania		Cakończenie sesji Dołączenie do sesji Ostawiema powiadomie Odłączenie od sesji Wykrycie wzorca
₽		Polityki	Polityki proaktywn
≡		Użytkownicy	• • Użytkownicy upra
Ust	awlenia		

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

Polityka czasi	u dostępu		×
Włącz politykę	czasową 🛛 🖉 🗹	Pokaż hasło	
00:00		23	:59
Poniedziałek	05:24		
Wtorek		· · · · · · · · · · · · · · · · · · ·	
Środa		17:42	
Czwartek			
Piątek			
Sobota			
Niedziela			
		Anu	luj OK

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

J.		Funkcjonalność protoko	ołów 📃 🗖	Funkcje protokołów udostępniona użytkownikon	
¢ŝ	Konfiguracja sieci	RDP	Przekierowanie schowka	Przekierowanie dźwięku	
•	External storage		 Przekierowanie urządzeń Przekierowanie wejścia audio 	 Dynamiczne wirtualne kanały Przekierowanie multimediów 	
			Maksymalna rozdzielczość \$	Maksymalna głębia \$	
ß			Rozdzielczość	6 Giębia kolorów	
a,		SSH 🖸	🛛 Sesje 💟 Terminal	 Przekierowanie portu Środowisko 	
	Zewnętrzne repozytoria haseł		 X11 Powłoka 	SSH Agent forwarding	
-	Zasoby		SFTP		
-	Kopie zapasowe i retencja	VNC	Schowek klienta	Schowek serwera)

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

å	Klaster	Uprawnienia	Użytkownicy uprawnieni do zrządzania obiektem	
≓	Synchronizacja LDAP	Uprawnieni użytkownicy	operator operator2 O Q	
≡	Dziennik zdarzeń			

- 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.

	Wybierz kont	0 Z	definiuj przypisanie gniazd na	asłuchiwania
1 dzień i 00000003 \$ 3-34482 # Nie skonfigurowany	konto	¢ Estatur	0	Q ×
	Wybierz konto	\$	0	Q ×
	-Doda	aj konto		

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.

Za	rządzanie <	Fud	o '					
M	Dashboard	Raife	+ Dodaj O Bloku	j Odbiokuj	🖹 Usuń		▼ Dodaj filtr ~	Szukaj
₿		Sejiy						
*		🗆 Nazwa	<u>^</u>	Użytkownicy		Konta		Gniazda nas
8	Serwery	anonyr ANON	Anonyme Edytuj wybrany obiekt				0.0.35.54, RDP-0- S	RDP-0-10.0
		anonyr 10.0.40	mous > RDP-0-TLS- 0.100-AN	anonymous		anonymous for RDP-0-TL RDP-0-TLS-10.0.40.100-	.S-10.0.40.100, ANONYMOUS	RDP-0-TLS ANONYMO
	Sejfy	anonyr	mous > RDP-0-TLS-NLA-	anonymous		anonymous for RDP-0-TL	S-NLA-	RDP-0-TLS
۳		10.0.40	0.10			10.0.40.101, RDP-0-TLS- 10.0.40.101-ANONYMOU	NLA- JS	ANONYMO
ń-	Modyfikatory haseł	 anonyr 	mous > RDP-10.0.8.103-			anonymous for RDP-10.0	.8.103-	RDP-10.0.8
U	Polityki	anonyr 10.0.3	nous > TELNET-0- 5.52-ANON	anonymous		anonymous for TELNET-0 TELNET-0-10.0.35.52-AN)-10.0.35.52, ONYMOUS	TELNET-0-1 ANONYMO

4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

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

Ogólne		Niezapisane zmi	any w konfiguracji
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy		
	Opis	Opis	

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.

Za	arządzanie <	Fudo			
	Dashboard	Sejfy + Dodaj O Blokuj	Odbiokuj 🗟 Usuń	₹ Dodaj f	filtr ~ Szukaj
4		Zaznacz obiekt	Užvtkownicy	Konta	Gniazda nas
8	Serwery	ANONYMOUS > RDP. Zabiokuj	oblektus	anonymous for RDP-0-10.0.35.54, RD 10.0.35.54-ANONYMOUS	P-0- RDP-0-10.0
		anonymous > RDP-0-TLS- 10.0.40.100-AN	anonymous	anonymous for RDP-0-TLS-10.0.40.10 RDP-0-TLS-10.0.40.100-ANONYMOU	00, RDP-0-TLS IS ANONYMO
	Sejfy	anonymous > RDP-0-TLS-NLA-	anonymous	anonymous for RDP-0-TLS-NLA-	RDP-0-TLS
2		10.0.40.10		10.0.40.101, ANONYMOUS	ANONTINO
÷	Modyfikatory haseł	anonymous > RDP-10.0.8.103-		anonymous for RDP-10.0.8.103-	RDP-10.0.8
U	Polityki	anonymous > TELNET-0- 10.0.35.52-ANON	anonymous	anonymous for TELNET-0-10.0.35.52, TELNET-0-10.0.35.52-ANONYMOUS	TELNET-0-1 ANONYMO

4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij Zatwierdź.

Zablokuj oblekty	×
Powód	
Wprowadź powód zabokowania	Anuluj Zatwierdź
Zabloku	j obiekt

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.

Zŧ	arządzanie	< Fudo		
	Dashboard	Potter + Dodaj O Biokuj O Odblokuj B Usuń	▼ Dodaj filtr ~	Szukaj
₿				
-		Nazwe Użytkownicy Konta	G	iniazda nasłu
0	Serwery	anonymous > RDP-0-10.0.35.54- anonymous anonymous 0-10.0	mous for RDP-0-10.0.35.54, RDP- R 0.35.54-ANONYMOUS	DP-0-10.0.3
	Konta	kuj zaznaczone obiekty anonymous anony 10.0.40.100-AN RDP-0	mous for RDP-0-TLS-10.0.40.100, R D-TLS-10.0.40.100-ANONYMOUS A	NONYMOU
	Sejfy	anonymous > RDP-0-TLS-NLA- anonymous anonymous	mous for RDP-0-TLS-NLA-	DP-0-TLS-N
2		10.0.40.10 10.0.4 10.0.4	0.101, RDP-0-TLS-NLA- A 0.101-ANONYMOUS	NONYMOU
ń-	Modyfikatory haseł	anonymous > RDP-10.0.8.103- anony	mous for RDP-10.0.8.103- F	DP-10.0.8.1

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.

Za	arządzanie <	Fudo"		
M	Dashboard	Saifu + Dodaj O Blokuj O Odblokuj	▼ Dodaj filtr ~	Szukaj
₿				
*		Nazwo Użytkownicy	Konta (Gniazda nas
8	Serwery	anor Usun zaznaczone obiekty	anonymous for RDP-0-10.0.35.54, RDP-0- 1 10.0.35.54-ANONYMOUS	RDP-0-10.0
		anonymous > RDP-0-TLS- anonymous 10.0.40.100-AN	anonymous for RDP-0-TLS-10.0.40.100, RDP-0-TLS-10.0.40.100-ANONYMOUS	RDP-0-TLS ANONYMO
	Sejfy	anonymous > RDP-0-TLS-NLA- anonymous	anonymous for RDP-0-TLS-NLA-	RDP-0-TLS
۳		10.0.40.10	10.0.40.101, RDP-0-TLS-NLA-	ANONYMO
ń -	Modyfikatory haseł	anonymous > RDP-10.0.8.103-	anonymous for RDP-10.0.8.103-	RDP-10.0.8
U	Polityki	anonymous > TELNET-0- anonymous 10.0.35.52-ANON	anonymous for TELNET-0-10.0.35.52, TELNET-0-10.0.35.52-ANONYMOUS	TELNET-0-1 ANONYMO

4. Potwierdź operację usunięcia zaznaczonych obiektów.



- 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.

Odblok	kuj zaznaczone obiekty –				
Blol	kuj zaznaczone obiekty 🗕		Usur	i zaznaczone o	biekty
Zarządzanie Do	odaj gniazdo nasłuchiwania			Zdefini	uj filtr dla listy obie
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Blokuj O Od	blokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje	Gillazud Husidolliwalila				
볼 Użytkownicy	🗇 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączenia
🖴 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	□ ss <mark>H - Ar</mark> Edvtui obiekt	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
	 ssh-listener 		10.0.8.60:666	SSH	Gniazdo nasłuchiw
3 Gniazda nastuchiwania	o vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
n- Modyfikatory hasel				Powód	zablokowania obie
Polityki					

9.1 Dodawanie gniazda nasłuchiwania

Ostrzeżenie: Obiekty modelu danych: *sejfy, użytkownicy, serwery, konta* i *gniazda na-słuchiwania* 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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
J Dashboard	Gajazda pashushiwania	+ Dodaj O Blokuj O Odbie	okuj 🕆 Usuń	▼ Dodaj filtr ~	Szukaj
日 Sesje	Gniazda hasuchiwania				
o Użytkownicy	🔿 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
🕀 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	C SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Coiazda packuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Grilazua nasiucriiwania	vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
n- Modyfikatory haseł					
10 Polityki					

- 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 *In*formacje 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 opcjęWlącz obsług
ęSSLv3,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.

Zarządzanie	Dodaj gniazdo nasłuchiwani	ia			
J Dashboard	Gniazda nasłuchiwania	+ Dodaj O Blokuj O Oc	fblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje	Gillazua Hasuciliwania				
督 Użytkownicy	🔿 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Cojazda packuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Giliazua nasiochiwania	vnc	whisys	10.0.8.60:59102	VNC	Pośrednik

- 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 *In*formacje 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 $Włącz \ obsług
ę<math display="inline">SSLv2,$ aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
- 10. Zaznacz opcjęWlącz obsług
ęSSLv3,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.

- 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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	nia) — — n			
Jashboard	Gaiazda pashushiwania	+ Dodaj © Biokuj © Odł	blokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🗄 Sesje	Gniazda nasiucniwania				
륳 Użytkownicy	🔿 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
A Serwerv	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	C SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Cojezda packuobiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Gillazua hasiochiwania	o vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
n- Modyfikatory haseł					
0 Polityki					

- 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 $In-formacje \ ogólne > Scenariusze \ wdrożenia.$

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 $Włącz \ obsług
ę<math display="inline">SSLv2,$ 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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
Jashboard	Gniazda nashuchiwania	+ Dodaj O Blokuj O Odbio	okuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje	Gillazda hasideniwania				
🐨 Użytkownicy	🔿 Nazwa 🔺	Selfy	Adres lokalny	Protokół	Tryb połączeni
B Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	C SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
S Gojazda paskuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Cilliazua hasiociliwalila	vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
n- Modyfikatory haseł					
0 Polityki					

- 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 *In*formacje 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.

Zarządzanie	Dodaj gniazdo nasłuchiwani	ia —			
Jashboard	Gniazda nasłuchiwania	+ Dodaj © Blokuj © Or	dblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje	Gillazua Hasuciliwania				
🐨 Użytkownicy	🔿 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączenia
🕀 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	□ SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
S Gnjazda naskuchiwanja	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Gillazua hasiocilima lia	vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
n- Modyfikatory haseł					
Polityki					

- 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 $In-formacje \ ogólne > Scenariusze \ wdrożenia.$

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.

- Model danych
- Pierwsze uruchomienie
- Użytkownicy
- Sejfy
- Konta

9.1.6 Dodawanie gniazda Oracle

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

z	arządzanie	Dodaj o	qniazdo nasłuchiwani	a —	7				
.lt) Dashboard		Gniazda nasłuchiwania	+ Do	daj O Blokuj	© Odbiokuj	🕆 Usuń	▼ Dodaj filtr ~	Szukaj
B		- E							
-		C) Nazwa -		Sejfy		Adres lokalny	Protokół	Tryb polączer
a	Serwery	C	RDP		adusers, whisys		10.0.8.60:3389	RDP	Bastion
_		0	SSH		whisys		10.0.8.160:22	SSH	Bastion
#		0	SSH - Anonymous		safe - anonymous		10.0.8.60:222	SSH	Pośrednik
		C	rdp2		whisys		10.0.8.60:9999	RDP	Bastion
	Gniazda naskuchiwania	0	ssh-listener				10.0.8.60:666	SSH	Pośrednik
	Gillazua hasiuchiwalila	9	vnc		whisys		10.0.8.60:59102	VNC	Pośrednik
ń									
U									

- 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
- \bullet Sejfy
- Konta

9.1.7 Dodawanie gniazda RDP

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

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Biokuj	Odblokuj 🔋 Usuń	▼ Dodaj filtr ∨	Szukaj
🖽 Sesje					
설 Użytkownicy	🗆 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
😑 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	C SSH	whisys	10.0.8.160:22	SSH	Bastion
🗟 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Gojazda paskuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A GINAZUA NASIUCITIWATIIA	🗆 vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
0 Polityki					

- 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 *In-formacje 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.

Host docelowy					
Adres	10.0.45.200	Port	3389		÷
Certyfikat serwera	9w0BAQEFAAOCAQ IvtqlxgNstaQBI12VA srcXv/sxwi40tX+10jv 8Lm/YAebUYSniYYU jsMUN150ZGASskP RpvdGrJmJMUK6F0 JaWQk4Pm/RtBvfQs wyLF0JJIGJzOK/gnQ	08AMIIBCgK Xol5MFo cl3AkGcQG(LyFYr lqWzavchFt) 18gJC/z8Bdt shOZDIVskci Lo9wWUAY	CAQEAvitoHrsjU/2 GovEW1MILzuzzIO (wRrV2zissxTHWE uLmec9UHXW35n 1	•	
Kliknij, aby prz	zełączyć pomięc	dzy SHA	1 i MD5		
	a1:3e:eb:c6:52:1c:3b	b:a5:a2:94:e6	5:55:97:f0:a1:ca	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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Blokuj	Odblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje					
볼 Użytkownicy	🗆 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
😑 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	□ SSH	whisys	10.0.8.160:22	SSH	Bastion
🗟 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Gnjazda naskuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A GINAZUA NASIUCITIWATIIA	🗆 vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
0 Polityki					

- 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.

Adres	10.0.45.200	Port	3389	1
Certyfikat serwera	9w0BAQEFAAOC/ IvtqlxgNstaQBI12V srcXv/sxwl40tX+I0 8Lm/YAebUYSnirA jsMUN15QZGA53 RpvdGrJmJMUKe JaWQk4Pm/RtBvf wyLF0JJIGJzOK/gI	AQ8AMIIBCgK /AXol5MFo liycl3AkGcQG(YvLyFYr kPqWzavchFt) F08gJC/z8Bdt QshOZDIVskci nQLo9wWUAY	CAQEAvitoHrsjU/Z BovEW1MILzuzzIO KwRrV2zIssxTHWE uLmec9UHXW35n 1	٢
Kliknii oby pr	zołaczyć pomi	odzy SHA	1 ; MDE YFSU	

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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	iia			
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Blokuj	Odblokuj 🔒 Usuń	▼ Dodaj filtr ∨	Szukaj
🖽 Sesje					
볼 Użytkownicy	 Nazwa * 	Sejfy	Adres lokalny	Protokół	Tryb połączenia
🖴 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	⊖ SSH	whisys	10.0.8.160:22	SSH	Bastion
🗟 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Coiezda packuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A Griazda nasiochiwania	o vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
🛡 Polityki					

- 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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Blokuj	Odblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje					
볼 Użytkownicy	🗆 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
😑 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	□ SSH	whisys	10.0.8.160:22	SSH	Bastion
🗟 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Gnjazda naskuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A GINAZUA NASIUCITIWATIIA	🗆 vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
0 Polityki					

- 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 $Włącz \ obsług
ę<math display="inline">SSLv2,$ aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
- 10. Zaznacz opcjęWlącz obsług
ęSSLv3,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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
Jashboard	Gniazda nasłuchiwania	+ Dodaj O Biokuj	Odblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje					
볼 Użytkownicy	🗇 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
😑 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	SSH	whisys	10.0.8.160:22	SSH	Bastion
🗟 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	□ rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Gnjazda naskuchiwania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A GINAZUA NASIUCITIWATIIA	🗆 vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
10 Polityki					

- 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 $Włącz \ obsług
ę<math display="inline">SSLv2,$ aby obsługiwać połączenia szyfrowane protokołem SSL w wersji 2.
- 10. Zaznacz opcjęWlącz obsług
ęSSLv3,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.

Zarządzanie	Dodaj gniazdo nasłuchiwan	ia			
M Dashboard	Gniazda nasłuchiwania	+ Dodaj © Blokuj	Odblokuj 🔒 Usuń	▼ Dodaj filtr ~	Szukaj
🖽 Sesje					
皆 Użytkownicy	🗆 Nazwa 🔺	Sejfy	Adres lokalny	Protokół	Tryb połączeni
🖴 Serwery	RDP	adusers, whisys	10.0.8.60:3389	RDP	Bastion
	C SSH	whisys	10.0.8.160:22	SSH	Bastion
🖉 Konta	SSH - Anonymous	safe - anonymous	10.0.8.60:222	SSH	Pośrednik
Sejfy	rdp2	whisys	10.0.8.60:9999	RDP	Bastion
> Cojazda packuobiuania	ssh-listener		10.0.8.60:666	SSH	Pośrednik
A GINAZUA NASIUCINWAINA	vnc	whisys	10.0.8.60:59102	VNC	Pośrednik
10 Polityki					

- 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 \mathbb{Z} .

Ogólne	Niezapisane zmiany w konfiguracji		
	Nazwa	Nazwa	
	Zablokowane		
	Protokół	VNC	\$
	Anonimowy		
	Opis	Opis	

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.

Za	rządzanie <	Fudo [•]		
M	Dashboard	Chienda nachushiwania + Do	daj OBlokuj © Odblokuj 🔒 Usuń	T Dodaj filtr ~ Szukaj
₿		Zaznacz obiekty		
쓭		Ale Zablokuj wybrane objek	stv ¥	Adres lokalny
8		10.0.40.50:9000	test-safe-2	10.0.40.50:9000
		0 10.0.40.50:9999	http	10.0.40.50:9999
-		Listner-10.0.40.50:8000	test-safe-1	10.0.40.50:8000
-		MYSQL-0-10.0.35.52	db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3306
۳	Gniazda nasłuchiwania	ORACLE-10.0.40.149	db-0 > ORACLE-10.0.40.149	10.0.40.50:1521
ń-	Modyfikatory haseł	RDP-0-10.0.35.54	rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:1005
D	Politvki	BDP-0-10.0.35.54-ANONYMOUS	anonymous > RDP-0-10.0.35.54-ANONYMOUS	10.0.40.50:2005

4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij Zatwierdź.

Zablokuj obiekty	×
Powód	
Wprowadź powód zabokowania	Anuluj Zatwierdź
Zablokuj	obiekt

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.

Z٤	arządzanie <	Fudo		
and the	Dashboard	Cojazda pachuchiwania + Do	daj 🗢 Blokuj 🕞 Usuń	T Dodaj filtr ~ Szukaj
₿		Zaznacz obiekty		
쓭		Nazwa Odblokuj wybrane ol	piekty	Adres lokalny
8		0 10.0.40.50:9000	test-safe-2	10.0.40.50:9000
		0 10.0.40.50:9999	http	10.0.40.50:9999
		Listner-10.0.40.50:8000	test-safe-1	10.0.40.50:8000
		MYSQL-0-10.0.35.52	db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3306
۳	Gniazda nasłuchiwania	ORACLE-10.0.40.149	db-0 > ORACLE-10.0.40.149	10.0.40.50:1521
ń-		RDP-0-10.0.35.54	rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:10054
U	Polityki	BDP-0-10.0.35.54-ANONYMOUS	anonymous > RDP-0-10.0.35.54-ANONYMOUS	10.0.40.50:20054

4. Kliknij Zatwierdź, aby potwierdzić odblokowanie obiektu.

Odblokuj obiekty	×
Jesteś pewien że chcesz odbiokować 1 obiekt?	
	Anuluj Zatwierdź
Odblokuj obiek	

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.

Za	arządzanie <	Fudo [*]	
	i Dashboard	Opierde perskuskiuwnia + Dodaj O Blokuj O Odblokuj 🔒 U	suń T Dodaj filtr ~ Szukaj
₿		Zaznacz obiekty	
*		Usuń wybrane obiekty	Adres lokalny
0		(c) 10.0.40.50:9000 test-safe-2	10.0.40.50:9000
		0 10.0.40.50:9999 http	10.0.40.50:9999
		Listner-10.0.40.50:8000 test-safe-1	10.0.40.50:8000
-		MYSQL-0-10.0.35.52 db-0 > MYSQL-0-10.0.35.52	10.0.40.50:3306
٣	Gniazda nasłuchiwania	ORACLE-10.0.40.149 db-0 > ORACLE-10.0.40.149	10.0.40.50:1521
ń-	Modyfikatory hasel	RDP-0-10.0.35.54 rdp-podmiana-0 > RDP-0-10.0.35.54	10.0.40.50:1005
D	Politvki	RDP-0-10.0.35.54-ANONYMOUS anonymous > RDP-0-10.0.35.54-ANONYM	OUS 10.0.40.50:2005

4. Kliknij Zatwierdź, aby potwierdzić usunięcie zaznaczonych obiektów.

Usuń obiekty	×
Jesteś pewien że chcesz usunąć 1 obiekt?	
	Anuluj Zatwierdź
	Usuń obiekt

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.

Za	arządzanie	Fudo	
	Dashboard	Delinite	
₿		Ролтука	
쓭	Użytkownicy	Ogólne Unikatowa nazwa obiektu	
8		Nazwa	
æ			
		Zmiana hasta włączona 🔽 🖉 10 minuty – Określ	częstość z
٣		Weryfikacja hasła włączona 🔽 🖉 5 minuty	
÷	Modyfikatory haseł	Określ częstość weryfikacji haseł	
U		Specyfikacja nasła	
±.	Do pobrania	Okresi złożoność generowanego nasła	
₽		Długość Z 20	
≡	Produktywność	Male litery 2 2 5	
Us	stawienia	Wielkie litery Z 🛛 5	
5		Znaki specjalne 🕎 🖉 6	
¢0	Konfiguracja sieci		
		Cyrry Col 4	
ď			
a. 	Zewnętrzne uwierzytelnianie	C Przywróć Zapisz definicj	ję obiektu

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

Wery fikacja

- 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
- $\bullet \ Konta$
- 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.

Zarządzanie	Fudt Dodaj pol	itykę zmiany hase	el —	
Jul Dashboard				
🗄 Sesje	Password policies	Custom changers	+ Dodaj 🛛 Usun	Szukaj
🔮 Użytkownicy	🗆 Nazwa 🔺		Częstotliwość zmian	
Serwery	 20 minut 		20	
	 Custom password polici 	^{zy}	1	
😹 Konta	Static, without restriction	ons	None	
Sejfy	 blaster 		10	
Gniaz Zarządzaj modyfikatorami haseł				
(h- Modyfikatory haseł)				

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.

