Wykaz zmian w programie SysLoger

Pierwsza wersja programu 1.0.0.1 powstała we wrześniu 2011.

Funkcjonalność pierwszej wersji programu:

1. Zapis logów do pliku tekstowego,
2. Powiadamianie e-mail tylko dla wskazanych typów informacji/kategorii (alert, critical, error, warning, notice, info, debug).

– kod źródłowy programu zawiera ponad 1 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.2 (styczeń 2012):

1. Dodano definicje urządzeń, raportowanie według webfilteringu oraz logowań użytkowników,
2. Dodano powiadamianie według definicji fraz (pułapki w tekście logu),
3. Dodano wysyłanie powiadomień:
   - dla wskazanych kategorii webfilteringu,
   (…)

– kod źródłowy programu zawiera ponad 4 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.3 (marzec 2012):

1. Dodano obsługę bazy w tym tworzenie bazy, tabel, importowania z plików tekstowych, usuwania tabel, czyszczenia tabel, usuwania bazy,
2. Dodano warunkowe wykluczenia powiadomień dla adresów IP – wykluczenie działa na zasadzie wskazania ilości wystąpień w czasie (w sekundach),
   (…)

– kod źródłowy programu zawiera ponad 6 500 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.4 (marzec 2012):

1. Wersja zawiera poprawki funkcjonalne do wersji poprzedniej.

– kod źródłowy programu zawiera ponad 6 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.5 (sierpień 2013):

1. Dodano serwis PING, którego zadaniem jest sprawdzanie dostępności adresów IP w sieci wraz z powiadamianiem e-mail o braku odpowiedzi urządzenia,
   (…)

– kod źródłowy programu zawiera ponad 7 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.6 (listopad 2013):

1. Rozbudowano opcje raportu z tekstowego pliku logu o możliwość raportowania z definiowanego zakresu dat,
2. Przebudowano opcje raportu z bazy dodając opcje raportowania według wcześniej zdefiniowanych parametrów:
   - kategorii,

- webfilteringu,
(…)

3. Dodano kontrolę dla możliwych ataków.
(…)

– kod źródłowy programu zawiera ponad 10 400 wierszy.

Modyfikacje/zmiany w wersji 1.0.0.7 (listopad 2013):

1. Dodano opcje filtrowania w oknie monitora według:
- kategorii,
- urządzeń.
2. W oknie monitora dodano informację o zastosowanych filtrach,
(…)

– kod źródłowy programu zawiera ponad 11 300 wierszy.

Modyfikacje/zmiany w wersji 1.0.1.0 (luty 2014):

1. Przebudowano program dodając obsługę działania syslog'a w serwisie systemu Windows. Funkcjonalność spowodowała uruchamianie serwisów i zapisywanie logów bezpośrednio po uruchomieniu systemu Windows bez konieczności logowania. Logowanie niezbędne w zakresie uruchomienia monitora oraz powiadomień e-mail,
2. Dodano opcje sterujące uruchomieniem serwisów:
- syslog'a – odpowiedzialnego za odbiór logów z urządzeń, zapis w pliku tekstowym i/lub bazie, przesłanie logu do monitora,
- raportowania – serwis odpowiedzialny za automatyczne wygenerowanie raportu o wskazanej godzinie na podstawie logu z pliku tekstowego z dnia poprzedniego według ustalonych parametrów i przesłanie na wskazany adres e-mail,
(…)

– kod źródłowy programu zawiera ponad 18 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.1.1 (maj 2014):

1. Dodano możliwość definiowania numeru portu UDP nasłuchu monitora programu,
2. Przeniesiono opcje wykrywania ataków do odrębnej zakładki,
(…)

– kod źródłowy programu zawiera ponad 20 600 wierszy.

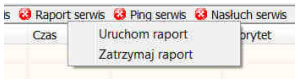
Modyfikacje/zmiany w wersji 1.0.1.2 (czerwiec 2014):

1. W głównym oknie monitora dodano:
- prezentację uruchomienia poszczególnych serwisów,
- informację o porcie nasłuchu monitora oraz uruchomienia serwisu Syslog'a,
(…)

– kod źródłowy programu zawiera ponad 21 700 wierszy.

Modyfikacje/zmiany w wersji 1.0.2.0 (czerwiec 2014):

1. W głównym oknie monitora dodano opcje szybkiego uruchomienia i zatrzymania danego serwisu

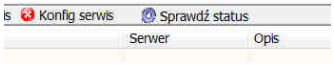


   (...)

