Integracja systemu ADS z systemem FUDO

STM SOLUTIONS

Dane firmy
STM Solutions Sp. z o. o. Sp. k.
ul. Równoległa 2
02-235 Warszawa
+48 22 823 72 18
kontakt@stmsolutions.pl

Data powstania dokumentu
14.12.2018

Data ostatniej aktualizacji
25.03.2019

Wersja
1.1

Autor
STM Solutions

Klasyfikacja
Publiczna dokumentacja techniczna

Spis Treści

O dokumencie

Niniejszy dokument opisuje zakres integracji systemu ADS z systemem FUDO. W dalszej części dokumentu wymienione są dokładne obszary oraz sposoby, w których wykonana została integracja. Ponadto pokazane są przykładowe rozszerzone funkcje, ukazujące dodatkowe wartości płynące z integracji systemu ADS z systemem FUDO.

Integracja komunikatów syslog

Monitorowane obszary

Integracja sytemu ADS z systemem FUDO ma na celu pozyskiwanie zarówno intersujących informacji o prowadzonych sesjach zdalnych użytkowników, a także stanie samych urządzeń oraz monitorowanie zmian administracyjnych. Poniżej prezentowane są zagadnienia możliwe do monitorowania dzięki wykonanej integracji po syslogu:

- Wykrywanie nieudanych prób nawiązania sesji

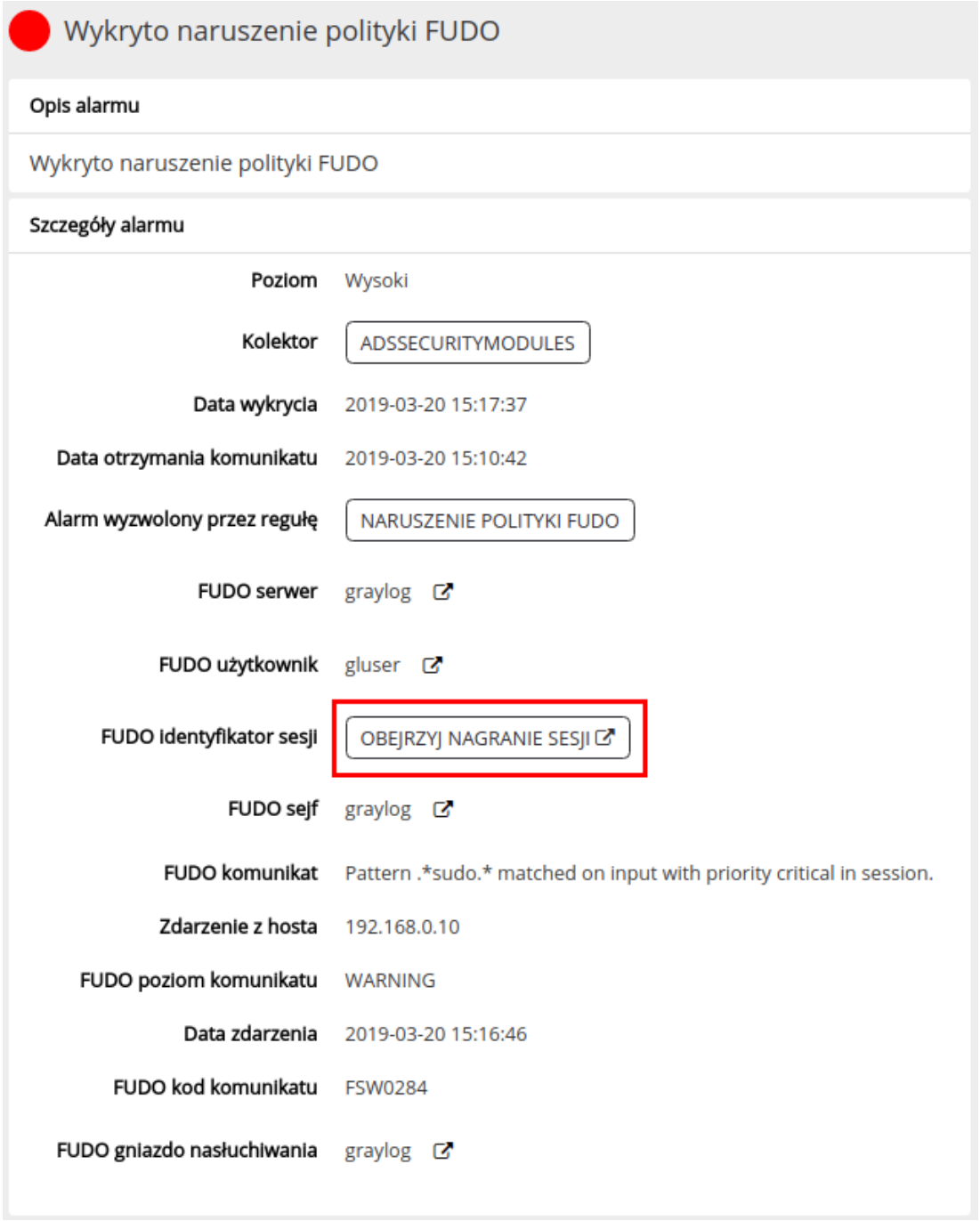
Użytkownicy korzystając z systemów zdalnych za pomocą systemu FUDO, nie zawsze muszą działać w sposób zgodny z przeznaczeniem. Dzięki integracji z systemem ADS, istnieje możliwość wykrywania prób nawiązania sesji, do których np. użytkownik nie miał pewnych praw lub uprawnienia zostały mu odebrane.