Management	< Fudo*	
Dashboard	Policy	
E Sessions	. only	
쌸 Users	General	Provide descriptive name
⊖ Servers	Name	10 minutes, 20 chars, lowercase, digits
Accounts	Enable password change	
E Cafee	Password change enabled	0 10
Odits	Password verification enabled	Opefine how frequently the password will be changed
ふ Listeners		Enable password verification

6. Wprowadź liczbę znaków hasła.

7. Zaznacz wybrane opcje złożoności hasła i wprowadź minimalną liczbę znaków dla każdej z nich.

n- Modyfikatory haseł	Specyfikacja hasła	
Polityki		Określ długość hasła
📥 Do pobrania	Długoś	ć 20
🔒 Raporty	Małe liter	y 🛛 15
E. Produktywność	Aktywuj wybraną opcję złożoności	Wprowadź minimalną liczbę znaków
Ustawienia	Znaki specjaln	e 🗆
😂 System	Digit	is 🖸 5
¢% Konfiguracja sieci		

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.

z	arządzanie <	Fudo					
æ	i Dashboard	Konta + Dodaj O	0 8			▼ Dodaj filtr ~	Szukaj
E	8 Sesje						
-	Użytkownicy	🗆 Nazwa 🔺	Serwer *	Nagrywanie sesji 👻	Тур	Polityka modyfikatora haslą	Modyfikator
8	Serve Zarzadzai kontami uprz	zvwileiowanymi	10.0.235.254	all	regular	Statyczne, bez ograniczeń	Brak
\sim			10.0.235.254	all	anonymous	None	None
C	Konta	 linux1-nginx-account 	linux1-nginx	all	forward	None	None
	l Sejfy	linux1-ssh-user1	linux1-ssh	all	regular	Statyczne, bez ograniczeń	Brak
	Gniazda nashurhiwania	Inux1-ssh-user2	linux1-ssh	all	regular	Statyczne, bez ograniczeń	Konto Unix
	Ghiazua hasiooniwania	linux1-telnet-user1	linux1-teinet	all	regular	Statyczne, bez ograniczeń	Brak
ń	 Modyfikatory haseł 	 mysql-root 	mysql	all	regular	Statyczne, bez ograniczeń	Brak
U	Polityki	rdp-forward Edytuj kont	win2008r2	all	forward	None	None
📩 Do pobrania		root-BSD	BSD	all	regular	Statyczne, bez ograniczeń	Brak
	terminalserver-anonymous	terminalserver	all	anonymous	None	None	

- 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.

a, Zewnętrzne uwierzytelnianie	Dane uwierzytelniające	
III Zewnętrzne repozytoria haseł	Whicz nazwo użył	kownika konta uprzywilojowanogo
Zasoby	Vvpisz nazwę uzyt	
Wybierz opcję zastępow	wania sekretu hasłem	usei
A Klaster	Zastąp sekret	hastem
Wprowadź hasło do konta up	orzywilejowanego Hasto	[
≡ Dziennik zdarzeń	Powtórz hasło	L
	Polityka modyfikatora hasłą	10 minut, 20 znaków, małe litery, cyfry
lipern-29507 ∴ Nie skonfigurowany		Wybierz politykę zmiany haseł

- 7. W sekcji Modyfikator hasła, wybierz Unix Account over SSH.
- 8. Uzupełnij dane logowania superużytkownika.

	Modyfikator bools Wybierz modyfikator właściwy dla systemu docelowe
	Modyfikator hasta None
Wprowadź login użytkownika	a uprzywilejowanego
	Użytkownik uprzywilejowany root
	Hasło użytkownika
	Podaj hasło użytkownika uprzywilejowanego

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
- $\bullet\,$ 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 $Sie\acute{c}$ 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.

Zarządzanie	< Fudt Dodaj politykę zmiany haseł	Fudr Dodaj politykę zmiany haseł		
M Dashboard				
🖽 Sesje	Password policies Custom changers	+ Dodaj 🛛 Usun	Szukaj	
🗑 Użytkownicy	Nazwa 🔺	Częstotliwość zmian		
Serwery	20 minut	20		
	 Custom password policy 	1		
🚇 Konta	Static, without restrictions	None		
Sejfy	blaster	10		
Gniaz Zarządzaj modyfil	atorami haseł			
(🕂 Modyfikatory haseł)				

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.

Management <	Fudo	
M Dashboard	Policy	
E Sessions	Policy	
🖆 Users	General	Provide descriptive name
⊖ Servers	Name	10 minutes, 20 chars, lowercase, digits
Accounts	Enable password change	
Safes	Password change enabled	0 10
> Listenere	Password verification enabled	Opfine how frequently the password will be changed
M LISCONOIS		Enable password verification

- 6. Wprowadź liczbę znaków hasła.
- 7. Zaznacz wybrane opcje złożoności hasła i wprowadź minimalną liczbę znaków dla każdej z nich.

n- Modyfikatory haseł	Specyfikacja hasła		
🛡 Polityki		Określ długość hasła	
📥 Do pobrania	Długość	ść (20	
🔒 Raporty	Male litery	ry 015	
E. Produktywność	Aktywuj wybraną opcję złożoności	Wprowadź minimalną liczbę zn	aków
Ustawienia	Znaki specjalne	wybranego typu	
😂 System	Digits	its 🗹 5	
¢° Konfiguracja sieci			

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.

e Zewnętrzne uwierzytelnianie	Dane uwierzytelniające	
III Zewnętrzne repozytoria haseł	Whicz nazwo użu	tkownika konta uprzywilojowanogo
🖬 Zasoby	vvpisz nazwę uzy	
K Wybierz opcję zastępow	wania sekretu hasłem	(ballet
A Klaster Warowadź boola do konto ur	Zastąp sekret	nasrem
wprowadz nasio do konta up	Hasto	
≡ Dziennik zdarzeń	Powtórz hasło	
	Polityka modyfikatora hasłą	10 minut, 20 znaków, małe litery, cyfry
li>pam-29807		— Wybierz politykę zmiany haseł ———

- 7. W sekcji Modyfikator hasła, wybierz Windows Account over WMI.
- 8. Uzupełnij dane logowania superużytkownika.

	Modyfikator bools Wybierz modyfikator właściwy dla systemu docelowe
	Modyfikator hasta None
Wprowadź login użytkownika	a uprzywilejowanego
	Użytkownik uprzywilejowany root
	Hasło użytkownika
	Podaj hasło użytkownika uprzywilejowanego

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.

Zarządzanie <	Fudo [*]		
Dashboard	Polityki Wzorce	Wybierz zakładke definiowania wzorc	ów
🖽 Sesje	Polityki	wybielz zakładkę deliniowalna wzorc	
🗑 Użytkownicy	Nazwa	delete all	
⊖ Serwery	Wzorzec	rm -Rf	
- Bastiony	Usuń	0	
🕂 🖻 Przejdź do widoku zarza	ądzania politykami 🗤	assasinate all	
🛡 Polityki	Wzorzec	killall	
📩 Do pobrania	Usuń	0	
🔒 Raporty			
Produktywność			
Ustawienia			
System			
¢° Konfiguracja sleci			
Powiadomienia			Dodaj definicję wzorca
Znakowanie czasem		C Przywróć Zapisz	0

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.

Zarządzanie	<	Fudo		
Jef Dashboard		Polityki	Wzorco	
🗄 Sesje		Polityki	WZOICe	
별 Użytkownicy			Nazwa	delete all
⊖ Serwery			Wzorzec	rm -Rf
• Bastiony			Usuń	0
🕂 Połączenia			Nazwa	assasinate all
🛡 Polityki			Wzorzec	killall
📥 Do pobrania			Usuń	 Wprowadź nazwę wzroca
🖨 Raporty			Nazwa	
Produktywność			Wzorzec	
Ustawienia				
😂 System			Usuń	Wprowadź ciąg znaków stanowiących wzorze
¢6 Konfiguracja sieci				
🖂 Powiadomienia				Zapisz zmiany
Znakowanie czasem				C Przywróć Zapisz

Informacja: Przykłady wyrażeń regularnych

 $Komenda \ \texttt{rm}$

(^|[^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.

Za	arządzanie <	Fudo			
M	Dashboard	Polituki Wzorzo			
₿		Polityki Wzorce			
쓭	Użytkownicy	Nazwa	notif law in		×
8					-
		Wzorzec	test1	0	Q
۳	Gniazda nasłuchiwania	Poziom zagrożenia	Niski		• ==
•	Sejfy	Dopasuj tylko dane wejściowe	0		
ń-	Mpoy Przejdź do widoku z	arządzania politykami			
Ū	Polityki				
*	Do pobrania				
₽					
≡	Produktywność				
U	stawienia				
5					
¢°	Konfiguracja sieci				
•	Zewnętrzna macierz dyskowa				Dodaj definicję polity
	Powiadomienia		0.0		
12	Znakowanie czasem		C Przywroc	✓ Zapisz	

- 3. Wprowadź nazwę dla definiowanej polityki.
- 4. Określ akcje, które Wheel Fudo PAM podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców.

\geq	Wyślij powiadomienie email do administratora systemu.
	Wstrzymaj połączenie.
<u>ې</u> ځ	Przerwij połączenie.
0	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.

Zar	ządzanie <	Fudo	🛓 at
	Dashboard	Deliniti Manage	
₿		Polityki Wzorce	
쓭	Użytkownicy	Nazwa notif low in 🖂 🔢 💱	0 x
8			•
		Wzorzec testi	ଁ ଷ୍
٣	Gniazda nasłuchiwania	Poziom zagrożenia Niski	¢
•		Dopasui tvlko dane weiściowe	
ń-	Modyfikatory haseł	Wprowadź nazwę definiowanej polityki	pierz akcje
U	Polityki	Nazwa	• ×
*	Do pobrania	Wzorzec	Wybierz wzorce, które
₽		Poziom zagrożenia	* Whathach dem
Ξ.			reśl poziom zagrożenia
Ust	awienia	Zaznacz, aby analizie podlet	nesi pozioli zugiozenia
			gai jeuyille struttilen wejsclowy
00	Konfiguracja sieci		
•		Zapisz zmiany	
	Powiadomienia	C Prowership and Tapian	-
ß	Znakowanie czasem	C Przywiec Zapisz	

Informacja: Po utworzeniu polityki, przypisz ją do wybranego sejfu.

Zarządza	anie <	Fudo				
🖬 Dash		Colif				
🖽 Sesje		36)1				
· Użytk		Ogólne				
🔒 Serw	rery	D	688817234205736975			
🔊 Konta						
🗟 Gniaz	zda nasłuchiwania	Nazwa	Policy_test			204
Sejfy		Zablokowane				
nh- Mody		Powiadomienia 🗆	Rozpoczęcie sesji	Session start (push)		
I Polity			 Zakonczenie sesji Odłączenie od sesji 	 Dotączenie do sesji Wykrycie wzorca 		
📥 Do po		Powód logowania				
🔒 Rapo		_{wyr} Przypisz poli	tykę do sejfu	_		
🖹 Produ	uktywność	Polityki	notif_low_in		Q	
Ustawier	nia					
🕒 Syste	em	Użytkownicy	user1 userxy	0	Q	

Usuwanie definicji wzorców

- 1. Wybierz z lewego menu Zarządzanie > Polityki.
- 2. Wybierz zakładkę *Wzorce*.
- 3. Zaznacz opcję $\mathit{Usu\acute{n}}$ przy wybranym wzorcu.
- 4. Kliknij Zapisz.

Zarządzanie <	Fudo [®]	
Jashboard	Deliberi Wesses	
🗄 Sesje	Polityki wzorce	
😵 Użytkownicy	Nazwa delete all	
⊖ Serwery	Wzorzec rm -Rf	
•# Bastiony	Usuń 🗆	
🕂 Polączenia	Nazwa assasinate all	
🛡 Polityki	Wzorzec killall	
📥 Do pobrania	Usuń 🗆	
🖨 Raporty	Zaznacz, aby usunąć wybrany wzorzec	
Produktywność		
Ustawienia		
😂 System		
¢° Konfiguracja sieci		
Powiadomienia	Zapisz zmiany	
Znakowanie czasem	C Przywróć Zapisz	

Usuwanie definicji polityk

Aby usunąć definicję polityki, postępuj zgodnie z poniższą instrukcją.

- 1. Wybierz z lewego menu Zarządzanie > Polityki.
- 2. Zaznacz opcję $\mathit{Usu\acute{n}}$ przy wybranej polityce.
- 3. Kliknij Zapisz.

Za	rządzanie	< Fudo	
M	Dashboard	Przejdź do widok	u zarządzania politykami
₿	Sesje	Zaznacz	z, aby usunąć wybraną definicję polityki
쓭	Uzytkownicy	Nazwa	
⊜	Serwery		
	Konta	Wzorzec	
٣	Gniazda nasłuchiwania	Poziom zagrożenia	Niski 🗣
•	Sejfy	Dopasuj tylko dane wejściowe	0
÷.	Modyfikatory haseł		
U	Polityki		
*	Do pobrania		
₽			
≡	Produktywność		
Us	tawienia		
Ŀ			
¢°	Konfiguracja sieci		
•	Zewnętrzna macierz dyskowa		Zapisz zmiany
Ø	Znakowanie czasem		

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).
0	Sesja opatrzona znacznikiem czasu.
•	Powód nawiązania sesji.
•	Sesja zawiera naniesione komentarze.
-	Sesja została przetworzona na potrzeby przeszukiwania pełnotesktowego.
C	Otwórz zarządzanie udostępnianiem sesji.
*	Pobierz materiał sesji w wybranym formacie (<i>dotyczy sesji nagranych z opcją</i> rejestrowania pełnego lub surowego ruchu).
I	Monitor aktywności użytkownika (dotyczy sesji aktualnie trwających).
å	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.

	Indeksuj sesje	e graficzne											
Zarządzan	le Usuń zaznacz	zone sesie D								Zdefiniuj f	filtr dla list	ty obieł	któw
Jan Dashbo	ard			D Conor	ul raport				T Dodai fil	47 4 Com	kel		
⊟ Sesie		Sesje	sun la och la ca		aj raport				r Dodaj m	SZU SZU	кај	0	u.
ali Lindkos	uniew	Przetwórz zazna	aczone sesje	Serwer	Konto	Sojf	Rozpoczęta =	Zakończona	Czas trwania	Aktywność	Rozmiar		
_ OLYNO		Generuj raport	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:51	2017-02-17 07:52	15:00:42	0%	131.0 KB		土
😑 Serwen		□ ► anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:49	2017-02-16 16:51	0:02:24	42%	792.0 KB		\pm
🖉 Konta		anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:46	2017-02-16 16:46	0:00:04	0%	83.0 KB	998	±
S Gniazda		□ ▶ anor Odt	wórz zareiestrowan	v materiał	ica-anon	citrix-anon	2017-02-16 16:45	2017-02-16 16:46	0:00:05	onv stat	usowe se	sii	*
Seify		anonymous	ICA	citrix	ica-anon	citrix-anon	2017-02-16 16:43	2017-02-16 16:45	0:02:05	48%	443.0 KB		\pm
_		□ ► user1	ICA	citrix	ica-reg	citrix2	2017-02-16 16:37	2017-02-16 16:37	0:00:03	0%	5.0 KB		± د
ni- Modyfil		□ ► user1	ICA	citrix	ica-reg	citrix2	2017-02-16 15:16	2017-02-16 15:16	0:00:12	0%	31.0 KB		±
I Polityki		Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:13	2017-02-16 15:14	0:00:29	0%	1.0 KB		<u>ن خ</u> ا
📥 Do pob		Anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:05	2017-02-16 15:05	0:00:11	0%	44.0 KB		는 초
A Report		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:04	2017-02-16 15:04	0:00:19	100%	250.0 KB		: ≛
e napong		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:03	2017-02-16 15:03	0:00:11	0%	31.0 KB		<u>ت د</u>
■ Produkt		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 15:02	2017-02-16 15:02	0:00:11	0%	67.0 KB		±
Ustawienia		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	29.0 KB		Ľ.≛.
🖨 System		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 14:58	2017-02-16 14:58	0:00:12	0%	62.0 KB		는 초
the Kanfini		Anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:39	0:18:29	0%	144.0 KB	E	∷ ≛
W ₆ Konigu	racja sieci	Anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 14:20	2017-02-16 14:20	0:00:01	0%	22.0 KB) - E	i: ±
Powiad		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:31	2017-02-16 12:31	0:00:00	0%	1.0 KB		≝ ±
C Znakow		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB		Ľ ≛
د Zewnet	rzne uwierzytelnianie	anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:30	2017-02-16 12:30	0:00:00	0%	1.0 KB		_ ₹
		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:28	2017-02-16 12:28	0:00:00	0%	1.0 KB		<u>ت ځ</u>
III Zewnęt		anonymous	ICA	citrix	ica-anon	citrix2	2017-02-16 12:24	2017-02-16 12:24	0:00:00	0%	1.0 KB		11 A
🔚 Zasoby		anonymous	Citrix StoreFront (HTTP)	storefront	sf-anon	citrix2	2017-02-16 12:21	2017-02-16 12:48	0:26:47	0%	17.0 KB		<u> </u>
🖬 Kopie z		D ▶ ad-user10	Citrix StoreFront (HTTP)	storefront	sf-forward	citrix	2017-02-16 12:02	2017-02-16 12:15	0:12:51	0%	20.0 KB		<u> </u>
# Klaster		□ ► Administrate	or RDP	rdp1.endpoint	Forward	Rdp	2017-02-14 14:23	2017-02-14 14:24	0:00:02	0%	226.0 KB	0	
-		D ► ad-user10	HUP	rap1.endpoint	Forward	нар	2017-02-14 14:20	2017-02-14 14:20	0:00:05	096	164.0 KB		2
		□ ► ad-user10	RDP	rdp1.endpoint	Forward	Hdp	2017-02-14 14:17	2017-02-14 14:18	0:00:56	100%	242.0 KB	6	_ ≛
⊟ Dzienni	k zdarzeń												

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.

Zarządzanie <	Fudo	🛔 admin < 🔹 ?
Jul Dashboard	Sesje J Wybierz parametr filtrowania Toodaj filtr - 🔒 Generuj raport Szukaj	0 Q.~
🖽 Sesje	Według protokołu	
Użytkownicy	Użytkownik Serwer Protokół Połączenie Rozp Według użytkownika Czas trwania Aktywność Rozmiar	
🖴 Serwery	► Mickey Mouse fudo4 SSH ssh 2015 Wedkug servera 26:01 0:00:00 0% 16.0 KB	이 아들 것 수
e Dentione	► Mickey Mouse fudo4 SSH ssh 2015 Wedkug organizacji 08:01 0:00:00 0% 15.0 KB	이 이는 것 수 이 아
Hastiony	Mickey Mouse fudo4 SSH ssh 2015 Od daty D8:01 0:00:00 0% 15.0 KB	이 아들 문 소
++ Połączenia	Do daty	
🛡 Polityki	Con	

2. Wybierz wartości dla wcześniej dodanego parametru filtrowania.

Zarządzanie	< Fudo'	admin ~ ?
Jashboard	Sesie "I Aktywne 🖹 Usuń 🖾 OCR 💦 🕇 Dodai filtr.» 🗛 Generui raport Szukal	0 Q v
🖽 Sesje	Wprowadź ciąg znaków, aby ograniczyć liczbę	obiektów na liście
발 Użytkownicy	Według użytkownika Ole Vulkownika	e obiekty
🖴 Serwery	Zaznacz wszystkie obiekty - O	
• Bastiony	Mickey Mouse Spiderman	
🕂 Połączenia	Użytkownik Serwer Protoko Winnie the Pooh Aktywność Rozmiar	
🛡 Polityki	Mickey Mouse fudo4 SSH anonymous 0% 16.0 KB	5 C A
🛓 Do pobrania	 ► Mickey Mouse fudo4 SSH ► Mickey Mouse fudo4 SSH Wybierz z listy obiekty dla wybranego parametru filt 	rowania

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.

Zarządzanie	<	Fudo	t i							🏝 adm	iin ~ 🥐
Dashboard		Secie	al Aktywne	🖹 Usuń	C OCR		▼ Dodaj filtr ∨	🔒 Generuj raport	Szukaj	0	Q.~
🖽 Sesje		ocaje									_
쑬 Użytkownicy			Według użytk	ownika	Mickey Mouse	- Wpr	owadź nazwę	użytkownika,	rolę lub org	ganizację	
⊖ Serwery					user			T	B		
-# Bastiony	Wybier	z wcześn	iei dodany (obiekt	 Mickey Mouse Spiderman 						
🕂 Połączenia	aby us	unąć go z	listy filtrow	ania	Winnie the Po	sh		wr	ość Rozmiar		

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.

Zarządzanie <	Fudo	i							📤 adr	nin ~ 🥐
	Cosio		8 Usuń	OCR		▼ Dodaj filtr ∨	🕀 Generuj raport	Szukaj	0	Q٧
日 Sesje	Sesje									
📽 Użytkownicy	Według użytkownika			Mickey Mouse Spideman Winde the Pooh O						
		Według :	serwera	MySQL self	rssh		O Q	×		
	Nezwa fir Mechanizm filtrowania pozwala na dodanie wielu									
+ Połączenia	obiektów dla wybranego parametru filtrowania									

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.

Zarządzanie	<	FUC	10 °										🕹 ad	min 🕤 🥐
		Socio		ktywne	19 Usu	ń 🖬 00	CR	▼ Dodaj filtr ~	e	Generuj rapo	rt Szul	(a)	0	Q.~
🖽 Sesje		Jesje					(✓ Według protokołu						
🗑 Użytkownicy			w	edług pro	otokołu			Według użytkownika Według połaczenia	1	େ ଷ୍	×			
Serwery						Nazwa f	iltra	Według serwera		Klikni	j, aby w	yłączyć	: filtrow	anie we
+ Bastiony								Według organizacji Od daty						
🕂 Połączenia			Jżytkownik	Serwer	Protokół	Połączenie	Rozpoczęt	Do daty		Czas trwania	Aktywność	Rozmiar		
		□ ▶ ₹	admin	fudo4	SSH	ssh	2015-07-2	OCR	52	0:00:05	100%	7.0 KB	0.5	s na

12.1.2 Przeszukiwanie pełnotekstowe

Wheel Fudo PAM pozwala na przeszukiwanie zapisanego materiału, ograniczając listę sesji do pozycji zawierających wskazany ciąg znaków.

Zarządzanie <	Fuda	ı '								📥 admi	n~ ?
J Dashboard	Sesie	al Aktywne	🖹 Usuń		3	▼ Dodaj filtr ~	🔒 Generuj rapo	rt Szuk	aj		٩×
🖽 Sesje	ocaje			Znai	dź sesie zawi	eraiace wprov	vadzonv cia	o znakóv	v		
Użytkownicy	Uź,	tkownik Serwer	Protokół	Połączenie	Rozpoczęta -		kres przesz	ukiwani	lozmiar		
🖴 Serwery	□ ► a	fudo	SSH	ssh	2015-07-21 13:32	2015-07-21-10/02		10070	14.0 KB		. ₹
. Bashing	□ ► a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:32	0:01:47	56%	34.0 KB	- 1 6	∴±
• Bastiony	□ ► a	fudo	SSH	ssh	2015-07-21 13:30	2015-07-21 13:30	0:00:05	100%	14.0 KB		±
+ Połączenia	□ ► a	fudo	SSH	ssh	2015-07-21 13:28	2015-07-21 13:29	0:00:07	100%	14.0 KB		<u>له</u>

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.

Zarządzanie <		Fudo	·							å adr	nin 🕤 📍
💷 Dashboard		Sesie	d Aktywne	🕆 Usuń	G OCR		▼ Dodaj filtr ~	🔒 Generuj raport	Szukaj	0	Q.~
🖽 Sesje	Ľ	,.									
督 Użytkownicy			Według pro	otokołu	SSH	Wpr	owadź nazwę	definicji parame	etrów filtrowania		
🖴 Serwery				(mój_własny_	filtr			×		
							Zapisz definicj	ję filtrowania 🗕			

Edycja definicji filtrowania

- 1. Kliknij Dodaj filtr i wybierz żądaną definicję filtrowania.
- 2. Zmodyfikuj opcje filtrowania zgodnie z potrzebą.
- 3. Kliknij ikonę zapisu ustawień.

Zarządzanie <	Fudo									≜ ad	imin ~	?
Dashboard	Sasia	ktywne 🖹 Us	uń 🖾 OC	R	▼ Dodaj filtr ~		🔒 Generuj rapo	ort S	Szukaj	0	Q	~
🖽 Sesje	ousju				Według protokołu	r						
🖀 Użytkownicy	Użytkownik	Serwer Protok	it Połączenie	Rozpoczęt	Według użytkownika Według połaczenia		Czas trwania	Aktywn	ość Rozmiar			
⊖ Serwery	admin	fudo4 SSH	ssh	2015-07-2	Według serwera	52	0:00:05	100%	7.0 KB	9.5	ь÷.	÷
	admin	fudo4 SSH	ssh	2015-07-1	Według organizacji	D1	0:00:00	0%	16.0 KB	19.54	5 U.	*
• Bastiony	🗆 🕨 admin	fudo4 SSH	ssh	2015-07-1	Od daty	D1	0:00:00	0%	15.0 KB	~ 10	b D.	÷
🕂 Połączenia	admin	fudo4 SSH	ssh	2015-07-1	Do daty	D1	0:00:00	0%	15.0 KB	= 5.6	5	÷
ID Dalibuki	admin	fudo4 SSH	ssh	2015-07-1	OCR	D1	0:00:00	0%	18.0 KB	(p, γ)	b 11.	±.
e Polityki	admin	fudo4 SSH	ssh	2015-07-1	mój_własny_filtr	01	0:00:00	0%	15.0 KB	19.54	5 U.	÷
📩 Do pobrania	🗆 🕨 admin 🕠	Wybierz z lis	sty definic	ję filtrov	vania 2015-07-16 08	:01	0:00:00	0%	15.0 KB	25	b 11	Ŧ

Usuwanie definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.