– kod źródłowy programu zawiera ponad 23 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.2.1 (listopad 2014):

1. W głównym oknie monitora dodano przycisk wymuszenia kontroli statusów poszczególnych serwisów



2. Rozbudowano opcje wykrywania ataków o dodatkowe kontrole wielkości logu pliku tekstowego

– kod źródłowy programu zawiera ponad 23 400 wierszy.

Modyfikacje/zmiany w wersji 1.0.3.0 (marzec 2015):

1. Poprawiono kontrolę działania bazy podczas uruchamiania okna monitora programu, skrócono czas uruchamiania okna monitora,
2. Dodano informację o logach działania programu: nazwa logu, wielkość logu,
   (...)

– kod źródłowy programu zawiera ponad 24 000 wierszy.

Modyfikacje/zmiany w wersji 1.0.3.1 (kwiecień 2015):

1. Przebudowano niektóre funkcje programu optymalizując kod źródłowy i działanie serwisu syslog, uzyskano poprawę wydajności podczas obsługi bazy,
   (...)

– kod źródłowy programu zawiera ponad 24 400 wierszy.

Modyfikacje/zmiany w wersji 1.0.4.0 (sierpień 2015):

1. Wprowadzono drobne zmiany graficzne,
2. Dodano dodatkową aplikację analizującą ruch w sieci na wskazanej karcie sieciowej,
   (...)

– kod źródłowy programu zawiera ponad 27 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.4.1 (wrzesień 2015):

1. W ramach serwisu kopii konfiguracji dokonano
   - przebudowy opcji sterujących w monitorze syslog'a
   - przebudowy serwisu kopii konfiguracji
2. Dokonano optymalizacji w zakresie powiadamiania o wykonaniu konfiguracji,
   (…)

– kod źródłowy programu zawiera ponad 28 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.0 (grudzień 2015):

1. Uruchomiono nową wersję klienta … – brak ograniczenia wielkości przesyłanego pliku,
2. Dokonano zmian graficznych oraz zmian w budowie raportów wysyłanych pocztą e-mail w zakresie powiadomień o dostępności urządzeń oraz raportów podsumowujących,
3. Uruchomiono archiwizację logów,
4. Dodano możliwość wykonania kopii spakowanych plików logów do zewnętrznego repozytorium.
   (…)

– kod źródłowy programu zawiera ponad 31 100 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.1 (luty 2016):

1. Poprawa wizualna zaznaczonych opcji poprzez zmiany w prezentacji danych pokazujących zestawienia,
2. Poprawiono odczyt listy adresów IP dla klienta monitora,
3. Zwiększono kolumny dla adresu IP oraz kolumnę nazwy dla definicji webfilteringu,
   (…)

– kod źródłowy programu zawiera ponad 32 300 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.2 (luty 2016):

1. Poprawiono wysyłkę wiadomości e-mail w ramach list dystrybucyjnych,
   (…)

– kod źródłowy programu zawiera ponad 32 500 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.3 (kwiecień 2016):

1. Zmodyfikowano okno konfiguracji kontroli dostępności listy hostów (ping),
2. Zmodyfikowano procedurę kontroli dostępności hosta podczas wykonania testu uruchomianego przyciskiem „Sprawdzenie hosta",
   (…)

– kod źródłowy programu zawiera ponad 33 900 wierszy.

Modyfikacje/zmiany w wersji 1.0.5.4 (maj 2016):

1. Dodano obsługę kolejnych tabel w bazie,
   (…)

– kod źródłowy programu zawiera ponad 37 500 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.0 (październik 2016):

1. Zmiana platformy – narzędzia developerskiego– analiza, dopasowanie w tym uruchomienie funkcji i procedur w nowej wersji oraz współpracy z nową wersją komponentów,
   (…)

– kod źródłowy programu zawiera ponad 42 800 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.1 (styczeń 2017):

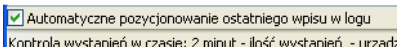
1. Dodano opcje inicjacji wersji (Opcje -> zakładka: Ogólne -> Inicjacja wersji),
2. Rozszerzono obsługę programu w zakresie komunikatów emergency,
   (…)

– kod źródłowy programu zawiera ponad 43 700 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.2 (luty 2017):

1. Poprawa prezentacji działania usługi syslog serwis w oknie monitora,

2. Dodano opcję automatycznego pozycjonowania ostatniego wpisu logu w oknie monitora,



3. Rozszerzono filtr okna logu, filtr powiadomień oraz filtr zapisu do bazy o opcje emergency,
   (…)

– kod źródłowy programu zawiera ponad 43 800 wierszy.