- Wykrywanie problemów technicznych z sesjami

Kolejny z obszarów integracji dotyczy możliwości wykrywania problemów technicznych związanych z prowadzonymi sesjami. Wykrywane problemy mogą być poddawane analizie, która ma na celu usunięcie problemów, w niektórych przypadkach jeszcze przed ich zauważeniem przez użytkowników systemu.

- Monitorowanie naruszeń polityk FUDO

Integracja pozwala na wykrywanie naruszeń polityk skonfigurowanych w systemie FUDO. Dzięki temu istnieje sposób szybkiego wykrywania oraz powiadamiania w przypadku problemów bezpieczeństwa w sieci firmowej (dzięki wykorzystaniu części SIEMowej ADS) oraz w systemie FUDO. W ramach każdego alarmu istnieje możliwość szybkiego przeskoczenia do podglądu sesji w systemie FUDO. Poniżej prezentowany jest przykładowy alarm z wykrycia naruszenia polityki:



- Monitorowanie nowych sesji

W niektórych przypadkach może istnieć możliwość monitorowania aktywności użytkowników w ramach poprawnie nawiązanych sesji. Przy wykorzystaniu systemu ADS istnieje możliwość przeszukiwania również archiwalnych wpisów o prowadzonych sesjach zdalnych w celu np. oszacowania ilości połączeń konkretnego użytkownika lub do konkretnego systemu.

- Śledzenie logowań administracyjnych

Integracja umożliwia także monitorowanie logowań na konta administracyjne do samego systemu FUDO. Mechanizm ten umożliwia szacowanie ilości wykonywanych logowań oraz ich ilości w zadanym czasie.

- Monitorowanie zmian konfiguracji

Kolejna z integracji umożliwia śledzenie zmian konfiguracyjnych przeprowadzanych w systemie FUDO. Istnieje możliwość wglądu w przeprowadzone zmiany konfiguracji oraz określenie czasu i ilości wykonywanych operacji.

- Monitorowanie stanu systemu

Integracja umożliwia monitorowanie stanu systemu w kontekście poprawności i stabilności działania. Wszelkie komunikaty o błędach i ostrzeżeniach są przesyłane do systemu ADS, w celu umożliwienia jak najszybszej reakcji na zaistniałe problemy.