Zarządzanie <	Fudo									≜ ac	imin ·	~ ?
I Dashboard	Seele	tywne ⊜ Usu	ń 🖾 OCR		▼ Dodaj filtr ~		🔒 Generuj rapo	ort Szu	ukaj	0	Q	
日 Sesje	Jesje				Według protokołu	٢						
🐨 Użytkownicy	 Użytkownik 	Serwer Protokół	Połączenie R	ozpoczęt	Według użytkownika Według połaczenia		Czas trwania	Aktywnoś	é Rozmiar			
Serwery	admin	fudo4 SSH	ssh 2	015-07-2	Według serwera	52	0:00:05	100%	7.0 KB	93	6	Ŧ
d Destingu	🗆 🕨 admin	fudo4 SSH	ssh 2	015-07-1	Według organizacji	D1	0:00:00	0%	16.0 KB	9.9	5	*
•li Bastiony	admin	fudo4 SSH	ssh 2	015-07-1	Od daty	D1	0:00:00	0%	15.0 KB	9.5	5	*
🕂 Połączenia	🗆 🕨 admin	fudo4 SSH	ssh 2	015-07-1	Do daty	D1	0:00:00	0%	15.0 KB	93	5	*
	🗆 🕨 admin	fudo4 SSH	ssh 2	015-07-1	OCR	01	0:00:00	0%	18.0 KB	93	5	÷
Ф Рошукі	admin	fudo4 SSH	ssh 2	015-07-1	mój_własny_filtr	01	0:00:00	0%	15.0 KB	95	5	±
📩 Do pobrania	□ ► admin W	/ybierz z list	y definicję	filtrow	ania 2015-07-16 08	:01	0:00:00	0%	15.0 KB	> 5	6	Ŧ

2. Kliknij ikonę usunięcia definicji filtrowania.

Zarządzanie		fudo	•							🛔 admin 🕤 📍
🔟 Dashboard		Sesie	d Aktywne	🖹 Usuń	I OCR		T Dodaj filtr √	🔒 Generuj raport	Szukaj	0 Q~
日 Sesje	11									
볼 Użytkownicy			Według pro	otokołu	SSH			ଁ ପ୍	×	
⊟ Serwery					mój_własny_f	itr)
							Usuń d	efinicję filtrowar	iia ——	

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.

000	Secia 6871947604880708823	.,л
	Sesja 00/194/004000/00025	K
https://10.0.8.64/sessions/	6871947604880708823/	
Last login: Tue Oct 7 root@marcin-fudo:~ #	08:38:17 2014 from 10.0.1.13	
Kliknij,	, aby przełączyć pomiędzy wyświetlaniem czasu rzeczywistego a czasu względnego połącz	enia
II » »» ເ⊅ 01:17:05	01:17:05 Ø Informacje Szczegóły 🗈 Udostęp	onij 🥜
🙂 Zakończ Wstrzymaj 🕩 Dołącz	Wide	ok na żywo
01:16:50	01:16:55 01:17:00	01:17:05

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

 ${\rm W}$ 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.

0	O O Sesja 671923719081296897 ₽
6	https://10.0.8.63/apps/play/671923719081296897/
Wel	ome to FreeBSDI
Bef	re seeking technical support, please use the following resources:
•	ecurity advisories and updated errata information for all releases are t http://www.FreeBSD.org/releases/ - always consult the ERRATA section or your release first as it's updated frequently.
0	he Handbook and FAQ documents are at http://www.FreeBSD.org/ and, long with the mailing lists, can be searched by going to ttp://www.FreeBSD.org/search/. If the doc package has been installed or fetched via pkg_add -r lang-freebsd-doc, where lang is the letter language code, e.g. en), they are also available formatted in /usr/local/share/doc/freebsd.
If `un as unf man Edi	ou still have a question or problem, please take the output of me -a', along with any relevant error messages, and email it question to the questions@FreeBSD.org mailing list. If you are niliar with FreeBSD's directory layout, please refer to the hier(7) al page. If you are not familiar with manual pages, type `man man'. /etc/motd to change this login announcement.
fba	-radius#
	» »» ₺ 00:00:03
¢	Zakończ Wstrzymaj + Dołącz Widok na żywo
00:	00:00:05 00:00:10
	Wstrzymaj sesję

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.

(00			Ses	ija 67192371	9081296897			R _M		
6	🖹 https://1	L0.0.8.63/a		ay/671	9237190812	296897/					
Ke)	lcome to Free	BSDI									
Be	fore seeking	technical su	pport, pl	lease us	e the following	g resources:					
•	Security advisories and updated errata information for all releases are at http://www.FreeBSD.org/releases/ - always consult the ERRATA section for your release first as it's updated frequently.										
0	The Handbook and FAQ documents are at http://www.FreeBSD.org/ and, along with the mailing lists, can be searched by going to http://www.FreeBSD.org/search/. If the doc package has been installed (or fetched via pkg_add -r lang-freebsd-doc, where lang is the 2-letter language code, e.g. en), they are also available formatted in /usr/local/share/doc/freebsd.										
If `ur as uni mar	you still ha name -a', alo a question f familiar with nual page. 1	nve a questio ong with any to the questi n FreeBSD's d if you are no	n or prob relevant ons@Free irectory t familia	error m SSD.org t layout, ar with t	ease take the essages, and esmailing list. please refer manual pages,	output of mail it If you are to the hier(7) type `man man'.					
Bd.	it /etc/motd	to change th	is login	announc	ement.						
fb	sd9-radius#										
	► × ××	¢ 00:00	0:03		₩00:01:18	Informacje	Szczegóły	C Udostępnij	~		
	ථ Zakończ	Wstrzymaj	🔹 Dołą	cz				Widok na	żywo		
00:00:00 Dołącz o		Dołącz d	o sesji		00:0	00:10					
								Sector Barrier B. Martin B. Barrier			

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.



4. Określ ramy czasowe dostępności sesji i kliknij Zatwierdź, aby wygenerować adres URL, pod którym udostępniony zostanie zapis sesji.

00:00:10

Szczegóły

🖻 Udostępnij 🕽 🛃

Widok na żyw

Udostępnij sesję 🗙
Zdefiniuj ramy czasowe dostępności sesji
Dostępne od
2014-03-07 16:02:02
Dostepne do
2014-03-08 00:02:02
Kliknij, aby wygenerować adres url dla sesji Określ możliwość ingerencji w sesję - dotyczy sesji na żywo
Zamknij Udostępnij

5. Skopiuj odnośnik i kliknij Zamknij.

▶ » »» ₺ 00:00:03 ▶ 00:01:18 Informacje

00:00:05

U Zakończ Wstrzymaj → Dołącz

00:00:00

Udostępnij sesję	×
Udosteonii ten adres Skopiuj adres url, aby udostępnić https://10.0.35.10/sessions/848388532111147457/?key=MdvjVmaS:8483885321111	. zapis sesji 147457:84
(Zamknij
Zamknij okno udostępniania sesji	

- 1. Wybierz z lewego menu Zarządzanie > Sesje.
- 2. Znajdź żądaną sesję i kliknij ikonę udostępniania, aby otworzyć okno zarządzania odnośnikami.

🗆 🕨 admin	win-2003	RDP	rdp-podmiana	07.11.2014 11:28	07.11.2014 15:11	3:43:43	4%	10.0 MB	• = : 🕑 ±
	Otwórz widok zarządzania odnośnikami								

3. Kliknij ikonę unieważnienia odnośnika.

Zarządzanie	udostępnia	niem sesji	Dodaj filtr	Generuj
URL	Od	Do	Unieważnij odnośnik Stworzony przez	
https://10.0.45.212 key=vp4qHkoBH2f	2014-12-31 11:53	2014-12-31 19:53	admin	0
https://10.0.45.212 key=DdKHqOiw1y	2014-12-30 09:57 Odnośnik utra	2014-12-30 17:57 acił ważność	admin	
https://10.0.45.212 key=Jg5sElcXl6QA	2014-12-31 09:56	2014-12-31 17:56	admin	
Odnośnik uni	eważniony przez admi	nistratora		
				Zamknij

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.

Edytuj komentarz
Usuń komentarz
0:02:30 - 0:02:31
#tag2
admin 2014-12-30 14:12
odpowiedź
Dodaj odpowiedź 2014-12-30 14:13
Edytuj odpowiedź
Odpowiedz 🕎
#tag2

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.

Zarządzanie	< 🗗	Fudo								4	admin ~ 🤶 ?
Jashboard	Sec		🕆 Usuń	G OCR			▼ Dodaj filtr ~	A Generuj raport	Szukaj		0 9.4
日 Sesje	Jesj	9			_						
😁 Użytkownicy	0	Użytkownik Serwer			Kliknij, a	by wyświetlić	opcje konwersji	i pobierania z	arejestrowa	nego materiałi	U
Serwerv		anonymous RDP-10	.0.8.103-		RDP	anonymous	2016-01-11 12:31	2016-01-11 13:37 1:	06:24 8%	24.0 MB	
		anonymous RDP-0-	TLS-10.0.40.1	00-ANONYMOUS	S RDP	anonymous	2016-01-11 12:13	2016-01-11 12:27 0:	14:22 63%	26.4 MB	

3. Wybierz format pliku wyjściowego.

Informacja: Format pliku wyjściowego oraz rozdzielczość obrazu wideo wpływają na czas trwania konwersji oraz rozmiar pliku wynikowego.

Pobierz sesję	Wybierz opcje konwersji 🗮
Format	DivX5 (AVI)
Rozdzielczość	Automatyczna 💠
	Anuluj
	Rozpocznij konwersję

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.

Zarządzanie <	fudo"			🕹 admin 🗸 💡
Dashboard	De pobrania 🔒 Usuń			
🕒 Sesje	Do pobrania			
Użytkownicy	D ID ID sesji	Rozmiar	Format	Rozdzielczość
⊖ Serwerv	7 848388532111147069	0 bajtów	DivX5 (AVI)	Monitoruj postęp konwersji
,	6 848388532111147083	0 bajtów	DivX5 (AVI)	Automatyczna 3
•∉ Bastiony	5 848388532111147076	444.5 KB	DivX5 (AVI)	Automatyczna 📥
💠 Połączenia	4 848388532111147076	465.6 KB	Flash Video (FLV)	Automatyczna 🛓
E Delinia	3 848388532111147076	4.5 MB	MJPEG (wysoka jakość)	Pobierz skonwertowany materiał — 🙆
V Polityki	2 848388532111147075	22.1 MB	MPEG-2 (popularny format)	Automatyczna 🛓
📥 Do pobrania	1 848388532111147076	529.9 KB	Xvid (AVI)	Automatyczna 🛓
A Raporty				

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.

Zarządzanie <	Fudo	
Jashboard	Delegenie	
🖽 Sesje	Polączenie	
🔮 Użytkownicy	Ogólne	
⊖ Serwery	ID 84838853	2111147016
-∉ Bastiony	Nazwa ssh-przek	azywanie-0
+ Połączenia		
🛡 Polityki	Zablokowane	
📥 Do pobrania	Powiadomienia 🗹 🗹 Rozpoczę V Dołączeni	cie sesji 😨 Zakończenie sesji le do sesji 😨 Odłączenie od sesji
🔒 Raporty	Wykrycie	WZOFCA
Produktywność	Użytkownicy	େ ଭ୍
Ustawienia Przetwarzaj poła	czenia RDP i VNC	\$
🛎 System	OCR sesji 🛛 🖾	
📽 Konfiguracja sieci	Język OCR 🗌 🗆 Angielski	Polski
Powiadomienia	Norweski	Rosyjski
Znakowanie czasem	Usuń dane sesji po upływie Określ jęz	zyk przetwarzanych treści dni

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.

Zarządzanie	< <mark>Eudo</mark>	Zaznacz żąd	lane sesje			🛔 admin 🐇 🤶 📍
	SesieAkt	ywne ⊜ Usuń	C OCR	▼ Dodaj filtr ~ 🔒 Generuj rap	ort Szukaj	0 Q
🖽 Sesje			-			
📽 Użytkownicy	Użytkownik	Server Protokół Poli fudo4 SSH ssh	aczenie Rozpoczęta + 2015-05-07 11:18	Zakończona Czas trwania 2015-05-07 11:19 0:00:18	Aktywność Rozmiar 100% 27.0 KB	6 ±
A Serwery	wórz zaznaczony mat	eriał SSH ssh	2015-05-07 11:10	2015-05-07 11:10 0:00:31	100% 43.0 KB	
+ Bastiony	U 🕨 aumin	10004 SSH ssh	2015-05-05 13:06	2015-05-05 13:06 0:00:00	0% 4.0 KB	이 아들 문 소
	🗆 🕨 admin	fudo4 SSH ssh	2015-05-05 13:06	2015-05-05 13:06 0:00:00	0% 4.0 KB	이 아들 말 소
++ Porączenia	□ ► admin	fudo4 SSH ssh	2015-05-05 13:06	2015-05-05 13:06 0:00:00	0% 4.0 KB	

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.

Za	arządzanie <	reudo Za	aznacz żądane se	esje						
æ	Dashboard	Sesie 🔒 Usuń	OCR Czas	🕀 Generuj raport				▼ Dodaj filt	tr v Szu	kaj.
₿	Sesje		\neg							
-	Użytkownicy	 Użytkownik Pro 	itokół Se	arwer Konto	Sejf	Rozpoczęta +	Zakończona	Czas trwania	Aktywność	Re
A	Serwerv	anonymous ICA	A cit	trix ica-anon	citrix-anon	2017-02-16 16:51	2017-02-17 07:52	15:00:42	0%	13
	Przetwórz zaz	naczony materiał	A cit	trix ica-anon	citrix-anon	2017-02-16 16:49	2017-02-16 16:51	0:02:24	42%	79
	Konta	- enonymous ICA	A cit	trix ica-anon	citrix-anon	2017-02-16 16:46	2017-02-16 16:46	0:00:04	0%	83
2	Gniazda nasłuchiwania	anonymous ICA	A cit	trix ica-anon	citrix-anon	2017-02-16 16:45	2017-02-16 16:46	0:00:05	0%	12
	Sejfy	□ ► anonymous ICA	A cit	trix ica-anon	citrix-anon	2017-02-16 16:43	2017-02-16 16:45	0:02:05	48%	44

3. Kliknij Zatwierdź.

Potwierdzenie znakowania czasem	×
Jesteś pewien, że chcesz oznaczyć czasem 1 sesję?	
	Anuluj Zatwierdź

Informacja: Aby wyświetlić znacznik czasu, kliknij ikonę Ø.

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

Za	rządzanie <	Fudo'								å admin 🗸	?
		Casia 🗎	C OCR	Czas	🔒 Generuj raport	☑ Akceptuj	× Odrzuć	▼ Dodaj filtr ~	Szukaj	0	٩v
₿	Sesje	Sesje									
쓭		Użytkowni	k Protokół	Serwer Konto	Sejf Roz	oczęta = Z	Ľakończona	Czas trwania Aktyw	ność Rozmiar		
	Serwery	system	SSH	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 day, 0:00:00 0%	5 bajtów	$\Delta = 0.0$	5 ° 4
		system	Teinet 3270	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 day, 0:00:00 0%	97 bajtów	$\Delta = 0.6$	는 말 두
		? system	SSH	system syste	m system 201	-08-29 04:04 2	2017-08-30 04:04	1 day 0:00:00 0%	69 baitów		✓ ×
2		C × system	Teinet 3270	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 d Akceptuj ża	įdanie dostęj	pu	4.2
		r system	SSH	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 day, 0:00:00 0%	15 bajtów		(v) e
		r system	Teinet 3270	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 day, 0:00:00 0%	118 bajtów		✓ ×
÷-	Modyfikatory haseł	r system	SSH	system syste	m system 201	7-08-29 04:04 2	2017-08-30 04:04	1 day, 0:00:00 0%	35 bajtów		✓ ×

lub zaznacz żądane sesje oczekujące i kliknij Akceptuj.

Za	rządzanie <		۴ı	udo'												🌡 admir	۱v	?	
	Dashboard		So	io B	OCR	Cza	•	Generuj r	aport	🗹 Akcep	otuj	× Odrzuć	₹ Do	laj filtr ~	Szukaj		0	q.~	ŋ
₿	Sesje		30	510	6	_													
쓭	Użytkownicy	0		Użytkownik	Protokół Za	aznacz	sesje	oczeł	cujące	ta v	Zakoń	czona	Czas trwania	Aldywno	ść Rozmiar				
a	Serwery	0	►	system	SSH A	kceptu	j połąc	zenie	2017-08	29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 0%	5 bajtów	≜	6	• II 4	t.
		0	►	system	Teinet 3270	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 %	97 bajtów	4	1.6	• 11 4	<u>t.</u>
- #	Konta	0	?	system	SSH	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 0%	58 bajtów			~:	×
2	Gniazda nasłuchiwania	0	×	system	Teinet 3270	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 %	93 bajty			49	
	Sejfy	C	?	system	SSH	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 0%	15 bajtów			~ :	×
		C	?	system	Teinet 3270	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 0%	118 bajtów			~ ;	×
- 19-	Modyfikatory haseł	0	?	system	SSH	system	system	system	2017-08	-29 04:04	2017-	08-30 04:04	1 day, 0:00:0	0 0%	35 bajtów			~:	×

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 \checkmark .

Tematy pokrewne:

- Filtrowanie sesji
- $\bullet \ Konta$
- Gniazda nasłuchiwania

12.14 Odrzucanie połączeń oczekujących

12.14.1 Interfejs administracyjny Fudo

1. Wybierz z lewego menuZarządzanie > Sesje.

2.	Kliknij	×	przy	wybranym	połączeniu
----	---------	---	------	----------	------------

Za	rządzanie <		FUC	to '													🕹 admi	in ~	1	?
			Secio	8	C OCR	Cza		Generuj r	raport	I Akcept	tuj	× Odrzuć		▼ Dodaj	filtr ~	Szukaj		0	Q	Ļ
B	Sesje	Ε.	Sesje																	-
쓭		9	U	żytkownik	Protokół	Serwer	Konto	Sejf	Rozpoca	ięta 🛩	Zakoń	iczona	Czas	trwania	Aktywno	ść Rozmiar				
		_	► sj	rstem	SSH	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	, 0:00:00	0%	5 bajtów		1.1	5	*
		0	► sj	/stem	Teinet 3270	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	, 0:00:00	0%	97 bajtów	A 1	1.6	5	*
			? S)	rstem	SSH	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	, 0:00:00	0%	58 bajtów			~	×
		0	×s	/stem	Teinet 3270	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	, 0:00:00	0%	93 bajty			۵	•
-		0	? S)	rstem	SSH	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	0:00:00	0%	15 bajtów			-	×
		C	? s	rstem	Teinet 3270	system	system	system	2017-08	3-29 04:04	2017-	-08-30 0)drzuć	pojedy	ncze:	żądanie do	stępu)-	~	*
÷.	Modylikatory naseł	0	? S	/stem	SSH	system	system	system	2017-08	3-29 04:04	2017-	-08-30 04:04	1 day	0:00:00	0%	35 bajtów			~	×

lub zaznacz żądane sesje oczekujące i kliknij $\mathit{Odrzuć}.$

Zarządza	anie <	F	udo'												🕹 admir	۱v	?
Jal Dashi	board	6.	eio 🔋	M OCR	Cza	a - a	Generuj n	aport	☑ Akcept	tuj 🗙 Odrzu	ιć	T Dodaj	filtr ~	Szukaj		0	۹v
🖽 Sesje	,	36	sje	6													
쵛 Użytk	kownicy	0	Użytkownik	Protokół	aznacz	sesje	oczek	kujące	ta *	Zakończona	(Czas trwania	Aktywnoś	ić Rozmiar			
🔒 Serwe	very	0 •	 system 	SSH	Odrzuć	: połąc	zenie	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	5 bajtów	4	0	* ±
C. Kanta	-	••	 system 	Teinet 3270	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	97 bajtów	4	0.5	- L -
👜 Konta	a	0 ?	e system	SSH	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	58 bajtów			✓ ×
ন Gniaz	zda nasłuchiwania	• •	 system 	Teinet 3270	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	93 bajty			49
Seifv	,	0	system	SSH	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	15 bajtów			~×
		0 ?	system	Teinet 3270	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	118 bajtów			✓×
n- Mody	vlikatory hasel	0	system	SSH	system	system	system	2017-08	29 04:04	2017-08-30 04	:04	1 day, 0:00:00	0%	35 bajtów			✓ ×

3. Opcjonalnie, wprowadź powdód odrzucenia żądania dostępu.

Informacja: Powód odrzucenia wyświetlany jest na liście sesji po najechaniu kursorem na ikonę \mathbf{P} .

- 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 \times .

- 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.

Zarządzanie <	FUDD [®] Panel administracyjny	Pokaż opcje zarządzania subskrypcją 🛁 🕯 admin 🗸								
	Baporty Usuń	✓ Zarządzaj subskrypcją								
	Wybierz definicję raportu									
Y Użytkownicy	mój_własny_filtr + Codzienny Tygodniow	Mlesięczny Kwartalny Roczny x								
	(+) Wybi	erz częstotliwość generowania raportu								
🛡 Polityki	Dodaj kolejną subskrypcję raportu pr	zywróć Zapisz								
Zapisz zmiany konfiguracji										

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.

Zarządzanie <	Fudo [*] Panel administracyjny Pokaż opcje zarządzania subskrypcją 🛁 ⁴ admini -	
🐱 Dashboard	Baporty Usuń / Zarządzaj subskrypcją	
E Sesje		
º Użytkownicy	mój_własny_filtr ‡ Codzienny Tygodniowy Miesłęczny Kwartalny Roczny	
💠 Połączenia	🛊 Codzienny Tygod Usuń wybraną subskrypcję 🖓 🖌	
Serwery	+	
🛡 Polityki		
🛓 Do pobrania	C Przywróć V Zapisz	
	Zapisz zmiany konfiguracji	

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.

Zarządzanie <	Fudo	Określ parame	try filtrowania		🛔 admin 🐇 🤶
Dashboard	Sesie	wne 🖹 Usuń 🖾 OC	R T Dodaj filtr ~ 🔒	Generuj raport Szukaj	
E Sesje	enerui raport na r	nodstawie zdefiniov	anych parametrów filtrowa	nia	
o Użytkownicy		a prototolo		© @ ×	
⊖ Serwery		Nazwa filt	8		
• Bastiony					
🕂 Połączenia	 Użytkownik Ser 	rwer Protokół Połącze	ie Rozpoczęta + Zakończona	Czas trwania Aktywność	Rozmiar
10 Polityki	□ ► admin ms	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	3.0 KB 💿 🔊 🖕 면 🕹
*. Do pobrania	admin ms:	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	8.0 KB 🔊 🖕 📥
ilia Do pobrania	□ ▶ admin mst	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	3.0 KB 💿 🛯 🛎
🖨 Raporty	admin ms	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	3.0 KB 💿 🔊 😂 🖱 🕹
E Droduktauność	□ ► admin mst	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	8.0 KB 💿 🔊 😂 🗂 🛓
E. Produktywnoso	□ ► admin ms	ssql MS SQL (TDS) mssql	2015-06-02 05:51 2015-06-02 05:51	0:00:00 0%	3.0 KB 🔊 🕒 Ե 🗆 🛓

4. Kliknij identyfikator raportu, aby wyświetlić jego treść.

Zarządzanie <	Fudo [*]	🛔 admin 🐇 💡 🤶
M Dashboard	Sesje _dAktywne 🖹 Usuń 🖾 OCR 🍸 Dodaj filtr 🗸 🔒 Generuj raport Szukaj	© Q.~
📑 Sesje		
o Użytkownicy	Według protokołu 🛛 Mis sou. (706) O Q. 🗙	
🖴 Serwery	Nazwa filtra	
•# Bastiony		
+ Połączenia	Rapor 8871947604880523308 codany pomyślnie.	×
🛡 Polityki	Kliknij identvfikator raportu, aby wyświetlić jego treść	
🛓 Do pobrania	Użytkownik Sarwar Protokon Połączenia Hozpoczęta zakonczonia Czas awania Aktywność Rozmiar	
	□ ► admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 3.0 KB	
Raporty	□ ► admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 8.0 KB	网络哈拉
Produktywność	□ ► admin mssql MS SQL (TDS) mssql 2015-06-02 05:51 2015-06-02 05:51 0:00:00 0% 3.0 KB	 <!--</th-->

- 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.