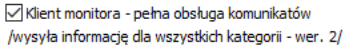
Modyfikacje/zmiany w wersji 2.0.0.3 (marzec 2017):

1. Dodano obsługę tworzenia kolejnych plików logów tekstowych w przypadku osiągnięcia wartości maksymalnej,
2. Dodano obsługę raportów w zakresie kolejnych plików logów tekstowych.
   (…)

– kod źródłowy programu zawiera ponad 45 100 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.4 (lipiec 2017):

1. Dodano obsługę przekazywania informacji do monitora przez WWW w zakresie komunikatów z urządzeń oraz kontroli dostępności urządzeń,
2. Poprawiono obsługę pliku ini w zakresie działania programu do skanowania zasobów sieci,
3. Dodano opcję pełną obsługę komunikatów przekazywanych do klienta monitora (wer. 2)



(…)

– kod źródłowy programu zawiera ponad 45 500 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.5 (październik 2017):

1. Dodano obsługę zapisu wyniku pakietu ICMP (ping) do pliku INI w celu możliwości szybkiej prezentacji w monitorze przez WWW,
2. Poprawiono odczyt parametrów po wprowadzeniu zmian w opcjach filtru rozszerzonego, dodano komunikat o możliwej konieczności restartu monitora po wprowadzeniu zmian z uwagi na bieżące użycie parametrów podczas analizy otrzymywanych komunikatów,
   (…)

– kod źródłowy programu zawiera ponad 45 700 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.6 (grudzień 2017):

1. Dodano możliwość sterowania czasem oczekiwania pomiędzy kolejnymi poleceniami PING w usłudze „Ping”: Opcje -> Serwisy -> Ping
2. Poprawiono opcje podliczają wielkość logów tekstowych zawierających informacje z urządzeń.
   (…)

– kod źródłowy programu zawiera ponad 45 800 wierszy.

Modyfikacje/zmiany w wersji 2.0.0.7 (styczeń 2018):

1. Poprawiono sposób zapisu informacji polecenia Ping do pliku wyniku (…),

– kod źródłowy programu zawiera ponad 45 900 wierszy.

Modyfikacje/zmiany w wersji 2.1.0.0 (styczeń 2018):

1. Zmiana platformy – narzędzia developerskiego (…),
2. Dodano funkcję Trace Route w opcji konfiguracji usługi polecenia Ping
   (…)

– kod źródłowy programu zawiera ponad 45 900 wierszy.

Modyfikacje/zmiany w wersji 2.1.0.1 (maj 2018):

1. Przebudowano usługę kontroli dostępności urządzeń (PING) uruchamiając wielowątkowy proces weryfikacji,
2. Poprawiono proces zerowania licznika kontroli dostępności urządzeń (PING),
   (…)

– kod źródłowy programu zawiera ponad 46 200 wierszy.

Modyfikacje/zmiany w wersji 2.1.0.2 (lipiec 2018):

1. Zmieniono sposób uruchomienia wątków dla kontroli dostępności urządzeń (PING) ustawiając priorytet wykonania na poziomie niskim (Lower) … ,
2. Podczas generowania potwierdzenia o nawiązaniu połączenia z urządzeniem (dostępność urządzeń PING) dodano dodatkową kontrolę wystąpienia ilości
   (...)

– kod źródłowy programu zawiera ponad 46 200 wierszy.

Modyfikacje/zmiany w wersji 2.1.0.3 (październik 2018):

1. Zmieniono sposób weryfikacji nawiązania połączenia (przywrócenia dostępności urządzeń) dla poleceń PING dodając zmienną czasową przy kontroli ilości błędów,
2. Dodano parametry sterujące weryfikacją kontroli poprawnych pakietów PING oraz wysyłki wiadomości e-mail …
   (…)

– kod źródłowy programu zawiera ponad 46 300 wierszy.