- Monitorowanie stanu urządzeń

Dzięki integracji ADS ma możliwość pozyskiwać informacje o stanie urządzeń FUDO, w tym także o problemach sprzętowych np. z dyskami. Szereg rozpoznawanych alarmów może posłużyć jako centralne miejsce wczesnego wykrywania awarii sprzętowych, umożliwiając przygotowanie się do usunięcia problemów.

Połączenie komunikatów sysloga z API FUDO

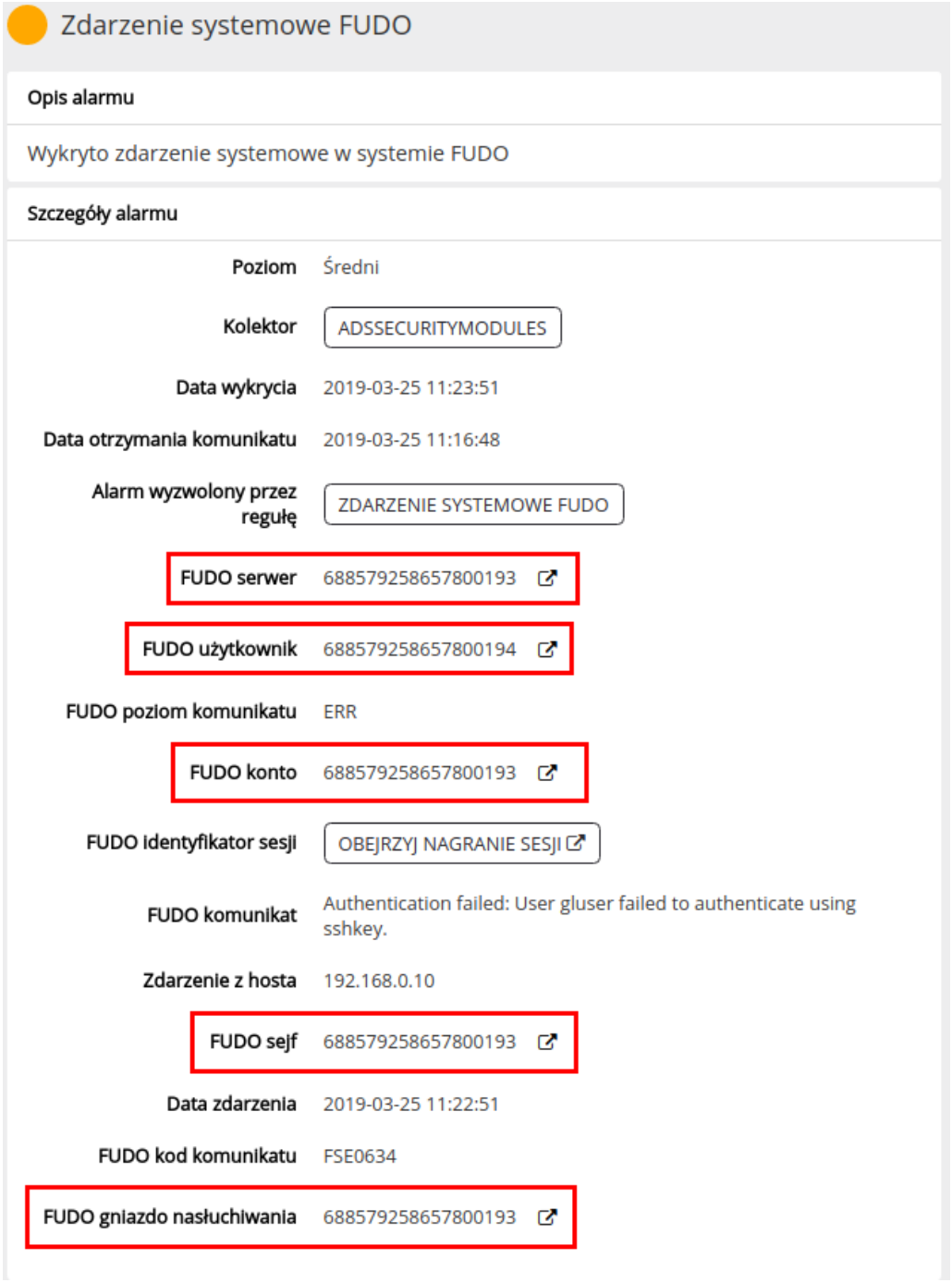
W ramach integracji komunikatów po syslogu dodana została dodatkowa funkcjonalność, która wzbogaca informacje pozyskiwane od systemu FUDO. Otrzymywane komunikaty w większości posiadają techniczne pola identyfikujące encje, które są powiązane z danym zdarzeniem. Pole to przeważnie jest identyfikatorem numerycznym w systemie FUDO, który w surowej postaci niewiele wnosi do prezentacji zdarzenia.