Zarządzanie	< Fudo [*]				🕹 admi	n~ ?
🗐 Dashboard	Baporty 🔒 Usuń			▼ Dodaj filtr ~	🖋 Zarządzaj subskryp	pcją
日 Sesje	haporty					
출 Użytkownicy	□ ID +	Utworzony	Tytuł		Stworzony przez	
A Serwerv	□ 6871947604880523300	2015-08-19 01:00:03	Daily (2015-08-18) - System d	efault report	system	B
	Wyświetl listę raportów	2015-08-18 07:22:59	Report generated by admin		admin	₽
•🗄 Bastiony	6871947604880523298	2015-08-18 07:05:31	Report generated by admin		admin	
💠 Połączenia	6871947604880523297	2015-08-18 01:00:02	Daily (2015-08-17) - System d	efault report	system	B
ID Politviki	□ 66 <mark>7194766</mark> Wyświetl	treść raportu 🛏	Weekly (2015-08-16) - System	default report	system	
	6871947604880523295	2015-08-17 01:00:03	Daily (2015-08-16) - System d	efault report	system	B
📥 Do pobrania	6871947604880523294	2015-08-16 01:00:01	Daily (2015-08-15) - System d	efault report	system	₽
Raporty	6871947604880523293	2015-08-15 01:00:01	Daily (2015-08-14) - System d	efault report	system	B

3. Kliknij CSV, PDF, HTML, aby zapisać raport w wybranym formacie.

Zarządzanie	Fudo [•]	Panel administra	cyjny				🚢 admin 🗸
Dashboard	Raport 687194	47604880523543				Ca	SV PDF HTML
🖽 Sesje					Zapis	z raport w wybranyr	m formacie
볼 Użytkownicy	Kryteria ra	aportu					
🕂 Połączenia	 Według pro 	otokołu = HTTP, SSI	Ŧ				
⊖ Serwery	Serwery						
🛡 Polityki	Serwer Licz	zba sesji 🛛 Liczba u	żytkowników	Sumaryczny czas trwania sesji	Sumaryczny rozmiar sesji	Średni czas trwania sesji	Średni rozmiar sesji
* De pobrania	centos-eb	2	1	0:45:44	184.0 KB	0:22:52	92.0 KB
2 Do pobrania	localhost	1	1	0:06:47	78.0 KB	0:06:47	78.0 KB
A Raporty	Użytkownie	icy					

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.

Zarządzanie	<	Fudo' Wyg	eneruj zestawien	ie prezentowa	nych danych v	v formacie ht	ml –	≜.admin ~
Jashboard		Zestawienie 4	analiza sesii Poré	wnanie	(Dodaj filtr ~	Gene	aruj raport
🖽 Sesje								
볼 Użytkownicy		Dodaj filtr, a	aby ograniczyc ii	czbę wyswietia	anych pozycji			
+ Połączenia	Kliknii oby o	ocortować na ve	desamum kentariuu					
⊖ Serwery	клікпіј, ару р	Zestawienie	ybranym krytenur					
Polityki		Organizacje/Użytkownik	Sumaryczny czas sesji *	Czas aktywności	Czas nieaktywności	Produktywność	Sesje	Serwery
📩 Do pobrania		Wszyscy	5:59	0:16	5:43	4%	10	3
⊖ Raporty		Wsparck	Wyświetl użytk	owników należ	ących do orga	nizacji	5	1
E Produktavność		Adminstratorz	5:29	0:14	5:15	4%	5	2
E Froduktywnoso		admin	5.00 Ulkovi užutkov	uników naloża	eve ovob do organ	izacii	5	2
Ustawienia		badmin		wnikow nalezą	cych do organ		5	2
¢ ^e Konfiguracja sieci		cadmin	5:29	0:14	5:15	4%	5	2
Ø Data i czas								

Zarządzanie <	Fudo						🛔 admin 🗸
Jashboard	Zostawionio	Apolizo sosii Porów	mania		Dodaj filtr ~	Gene	eruj raport
🖽 Sesje	Zestawienie	Analiza sesji Porow	name				
曫 Użytkownicy		Data od 2014-09-28	do 201	14-10-05			
	Zestawienie	e					
	Organizacja/Użytkownik	Sumaryczny czas sesji =	Czas aktywności	Czas niesktywności	Produktywność	Sesje	Serwery
	Wszyscy	5:59	0:16	5:43	4%	10	3
	Wsparcie -	Pokaż tylko użytkow	ników należ	ących do wyb	ranej organiz	acji	1
🚍 Produktawacéć	Adminstratorzy ~	5:29	0:14	5:15	4%	5	2
E. Produktywnoso	admin	5:29	0:14	5:15	4%	5	2
Ustawienia	badmin	Kliknii abv wyświetli	ć liste sesii (da wybranei n	ozvcii	5	2
	cadmin	5:29	0:14	5:15	4%	5	2
O Data i czas		Przedstaw analizę se	sji dla wybra	nego użytkow	/nika		

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.

Bréz ditaunalai d 20	Kliknij, aby wyświetlić na wykres	ie dane tylko dla w	ybranej organizac	ji
Prog aktywnosci 🗙 20	Kliknij, aby wyświetlić na wykres	ie sesje wybranego	użytkownika w d	anym dniu
Poniżej progu: 🎍 11 🖉 1 🖽 14	0 Powyzej progu: 🛎 13 🖀 2 🖽 156			
É C I S N I	• W Ś C P S N P W Ś C P S N P	Paź. 24, 2014	V É C P S	
(dewelopment)		0	12:49	31:10 41%
user-33		Czas sesji: 1:29 Czas aktywności: 0:22	12:49	31:10 41%
serwis		Czas nieaktywności: 1:07	21:54	160:53 14%
user-25		llość sesji: 1	21:01	157:02 13%
user-26		Produktywnosc: 25 %	0:53	3:51 23%
Nieprzydzielony			<mark>54:0</mark> 4	242:55 22%
user-60		Y III	0:03	0:03 100%
Najedź kursorem na wybra	any element, aby wyświetlić szczeg	jóły		

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 nie-prawidłowości 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.

Zarządzanie	Fudo"	🛔 admin 🐇 ?
Jashboard	Ogálao Aktualizacia Licencia Disgoostyka	
日 Sesje		
😤 Użytkownicy	Data i czas Wybierz strefę czasową	
⊖ Serwery	Strefa czasowa Warsaw 🗘 🕸	
•# Bastiony	Data i czas 2016-02-07 23:45	
+ Polączenia	Ustaw datę i godzinę	
🛡 Polityki	Serwery NTP	
📥 Do pobrania		
🖨 Raporty		
Produktywność	+	

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.

$Dodawanie\ servera\ NTP$

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.

Zarządzanie <	Fudo'	🛔 admin 🐇 🤰 🤶
I Dashboard	Ogólga Aktualizacia Licencia Diagnostyka	
🖽 Sesje		
嶜 Użytkownicy	Data i czas	
🖴 Serwery	Strefa czasowa Warsaw 🗘 🕸	
•# Bastiony	Data i czas 2016-02-07 23:45	
🕂 Połączenia	Dodai serwer NTP	
Polityki	Serwery NTP Worowadź pazwe bosta lub adres IP	
📥 Do pobrania	vipiowadz nazwę nosta lub adles IP	
B Raporty	×	
Produktywność		

- 4. Kliknij Zapisz.
- 5. Wybierz z menu użyktownika opcję Uruchom ponownie.

			Wyświetl opcje użytko	ownika —
Zarządzanie	< Fudo	Panel administracyjny		
Dashboard	Dashboard			PL EN
当 Sesje	Sesje		Aktywne połączenia	C' Uruchom po
🕂 Połączenia	22:00 00:00	02:00 04:00 06:00 08:00	2014-03-17 09:15:12 SS	e system
🖴 Serwery				G♦Wyloguj
Polityki	Sesie			
📥 Do poorania	- 003j6			

$Modyfikowanie\ servera\ NTP$

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.

Zarządzanie <	Fudo	🛔 admin 🐇 💡
Dashboard	Ogólog Aktualizacia Licencia Diagostyka	
🖽 Sesje	Ogoine Aktualizacja Licencja Diagnostyka	
😁 Użytkownicy	Data i czas	
⊖ Serwery	Strefa czasowa 🗍 🕸	
•∉ Bastiony	Data i czas 2016-02-08 15:08	
🕂 Połączenia		
🛡 Polityki	Serwery NTP	
🏝 Do pobrania	al pool ato ara	
A Raporty		
E Produktywność	lienic adres IP/nazwę hosta serwera NTP	

- 3. Kliknij Zapisz.
- 4. Wybierz z menu użyktownika opcję Uruchom ponownie.

							Wyświetl opcje	užyti	kownika	
Zarządzanie	<	Fudo	Panel ad	ministrac	yjny				(۵
Dashboard		abbaard							PL	
ਊ Sesje	D,	Ishboard							EN	_
🔮 Użytkownicy	Ses	je					Aktywne połączenia		C Uruchon	1 po
+ Połaczenia	22:00	00:00	02:00	04:00	06:00	08:00	 🔤 Uruchom po	nown	iie syster	n
							2014-03-17 09:15:12	SS	F#Wvloqui	
									,	
V Polityki										
📥 Do pobrania	• Se	sje								

$Usuwanie\ serwera\ NTP$

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.

Management <	Fudo'		📥 admin 🕤 🤶
J Dashboard	General Ungrade Licens		
E Sessions	deneral opgrade Licens	e plagitorica	
🖶 Users	Date and time		
🖴 Servers	Timezone Warsaw	\$ als	
•@ Bastions	Date & time 2016-02-	08 15:07	
++ Connections			
U Policies	NTP servers		
📥 Downloads			
🖨 Reports	photon		
E Productivity	+	Usun serwer NTP	

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.

Zarządzanie	< Fudo [*]	🛔 admin 🕤 📍
I Dashboard	Océlne Aktualizacia Licencia Diagnostyka	
🗈 Sesje	Ogoline Aktualizacja Licencja Diagnostyka	
📽 Użytkownicy	Data i czas	
⊖ Serwery	Strefa czasowa Warsaw 🗘 🕸	
•∉ Bastiony	Data i czas 2016-02-08 15:08	
🕂 Połączenia		
🛡 Polityki	Serwery NTP	
📥 Do pobrania	al seal sta ara	
🖨 Raporty	pr.pool.np.org	
Produktywność	+	
Ustawienia	Certyfikat HTTPS	
🗁 System	Wgraj plik certyfikatu w formacie PEM	
¢ ^e Konfiguracja sieci	Certyfikat HTTPS Wybierz plk Nie wybrano pliku	
Powiadomienia	Klucz prywatny HTTPS wybierz pik Nie wybrano pliku	
Znakowanie czasem	Wgraj klucz prywatny	
a, Zewnętrzne uwierzytelnianie	Dostęp SSH	
III Zewnętrzne repozytoria haseł	Włączone 🛛	
🖾 Zasoby		
Kopie zapasowe i retencja	Funkcjonalności wrażliwe	
🚓 Klaster	Aktywacja tunkcjonalnosci wymaga zgody dwoch uzytkowników superadmin.	
🛱 Synchronizacja LDAP	wprowadzone na klawiaturze	
≡ Dziennik zdarzeń		
© 16 dni i 99999999 % oracle10-25511.d, Master		
	C Przywróć 🗸 Zapisz	

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.

Zarządzanie <	Fudo	🛔 admin 🕤 📍
M Dashboard	Océlne Aktualizacia Licencia Disenestyka	
🖽 Sesje	Ogonie Aktualizacja Licencja Diagnostyka	
📽 Użytkownicy	Data i czas	
⊖ Serwery	Strefa czasowa 🗘 🕸	
-# Bastiony	Data i czas 2016-02-08 15:08	
+ Połączenia		
🛡 Polityki	Serwery NTP	
📥 Do pobrania		
🖨 Raporty	pi-pooring-org	
🖹 Produktywność	+	
Ustawienia	Certyfikat HTTPS	
🗁 System		
	Certyfikat HTTPS	
Powiadomienia	Klucz prywatny HTTPS Wybierz plik Nie wybrano pliku	
Znakowanie czasem		
& Zewnętrzne uwierzytelnianie	Dostęp SSH	
III Zewnętrzne repozytoria haseł	Włączone	
🖬 Zasoby	Włącz możliwość nawiązywania połączeń serwisowych SS	
Kopie zapasowe i retencja	Funkcjonalności wrażliwe	
♣ Klaster	Aktywacja tunkcjonalnosci wymaga zgody dwoch uzytkownikow superadmin.	
≓ Synchronizacja LDAP	wprowadzone na klawiaturze	
≡ Dziennik zdarzeń		
© 16 dn £ 9999999 ♥ onacle10-25511 ∰ Milater		
	C Przywróć V Zapisz	

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.

Zarządzanie	< Fudo [®] & admir	n~ ?
Dashboard	Ogólne Aktualizacia Licencia Diagnostyka	
日 Sesje		
嶜 Użytkownicy	Data i czas	
⊖ Serwery	Strefa czasowa 🗘 🕸	
•# Bastiony	Data i czas 2016-02-08 15:08	
🕂 Połączenia		
🛡 Polityki	Serwery NTP	
📥 Do pobrania		
🖨 Raporty	pi.pool.nip.org	
Produktywność	+	
Ustawienia	Certyfikat HTTPS	
🗁 System		
¢6 Konfiguracja sieci	Certyfikat HTTPS wybierz plik Nie wybrano pliku	
Powiadomienia	Klucz prywatny HTTPS Wybierz plik Nie wybrano pliku	
Znakowanie czasem		
a, Zewnętrzne uwierzytelnianie	Dostęp SSH	
III Zewnętrzne repozytoria haseł	Włączone 🛛	
🖾 Zasoby		
Kopie zapasowe i retencja	Funkcjonalności wrażliwe	
🚓 Klaster	Aktywacja tunkcjonalnosci wymaga zgody dwoch uzytkownikow superadmin.	
≓ Synchronizacja LDAP	wprowadzone na klawiaturze	
≡ Dziennik zdarzeń	Zaznacz, aby w odtwarzaczu wyświetlane były dan <u>e weiściowe klawiatury</u>	
© 16 dnl & 93999999 ♥ cracle10-25511,∰ Master		
	C Przywróć 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.

Zarządzanie	Fudo					📥 admir	· ?
Jashboard	0-11	Alderstein		Discontrolog	× Usuń migawke aktualizacji	i Usuń	• Wgraj
目 Sesje	Ogoine	Aktualizacja	Licencja	Diagnostyka			
👻 Użytkownicy	🗆 Wersja	Nazwa pliku	Rozmiar	Status próbnej aktualizacji			
Serwery	3.4-34668	fudo-3.4-34668.upg	109.3 MB	Próbna aktualizacja nie zost	ała przeprowadzona. SPróbne ał	tuelizacje 🖬 Akt	ualizacja
🔊 Konta				Aktualizuj sys	stem do wybranej wersji)	

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 $\mathit{Ustawienia} > \mathit{System}.$
- 2. Wybierz zakładkę Aktualizacja.

- 3. Kliknij Wgraj.
- 4. Wskaż plik zawierający aktualizację systemu (.upg).
- 5. Kliknij przycisk Próbna aktualizacja.

Za	rządzanie <	Fudo'					📥 admir	·~ ?
		Osílas	Aktualizaala	Lissasia	Diagaashda	× Usuń migawkę aktualizacji	🗑 Usuń	() Wgraj
₿		Ugoine	Aktualizacja	Licencja	Diagnostyka			
*		🗆 Wersja	Nazwa pliku	Rozmiar	Status próbnej aktualizacji			
8		3.4-34668	fudo-3.4-34668.upg	109.3 MB	Próbna aktualizacja nie zosta	ała przeprowadzona.	tuelizacja 🖸 Akt	ualizacja
₽	Konta				Wykonaj prób	ną aktualizację		

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.

Za	rządzanie <	Fudo'						📥 admin	· ?
		Osílas	Aktualizzatia	Linensia	Diagnostuka	× Usuń migawkę	aktualizacji	🗟 Usuń	① Wgraj
		Ugoine	Aktualizacja	Licencja	Diagnostyka suń poprzednia w	versie systemu -			
쓭		🗆 Wersja	Nazwa pliku	Rozmia	san popizoaniq n	iolojų oyotolila			
		3.4-34668	fudo-3.4-34668.upg	109.3 MB	Próbna aktualizacja nie z	została przeprowadzona.	Próbna akt.	valizacja 🔽 🖓 Aktu	alizacja
	Konta								

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*.

Zarządzanie <	Fudo					🛔 admin 🕤 📍
Dashboard	Ogélpo Aktualizacia Li	Diagnostyka				@ Wgraj
🗐 Sesje	Ogoine Aktualizacja Li	Diagnostyka			Marai alik lioon	
📽 Użytkownicy	Numer seryjny	12345678			vvgraj plik licen	
⊖ Serwery	Data wygaśnięcia	2016-03-31				
•# Bastiony	Właściciel licencji	Wheel Systems sp. zoo				
+ Polączenia	Typ licencji	test				
🛡 Polityki	Tryb rozliczania	host.port				
📥 Do pobrania						
🔒 Raporty	Limit liczby węzłow w klastrze					
Produktywność	Liczba serwerów	25	11 w użyciu	14 dostępne)	
Ustawienia	Statystyki użycia		Parametry lic	encji		
🗁 System	Data ad	2016 11-01	da	2016-02-08		
Ø ^e Konfiguracja sieci	Statuatuka réwnoozoon		uo	2010-02-00		
Powiadomienia	Statystyka rownoczesny	ych połączen				
C Znakowanie czasem	4.5					
& Zewnętrzne uwierzytelnianie	3.5 -					
III Zewnętrzne repozytoria haseł	3.0 - 2.5 -					
🖾 Zasoby	2.0 - 1.5 -					
Kopie zapasowe i retencja	1.0-					
🚓 Klaster	0.0	Sr 23	Gz 17	P1 08	Pn11	
= Supebropizacia I DAR	Liczba sesji równoległych					

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.

Zarządzanie <	Fudo	🕹 admin 🗸 🤶 🤶
🖩 Dashboard	Ozálao Aktualizacia Licancia Disanactuka	Pobierz dane serwisowe
🖽 Sesje	Ogoine Aktualizatja Litelitoja Diagriostyka	
😵 Użytkownicy	ping Wprowadź adres hosta Wgraj plik	licencji
⊖ Serwery	Adres	
• Bastiony	Opcje 💿 Wyświetlaj adresy w formie 💿 Zapisz trasę	
💠 Połączenia	numerycznej	
Polityki	netcat Wybierz opcje wykonania polecenia	
📥 Do pobrania	Adres Port 📌	
🖨 Raporty	had a second sec	
Produktywność	nost	
Ustawienia	Adres 🛃	
system 😂	traceroute	
¢e Konfiguracja sleci		
Powiadomienia	Adres A	
Znakowanie czasem	Opcje Nie rozwiązuj nazw skoków Uzyj protokolu ICMP zamiast UDP	
at Zewnętrzne uwierzytelnianie	Tryb omijania firewali-a Ustaw flagę "Nie fragmentuj"	
III Zewnętrzne repozytoria haseł		

Komenda/ parametr	Opis
Ping	Ping wysyła sekwencję 10 pakietów icmp do wskazanego hosta.
Wyświetlaj adresy w for-	Nie rozwiązuje adresu IP hosta do nazwy mnemonicznej.
mie numerycznej	
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 pomię-
	dzy Wheel Fudo PAM i hostem docelowym.
Nie rozwiązuj nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do
	nazw mnemonicznych.
Uzyj protokołu ICMP za-	Wymusza użycie pakietów UDP zamiast ICMP.
miast UDP	
Tryb omijania firewall-a	Wymusza użycia niezmiennyh numerów portu dla pakietów
	UDP i TCP. Port docelowy nie jest inkrementowany z każdym
	wysłanym pakietem.
Ustaw flagę "Nie fragmen-	Nie pozwala na fragmentację pakietów, w przypadku gdy prze-
tuj"	syłany 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 $\mathit{Ustawienia} > \mathit{Konfiguracja sieci}.$

Zarządzanie <	Fudr	🛓 admin 🗸 🛛 💡
	Kontiguracja tras routingu	
嶜 Użytkownicy	Koniiguracja serwerow nazw	
	% net0 08:00:27:6A:A3:A9	Aktywne OHCP
Sejfy	10.0.40.50 / 16 🗲 🔮 🗙	
	10.0.40.51 / 16 🗲 🔾 🗙	
	•	
	% net1 1000002-00-12-05	Q Aktywne Q DHCP
	VIIVII 00000.81.000 IA00	
	+	
Ustawienia		
😂 System	% net2 08:00:27:57:B2:BA	Aktywne OHCP
¢° Konfiguracja sieci		
	+	
	% bridge0 02:00:BC:61:4E00	© Aktywne OHCP
	172.128.0.10 / 24 F Q X	
Kopie zapasowe i retencja	+	
≓ Synchronizacja LDAP	Propagacja drzewa Dodoji Konstiguracjo VI AN	
	Członkowie neti netż Dodaj Konligurację VLAN	
	😂 Przywróć 🛛 🛩 Zapisz	X Most P VLAN

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 nie
aktywny, 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.

£

Zarządzanie <	Fudo	👗 admin 🗠 💡
	Interfeisy Nazwa i DNS Tablica trasowa	Udostępnij panel administracyjny pod wskazanym adresa
		Udostępnij Portal użytkownika pod wskazanym adresem
嶜 Użytkownicy	% net0 00:0C:29:AF:54:E8	9 Aktywne ODHCP
		Usuń alias interfejsu sieciowego
	(10.0.235.153 / 16 🕑 🔿 🛦 💌	Pobieraj adres IP z serwera DHCP
Sei Wpisz adres oraz masi	kę podsieci — / 16 🖌 🔍 🌰 👦	¢ ×
	\bigcirc	Przynisz adres do grupy redundancij
		Wirtualny adres IP, który zostanie przejety przez
	x net1 00:00:23:4F:54:F2	inny węzeł klastra w przypadku awarii węzła
	Interfejs nie jest aktywny.	
Ustawienia	0.0.0.0 / 16 🕨 🗭 📥 🗙	
	+	
¢° Konfiguracja sieci		
	C Przywro	2C Most V VLAN

Informacja: Każdy interfejs sieciowy opatrzony jest ikoną statusu.

S	Interfejs aktywny i podłączony.
<u></u> 5	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.
| Zarządzanie < | Fudo [*] & admin ~ ? |
|-------------------------|---|
| I Dashboard | Interfeisy Nazwa i DNS Tablica tracowania |
| 🖽 Sesje | |
| 쓸 Użytkownicy | Shet0 to occ28:AF:54:E8 |
| ⊖ Serwery | Usuń alias interfejsu sieciowego |
| 🖉 Konta | 10.0.235.153 / 16 🗡 🛛 🚓 💌 |
| Sejfy | 10.0.235.154 / 16 🗲 🥺 🚓 rg1 💠 🗙 |
| か Gniazda nasłuchiwania | + |
| n- Modyfikatory haseł | |
| 🛡 Polityki | X net1 00:0C:29:AF:54:F2 Q Aktywne ♀ DHCP |
| 📥 Do pobrania | |
| 🕀 Raporty | Interfejs nie jest aktywny. |
| 🖹 Produktywność | |
| Ustawienia | 0.0.0.0 / 16 🗡 😔 🎰 🗙 |
| 🖨 System | + Zapisz zmiany w konfiguracji |
| ¢° Konfiguracja sieci | |
| Powiadomienia | C Przywróć Zapisz Z Mest PYLAN |

$Wyłączanie\ interfejsu\ sieciowego$

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.