Modyfikacje/zmiany w wersji 2.1.1.0 (listopad 2018):

1. Dodano nową funkcjonalność – analizator występowania (…) w komunikacie w czasie. (…)
2. Syslog_klient – poprawiono odczyt i przypisanie numeru portu,
3. Syslog_services – poprawiono identyfikację nazwy urządzenia (…),
4. Dodano dodatkową opcję odpowiedzialną za wysyłanie potwierdzeń e-mail w przypadku wykrycia frazy w treści logu.
   (...)

– kod źródłowy programu zawiera ponad 52 900 wierszy.

Modyfikacje/zmiany w wersji 2.1.1.1 (grudzień 2018):

1. Poprawiono konwersję odczytanego stringu do formatu daty definiując format daty niezależnie od formatu zdefiniowanego w opcjach regionalnych dla postaci daty krótkiej (…).
2. Poprawiono zapis z pól edycyjnych RichEdit eliminując powstawanie problemu dodawania dodatkowych znaków formatujących przy zapisie do nowych plików (tworzenia plików). Problem występuję pomimo wyłączenia zapisu formatowania parametrem PlainText ustawionym na false (…).
3. Analizator - dodano nowe opcje konfiguracyjne „Opcje rozszerzone” umożliwiające uruchomienie analizy rozszerzonej, w ramach której dostępne jest:
   - (…),
   - analiza występowania portów docelowych na podstawie zdefiniowanej listy,
   - analiza występowania adresów docelowych na podstawie zdefiniowanej listy,
   - (…).

   W ramach opcji dostępne jest uruchomienie powiadamiania e-mail niezależne od uruchomionego parametru „Włącz powiadamianie e-mail” w opcji „Powiadamianie e-mail”.

   (…).

4. Analizator – rozbudowano opcje konfiguracji ogólnej dodając zakładkę obsługi tabel analizatora. W celu uruchomienia działania opcji analizy rozszerzonej niezbędne jest (…).

– kod źródłowy programu zawiera ponad 56 400 wierszy.

Modyfikacje/zmiany w wersji 2.1.1.2 (luty 2019):

1. Zmodyfikowano Raport z pliku tekstowego dodając opcje zapisu wyniku wyszukiwania bezpośrednio do pliku tekstowego i/lub prezentowania wyniku w oknie raportu. Bezpośredni zapis wyniku do pliku tekstowego bez prezentacji wyniku w oknie raportu znacznie przyśpieszył wyszukiwanie. (…)
2. Raport z pliku tekstowego – poprawiono prezentację danych w oknie raportu wyniku wyszukiwania, przed zmianą program dokonywał automatycznego skrócenia prezentowanych danych. Zastosowanie funkcji DrawItem dla elementu ListView wyeliminowało powyższy problem.
3. Raport z pliku tekstowego – dostosowano raport dostępności urządzeń do nowego sposobu weryfikacji PING oraz zapisu informacji do logu (…).
4. Serwis dostępności urządzeń (PING) – wydłużono czasy oczekiwania pomiędzy kolejnymi wywołaniami polecenia ICMP (…).
5. Archiwum logów – dodano opcje pakowania raportów wyniku kontroli dostępności urządzeń PING (…).
6. Archiwum logów – dodano opcje konfiguracyjną w zakresie godziny wykonania pakowania logów oraz przesłania do zewnętrznego archiwum (…).
7. Poprawiono obsługę kopii konfiguracji z urządzeń w przypadku pobierania plików wbudowanym klientem SFTP.
   (…)
8. Poprawiono w raporcie codziennym wyliczanie ilości wystąpień poszczególnych kategorii na podstawie zapisów w logach tekstowych,
   (…).

– kod źródłowy programu zawiera ponad 59 200 wierszy.

Modyfikacje/zmiany w wersji 2.1.1.3 (czerwiec 2019):

1. Poprawiono instalację usług w przypadku uruchomienia programu w katalogu ze znakiem spacji w nazwie (na przykład: c:\Program Files (x86)\),
2. Poprawiono kolejność przechodzenia tabulatora w opcjach:
   - powiadomienia -> opcje powiadomienia
     (…)
3. Dodano dodatkowe opcje w konfiguracji webfilteringu:
   - ustawienie zestawu kategorii dla kilku wybranych dostawców urządzeń wraz z możliwością wykonania bieżącej kopii konfiguracji,
     (…)

- kod źródłowy programu zawiera ponad 60 100 wierszy.