Wykonana integracja pozwala na rozszycie parametrów numerycznych na nazwy skonfigurowane w systemie FUDO aby móc przejrzyściej prezentować otrzymywane zdarzenia.

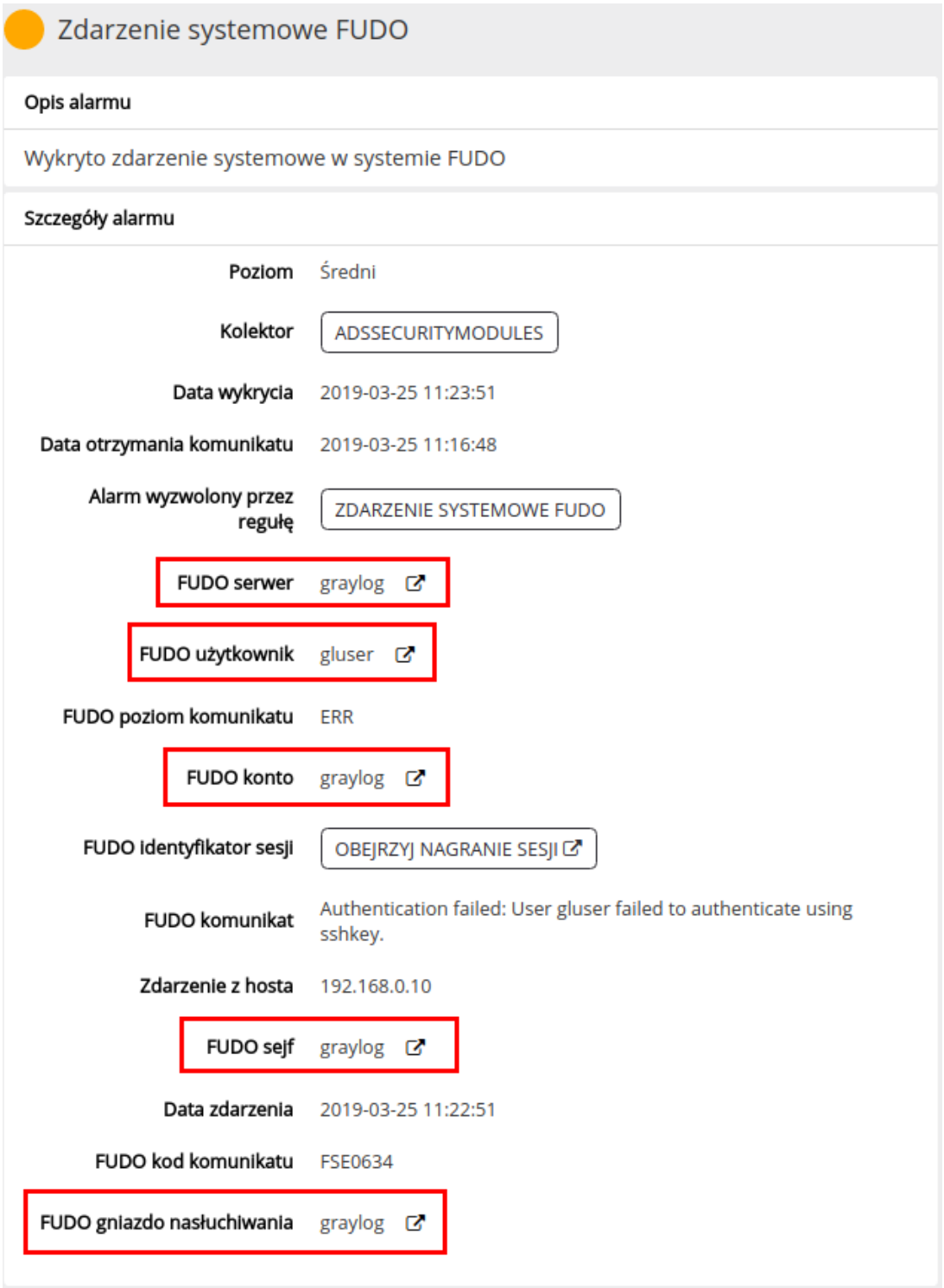
Dodatkowo przy każdej encji, dla której jest możliwość obejrzenia jej w systemie FUDO, generowany jest link, który umożliwia szybkie przeskoczenie do konkretnego rekordu konfiguracji w systemu FUDO.