Zarządzanie <	Fudo" **	admin 🕤 📍
Ja Dashboard	Interfaisy Nazwa i DNS Tablica trasowania	
🖽 Sesje		
🚰 Użytkownicy	% net0 mod 29:AE54.E8	DHCP
⊖ Serwery		
🔊 Konta	10.0.235.153 / 16 / 9 & X	
Sejfy	10.0.235.154 / 16 🗲 🤐 🚓 rg1 💠 🗙	
A Gniazda nasłuchiwania	+	
n- Modyfikatory hasel		
🛡 Polityki	X net1 00:0C:29:AF:54:F2 Q Aktywne Q	DHCP
📥 Do pobrania		
🕀 Raporty	Interfejs nie jest aktywny.	
Produktywność		
Ustawienia	0.0.0.0 / 16 🖋 🐼 🏧 🗙	
🖨 System	+ Zapisz zmiany konfiguracji	
¢° Konfiguracja sieci		
🖂 Powiadomienia	C Przywróć Zapisz	LAN

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.

```
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:
```

2. Wprowadź hasło do konta administratora.



3. Wpisz 2 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):
```

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 FUDD to factory defaults, login as "reset".

To fix admin account and change network settings,

login as "admin" with an appropriate password.

FUDD (fudo.wheelsystems.com) (ttyv0)

login: admin

Password:

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

*** FUDD configuration utility ***

Logged into FUDD, 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 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.

4 Zewnętrzne uwierzytelnianie	% bridge0 02:00:BC:61:4E:00			X Aktywne Q DHCP
			Lloué dofinicio mostu	
	172.128.0.10 / 24	7 9 X	Aktywui konfiguracie	
Kopie zapasowe i retencja	+ Wprowadź	adres IP i maske podsieci	v ukrywaj koningarację	
	Propagacja drzewa rozpinającego	Zaznacz aby zapobi	egać powstawaniu pętli	
	Członkowie	neti net2	0 Q	
2 dni i 12345678 \$-30775	* vlan0 + vLAN	Przypisz do mostu i net0	interfejs fizyczny albo siec	É VLAN x @ Aktywne @ DHCP
		C Przywróć 🗸 Zapisz		X Most V VLAN

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 *konfi*guracji serwerów.

- 5. Kliknij Aktywne, aby aktywować VLAN.
- 6. Kliknij Zapisz.

¢° Konfiguracja sieci		Aktywuj konfigurację VLAN	
🖂 Powiadomiania	≭ vlan0	× CAldywno Q DHCP	
Wprowadź adres IP i m	askę podsieci	Przypisz adres IP do grupy redundancji	
4 Zewnętrzne uwierzytelnianie	· · ·		
III Zewnętrzne repozytoria haseł	\bigcirc	Podaj identyfikator sieci VLAN	
🛯 Dodaj alias IP sieci VLAN	VLAN		
Kopie zapasowe i retencja	Interfejs nadrzędny	net0	
🚓 Klaster	Wybierz interfejs	nadrzędny sieci VLAN	
≓ Synchronizacja LDAP			
≡ Dziennik zdarzeń		C Przywróć Zapisz Z Most P VLAN	

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.

Host docelowy

Adres IP Adres źródłowy	Dowolny 10.0.150.150 Etykietowane adresy IP	1
Klucz publiczny serwera	label_1 [10.0.150.153] label_2 [10.0.0.6] label_3 [10.0.150.151] label_4 [10.0.150.152] MISK9GIW+oGMJtrwiEe9zbl4LQndQum2[MaeuTCFD+sF/rBmo+ K2QVHin2zm/253IK07[9W2] E50[JOPErMV/or/XEI99]x101] kQl	+hB0z
	GbZjn/NLaDD9PKKnmTia528itBr+aG8gRzwMW6JT8EhV0hJOiQ LMgCIUKXn1XH9iHrZZFhsN61FWiufZGFgn7oN+utuaDDCmVitLg HLGXzzPtrxkiscD9itV+aFfn322oXDBrcZ2ubhV4W38IN6zAHFjHR ND87/kEYQpVZZrL3ZED04mih03qGaDJHKRCVP	qW1XD jauQEt 1FQ9ZH
	a0:5f:e4:a3:31:b0:9f:f4:e8:72:d9:d5:ee:4d:5a:c7:d9:54:29:57	SHA1

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.

	el admin	istracyjny		📥 admin 🗸	
Interfeis Nazw	a i DNS	Tablica trasowania			
interrejo inazir				Domyślna tras	a routowania pakietów
Trasa	Sieć	default	Brama	10.0.0.1	×
Trasa	Sieć	192.168.0.16/29	Brama	10.0.0.2	×
	Interfejs Nazw Trasa	Interfejs Nazwa i DNS Trasa Sieć Trasa Sieć	Trasa Sieć default Trasa Sieć 192.168.0.16/29	Trasa Sieć default Brama Trasa Sieć 192.168.0.16/29 Brama	Trasa Sieć 192.168.0.16/29 Brama 10.0.0.2

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.

Zarządzanie <	Fudo [®] Panel administracyjny					📤 admin 🗸
I Dashboard	Interfeis Nazy	va i DNS	Tablica trasowania			
🖽 Sesje	interrejo Hazv		Tablica dasowania			
🔮 Użytkownicy	Trasa	Sieć d	default	Brama	10.0.0.1	×
💠 Połączenia	Trasa	Sieć 1	92.168.0.16/29	Brama	10.0.0.2	×
⊖ Serwery			Zaznacz, aby usuna	ąć wska	ızaną definicję trasy	
🛙 Polityki						
🛓 Do pobrania						
🖨 Raporty						
Ustawienia						
🕫 Konfiguracja sieci						
O Data i czas						
🖂 Powiadomienia						
Znakowanie czasem						
a Zewnętrzne uwierzytelnianie		7anisz z	miany konfiguracii			
Certyfikat HTTPS				_		
🏝 Aktualizacja			2 Przywróć	✓ Zapisz		+ Dodaj trasę

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.

Zarządzanie	< Fudo*			admin 🕤 ?
Jashboard	Interfeie	Namus i DNC		
🗄 Sesje	Interrejs	Nazwa I DNS	Nadaj nazwę hosta	
嶜 Użytkownicy		Nazwa hosta	fudo.wheelsystems.com	
⊖ Serwery		DNS	10.0.0.1	
Bastiony		DNS	×	
🕂 Połączenia			Wprowadź adres IP serwera DNS	
Polityki				
📥 Do pobrania				
🔒 Raporty				
Produktywność				
Ustawienia				
😂 System				
🕫 Konfiguracja sieci				
🖂 Powiadomienia				
Znakowanie czasem				
a, Zewnętrzne uwierzytelnianie			Dodaj serwer DNS	
III Zewnętrzne repozytoria haseł			C Przywróć V Zapisz + Dodaj serwer	DNS

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.

Za	rządzanie <	≓udo'							📥 admin 🗸	?
Jıl						-				
₿		Interfejsy	Nazwa i DNS	lablica trasowania	Etykiety IP	Proxy				
*		Eudo Mobil	۵							
æ			0							
ø			Certyfikat	BEGIN CERTIFICAT MILEYDCCA0gCCQDVK	E J3dc/jMfDANBgkqhl	kiG9w0BAQUFAD	CB8TELM	*		
۳				AkGA1UEBhMC UEwxDzANBgNVBBEM	BjAyLTQ4NjEUMBIG	A1UECAwLbWF6	b3dpZWN			
				raWUxETAPBgNV BAcMCFdhcnN6YXdhV	R4wHAYDVQQJDBV	/BbC4gSmVyb3pv	/bGltc2tp			
÷.				ZSAxNzgxITAf BgNVBAoMGFdoZWVs	FN5c3RlbXMgU3Aul	Hogby5vLjEWMB	QGA1UE			
U				CwwNV2hlZWwg U3VwcG9ydDEkMCIGA	1UEAwwbV2hIZWwg	VGVtcG9yYXJ5IE	NIcnRpZ			
¥				63:79:58:45:ae:6c:08:a4	:4d:e4:18:71:63:94:0	1:62:ac:6c:e7:c4	SHA1			
₽			Adres hosta	10.0.8.200	Port 44300					
≡				•						
Us	tawienia		Add host	Ŧ						
-		Proxy serve	ers							
¢ °	Konfiguracja sieci		Adres hosta	10.0.8.200	Port 44300					
		Klucz	publiczny serwera	ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYT	ItbmlzdHAyNTYAAA	AlbmizdHAyNTYA	AABBBFz	10		
đ				xvWzA73pl2a3mki5oo0	EK6setbhJo=	/PUBIDIRK9ECTJ40	omzsseg			
0,										
-										
				b6:97:c8:d6:c7:e9:29:10	:73:a1:4d:c5:a5:ad:4	4:82:a8:36:cb:76	SHA1			
47			Usuń							
*			Dodaj proxy	+						
₽							_			
≡					2 Przywró	ć 🗸 Zapisz				

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 ⁽²⁾, 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.

Zarządzanie	<							📥 admin 🗸	?
Dashboard		Dodaj w		Tabli	oo tracowania	Tablica ADD	Etykisty ID		_
🗄 Sesje		► Podaj ad	Ires IP i adres MA		ca trasowania	Tablica ARP	Etykiety IP		
쑿 Użytkownicy		Adres IP	10.0.02	MAG	R2:D2:C3:P0:YO:	0 *			
Serwery									
😹 Konta		Adres IP		MAC		×			
እ Gniazda nasłuchiwania									
Sejfy									
+ Modyfikatory haseł									
Polityki									
📥 Do pobrania									
🕀 Raporty									
Produktywność									
Ustawienia									
😂 System									
¢6° Konfiguracja sieci								_	
External storage					2 Przywróć 🗸 🗸	apisz		+D	odaj

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.

Zarządzanie	C	🛓 admin 🐇 🛛 🤶
Dashboard	Interfeirer Manuel DMC Tablics treasuration Tablics ADD Stabiate ID	
🗄 Sesje	Interrejsy Nazwa i DNS Tablica trasowania Tablica AHP Etykiety IP	
쓸 Użytkownicy	Adves IP 10.0.0.2 MAC R2-D2-C3-P0-Y0-I 0	
Serwery		
😹 Konta		
ふ Gniazda nasłuchiwania		
Sejfy	Usuń wybrany wpis ARP	
n- Modyfikatory haseł	Zapisz zmiany	
Polityki		
📥 Do pobrania		
🖶 Raporty		
Produktywność		
Ustawienia		
🖕 System		
¢6 Konfiguracja sleci		
External storage	C Przywróć Zapisz	+ Dodaj

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.

Zarządzanie <	Fudo		🕹 admin 🗸 🤗
Jashboard	Listawionia Nied		
🖽 Sesje	Wła	ącz usługę powiadomień email	
쑬 Użytkownicy	Włączone		
⊖ Serwery	Główny serwer SMTP	Określ parametry głównego serwera S	SMTP
- Bastiony	Adres	smtp.wheelsystems.com	
🕂 Połączenia	Port	25	
Polityki	Adres źródłowy	Dowolny +	
📥 Do pobrania	A drag and average		
🖨 Raporty	Adres nadawcy	1000-0wt-40.30wwneelsystems.com	
Produktywność	Wymaga uwierzytelnienia		
Ustawienia	Użytkownik	notify	
😂 System	Haslo		
¢¢ Konfiguracja sieci	Powtórz hasło		
Powiadomienia	Użyj bezpiecznych połączeń		
Znakowanie czasem	(TLS)	Test polączenia z serwereni	
e Zewnętrzne uwierzytelnianie		Lestul poleczenie	

Parametr	Opis	
Adres	Adres IP serwera SMTP.	
Port	Numer portu, na którym działa usługa	
	SMTP.	
Adres nadawcy	Adres email, z którego wysyłane będą powia-	
	domienia.	
Wymaga uwierzytelnienia	Czy serwer SMTP wymaga uwierzytelniania.	
Użytkownik	Nazwa użytkownika dla uwierzytelnienia	
	usługi SMTP.	
Hasło	Hasło użytkownika dla uwierzytelnienia	
	usługi SMTP.	
Użyj bezpiecznych połą-	Zaznacz, jeśli serwer pocztowy wykorzystuje	
czeń (TLS)	protokół szyfrujący TLS.	

Informacja: Kliknij *Testuj połączenie*, aby zweryfikować prawidłowość parametrów konfiguracyjnych.

4. Opcjonalnie, uzupełnij parametry konfiguracyjne dla zapasowego serwera SMTP.

III Zewnętrzne repozytoria haseł	Zapasowy serwer SM1	P Określ parametry zapasowego serwera SMTP
Zasoby	Adres	
Kopie zapasowe i retencja	Port	25
ሔ Klaster	Adres źródłowy	Downiny 1
≓ Synchronizacja LDAP	Planet Literativity	
≡ Dziennik zdarzeń	Adres nadawcy	noreply@fudo.wheelsystems.com
	Wymaga uwierzytelnienia	0
0 25 dni i 12345678 % 2.2-26195,5 Nie skonfigurowany	Użytkownik	
	Haslo	
	Powtórz hasło	
	Użyj bezpiecznych połączeń (TLS)	Wykonaj test połączenia z serwerem
		Testuj połęczenie

5. Wprowadź treść certyfikatu urzędu certyfikacji, w formacie PEM.

Certyfikat centrum	Wklej lub wgraj certyfikat centrum
Certyfikat centrum	MIIH3jCCBcagAwiBAgLIAPQhiAq26DJTMA0GCSqGSib3 DQEBBQUAAMIH5MQswCQYD VQQGEwJQTDEPMA0GA1UEERMGMDItNDk1MRQwEgY DVQQIEwtYXpvd2iIY2tpZTER MA8GA1UEBXMIV2Fyc3phd2ExFJAUBgNVBAkTDXVsLk9j aG9ja2EgMUYxITABgNV BAATGFdoZVVsIFN5G3RIbXMgU3AuIHogby5vLjEdMBsG A1UECxMURHppYWwgQmV6 cGIY3plbnN0d2ExLDAqBgNVBAMTT1doZVVsIFN5c3Rlb
	de:c8:09:9f:a8:24:53:35:d7:6f:e2:25:8a:1a:65:ad:3a:2a:55:c1 SHA1
	Wykonaj test połączenia z serwerem
	S Przywróć 🗸 Zapisz

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)

Zarządzanie	<	Fudo [*]	🕹 admin 🗸 🤶
Dashboard		Znakowanie czasem	
🖽 Sesje		Włącz usługę znakowania czasem	
Użytkownicy		Włączone	
⊖ Serwery		Dostawca Krajowa Izba Rozliczeniowa 🗘	
•# Bastiony		Plik z certyfikatem i wybierz plik. Nie wybrano pliku kluczem prywatnym w	
🕂 Połączenia		formacie PKCS12	
Polityki		Hasio	
📥 Do pobrania		Powtórz hasło	
🖨 Raporty		Zdefiniuj wartości parametrów konfiguracyjnych	

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.

Zarządzanie	< Fudo'	👗 admin < 📍
Jashboard	Zoumotrano uniorrato	Iniania
🖽 Sesje	Zewnętrzne uwierzyte	unane
볼 Użytkownicy	Тур	Typ systemu uwierzytelniania
Serwery	Adres	Adres IP i numer portu serwera uwierzytelniania
+# Połączenia	Whendai indania z	Adres IP FUDO do komunikacji z sewerem
🛡 Polityki	wysyłaj ządania z	uwierzytelnienia
🛓 Do pobrania	Usuń 🗆	
🔒 Raporty		Usuń definicję systemu uwierzytelniania
Produktywność	Zapisz zmiany konfiguracji –	
Ustawienia	Cofnij zmiany	
😂 System		
🕫 Konfiguracja sieci	C Przyw	wróć V Zapisz + Dodaj zewnętrzne źródło uwierzytelnienia
		lodaj definicję serwera uwierzytelniania

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 uwie- rzytelnienia.	
Serwis	Serwis w systemie CERB w oparciu o który będzie uwierzytel- niany użytkownik.	
Sekret	Sekret wykorzystywany do połączeń z serwerem. Sekret odpo- wiada hasłu zdefiniowanemu podczas konfiguracji klienta RA- DIUS 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 uwie- rzytelniania.	
NAS ID	Parametr, który zostanie przekazany w atrybucie NAS- Identifier do serwera RADIUS.	
Sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowni- ków.	
Powtórz sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowni- ków.	
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 uwie- rzytelniania.	
Bind DN	Miejsce w strukturze katalogowej, w której zawarte są defi- nicje 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 uwie- rzytelnienia.	
Domena Active Directory	Domena, w oparciu o którą będzie wykonywane uwierzytelnie- nie 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.

	Konfigurowalne logo
	Fudo
	Login (
K	omunikat globalny
Melo	one on FUDO
Plaa	actions could be recorded and stored in electronic format. Ne constact your FUDO administrator for more information.
Held	ome on RDP-100.35.53-WindowsXP
Your Plaa	actions could be recorded and stored in electronic format. ee constact your FUDD administrator for more information.
Ко	munikat lokalny serwera

Zmiana logo

- 1. Wybierz z lewego menu Ustawienia > Zasoby.
- 2. Przjedź na zakładkęRDPlub $\mathit{VNC}.$
- 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.

Zarządzanie	<	Fudo		🕹 admin 🕤 📍
Jashboard		000 1000		
🗐 Sesje		RDP VNC		
🔮 Użytkownicy		Logo		
⊖ Serwery		Maksymalny rozmiar grafik	i: 512 x 512 px.	
- Bastiony		Kolor tła: #02085A.	Wybierz plik z obrazem logo	
🕂 Połączenia			Wybierz plik Nie wybrano pliku	
🛡 Polityki				
🛓 Do pobrania		Aktuainy obraz	FUDO	
🔒 Raporty		Przywróć domyślne	0	
E. Produktywność		Komunikat globalny		
Ustawienia				
System				
¢\$ Konfiguracja sieci				
Powiadomienia	Wprowad	lź treść globalnego k	omunikatu na ekranie logowania	

Przywracanie domyślnego logo

- 1. Wybierz z lewego menu Ustawienia > Zasoby.
- 2. Przjedź 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. Przjedź na zakładkę RDP lub $\mathit{VNC}.$
- 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.

		Wyświetl opcje użytkownika
Zarządzanie <		🔺 admin 🗸
Dashboard	Dashboard	PL EN
Ei Sesje 營 Użytkownicy	Sesje	Aktywne połączenia C Uruchom ponownie
🕂 Połączenia	22:00 00:00 02:00 04:00 06:00 08:00	Car Uruchom ponownie system
🖴 Serwery		€♦Wyloguj
10 Polityki		
📥 Do pobrania	Sesje	

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.

^D onowne u	ruchomienie systemu	¥ Wybierz wersję systemu
Wersja	2.2-26195 (aktywna)	\$
		Anuluj Zatwierdź
		Zrostatuj svotom z verbrana warsja

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.

		Wyświetl opcje użytkownika
Zarządzanie <	Fudo [*] Panel administracyjny	🔔 admin 🗸
Dashboard	Dashboard	PL EN
≝ Sesje	Sesje 22:00 00:00 02:00 04:00 06:00 08:00	Aktywne połączenia
♣ Połączenia A Serwery		2014-03-17 09:15:12 SS SSH
10 Polityki		
🛓 Do pobrania	Sesje	

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.

Po pa	onowne u	ruchomienie systemu	¥ Wybierz wersję systemu
	Wersja	2.2-26195 (aktywna)	\$
			Anuluj Zatwierdź Zrestartuj system z wybraną wersją

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 "\${FUD0_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 wspie- rana przez wszystkie urządzenia Wheel Fudo PAM. Skontaktuj się z działem wsparcia tech- nicznego 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
                           +1 (415) 800 3230
                  Phone:
                  email:
                            info@wheelsystems.com"
        DESCRIPTION
        "Top-level infrastructure of the Wheel Systems enterprise MIB tree"
                    "201704240000Z"
        REVISION
        DESCRIPTION
        "Moved common to .1, fudo to .2."
                    "201703270000Z"
        REVISION
        DESCRIPTION
        "Added objects for checking CPU temperature."
                   "201703150000Z"
        REVISION
        DESCRIPTION
        "Added objects describing status of power supply units."
        REVISION
                   "201703060000Z"
        DESCRIPTION
        "New objects to monitor disk status."
                 "201702140000Z"
        REVISION
        DESCRIPTION
        "First draft"
        ::= { enterprises 24410 }
products OBJECT IDENTIFIER ::= { wheel 1 }
common OBJECT IDENTIFIER ::= { products 1 } -- Objects common to more than one
\rightarrow product.
      OBJECT IDENTIFIER ::= { products 2 }
fudo
zpool OBJECT IDENTIFIER ::= { common 1 }
syncPercentage OBJECT-TYPE
                 Integer32 (0..100)
        SYNTAX
        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,
                         OCTET STRING
       vdevStatus
}
vdevIndex OBJECT-TYPE
                 Integer32 (1..2147483647)
       SYNTAX
       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)

```
PowerSupplyEntry
        SYNTAX
        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
                    SEQUENCE OF CpuEntry
        SYNTAX
        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
                    SEQUENCE OF SmartEntry
        SYNTAX
        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,
                                                              (ciag dalszy na następnej stronie)
```
```
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
                 OCTET STRING
       SYNTAX
       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)

```
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
\rightarrow 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 \Box
\rightarrow 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)

```
Gauge32
       SYNTAX
       MAX-ACCESS read-only
       STATUS
                  current
       DESCRIPTION
               "The rate of seek errors. Reported as (normalized value - threshold) _{\Box}
⊶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,
                            OCTET STRING,
       sessionName
       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)

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>.

Zarządzanie <	Fudo* 🔺 admin - ?
Dashboard	Konia zanasowa i zetancia
🖽 Sesje	
쓸 Użytkownicy	Retencja danych
⊖ Serwery	(Włączone 2) — Włącz automatyczne usuwanie danych sesji po upływie zadanego czasu
-# Bastiony	Usuń dane sesji po upływie dni
🕂 Połączenia	Kopia zapasowa systemu Liczba dni, po których dane sesji zostaną automatycznie usunięte
Polityki	Nopia zapasowa systemu
📥 Do pobrania	W celu wykonania kopii zapasowej FUDO uruchom na zdalnej maszynie polecenie rsync -avze ssh backup@10.0.150.150./ <katalog docelowy=""></katalog>
🕀 Raporty	
Produktywność	Włączone w Włącz tworzenie kopii zapasowych na zdalnych serwerach
Ustawienia	Publiczny klucz SSH
🖕 Sy: Wgraj klucz publiczny	SSH użytkownika zdefiniowanego na serwerze kopii zapasowych
¢6 Konfiguracja sieci	
Powiadomienia	
Znakowanie czasem	
e Zewnętrzne uwierzytelnianie	SHA1
III Zewnętrzne repozytoria haseł	Usuń 🔍 — Usuń klucz SSH serwera kopii bezpieczeństwa
🖬 Zasoby	
Kopie zapasowe i retencja	
🚠 Klaster	
≓ Synchronizacja LDAP	Dodaj klucz och sopuora konij zapasovavsk
≡ Dziennik zdarzeń	
0 2:30:10 2328523 12945678 ♦ 2:1-25035 Ne shortqurowany	C Przywróć V Zapisz 2 miany koningeracji + Dodaj publiczny kłucz SSH
	Cofnii zmiany

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 \mathcal{Z} , 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.

Wyś	wiet	l menu użytkownika
		(<u></u> admin ~) ?
	ſ	PL
	F	EN
	N	C Uruchom ponownie
		ଓ Wyłącz
		⊕ Importuj konfigurację
	Γ	Importuj konfigurację systemu
		€+Wyloguj

- 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 czasuNTPna 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.

Zarządzanie <		📥 admin 🗸
M Dashboard	Klaster	
🖽 Sesje	Tuester	Inicjuj konfigurację klastrową
🖶 Użytkownicy	Utwórz klaster	
🕂 Połączenia	Dołącz do klastra	
🖴 Serwery		
🛡 Polityki		
📩 Do pobrania		
🖨 Raporty		

- 3. Wprowadź nazwę węzła oraz opis ułatwiający identyfikację obiektu.
- 4. Z listy rozwijalnej Adres wybierz adres IP do komunikacji z innymi węzłami klastra.

Zarządzanie <	Fudo [®] Panel administracyjny	🛓 admin 🗸
M Dashboard	Klaster	
🖽 Sesje	THEOLET	
營 Użytkownicy	Utwórz klas Nazwa węzła klastra	
🕂 Połączenia	Nazwa	
Serwery	Opis	
🛡 Polityki		Opis ułatwiający identyfikację zasobu
📥 Do pobrania		
🖨 Raporty		
Ustawienia		
¢ Konfiguracja sleci		
O Data i czas	Adres 10.0.35.10	
🖂 Powiadomienia	Adres IP do komunikacji z inyn	Ni węzłami klastra
Znakowanie czasem	Palazz da klastra Zanisz	ustawienia konfiguracii klastrowei
a, Zewnętrzne uwierzytelnianie	Longez do Nasira	- ustawienia koninguracji Mastrowej

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.

Zarządzanie <	Fudo [®] Panel	administracyjny	📥 admin 🗸
M Dashboard	Klaster		
🖽 Sesje	C		Dane węzła inicjującego klaster
🖶 Użytkownicy	Nazwa	HACluster	
🕂 Połączenia	Onis	Hinh Availability Cluster	
🖴 Serwery	C più	ingrivitanability onotor	
🛙 Polityki			
📩 Do pobrania			
🔒 Raporty			
Ustawienia			
¢ ^e Konfiguracja sieci	Adres	10.0.35.1	
② Data i czas	Wymuś pełną synchronizacie		
🖂 Powiadomienia	Usuń		
Znakowanie czasem			
4 Zewnętrzne uwierzytelnianie			Dodai definicie wezła
Certyfikat HTTPS			
🏝 Aktualizacja		C Przywróć 🗸	Zapisz + 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.

 Data i czas 	Wymuś pełną synchronizację	J	
Powiadomienia	Usuń		
Znakowanie czasem			
Q Zewnętrzne uwierzytelnianie		Nazwa węzła klastra	
Certyfikat HTTPS	Nazwa		
📩 Aktualizacja	Opis		
Kopie zapasowe i retencja danych			
🚓 Klaster		Opis ułatwiający	identyfikację zasobu
😅 Synchronizacja LDAP			
≡ Dzienniki			
⊙ 6 dni i 10000010	Adres		
● 1.3-17780 & Nie skonfgurowany	do komunikacji z	inymi węzłami klastra	
	Usuń	0	
		Zapisz zmia	ny konfiguracji
		C Przywróć Zapisz	+ Dodaj węzeł
		Cofnij zmiany	

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.

Zarządzanie		۵
M Dashboard	Klastor	
🖽 Sesje	TMBACH	
曫 Użytkownicy	Utwórz klaster	
🕂 Połączenia	Dołącz do klastra	
🖴 Serwery	Przyłącz węzeł do istniejącego klastra	
🛡 Polityki		
📥 Do pobrania		
🔒 Raporty		

11. Wklej wygenerowany wcześniej klucz i kliknij Zatwierdź.

Zarządzanie	FUDD [®] Pane	l administracyjny	A
Jashboard	Klaster		
🖽 Sesje	Ridator		
🖶 Użytkownicy	Utwórz klaster		
🕂 Połączenia	Dołącz do klastra		
🖴 Serwery	Klucz publiczny	AAAAE2VjZHNhLXNoYTItbmizdHAyNT	
🛡 Polityki	klastra	VAAAAIbmizdHayNTYAAABBBCpSyRi UGHIS3B6INpDISTtmuW5k1vOeOgpIG	
📥 Do pobrania		TJs04coVSPAvFGYGhn+w= 10000010	
⊖ Raporty			
Ustawienia			
🕫 Konfiguracja sieci	Przyłac	z wezeł do istniejącego kląstrą	
O Data i czas	r iz yiqu	2 Wyzer do Istinejącego nastra	
🖂 Prwiadomiania			Dołacz wezeł do kla

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.

Kopie zapasowe i retencja		
	Nazwa węzła	n2
🛔 Klaster	Opis węzła	n2
	Adres węzła	10.0.70.132
	Status replikacji	Aktywna. Ostatnio zsynchronizowane dane: 2017-12-10 17:02:39
13:51:16.253361 i 12345678 Splayground_6-39472 dJ, Ne skonfigurowany	Klucz publiczny SSH węzła	ssh-rsa AAAABNXaC1yc2EAAAADAQABAAABAQDD72+LQDwoYmO/DCh01 gk YshdesGaNaygOeE8m4XKalgcdOIBjRYgyPU3LUWuJINQNBaQzTm2PhRI 92K/Rq4D11talRFc9IhEvRsMsY/g35zh2H4hu/SUbYVP6+xPLcqMXinPgq hCbrKq-titw3NTAZFCPL3+0zEUJapaXGa7/p40goCP6Ddr+oeeJsiL397FE Y3IT3349/bX2UuJIVg3Ln-ta3htfl62ZD6ALA48-U38W5q6D4w9FD Ce/DCarCptituIDgEqrKMd02UpfiqNv6wBtSq6siDT2gRZ/sbkJVk73KM8oY Vhy1/wiHgUIp/dpBeDosfmMN53ZMkLh
	Usuń	

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.

Zarządzanie <	Fudo [®] Pan	el administracyjny	📥 admin 🗸
Jashboard	Klaster		
🖽 Sesje	Naster		
曫 Użytkownicy	Nazwa	HACluster	
💠 Połączenia	Opin	Link Auginbilly Churter	
⊖ Serwery	Opis	Figh Availability Graster	
🛙 Polityki			
📥 Do pobrania			
🔒 Raporty			
Ustawlenia			
¢6 Konfiguracja sieci	Adres	10.0.35.1	
 Data i czas 	Wymuś pełną synchronizację		
Powiadomienia	Usuń		
Znakowanie czasem		Zaznacz opcie, aby usunać wybrany v	wezeł klastra
4 Zewnętrzne uwierzytelnianie	Zapi	sz zmiany konfiguracji	t.
Certyfikat HTTPS	Zapi		
1 Aktualizacja		C Przywróć Zapisz	+ Dodaj węzeł

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 ozna-
	cza wyższy priorytet.
	Grupa redundancji o wyższym priorytecie przyjmuje rolę $master$ i obsłu-
	guje 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.

Zarządzanie <	Fudo admin ~	?
I Dashboard	Wazły Grupy redundancii	
E Sesje		
營 Użytkownicy	Automatyczne przełączanie W. węzłów	
⊖ Serwery		
• Bastiony		
🕂 Połączenia	Nazwa	
0 Polityki	ID #	
📩 Do pobrania	Priorytet 0	
🖨 Raporty	Interfejs sieciowy Wymuś tryb slave \$	
Produktywność	Wprowadź wartości parametrów konfiguracyjnych	
Ustawienia		
😂 System		
🕸 Konfiguracja sieci		
Powiadomienia	Kliknij, aby dodać grupę redundancji	
Znakowanie czasem		
a Zewnętrzne uwierzytelnianie		

- 5. Kliknij Zapisz.
- 6. Wybierz z lewego menu Ustawienia > Konfiguracja sieci.
- 7. Kliknij +, aby dodać adres IP.
- 8. Wprowadź adres IP i kliknij h, aby nadać mu atrybut klastrowy.
- 9. Z listy rozwijalnej wybierz wcześniej zdefiniowaną grupę redundancji.
- 10. Kliknij Zapisz.

Interfejs	y Nazwa i DNS	Tablica trasowania	Etykiety IP
% net0 ∞	.00.27:68:2A:11		
10.0.150.15	i0 / 16	× • • ×	
Włącz opcję a	adresu klastrowe	ego 🔍 🔸 💌	
10.0.150.15	i2 / 16	✓ Q A group#1	¢ x
+ Pr	zypisz grupę red	lundancji	_

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.

Zarządzanie <	Fudo		👗 admin 🗸 💡 📍
Dashboard	Waxh, Grupy rodunda	aali	
日 Sesje	węzty Grupy redunda		
嶜 Użytkownicy	Automatyczne przełączanie węzłów	W0.	
⊖ Serwery	ALLER ZECONALL		
•# Bastiony			_
+ Polączenia	Nazwa	Group 255	*
🛡 Polityki	D	255	*
📥 Do pobrania	Priorytet	0	- *
🖶 Raporty		[- [
🖹 Produktywność	Interrejs sieciowy	neti	
Ustawienia	Zmień wartośc	ci parametrów konfiguracyjnych	
😂 System			
¢° Konfiguracja sieci	Namua	an ma243	
Powiadomienia	1462.040	grupaceo	J.*
Znakowanie czasem	ID	243	*
a, Zewnętrzne uwierzytelnianie	Priorytet	0	*
III Zewnętrzne repozytoria haseł	Interfejs sieciowy	net1 t	
🖾 Zasoby	Usuń	0	
Kopie zapasowe i retencja			
🕼 Klaster		Zapisz zmiany	
≓ Synchronizacja LDAP		C Przywróć 🗸 Zapisz	+ Dodaj grupę redundancji

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.

Zarządzanie <	Fudo		🛓 admin 🖌 🤶
M Dashboard	Wezh Grupy redunda	neli	
🖽 Sesje	węzy Grupy rodulida		
🔮 Użytkownicy	Automatyczne przełączanie węzłów	WIL.	
⊖ Serwery	AMERTER ZEROSAGU		
• Bastiony			
🕂 Polączenia	Nazwa	Group 255	*
🛡 Polityki	ID	255	*
📥 Do pobrania	Priorytet	0	*
🖨 Raporty	Interfeis sieciowy	net1	
Produktywność	interiejs alectowy		
Ustawienia	Usuń		
🖕 System	1	Zaznacz, aby usunąć grupę redundancji	
¢e Konfiguracja sieci	Nazwa	grupa243	*
Powiadomienia		graphic re]*
Znakowanie czasem	di	243	_ ₽
4 Zewnętrzne uwierzytelnianie	Priorytet	0	*
III Zewnętrzne repozytoria haseł	Interfejs sieciowy	net1	\$
Zasoby	Usuń		
Kopie zapasowe i retencja			
👍 Klaster		Zapisz zmiany	
≓ Synchronizacja LDAP		C Przywróć 🗸 Zapisz	+ Dodaj grupę redundancji

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.

Zarządzanie <	Fudo		🛔 admin 🗸 🤗
Dashboard	Washing County and under		
日 Sesje	węzny Grupy redundan	ncji	
😁 Użytkownicy	Automatyczne przełączanie węzłów	WI.	
⊖ Serwery	AMERTER ZECONAL		
•# Bastiony			
🕂 Połączenia	Nazwa	Group 255	*
Polityki	ID	255	*
🛓 Do pobrania	Priorytet	0	*
🖶 Raporty			
■ Produktywność	Interfejs sieciowy	net1	
Ustawienia	Usuń		
🖨 System			
🕫 Konfiguracja sieci	Kliknij, at	by zdegradować wybraną grupę redundancji	
🖂 Powiadomienia	Nazwa	grupaz+o	
C Znakowanie czasem	ID	243	*
۹ Zewnętrzne uwierzytelnianie	Priorytet	0	*
III Zewnętrzne repozytoria haseł	Interfejs sieciowy	net1	\$
Zasoby	Usuń	0	
Kopie zapasowe i retencja			
🔥 Klaster		Zapisz zmiany	
≓ Synchronizacja LDAP		C Przywróć 🗸 Zapisz	+ Dodaj grupę redundancji

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.

Zarządzanie Dodaj filtr, aby ograniczyć liczbę	wyświetla	nych zdarz	zeń Eksportuj wpisy dziennika zdarzeń 🍓 admin 🗠 📍
Dashboard			Dodai filtr - Eksportui logi & Konfiguracia syslog Szukal 9
E Sesje			
M Libutkownicy	Ustaw	ienia logov	vania zdarzeń na zewnętrznym serwerze
	logowania	Komponent	
Serwery 2014-12-22 14:54:22	Informacje	tudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.35.
++ Połączenia 2014-12-22 14:08:25	Informacje	fudoauth	User admin authenticated using password logged in from IP addres: 10.0.1.35.
2014-12-22 14:07:28 0014-10-20 10:50:30	Informacje	fudoauth	User admin authenticated using password logged in from IP address 10.0.1.30.
0 Polityki 2014-12-22 12:39:39	Informacje	rudoautn	User admin authenticated using password logged in from IP addres. 10.0.1.30.
▲ Do pobrania	Informacje	gui	User admin created connection HDP (771109032230817793).
A Raporty 2014-12-22 12:05:45	Informacje	tudod	Meloading configuration.
2014-12-22 12:05:45	Informacje	gui	User admin created server WiNDOWS 2000 (7/1109032230617793).
■ Produktywność 2014-12-22 12:02:20	Informacje	gui	User admin created user tomek (771100932230017394).
Ustawienia 2014-12-22 12:02:20	Informacje	gui	User admin changed user tomek (771109032230617794), Changed field: [granted_to_users from [77110903223
System 2014-12-22 12:02:20	Informacje	gui	User admin changed user tomek (771109032230617794), Changed field, Ivalid tal form the rol (p).
2014-12-22 12:02:20	Informacje	gui	User admin changed user tomek (771100032230617784), Changed field, Valio_to from Note to [0.2015-01-21
Ø [®] ₀ Konfiguracja sieci 2014-12-22 12:02:20 Ø [®] ₀ Konfiguracja sieci 2014-12-22 12:02:20	Informacje	gui	User admin changed user tomek (771109032230617794), Changed field: Valio_sitice inclin None to [0.2014-12
✓ Powiadomienia	Informacie	gui	User somin changed user tomek (771109032230617784), changed teid, account_valuity from None to 30 .
2014-12-22 12:02:20	Informacje	gui	User admin changed user tomak (711109032230617794). Changed field: "phone" from "to 179560502"
2014-12-22 12:02:20	Informacio	gui	User admin changed user tomex (77110089090017704). Changed field, [provide iron 1:0:73306065.
Q₂ Zewnętrzne uwierzytelnianie	Informacje	gui	User admin changed user tomek (771109032230617794), Changed field, 50ganzation from Vite TD1
III Zewnetrzne repozytoria haseł	Informacje	gui	User admin changed user tomek (771109032230617794). Changed field: Ton_hame from ~ to TD .
2014-12-22 12:02:20	Informacje	gui	User admin changed user tomek (771109032230617784), changed field, lemail from 1 to "Lowornickwwneelsyst
Zasoby 2014-12-22 12:02:20	Informacje	gui	User admin orlanged user (ormox (77110905220017794), orlanged rend, hame norm to tomex.
Kopie zapasowe i retencja	Informacie	aui	User schills obsersed ashunk interfaces settings
L Klaster 2014-12-22 12:00:40	Informacia	gui	User scimin changed network interaces settings.
2014-12-22 12:00:40	Informacia	fuded	Palasting configuration
Synchronizacja LDAP	Informacia	qui	Hear schin, channad network interfaces settings
Dziennik zdarzeń 2014-12-22 11:09:01 2014-12-22 11:09:01	Informacie	gui	Veel events sharings nerrork interfaces adultings.
2014-12-22 11:09:01	Informacia	fuded	Palanting configuration
0 255 50 664207 \$ 11221122 2014-12-22 11:59:51	Informacia	fuctoreth	Lear ordering contegorizations.
	Informacie	fudoocrd	Started successfully.

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] (fudo_dp) (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_attrib	ute
fudo_connection_grant	-
fudo_connection_netwo	rk
fudo_erpm	-
fudo_external_authentie	cation
fudo_http_request	-
fudo_ldap_address	-
fudo_ldap_connection	-
fudo_ldap_server	-
fudo_ldap_server_exter	nal_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_authenticatio	on_method
_fudo_user_connection	_
_fudo_user_grant	_
reports_definedreport	_
reports_definedreportfilt	er
reports_definedreportsu	oscription
reports_report	_
reports_reportcriteria	_

 $Modyfikowanie\ servera\ Syslog$

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.

CERB - Panel	administr	racyj	NY (version v1.5)				polski english	wyloguj
Główne menu	~	List	a klientów					
Użytkownicy	+		IP klienta		Nazwa	Hasło serwera RADIUS	Blokada	
SS Grupy	+	1	127.0.0.1		None	a		
😭 Serwisy	+							
💻 Dziennik zdarzeń	+							
🟥 Licencja	+							
🕲 Ustawienia	+							
🐺 Klienci RADIUS	-							
C Dodaj klienk								
🐯 Usuń klienta								
퇞 Zablokuj klienta								
🐺 Odblokuj klienta								
zalogowany jako: <mark>admin</mark>	:							
data i godzina na serw 2012-11-21 08:5	verze:		4 Strona	1 z 1 🕨 🕅	2		Wyświetlono	0 1 - 2 z 2

• Podaj adres IP serwera Wheel Fudo PAM, nazwę klienta oraz hasło i kliknij Zapisz.

Podaj param	etry konfiguracyjne FUDO.	
Dodawanie klienta RADIUS		×
IP klienta: 👷	10.0.6.61	
Nazwa klienta: 👷	FUDO	
Hasło: 👳	•••••	Generuj
Wyczyść/Domy	ślne wartości Zapisz Za	ımknij
Kliknij aby dodać kli	enta RADIUS.	

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.

	_	Klikr	ij aby otworzyć okno definiowania nowej grupy.		
CERB - Panel ad	ministr	acy	NY (version v1.5)		
Główne menu	~	List	a grup		
🌡 Użytkownicy	+		Nazwa grupy	Opis	
S3 Grupy	-	1	cerb:admins		
SS Dodaj grupę		2	test_users		
Busun grupę					
👥 Serwisy	+				
📃 Dziennik zdarzeń	+				
🛅 Licencja	+				
Ostawienia	+				
🐺 Klienci RADIUS	+				
zalogowany jako: admin					
data i godzina na serwerz 2012-11-21 09:03	ze:				
		14	🖣 Strona 🚺 z 1 🕨 🕅	Wyświetlon	o 1 - 3 z 3

• Podaj nazwę grupy (fudo_users) i kliknij Zapisz.

	Uzupełnij podstawo	we informacje na temat grupy.	
odawanie grupy			X
Podstawowe usta Nazwa grupy: 👷 Opis: 👷	awienia grupy fudo_users Użytkownicy FUDO		22
Atrybuty dodatk	owe Serwisy Opcje serwera R	RADIUS (zewnętrznego)	
Nazwa	Wartość	Dodaj atrybut	Usuń
Nazwa	V	Vartość	
	Wyczyść/Do	omyślne wartości Zapisty Zamknij Zamknij	
	Kliknij aby dodać definicję g	rupy.	

- 3. Dodanie użytkownika.
- Wybierz z lewego menu $U\dot{z}ytkownicy > Dodaj u\dot{z}ytkownika,$ aby otworzyć okno definiowania nowego użytkownika.

CERB - Panel adr	ninist	(Klii racy	knij aby otworzyć okno j ny (version v1.5)	definiowania nowego uży	/tkownika.	polski er	ıglish ı	wyloguj
Głównę menu	~		Wszyscy użytkownicy	Aktywni użytkownicy	🔁 Zablokowani	i użytkownicy 🛛 📷 Konta wygasłe	e 🔵 l	Jżytkownie
Użytkownicy	-	Gru	py : Wszystkie grupy	v		1		
👃 Dodaj użytkownika			Nazwa użytkownika	Opis		Moduł uwierzytelnienia	St	
Susur użytkownika		1	admin			Hasło statyczne	۲	
邉 Zablokuj użytkownika		2	admin2	Drugi użytkownik admi	nistracyjny	Hasło statyczne		
凝 Odblokuj użytkownika								
🔊 Grupy	+							
🐏 Serwisy	+							
📃 Dziennik zdarzeń	+							
🟥 Licencja	+							
😳 Ustawienia	+							
🐺 Klienci RADIUS	+							
zalogowany jako: admin								
data i godzina na serwerz 2012-11-21 09:11	e:							

• Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).

jan.kowalski
Jan Kowalski
CerbToken (czasowy, wieloprofilowy)
znakowy
10 sekund
6
Ustaw hasło statyczne

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.

Wybierz z	akładkę aby przy	pisać użytkownikowi grupę.					
Dodawanie użytkownika			×				
Ustawienia użytkownika —							
Nazwa użytkownika: 👳	jan.kowalski						
Opis: 😠	Jan Kowalski	5					
Moduł uwierzytelnienia: 👳	CerbToken (czas	owy, wieloprofilowy)					
Opcje uwierzytelnienia Atrybut	y dodatkowe	Dostępne					
fudo_users	€ →	cerb:admins test_users					
Przypisz użytkownikowi grupę.							
Wyczyść/Domyślne wartości Zapisz hy Zamknij							
Kliknij aby dodać	użytkownika.						

- 4. Skonfigurowanie serwisu.
- Wybierz z lewego menuSerwisy > Dodaj serwis,aby otworzyć okno definiowania nowego serwisu.

Kliknij aby dodać okno definiowania nowego serwisu.								
CERB - Panel adr	CERB - Panel administracyjny (version v1.5) polski english wyloguj							
Główne menu	~	List	a serwisów					
Użytkownicy	+		Nazwa serwisu	Opis	Atrybut NAS-IP-Addr	Attrybut NAS-Ide		
🔊 Grupy	+	1	cerb:mgmt					
Dodaj serwis	-							
📃 Dziennik zdarzeń	+							
🛐 Licencja	+							
🙆 Ustawienia	+							
Klienci RADIUS	+							
zalogowany jako: admin data i godzina na serwerz 2012-11-21 09:21	ze:							
		14	🖣 Strona 1 z 1 🕨	▶ 2		Wyświetlono 1 - 2 z 2		

- Wpisz nazwę pod jaką identyfikowana będzie usługa uwierzytelniania (cerb_fudo) oraz opis serwisu.
- Dodaj do serwisu grupę fudo_users i kliknij *Dodaj*.

Uzupełnij podstawowe dane serwisu	
Dodawanie serwisu	\mathbf{X}
Dane serwisu	
Nazwa serwisu: 👷 fudo	
Opis: 👷 Uwierzytelnianie użytk	
Zaawansowane Atrybuty dodatkowe Grupy Kliknij aby przypisac grupę	-
Wybrane Dostepne	
tudo_users cerb:admins	
test_users	
Przypisz grupę do serwisu	
Dodaj (h.) Anuluj	
Kliknij aby dodać definicję serwisu.	

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.

Zarządzanie <	Fudo [*] Panel administracyjny	🕹 admin 🗸
Dashboard	Zewnetrzne uwierzytelnianie	
🖽 Sesje		
알 Użytkownicy		
++ Połączenia		
🖴 Serwery		
🛡 Polityki		
📥 Do pobrania		
🖨 Raporty		
Ustawlenia		
🕫 Konfiguracja sieci		
🕑 Data i czas		
Powiadomienia		
C Znakowa Przejdź do widoku	zarządzania systemami zewnętrznego uwierzytelniania	
(4 Zewnętrzne uwierzytelnianie)	Kliknii, aby dodać definicie systemu uwierzytelniania	
Certyfikat HTTPS		
1 Aktualizacja	C Przywróć V Zapisz	Dodaj zewnętrzne źródło uwierzytelnienia

• 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 RA-DIUS na serwerze CERB. Nazwa serwisu musi być zgodna z nazwą nadaną przy konfigurowaniu serwisu na serwerze CERB.

• Kliknij Zapisz.

		Wybierz Typ 'Cerb' i uzupełnij	parametry serwera
ſ	Тур	Cerb	
	Adres	10.0.35.52	
	Port	1812	
Wysyłaj żąd	dania z	10.0.35.10	Określ adres IP do komunikacji z serwerem CERB
	Serwis	fudo	Wprowadź nazwę serwisu skonfigurowanego w systemie CERB na potrzeby uwierzytlenianie użytkowników FUDO
	Sekret	••••	Warawadá basla uwiarzutalniania klianta DADIUS
Powtórz	sekret	••••	wprowadz nasio uwierzyteinienia kilenta KADIOS
	Usuń		

- 2. Dodanie użytkownika.
- Wybierz z lewego menu Zarządzanie > Użytkownicy.
- Kliknij + Dodaj.