Poniżej prezentowane są zrzuty ekranu z tego samego alarmu dla komunikatu pozyskanego poprzez syslog. Pierwszy ze zrzutów pokazuje alarm bez wykorzystania API, drugi natomiast ukazuje alarm z włączonym dostępem do API.

Alarm bez włączonej komunikacji API:



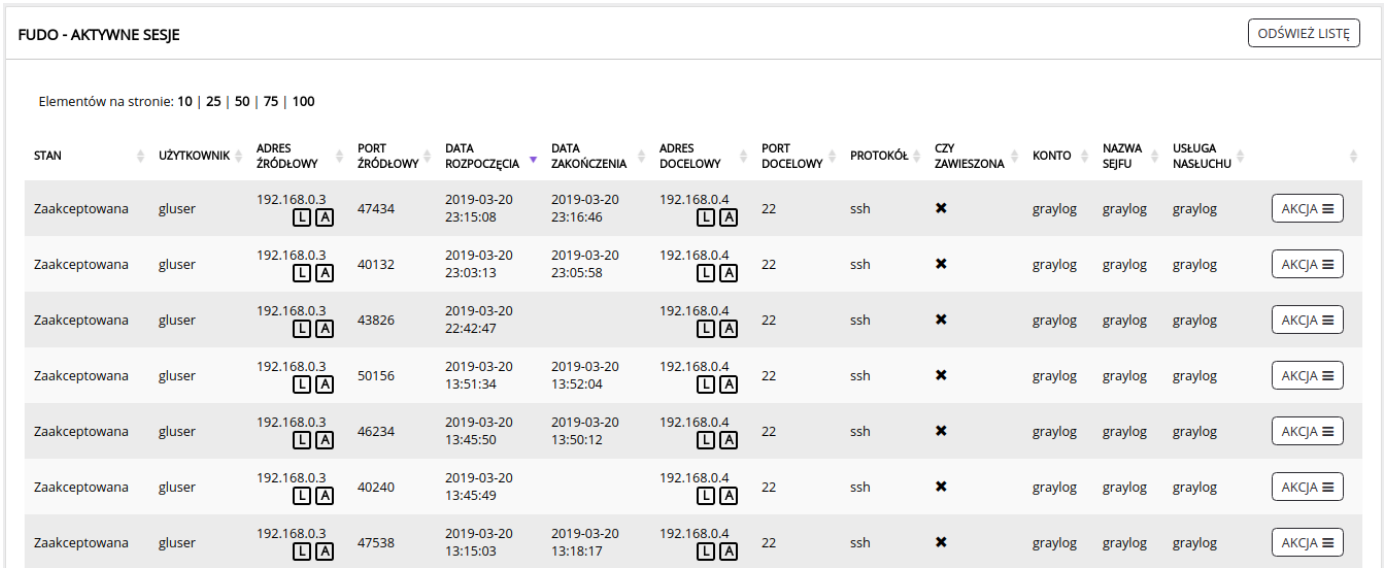
Alarm z włączoną komunikacją API:



Integracja z API FUDO

Lista aktywnych sesji

Integracja z API FUDO umożliwia prezentowanie listy aktywnych sesji bezpośrednio w oknie systemu ADS. Każda nowa sesja jest automatycznie dołączana do okna listy sesji. Poniżej prezentowany jest zrzut ekranu prezentujący przykładowe sesje:



FUDO - AKTYWNE SESJE

ODŚWIEŻ LISTĘ

Elementów na stronie: 10 | 25 | 50 | 75 | 100

STAN	UŻYTKOWNIK	ADRES ŹRÓDŁOWY	PORT ŹRÓDŁOWY	DATA ROZPOCZĘCIA	DATA ZAKOŃCZENIA	ADRES DOCELOWY	PORT DOCELOWY	PROTOKÓŁ	CZY ZAWIESZONA	KONTO	NAZWA SEJFU	USŁUGA NASŁUCHU	
Zaakceptowana	gluser	192.168.0.3 L A	47434	2019-03-20 23:15:08	2019-03-20 23:16:46	192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	40132	2019-03-20 23:03:13	2019-03-20 23:05:58	192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	43826	2019-03-20 22:42:47		192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	50156	2019-03-20 13:51:34	2019-03-20 13:52:04	192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	46234	2019-03-20 13:45:50	2019-03-20 13:50:12	192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	40240	2019-03-20 13:45:49		192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA
Zaakceptowana	gluser	192.168.0.3 L A	47538	2019-03-20 13:15:03	2019-03-20 13:18:17	192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA

Rekord każdej z sesji niesie ze sobą informacje o tym kto, kiedy, gdzie i za pomocą jakiego konta się łączy do serwera zdalnego. Dodatkowo, istnieje możliwość przeskoczenia do nagrania sesji (trwającej lub zakończonej). Poniżej prezentowany jest zrzut ekranu pokazujący odtwarzanie nagrania uruchomionego z poziomu systemu ADS:

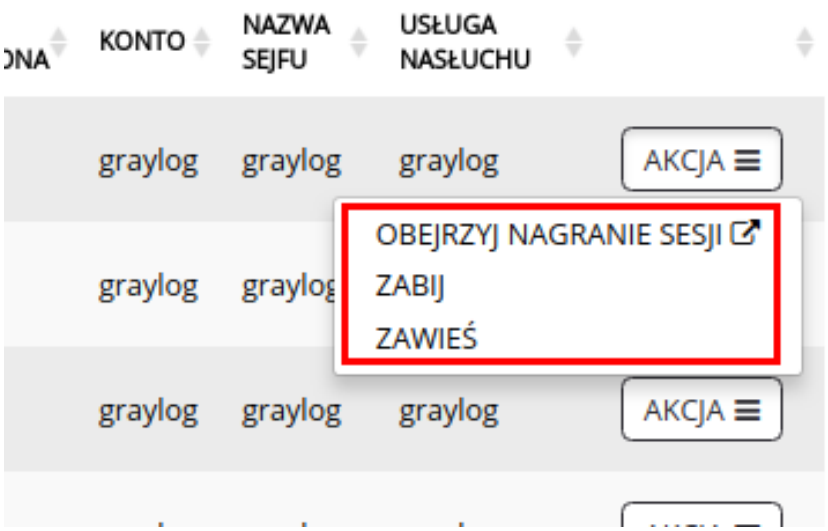
ADRES DOCELOWY	PORT DOCELOWY	PROTOKÓŁ	CZY ZAWIESZONA	KONTO	NAZWA SEJFU	USŁUGA NASŁUCHU	
192.168.0.4 L A	22	ssh	✔	graylog	graylog	graylog	AKCJA
192.168.0.4 L A	22	ssh	✖	graylog	graylog	graylog	AKCJA