Zarządzanie Przejdź do widoku zarządzania użytkownikami								Ý
Jasi board		żytkownie	Dod	aj użytkownik	a Blokuj Odblokuj	Usuń		Dodaj filtr ~
E Sesje	dai d	ofinicio u	żytkowni	ka				
🗑 Użytkownicy	uaj u	ennicję u	zytkowiii	nizacja	Email	Peina nazwa	Metoda uwierzytelnienia	Stan
		a2_user1	operator					Aktywne
+‡+ Połączenia		a2_user2	operator					Aktywne
🖴 Serwery		a2_user3	operator					Aktywne
ID Polityki		admin	superadmin				Hasło	Aktywne
e i ontyra		admin2	admin	Wheel			Hasio	Aktywne
📥 Do pobrania	0	adminat	superadmin		s.tempeluk@wheelpythems.com	Androg Termolika	Hasło	Aktywne
🖨 Raporty		anonymous	user					Aktywne
		bartlomiej	superadmin		e messelenselslikelseringelens som		Hasło	Aktywne
Ustawienia		f1_user1	user	Firma1			Hasło	Aktywne
🌣 Konfiguracja sieci		f1_user2	user	Firma1			Haslo	Aktywne
 Data i czas 		f1_user3	user	Firma1			Hasło	Aktywne
		f2_user1	user	Firma2			Hasło	Aktywne
Powiadomienia		f3_user1	user	Firma3			Hasło	Aktywne
C Znakowanie czasem		fudo_user1	user		adres@email.com	fudo_user1	Zewnętrzne Uwierzytelnien	iB Aktywne
6 Zeuretree uniersteleiseie		fudo_user2	user			fudo_user2	Zewnętrzne Uwierzytelnien	8 Aktywne
 Zewnętrzne uwierzyteinianie 		fudo_user3	user			fudo_user3	Zewnętrzne Uwierzytelnien	il Aktywne
Certyfikat HTTPS		fudo_user4	user			fudo_user4	Zewnętrzne Uwierzytelnien	8 Aktywne

• 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.

Dodaj użytkownik			
Daólny	Uzupełnij dane użytkownika		
-gom)			
Login	jan.kowalski		
Rola	user 🗘		
Synchronizacja z LDAP	Ω.		
Zablokowane	0		
Pełna nazwa	Jan Kowalski		
Email	jan@kowalski.pl		
Organizacja			
Telefon		J	
Domena AD			
Baza LDAP			
Iprawnienia			
Uprawnieni użytkownicy	۵.		
Jwierzytelnienie	1		
Тур	Zewnętrzne uwierzytelnienie \$	1	
Townstrans frédie	Carb 10 0 25 52 convictoria		
uwierzytelnienia	Cerb 10.0.35.32 Ser WIS:RU00	J	
Wybie	erz opcję zewnętrzengo uwierzy	telniania i wskaż wo	ześniej dodany serwer CE
	C Przywróć V Zapisz		
iknii abv dodać	definicję użytkownika		

- 3. Dodanie połączenia.
- Wybierz z lewego menu Zarządzanie > Połączenia.
- Kliknij + Dodaj.

Zarządzanie <	FU	Panel administracyjny	🛓 admin	
Dashboard	Połącze	ia Dodaj połączenie Blokuj Odblokuj	Usuń	Dodaj filtr ~
Przejdź do widoku z	arządzani	n połączeniami	Serwery	Stan
+ Połączenia	efinicję poł	iczenia ^{tous}	blaster , anonymous-TELESERG-SSH , anonymous 100038 ##-RDP	Aktywne
Serwery	f1_con	f1_user1, f1_user2, f1_user3, f2_user1, f3_user1, testadm1, testadm2	63%/01/01/07/07/07/07/02/05/04-0	Aktywne
D Politvki	http		www.wheelsystems.com-HTTP	Aktywne
🕹 Do pobrania	mysql- podmiar	user1 a	rest@100.00.02.601003. , rest@10.0.00.71 rrysep8.6.00. , rest@10.0.00.70 rrysep8.6.14	Aktywne
🖨 Raporty	 oracle- podmiar 	user1 a	Generold 111-OPHCLE	Aktywne
Ustawienia	rdp- podmiar	user1, user2 a	40%/05/05/97/01/05/97/0P	Aktywne
¢° Konfiguracja sieci	ssh- podmia	fudo_user1, fudo_user2, fudo_user3, fudo_user4, fudo_user5 a fudo_user6, fudo_user8, fudo_user9, user1	. reelleroodside-88H ; mellerbioldside-80LW16	Aktywne
O Data i czas	ssh- podmia	user2 a2	rent@10038-82-88H	Aktywne
	telent	admin	and sept 10.0.20.00-YOUNG T	Aktywne
Znakowanie czasem	vnc	admin, admin2, adminat, bartłomiej	10007490, 18.8.35448942	Aktywne

- 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.

Baddaadaaaad		
Dodaj połączenie	e	
Ogólny		
Nazwa	serwery_web_ssh Wprowadź nazwę połączenia	
Powiadomienia	C Rozpoczęcie sesji Zakończenie sesji Otwarcie zdalnej pomocy – Zdefiniuj opcje powiadomiń administ Zakończenie zdalnej pomocy O Wykrycie wzorca	tratora
Użytkownicy	Przypisz użytkownika do połączenia	
Czas retencji (w dniach)	Określ czas przechowywania sesji	
Funkcjonalność RDP	 Przekierowanie schowka Przekierowanie dźwięku Przekierowanie urządzeń Dynamiczne wirtualne kanały Przekierowanie multimediów 	
Funkcjonalność SSH	ම් Sesje ම් Przekierowanie portu ම් Terminal ම් Środowisko ම් X11 ම් SSH Agent forwarding ම් Powłoka ම් SCP	
Funkcjonalność VNC	Schowek klienta 🕑 Schowek serwera	
Uprawnienia		
Uprawnieni użytkownicy	ه	
Serwery		
Serwer	SSH-10.0.35.52 +	
Polityka	+	
Zastąp login?	Przekazuj login	
Zastąp sekret?	Przekazuj hasło	
W	/ybierz serwer i określ tryb uwierzytelniania	
	Coda server	
Klikn	ij aby dodać połączenie	

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*.

JRCE Device	e Selection - HDD Raw Copy Tool 1.10	Free			
HDD RAW	COPY TOOL 1.10 Free			WWW.HDDGUF	RU.COM
BUS SATA SATA	MODEL ST1000DM003-9YN162 (C:) SanDisk SDSSDHP256G	FIRMWARE CC48 X2306RL	SERIAL NUMBER 154D6GRM 313375042199	LBA 1,953,525,168 500,118,192	CAPACITY 1000.2 GB 256.06 GB
USB	Generic Flash Udisk (D:)	0000	ba9359411649	7,864,192	4026.46 MB
FILE	IMAGE of Generic Flash Udisk	0000	ba9359411649	7,864,192	4026.46 MB
opyright	© 2005-2013 HDDGURU.COM	Please	select SOURCE	Open Disk Manag	gement Console ontinue >>>

- 4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.
- 5. Kliknij $ST\!ART,$ aby rozpocząć procedurę kopiowania.

HDD Raw Copy Tool 1.10 Free	- 0 X
SOURCE: [2] Generic Flash Udisk 0000 [4026.46 MB] TARGET: [FILE] C:\Users\whee\\Documents\pen.imgc	About
	Copyright ©2005-2013 HDDGURU.COM
СОРУ	
12/15/2016 3:22:01 PM	^
12/15/2016 3:22:01 PM HDD Raw Copy Tool 1.10; http://hddguru.com 12/15/2016 3:22:01 PM	
12/15/2016 3:22:01 PM Source: [2] Generic Flash Udisk 0000 [4026.46 MB]	
12/15/2016 3:22:01 PM Target: [FILE] C:\Users\wheel\Documents\pen.imgc	
<	>
Current task progress	
Stop	START
[2] Generic Flash Udisk 0000 [4026.46 MB] >>> [FILE] C:\Use	rs\wheel\Documents\pen.imgc

6. Z chwilą wystąpienia komunikatu

Operation terminated at offset..., zamknij okno i odłącz napęd USB.

HDD Raw Copy Tool 1.10 Free		-		×
SOURCE: [2] Generic Flash Udisk 0000 [4026.46 fl TARGET: [FILE] C:\Users\wheel\Documents\pen.in	MB] hgc			About
	Copyright © 200	05-2013 HD	DGURI	J.COM
COPY				
12/15/2016 3:22:41 PM Copying	2 493 448 192: 186 4 870 016 (The system	n cannot fir	od the	A .
12/15/2016 3:26:37 PM Source was unplugged, abort	ing	in cannot m	io the	
12/15/2016 3:26:37 PM Average speed: 12.9 MB/s 12/15/2016 3:26:37 PM Operation terminated at offs:	at 2 493 448 192 184 4 870 016			
12/15/2010 5.20.57 PM Operation terminated at ons	2(2,455,440,152 (04 4,070,010			
4		_		×
				_
Current task progress				
62% complete 12.9 MB/s				
Current sector: 4,874,112	Stop	START		
[2] Generic Flash Udisk 0000 [4026.46 MB]	>>> [FILE] C:\Users\wheel\Docume	ents\pen.ir	ngc	

- 7. Podłącz nośnik pamięci flash i włącz program HDD Raw Copy Tool.
- 8. Na ekranie wyboru napędu źródłowego, zaznac
z $\it FILE$ i wskaż plik z obrazem kluczy szyfrujących.
- 9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij Continue.

TARGET Device	e Selection - HDD Raw Copy Tool 1.10	Free				×
HDD RAW COPY TOOL 1.10 Free			WWW.HDDGUP	IU.COM		
BUS SATA SATA USB FILE	MODEL ST1000DM003-9YN162 (C:) SanDisk SDSSDHP256G Generic Flash Udisk (D:) Double-click to open file	FIRMWARE CC48 X2306RL 0000	SERIAL NUMBER 154D6GRM 313375042199 ba9359411649	LBA 1,953,525,168 500,118,192 7,864,192	CAPACITY 1000.2 GB 256.06 GB 4026.46 MB	
Copyright Disks found:	© 2005-2013 HDDGURU.COM	Please se	lect TARGET	Open Disk Manaj	ontinue >>>	

- 10. Kliknij Continue.
- 11. Kliknij START.
- 12. Proces kopiowania obrazu zakończony jest z chwilą wystąpienia komunikatu:

Operation terminated at offset....

HDD Raw (Copy Tool 1.10 Free	-		\times
SOURCE: TARGET:	[0] IMAGE of Generic Flash Udisk 0000 [4026.46 MB] [2] Generic Flash Udisk 0000 [4026.46 MB]			About
	Copyright ©20	05-2013 HDI	OGURU	.com
COPY				
12/15/20	16 3:33:25 PM Locking device			^
12/15/20	16 3:33:25 PM Copying			
12/15/20	16 3:39:38 PM End of source image file; operation complete.			
12/15/20	16 3:39:38 PM Average speed: 6.7 MB/s			- 11
12/15/20	16 3:39:38 PM Operation terminated at offset 2,493,448,192 LBA 4,870,016			
				~
<			,	
Ourrent	task prograss			
corrent	task progress			
62% c	complete 6.7 MB/s			
Current	t costory 4 974 112	START		
Currer	it sector: 4,0/4,112	JIMAI		
[0] IMAGE of	Generic Flash Udisk 0000 [4026.46 MB] >>> [2] Generic Flash Udisk 0000	[4026.46 N	AB]	

13. Zamknij program i odłącz nośnik flash z zapisanym kluczem szyfrującym.

Mac OS X

- 1. Uruchom terminal.
- 2. Wykonaj komendę ${\tt sudo}~{\tt -s}$ 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:

- $\bullet \ Dziennik \ zdarze \acute{n}$
- 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.

	Minimalizuj panel opcji
Zarządzanie	Fudo [*]
I Dashboard	Menu opcji użytkownika —
🖽 Sesje	Rozkład liczby połączeń Aktywne sesje użytkowników
😤 Użytkownicy	Sesje Aktywne sesje O
👄 Serwery	02:00 02:00 04:00 06:00 08:00 10:00 Czas Server Użytkownik Protokół
a Konta	
Sejfy	
n Gniazda nasłuchiwania	• setile
n- Modyfikatory hasel	
🛡 Polityki	Aktywność dysku Wykorzystanie Status dysków 11:46 11:47 11:48 dysku
🛓 Do pobrania	
🕀 Raporty	68%
≘ Produktywność	Zajęte: 244.08 Wolne: 11.4.98
Ustawienia	eodczył ezapis
🖕 System	Wykorzystanie pamięci i procesora
¢. Konfiguracja sieci	Pamięć i procesor Sieć
🖂 Powiadomienia	11:46 11:47 11:48 00:00 02:00 04:00 06:00 10:00
C Znakowanie czasem	
e Zewnętrzne uwierzytelnianie	
III Zewnętrzne repozytoria haseł	
🖬 Zasoby	eparties envocesor
Kopie zapasowe i retencja	Aktywność połączenia sieciowego
🚓 Klaster	Dziennik zdarzeń
≓ Synchronizacja LDAP	Czas Typ Komunikat
≡ Dziennik zdarzeń	2016-06-10 11:44:36 user User admin authenticated using password logged in from IP address: 10.0.1.26.
 ○ 29 dmi k 12345678 ♦ pam-28485,5 Nie skonfiguroweny 	2016-06-10 11:12:48 User User admin authenticated using password logged in from IP address: 10.0.1.26.

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.

Wciśnij przycisk, aby zwolnić dźwignię kieszeni dysku Pociągnij za dźwigni	nię, aby wysunąć 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 zgod-
	nie z procedurą opisaną w rozdziale $Administracja > System > Licen-$
	cja.Jeśli problem będzie się powtarzał skontaktuj się z działem w sparcia
	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 li-
	cencję.
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 con- figuration.
FSE0068	<i>Error connecting to Lieberman ERPM server %s: incorrect protocol spe-</i> <i>cified.</i>
FSE0069	Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s.
FSE0070	<i>Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server.</i>
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 at- tempt%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

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	<i>Error fetching password from Thycotic server %s: unable to get password</i>
	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 błedu	Treść komunikatu i opis
FAE0153	Session indexing failure.
FAE0154	Session conversion failure for session %s.
FAE0165	Error authenticating user <user name="">.</user>
FAE0189	Error saving NTP servers: <server name="">.</server>
FAE0232	MuSQL 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
1510200	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
1,520001	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

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 odw
zorowania parametrów obiektów w Fudo2.2na nowy model danych Fud
o3.0.

16.2.1 Połączenie

Zarządzanie <	Fudo				Zarządzanie <	Fudo	
Jashboard	Połaczenie				Jashboard	Konto	
🖽 Sesje	1014020110				🖽 Sesje	Konto	
ở Użytkownicy	Ogólne				ở Użytkownicy	Ogólne	
🖴 Serwery	Nazwa			*	⊖ Serwery	Nazwa	
• Bastiony					Konta		
+ Połączenia	Zabiokowane				Sejfy	Zablokowane	
🛡 Polityki	Powiadomienia	Dołączenie do sesji Wykrycje wzorca	 Odłączenie od sesji 		Gniazda nasłucniwania	Тур	regular
📥 Do pobrania						Nagrywanie sesji	wszystko
🕀 Raporty	Użytkownicy			© Q	🕹 Do pobrania	OCR sesji	
Produktywność	Nagrywanie sesji	Pełne		¢ **	Raporty	Usuń dane sesji po upływie	
Ustawienia	OCR sesji	0				uniania	
🝃 System	Usuń dane sesji po upływie			dni	Ustawienia		
¢ ^e Konfiguracja sieci	Polityki czasowe				🝃 System	Uprawnieni użytkownicy	
Powiadomienia					¢6 Konfiguracja sieci	Serwer	
Znakowanie czasem	Funkcjonalnosc protokołow	N			🖂 Powiadomienia		
& Zewnętrzne uwierzytelnianie	RDP 🕑	Przekierowanie schowka Przekierowanie urzadzeń	Przekierowanie dźwięku Dynamiczne wirtualne kanały	v	C Znakowanie czasem	Serwer	SSH-0-10.0.35.52
III Zewnętrzne repozytoria haseł		Przeklerowanie wejścia audio	Przekierowanie multimediów		🔍 Zewnętrzne uwierzyte anie	Dane uwierzytelniające	
a Zasoby	Maksymalna rozdzielczość sesji RDP	Dowolny		\$	III Zewnętrzne repozytow haseł	Domena	
Kopie zapasowe i retencja	SSH 🛛	🛛 Sesje	Przekierowanie portu		Zasoby	Login	
🚓 Klaster		Terminal X11	Środowisko SSH Agent forwarding		Kopie zapasowe i retercija	20311	
≓ Synchronizacja LDAP		 Powłoka SFTP 	SCP		A Klaster	Zastąp sekret	
≡ Dziennik zdarzeń	VNC 🗹	Schowek klienta	Schowek serwera			Polityka modyfikatora i sła	Statyczne, bez ograniczeń
(*) (*38-14 942180) 12345878	Uprawnienia						
\$ 2.1-23500 L Ne skonfigurowany					6 days i 12345678		C Przywroc V Zapisz
	Uprawnieni uzytkownicy			ି କ			
	Serwery						
	Serwer			÷*			
	Politiki						
	Folityki			• u			
	Zastąp login						
	Zastąp sekret						
	Usuń	0					
		2 Przy	rwróć 🗸 Zapisz		+ Dodaj serwer		



16.2.2 Serwer

Zarządzanie <	Fudo		Zarządzanie <	Fudo		
Jashboard			Jashboard			
🖽 Sesje	Serwer		🖽 Sesje	Gniazdo nas	uchiwania	
🔄 Użytkownicy	Ogólne		🔮 Użytkownicy	Ogólne		
🖴 Serwery	Nazwa	*	🖴 Serwery		Name	
- Bastiony			Konta			
+ Połączenia	Zablokowane	0	Sejfy		Zablokowane	0
♥ Polityki	Protokół	RDP \$	℅ Gniazda nasłuchiwania		Protokół	RDP
🕹 Do pobrania	Bezpieczeństwo	Enhanced RDP Security (TLS) + NLA	n- Modyfikatory haseł		Bezpieczeństwo	Enhanced RDP Security (TLS) + NLA
A Raporty	•		Polityki			
■ Produktvwność	Anonimowy		📩 Do pobrania		Komunikat	
Ilstawienia	Pytaj o powod logowania		Raporty			
Svstem	Opis		Produktywność			
🕸 Konfiguracia sieci	Uprawnienia		Ustawienia	Uprawnienia		
Powiadomienia	Uprawnieni użytkownicy	ି ର୍	 System Konfiguracia sieci 			
Znakowanie czasem			Powiadomienia	Uprawr	ieni użytkownicy	
 Zewnetrzne uwierzytelnianie 	Host docelowy		C Znakowanie czasem	Połączenie		
III Zewnetrzne repozutoria baseł	Adres	Port 3389	& Zewnetrzne uwierzytelnianie	l ſ	Tryb połaczenia	
	Certyfikat serwera	٥	III Zewnętrzne repozytoria haseł			
E Konie zanasowe i retencia		_	Zasoby			
Klaster			Kopie zapasowe i retencja			
⇒ Synchronizacia I DAP			📥 Klaster			
		SHA1	Dziennik zdarzeń		_	
© 0:58:46.7467451.12345678 ♦ 2.1-23500 Nie skonfigurowany						C Przywróć 🗸 Zapisz
	Pośrednik		7 days 12345678			
	Tryb połączenia	\$*				
		C Przywróć Zapisz				

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 wersji3.0.

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></konto></typ>	Pobierz hasło do wybranego konta.
	typ:
	• direct - połączenie bezpośrednie, niemonitoro-
	wane;
	• fudo - połączenie monitorowane przez moduł
	PSM
Opcje	
-c <ścieżka>	Użyj pliku konfiguracyjnego znajdującego się we wska-
	zanej lokalizacji.
cfg <ścieżka>	
-	Wyćwietl liste opcji i peremetrów wywołanie skryptu



- 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.

Zarządzanie <	Fudo		
Jashboard	Użytkownik	ි Kopiuj użytkownika	
🖽 Sesje			
😁 Użytkownicy	Ogólne		
🖂 Serwery		ID	848388532111147042
🖉 Konta		Synchronizacja z LDAP	0
Sejfy		Login	fudopv2
n Gniazda nasłuchiwania			
h- Modyfikatory haseł		Zablokowane	0
🛡 Polityki			(T.).)
🛓 Do pobrania		Ważność konta	Bezterminowe
🔒 Raporty		Rola	user
■ Produktywność			(-)
Ustawienia		Preferowany język	Kliknij, aby otworzyć właściwości sejfu
😂 System		Sejfy	portal
¢ ^e Konfiguracja sieci			
🖂 Powiadomienia		Pełna nazwa	fudopv2

• Zaznacz opcję Pokaż hasło.

Polityka czasu dostępu	×
Włącz politykę czasową 💿 Pokaż hasło 😰	
Zaznacz opcję, aby umożliwić pobieranie haseł 📃 23:59	
Poniedziałek	
Wtorek	
Środa	
Czwartek	
Piątek	
Sobota	
Niedziela	
Anuluj	ОК

- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz Hasło lub Hasło jednorazowe.
- Dla uwierzytelnienia hasłem, wprowadź hasło w polach Hasło i Powtórz hasło.
- \bullet W sekcjiAPI,kliknij ikon
ę+i wpisz adres IP serwera, na którym uruchamiany będzie skrypt
 <code>fudopv</code>.
- Kliknij Zapisz.

4. Wykonaj komendę fudopv getcert, aby zainicjować konfigurację narzędzia.



5. Otwórz plik fudopv.cfg, aby skonfigurować skrypt pobierania haseł.

• •	📄 .fudopv — vi fudopv.cfg — 148×40
[FUDO] address=10.0.45.47 cert_path= <cert_path></cert_path>	
#[CONN] bind_ip=10.0.1.35	
[AUTH] username=fudopv2 #otp=/Users/zmroczkowski/.fudopv/otp.txt secret=/Users/zmroczkowski/.fudopv/secret.txt ~	

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 ha-
	słem.

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:

```
[FUD0]
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.

	😭 zmroczkowski — -basł	n — 148×40
cG9ydDEjMCEGA1UEAwwaRIVETyBUZW1wb3JhcnkgQ2Vyd hkiG9w0BCQEW0HN1cHBvcnRAd2hIZWxzeXN0ZW1zLmNvb NDJaFw0yNjA1MzAw0DE4NDJaM1HoMQswCQYDVQQGEwJQT NDk1MRQwEgYDVQQIDAttYXpvd2IIY2tpZTERMA8GA1UEB BgNVBAKMDXVsLk9jaG9ja2EgMUYxITAfBgNVBAoMGFdoZ IHogby5vLjEWMBQGA1UECwwNV2hIZWwgU3VwcG9ydDEjM ZW1wb3JhcnkgQ2VydGImaWNhdGUxJzAlBgkqhkiG9w0BC ZWxzeXN0ZW1zLmNvbTCCAiIw0QYJKoZIhvcNAQEBBQADg dSr7DqZ4kVuJoI7V/jhVIXA0CRpY5IFbcKHiNGFXn3vBu ZfRcWJ8HbpoVWo6qFYKGmpr0esRLR71301Xs0vzNNfsmq ZqpydVbAcmr0u7ZSIjsFbd2LEFyULme9cIsd3e808kLY0 WABvInzUrgbqrvaJKeIU37LTRyHZCa5/o1auxnp+EwI0m j+p0i0KXfYN9cJ3+950QYfupMPSN9dF/0+lbaThrRnqm5 dX1bJ/tUyAI7VDru7Vyn09/uUNtcJm7/8nifVda4WIN0a +bs+0ziLarQqMH27MWK6c7XXN4+PDqVnNNk0Q09f0YZYr 5mv00L200CAQNKJJ7D/TtR9vpJBDv9PXV67+p2ZAty9as 3rPQH2nC6WAW9CdI4GX1mxhey0Da5f1EJ0eEwEAX0XzDe 0jbYn2NI9ICfFCo71bGDAKAIDI2Z1100uaGSX9tBKTgLG yN/snn45UdwvWzyk9BM84z/0w+Rr?cPjLtVDSzdHAgMBA MA&wKQVJYIZIAYb4QgENBBwWGkZVRE8gVGVtcG9YX35I A1UdDgQWBBSXBvJ7BT1XBe8BxZHvQK9ILSnTbTAfBgNVH B88BxZHvQK9ILSnTbTANBgkqhkiG9w0BAQFAA0CAgEAq N513mrd2J0nxGBNMaohdTq7ZIL0XRRc5szrZXyhK1Vx1t Ur2s9hwABwSKEujrIpnT+rukq8BCEyDvCjucr3GVub/xe AMj10Yi2PTjyo15v9WixQA741IJP4nV4ed4N9gSM0cLcc IfXDqFuRs6Xj2zaczYQWK6RgBL600yng3t5Ey1vScHyT rLAxcjdGK+Aq7rPIJIMwz1vxtrrysvrDwjpq80KhNdU59 aB5BFJNW/Hmn7GghTMc+vBFTIkt5fXd2+TGdtinZaX7rd Li4To1oSTL/3VtbrzVdXqT80piLF23IAKMWhDkeqZPwqG cwdrsUShy01DZ0A1bHUyzc0G/s9NMasNctqkc29iRypnP ZVwKX0ftGZAx3YB0LH0kbQwCzEzwFXdpGBEzwiYE9JFm kqdng0QQNKiuojE9KKZT242T+32UwUpfJjfkhNazHQ4A yf0IGHrrafLJ9Qg2dtNhJo= END CERTIFICATE	GImaWNhdGUxJzAlBgkq TAeFw0xNjA2MDEwDDE4 DEPMA0GA1UEEQwGMDIt wwIV2Fyc3phd2ExFjAU WVsIFN5c3RlbXMgU3Au CEGA1UEAwwaRlVETyBU QEWGHN1cHBvcnRAd2hl gIPADCCAgoCggIBALc4 eNr9opedj/bwFiqD4p+ P2vC9wKHq1LKDwdBMKE femZBCcy0++AXvCNhE0 gI0RqwosQxZFoR0w5Fj NPXUMxUS5oBdxmcdbJL Qe43nynMuaAYb3fxJLC 4UP+7pDFBFFXY0N0qSI jAq/Iu6uXmmg8Tb/8MY Gzq/ZR7562Cbwe6he0c drllFKrJo7zjWEo400Y AGjeDB2MAkGA1UdEwQC ENLcnRpZmljYXRIMB0G SMEGDAwgBSXBvJ7BT1X PzZVty1N6UsD5oKUQj7 IJa1andttGBGTqi7eVp +ssCHjAXHqXxevX7Txn eQmEDjaNzvIUW1zZYhs KXSRLuha0Atav51LJmi xFgnxG6g3EAE9V802gA kH7JRK9p9G2j8Zrc5HT mhw0xcnTgSEu3yA1T2e uhQAZLfCDxPgiNv/LFx NGVIm21lzHz3rdXLkwX eQ1FzQ8H5HFzz7uhx7N	
SHA1 Fingerprint: 2cba43a291fdcf71849ae1dfa9e Do you want to accept this certificate (yes/n Certificate has been succesfully dowloaded. Configuration file has been updated. Zbigniews-MacBook-Pro:~ zmroczkowski\$	19bcfc2795df8 o)?: yes	

Informacja: Po prawidłowym wykonaniu komendy, ścieżka certyfikatu w pliku konfiguracyjnym zostanie automatycznie uzupełniona.

•••	.fudopv — vi fudopv.cfg — 148×40
[FUD0] address=10.0.45.47 cert_path=/Users/zmroczkowski/.fudopv/gui.cert.pem	
#[CONN] bind_ip=10.0.1.35	
[AUTH] username=fudopv2 #otp=/Users/zmroczkowski/.fudopv/otp.txt secret=/Users/zmroczkowski/.fudopv/secret.txt ~	
~	
~	
~	
~	
<u>~</u>	
<u> </u>	
~	
~	
~	
~	
~ 	
~	
~	
~	
~	
Ĩ.	
~	
~	
~	
~ "fudopv.cfg" 11L, 216C	

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*.

Uwierzytelnienie		
	Тур	Skopiuj hasło jednorazowe i zapisz w pliku otp.txt
Hasło j	ednorazowe	6c48b1e5d90746421e1791f41ae44f6724aa702d70c5ecc541af14bfd60db3c0
	Usuń	0

- 8. Wykonaj komendę:
- fudopv getpass direct <nazwa_konta>, aby pobrać hasło do nawiązania bezpośredniego połączenia z serwerem.

• • •	🏠 zmroczkowski — -bash — 148×40
[Zbigniews-MacBook-Pro:~ zmroczkowski\$./fudopv getpass rootZbigniews-MacBook-Pro:~ zmroczkowski\$	direct gc-konto-ssh

• fudopv getpass fudo <nazwa_konta>, aby pobrać hasło do nawiązania połączenia monitorowanego przez moduł PSM.

	🏠 zmroczkowski — -bash — 148×40
[Zbigniews-MacBook-Pro:~ zmroczkowski\$./fudopv getpo 499551c7-0c14-f8b4-5056-84e7d801b220Zbigniews-MacBoo	ass fudo gc-konto-ssh ok-Pro:∼ zmroczkowski\$

Ostrzeżenie: Prawidłowe działanie skryptu **fudopv** wymaga wyłączenia we właściwościach sejfu, opcji wymuszania na użytkowniku podania powodu logowania przy nawiązywaniu połączenia z serwerem docelowym.

ID	848388532111147017		
Nazwa	gc-sejf		
Zablokowane			
Powód logowania	Upewnij się, że opcj	a jest wyłączona	
Powód logowania Powiadomienia 🗆	Upewnij się, że opcj Otączenie do sesji Wykrycie wzorca	a jest wyłączona Zakończenie sesji Odłączenie od sesji	

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.

Management <	Fudo		🛓 admin \vee 🛛 📍
Jashboard	0 mm t		
E Sessions	General		
쓸 Users	Ena	🛯 🕖 — Włącz obsługę systemu zgłoszeń	
⊖ Servers	General	Adres IP lub nazwa domenowa serwera	
Accounts	Host add	ess dev15006 service-row com	
Դ Listeners	100100		
Safes		Port	Numer portu
+- Password changers	Bir	d to 10.0.8.192 +	Adres IP Fudo, z którego wysyłane sa żadania do systemu SeniceNow
Policies	Use	ns 💿 – Szyfrowanie połączenia z ServiceNow	są ządania do systemu Genicentow
🕹 Downloads	CA Certifi	ate O	Worai certyfikat CA
🖨 Reports		<u> </u>	
E Productivity			
Settings			
😂 System			
¢ Network configuration		SHA1	
External storage			

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_.

	Notifications	Nazwa użytkownika uprawr	iionego do dostępu poprzez interfejs API
ľ		Username	abel.tuter
ae		Password	
===			Thasio uzytkownika
	Resources		Test connection Sprawdź połączenie z systemem obsługi zgłoszeń

- 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.

Backups and retention	Template Nazwa grupy,	do której będą przypisane zgłoszenia	
Ticketing systems Gluster	Assignment group	IT Securities	
	Description	Zażółcić gęślą jaźń - taki opis.	– Tytuł zgłoszenia
≡ Events log	Comment	sdasd Zažółcić gęślą jaźń - taki komcio.	
5 days i00000002 ♥ servicenow-35671 L Not configured			Dodatkowe informacje zawarte w zgłoszeniu
	Fudo address	asd	
		URL Fudo używany do generowania dołączanych do	odnośników o 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 📕.

Fudo								admin 🗸
🖻 KONTA	_							
	<i>E</i> / L	ISTA KO	NT					
		NAZWA	TYP	NAZWA SERWERA	GNIAZDO NASŁUCHIWANIA	ADRES HOSTA	PROTOKÓŁ	SEJF
	⊛≣	⊕i≣ servicenow regular servicenow 10.0.235.3:22						
	-	P Wnioskuj o dostęp do wybranego sejfu 10.0.8.75:2222 ssh					servicenow	
	P.				servicenow	10.0.8.175:2222	ssh	servicenow

3. Zdefiniuj przedział czasowy i kliknij OK.



Informacja: Kliknij ikonę ^(C), 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 ikona **4**.

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.

Access time po	licy for user abel tu	Zaakceptuj żądanie o	dostęp
C: Kupid) użydław		Odrzuć żądanie o	dostęp
Zgłoszenie INC00	010033	ptuj X Odrzuć	Т
Zablok	owane 💽 🔿	dblokuj dostęp	- 1
Od		Określ interwał czas	
Włącz politykę cz	asową 🗌	Pokaż hasło	
00:00		23:59	- 1
Poniedziałek			- 1
Wtorek			- 1
Środa			- 1
Czwartek			- 1
Piątek			
Sobota			
Niedziela			
		Anuluj	ок

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.

Połączenie			
Tryb połączenia	Pośrec Adres IP, na którym nasłuchuje Fudo	¢ik	
Adres lokalny	10.0.150.151 ¢ Port 222	*	
Certyfikat TLS	BEGIN CERTIFICATE MIICOTCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgNV BAMMCXNzaF9wcm94eTAgFw0xNzExMjgxMTM5MzFaGA8yMDY3MTEyODExMzkzMVow FDESMBAGA1UEAwwJc3NoX3Byb3h5MIIBIJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB CgKCAQEAoknjS0KL1NaQfXxI9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFRxM +5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGhVBj4+B1O9zahwLVftDxTpH+MULK AYCb5Gd33GLS721RLWKO3jOwwwFICNW/3w/HHjiAKJq1XbGD3LcBRO1c6UjNKo8e 51SHUCxIY0Z/b+o0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hIgZ 1/J0WBPL/dC4eSIBAc/OfBingDa/JOgia+856aBMmbH22GbPUIYYZMBcOmgMZ+kowk		
	ssh_proxy Com	mon Name	
	82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a	SHA1	

3. Wprowadź numer portu zgodnie z definicją w obiekcie.

Połączenie			
Tryb połączenia	Pośrednik	Numer portu nasłuchiwa	nia 🕂 🔹
Adres lokalny	10.0.150.151	Port 222	
Certyfikat TLS	BEGIN CERTIFICATE MILCOTCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBQxEjAQBgN BAMMCXNzaF9wcm94eTAgFw0xNzExMjgxMTM5MzFaGA8yMDY3MTEyODExMzkzMVow FDESMBAGA1UEAwwJc3NoX38yb3h5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB CgKCAQEAoknjS0KL1NaQfXyxI9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFRxM +5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGhVBj4+B109zahwLVftDxTpH+MULK AYCb5Gd33GLS721RLWKO3JOwwwFICNW/3w/HHjiAkJq1XbGD3LcBR01c6UJNKo8e 51SHUCxIY02/b+o0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hIgZ TI (GWBPL 4G46SIBack/0RBingD_JOQia+8b5aPMnoH72GDPU 1VyZMBcDm/M4Z.kowk		
	ssh_proxy		Common Name
	82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c	9:50:4d:13:24:d1:9a	SHA1

4. W polu wyboru typu połączenia (Connection type), wybierz SSH.

RuTTY Configuration		8 23	
Category:			
Session	Basic options for your PuTTY session		
	Specify the destination you want to connect to		
	Host Name (or IP address)	Port	
Bell	10.0.150.151	222	
Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial	Connection type: ◎ Raw ◎ Telnet ◎ Rlogin ◎ SSH	H 🔘 Serial	
	Load, save or delete a stored session Saved Sessions		
	Default Settings	Load Save Delete	
	Close window on exit: Always Never Only on clean exit		
About Help	Open	Cancel	

- 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.

General Session F	Edit Remote Desktops -
Connection name	RDP connection
PC name	10.0.150.151:1234
Gateway	No gateway configured
Credentials	
User name	Domain\user
Password	Password
Resolution	Native
Colors	True Color (24 bit)
Full screen mode	OS X native
	V Start session in full screen
	Scale content
	Use all monitors

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.

	VNC Viewer	
10.0.150.151		👤 Sign in 🗸

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

	10.0.150.151 (Fudo) - VNC Viewer	
	e'ı ida	
Login	john smith	
	Jonn_omzen	
Password	**************************************	.n



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.

🖵 Connect to Server		×
	SQL Server	
Server type: <u>S</u> erver name: <u>A</u> uthentication: <u>L</u> ogin: <u>P</u> assword:	Database Engine 10.0.150.150 SQL Server Authentication john_smith	
Microsoft SQL Server Management Studio File Edit View Debug Tools Window Object Explorer Connect * * * * * • • • • • • • • • • • • • •	v Help Query ∰ A A A A A A A A A A A A A A A A A A	Quick Launch (Ctrl+Q) P = 🗈

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.

 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: emO
Internal IP address and netmask for em0: 10.0.8.201/16
Interface with an access to the Internet: emO
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\dots

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 uru- chamia 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.
chamia 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 połą-	Objawy:	
czenia z serwerem	• Użytkownik nie może się zalogować.	
	Podłączanie pulpitu zdalnego	
	Sesja usług pulpitu zdalnego została zakończona.	
	Połączenie z komputerem zdalnym zostało utracone, prawdopodobnie z powodu problemów	
	z łącznością sieciową. Spróbuj ponownie połączyć się z komputerem zdalnym. Jeśli ten problem będzie nadal występował, skontaktuj się z administratorem sieci lub pomocą	
	techniczną.	
	OK Pomo <u>c</u>	
	• 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 posrednictwem którego re-	
	niesktuslne dane logowania	
	meaktuame dane logowama.	
	Objawy: komunikat w dzienniku zdarzeń: Unable to establish	
	connection to server zbigniew (10.0.35.53:3399).	
	Przyczyna: błędna konfiguracja serwera.	
	• Zwerufikuj poprawność definicji danego serwera (adres IP	
	• Zwerynkuj poprawnose dennicji danego serwera (adres ir, 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 <i>Ping</i> i wykonaj polece-	
	nie, żeby sprawdzić osiągalność hosta.	
	• Sprawdz, czy serwer jest osiągalny pod wybranym nume-	
	1 Zalogui sie do papelu administracyjnego Wheel Fudo	
	PAM.	
	2. Wybierz Ustawienia > System, zakładka Diagnostyka.	
	3. w sekcji <i>Netcat</i> , wprowadź adres IP serwera wraz z nume-	
	rem portu wybranej usługi i wykonaj polecenie.	

Problem	Objawy i opis rozwiązania	
Przy próbie logowania nie wszyscy użytkownicy wi- dzą 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 docelo- wego.	
	Rozwiązanie: zmień dane logowania w konfiguracji obiektu serwera.	
	 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: <i>TLS certificate verifica- tion failed.</i> 		
	Rozwiązanie:		
	Poblerz nowy certyfil lowy.	kat serwera docelowego w sekcji <i>Host doce</i> -	
	Host docelowy		
	Adres Certyfikat serwera	10.0.40.101 Port 3389 Kliknij, aby pobrać aktualny certyfikat serweraBEGIN CERTIFICATE	
		MIIC3JCCAcagAwiBAgiQXQNZYnFJjKxHiLthDjAz5DANBgkqhkiG9v0 BAQUFADAY MRYwFAYDVQQDEw1kYzludGVjaDlud2hsMB4XDTE0MDgxODA3Mz M0M1oXDTE1MDlx NzA3MzM0M1owGDEWMBQGA1UEAxMNZGMyLnRiY2gyLndobDCC ASiwDQYJKoZlivcN AQEBBQADggEPADCCAQoCggEBAL35s9kUsbnBzgnBAfgeBaZg5D CrBgxhdWecHR1X n0RAcCwPK6oUt/Ck1NxDehpHi6IUYrZ3asWVnmmVRzehjcgyauXKk5	
		81:1b:d8:2d:8e:e7:5e:64:e5:ae:e9:47:b0:3e:f1:d5:17:eb:92:72 SHA1	
	 Objawy: Po wpisaniu na nie połączenia. Wpis w dzienni Rozwiązanie: spraw ściach TCP-Rdp, op FIPS Compliant. 	azwy użytkownika i hasła następuje zerwa- iku zdarzeń: <i>RDP connection error</i> . wdź czy w zakładce <i>General</i> we właściwo- cja <i>Encryption level</i> nie jest ustawiona na	
Brak połączenia z serwe- rem	 Objawy: Nie można zal user0 not allou w dzienniku za user0 not allou 	logować się do serwera, komunikat User ved to connect to server. darzeń wpis: Authentication failed: User ved to connect to server.	
	Przyczyna: użytko Rozwiązanie: doda połączenia.	wnik nie jest dodany do połączenia. aj użytkownika do odpowiedniego obiektu	

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=848388532111147010) ~is~blocked.
	Przyczyna: użytkownik jest zablokowany w Wheel Fudo PAM.
	Rozwiązanie: odblokuj użytkownika.
Uzytkownik musi logować	Objawy: uzytkownik łącząc się poprzez protokół RDP wpi-
sıę dwukrotnie	suje login i hasło po czym po chwili jest proszony o ponowne
	wprowadzenie danych autoryzujących.
	Przyczyna: serwer stanowi część infrastruktury zarządzanej
	przez broker połączen, ktory wykrył istniejącą aktywną sesję
	uzytkownika na innym serwerze.
	Obionary udutkonnik nomiozuica nakozania COII
	dono logowania na ozum nonownia programy jest a jeh podania
	Przyczyna: w obiekcje <i>notaczenie</i> właczone sa opcje zastone
	wania loginu i hasta ale te pola ich definicii pozostawione sa
	pusta co skutkuje podwójnym uwierzytalnianiem – w pierwszej
	kolejności przed Fudo, w drugiej przed serwerem docelowym
	kolejnoser przed i ddo, w drugiej przed serwereni docełowym.
Nie można nawiazać poła-	Objawy:
czenia z serwerem RDP	• użytkownik nawiązując połączenie RDP zostaje rozłą-
	czony chwilę po uwierzytelnieniu.
	• w dzienniku zdarzeń wpis: <i>RDP server 10.0.0.:33890 has</i>
	to listen on the default RDP port in order to redirect ses-
	sions.
	Przyczyna: serwer docelowy, na który następuje przekierowa-
	nie, nie nasłuchuje na porcie 3389.
	Rozwiązanie: skonfiguruj serwer docelowy tak, by oczekiwał
	na połączenia użytkowników na porcie 3389.
	Objawy:
	• w dzielninku zdarzen wpis: User usero nas no access to host 100 168 0 1:2280
	11051 192.100.0.1.3309
	Przyczyna: broker stwierdza, że użytkownik ma aktywna sesie
	na innym serwerze i iniciuje przekierowanie. ale docelowy ser-
	wer nie jest skonfigurowany na Wheel Fudo PAM lub użytkow-
	nik nie jest uprawniony do nawiazywania połaczeń z wybranym
	zasobem.
	Rozwiązanie:
	• Upewnij się, że obiekt serwera jest dodany do Fudo.
	• Dodaj użytkownika do odpowiedniego <i>sejfu</i> .

Problem	Objawy i opis rozwiązania
Nie można nawiązać po- łączenia z serwerem Tel- net5250 poprzez aplikację PC5250 w wersji 20091005 S oraz 20111019 S	Objawy: próba nawiązania połączenia kończy się niepowodze- niem.
	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 <i>TCP</i> i numerach portów odpowiednio 449, 8470 i 8476. Dodaj gniazdo nasłuchiwania <i>TN5250</i>, w trybie <i>Pośrednik</i>, z domyślnym numerem portu. Dodaj trzy gniazda nasłuchiwania <i>TCP</i>, w trybie <i>Pośrednik</i>, z numerami portów odpowiednio 449, 8470 i 8476. Dodaj konto typu <i>regular</i>, określ parametry uwierzytelnienia i przypisz do głównej definicji serwera TN5250. Dodaj trzy konta typu <i>anonymous</i> 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 poprawny. Ustaw adres IP Wheel Fudo stępując zgodnie z instrukcją <i>terfejsów sieciowych</i> w dokur PAM. Upewnij się, że adres IP ma w Wheel Fudo PAM. 	adres Wheel F PAM z poziom w rozdziale <i>Ka</i> nentacji system vłączoną funkcj	udo PAM jest u konsoli, po- onfiguracja in- u Wheel Fudo ję zarządzania	
	III Dashboard	Interfejs	Nazwa i DNS	Tablica tras
	🖽 Sesje			
	曫 Użytkownicy	% net0 08:0	00:27:6A:A3:A9	
	A Serwery Panel administracyjny FUDO) dostępny pod wskaz	anym adresem IP	
	•f Bastiony	10.0.40.50	/ 16	×
	🕂 Połączenia	10.0.40.51	/ 16	×
	Polityki	+		
	🕹 Do pobrania			
	A Raporty	% net1 08:0	00:27:9C:12:05	

21.4 Odtwarzanie sesji

Problem	Objawy i opis rozwiązania
Nie można odtworzyć wy-	Przyczyna: brak odpowiednich kodeków wideo.
eksportowanego materiału	
	Rozwiązanie: zweryfikuj czy masz zainstalowane odpowiednie
	oprogramowanie.
Użytkownik administrator	Objawy: na liście sesji nie ma spodziewanych pozycji.
nie widzi sesji	
	Przyczyna: brak stosownych uprawnień.
	Rozwiązanie: nadaj użytkownikowi uprawnienia do określo-
	nego obiektu połączenia, serwera oraz użytkownika.
Nie można odtworzyć sesji	$\mathbf{Objawy:}$ komunikat: Nie można odnaleźć danych sesji.
w odtwarzaczu	
	Przyczyna: połączenie miało miejsce przy wyłączonej opcji
	rejestrowania sesji.
	Rozwiązanie: włącz opcję rejestrowania sesji, aby w przyszło-
	ści mieć możliwość odtworzenia materiału.

21.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na	Objawy: Obiekty utworzone na jednym węźlę, nie pojawiają
drugi węzeł	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	Objawy:	
znacznikiem czasu	• Komunikat w dzienniku zdarzeń: <i>Timestamping service communication error</i> .	
	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 O przy wybranej sesji. 	
	Przyczyna: Problem z funkcjonowaniem usługi znakowania	
	czasem.	
	Rozwiązanie: Zweryfikuj poprawność konfiguracji usługi zna-	
	kowania 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.

Indeks

Symbole

4 eyes proxy, 292

А

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

В

blokowanie serwery, 158 broker połączeń RDP, 412 broker połączeń RDP, 45

С

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

 ${\tt fudopv},\, {\bf 412}$

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**

Η

Haslo 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
```

Κ

```
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

Μ

```
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

0

odblokowanie serwery, 159 Odcisk Palca, **410** Oracle protokoły, 7 protokół, 7 serwery, 142

Ρ

polityka, 411 polityka czasowa, 411 protokoły Citrix StoreFront, 4 HTTP, 5ICA. 5 Modbus, 6 MS SQL (TDS), 6MySQL, 6 Oracle, 7 RDP, 7SSH, 8 TCP, 11 Telnet, 9 Telnet 3270, 8 Telnet 5250, 9 VNC, 9 X11, 10 protokół Citrix StoreFront, 4 HTTP, 5ICA, 5Modbus, 6 MS SQL (TDS), 6MySQL, 6 Oracle, 7 RDP, 7SSH, 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, 14pośrednik, 16 wymuszony routing, 14 sejf, **411** sejf anonimowy, 411 serwer, 411serwer dynamiczny, 412 Serwery, 411 serwery blokowanie, 158 Citrix, 131 dodawanie, 131 dynamiczne, 156 HTTP, 132ICA, 134 konfiguracja, 130 Modbus, 136 modyfikowanie, 157 MS SQL, 138 MySQL, 140odblokowanie, 159 Oracle, 142RDP, 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, 240SSH, 410 SSH gniazda nasłuchiwania, 201 protokoły, 8 protokół, 8 sshserwery, 146 synchronizacja użytkowników, 122 konfiguracja, 122 Syslog, 410 systemy zewnętrznego uwierzytelniania, 299dodawanie serwera, 300 modyfikowanie serwera, 301 usuwanie serwera, 302

Т

```
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
Х
X11
```

```
protokoły, 10
protokół, 10
```

Ζ

```
zewnętrzny serwer uwierzytelnienia, 412znacznik czasu, 412
```