Sesja 68857925865

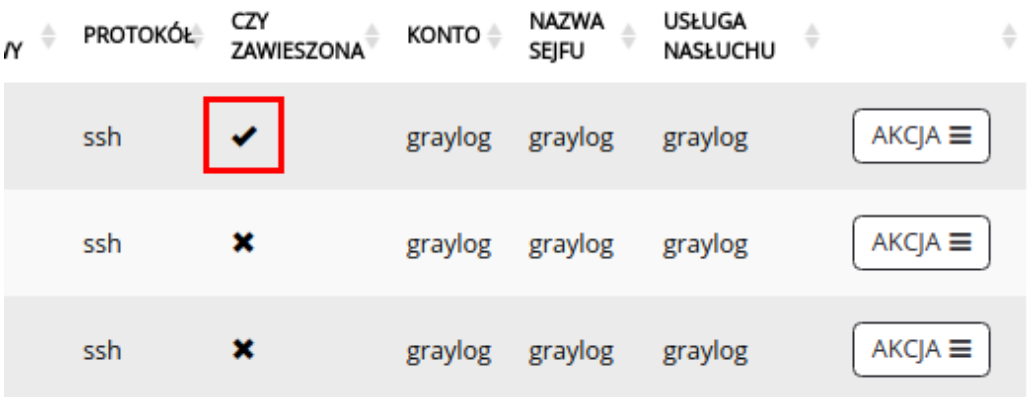
```
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

295 packages can be updated.
185 updates are security updates.


Last login: Wed Mar 20 15:26:17 2019 from 192.168.0.3
stmuser@ads-demo2-cs:~$
```

Wysyłanie komend do sesji

Sesje, którą są w dalszym czasie aktywne, pozwalają na wysyłanie do nich komend. Możliwe komendy do wysłania to „Zawieś” (pauza trwającej sesji), „Wznów” (zdejmuje pauzę) oraz „Zabij” (kończy sesję w trybie natychmiastowym). Dzięki wysyłaniu komend użytkownik może sterować sesjami bez konieczności przechodzenia do okna systemu FUDO i odszukiwania interesującej sesji. Poniżej prezentowany jest zrzut ekranu, który pokazuje dostępne menu przy rekordzie sesji:



Sesje, które zostaną zawieszone są oznaczane na liście w specjalny sposób, umożliwiający ich proste odnalezienie:



Ułatwiony rekonesans z poziomu sesji

W niektórych przypadkach nawiązane sesje mogą nie być autoryzowane – np. w przypadku utraty poświadczeń do logowania do danego serwera. W przypadku podejrzenia takiego zdarzenia, istnieje możliwość wykorzystać przyciski wyszukiwania, które są dostępne na liście sesji przy każdym adresie IP (klienta oraz serwera, do którego klient się łączy). Dostępne przyciski umożliwiają szybkie przeskoczenie do logów surowych („L”) lub alarmów ADS („A”), w których występuje dany adres IP.

W przypadku wykrycia podejrzanych logów lub alarmów z udziałem IP klienta, oznacza to, że klient został skompromitowany. Natomiast w przypadku wykrycia podejrzanych logów lub alarmów z udziałem serwera, oznacza, że atakujący wykorzystuje ją np. do pivotingu (wykonywania ataków na dalszej infrastrukturze poprzez punkt pośredniczący).

Analiza logów i alarmów w ramach systemu SIEM przyspiesza etap gromadzenia informacji o potencjalnie skompromitowanych klientach i serwerach, co przekłada się na szybszą reakcję i niezwłoczne przerwanie ataku.

STAN	UŻYTKOWNIK	ADRES ŹRÓDŁOWY	PORT ŹRÓDŁOWY	DATA ROZPOCZĘCIA	DATA ZAKOŃCZENIA	ADRES DOCELOWY
Zaakceptowana	gluser	192.168.0.3 L A	51388	2019-03-25 19:22:56		192.168.0.4 L A
Zaakceptowana	gluser	192.168.0.3 L A	47434	2019-03-20 23:15:08	2019-03-20 23:16:46	192.168.0.4 L A