INSTRUKCJA

wersja 0.21

1. Informacja o programie

Program Backup S3 Kielman służy do regularnego tworzenia kopii zapasowych plików użytkownika w systemach Windows. Kopia zapasowa przechowywana jest w chmurze.

2. Słowniczek pojęć

Kopia zapasowa (backup) – kopia danych przechowywana w celu odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia. Dane są przesyłane na zasadzie synchronizacji z komputera użytkownika (zabezpieczony) do zdalnej lokalizacji (serwer backupów) po wykryciu zmian w strukturze plików (nowe pliki, usunięte pliki, modyfikacja). Z tego też powodu należy zaznaczyć, że kopia zapasowa to nie to samo, co archiwizacja danych. Jej przeznaczeniem nie jest długoterminowe przetrzymywanie kopii danych, które zostały świadomie usunięte przez użytkownika.

Archiwizacja – przeniesienie swoich danych w inne, zwykle zewnętrzne miejsce przeznaczone do ich długotrwałego przechowywania. W procesie tym dane najczęściej przenoszone są na wolniejsze nośniki danych. Dodatkowo dane mogą przed przeniesieniem być poddawane procesowi kompresji, tworzenia archiwum lub deduplikacji. Omawiane w tej instrukcji rozwiązanie nie jest przeznaczone do archiwizacji.

S3 – usługa umożliwiająca obiektowe przechowywanie danych, dostępna poprzez webowy interfejs. Usługa ma szerokie zastosowanie, jako magazyn danych dla aplikacji internetowych, archiwów czy kopii zapasowych do odtwarzania awaryjnego. Technologia została opracowana przez firmę Amazon. Wraz ze wzrostem popularności powstały konkurencyjne rozwiązania zgodne ze standardem stworzonym przez Amazona. Jednym z tych rozwiązań jest Ceph Storage wykorzystywany w projekcie Prace-Lab.

Bucket – kontener tworzony w przestrzeni S3, dostępnej dla użytkownika, do którego zapisywane są wszystkie pliki (obiekty). Bucket posiada ograniczenie rozmiaru w bajtach, definiowany przez użytkownika w ramach dostępnych dla niego limitów przestrzeni. Użytkownik ma nad każdym swoim bucketem pełną kontrolę oraz możliwość deklaracji dostępu i różnych polityk, co daje duże możliwości kontroli nad obiektami zapisanymi w buckecie.

Poświadczenia S3 – dane dostępowe użytkownika do usługi S3. Na poświadczenia składają się: Access Key – tożsamy z identyfikatorem użytkownika 20 znakowy ciąg alfanumeryczny, Secret Key – tożsamy z hasłem 40 znakowy ciąg alfanumeryczny. Access Key i Secret Key należy traktować, jako dane poufne, nie udostępniać osobom trzecim.
W poniższej instrukcji poświadczenia pobierane są z portalu użytkownika i zapisywane w pliku credentials.json w lokalizacji User/AppData/Roaming/Kielman. W credentials.json wskazany jest również bucket, do którego zapisywane będę pliki oraz adres api usługi S3, do którego ustanawiane jest połączenie.

Wersjonowanie – metoda przechowywania pliku w wielu jego kolejnych wersjach. W tej metodzie każdy plik może posiadać pewną ilość swoich poprzednich, historycznych

wersji dostępnych dla użytkownika. Taka hierarchia pozwala na prześledzenie historii zmian pliku i odzyskanie wersji sprzed momentu niepożądanych zmian lub nawet usunięcia pliku.

SSE – Server Side Encryption – jest to mechanizm szyfrowania plików. Szyfrowanie odbywa się w tym przypadku po stronie serwera, nie obciążając zasobów maszyny użytkownika. Do szyfrowania plików wykorzystywany jest dostarczony wraz z wysyłanym plikiem klucz szyfrujący – ciąg znaków stworzony przez użytkownika. Klucz szyfrujący nie jest zapamiętywany na serwerze, lecz jest zapominany po operacji szyfrowania pliku. Dlatego ważne jest należyte zabezpieczenie klucza szyfrującego przed utratą. Zaszyfrowany plik jest niemożliwy do odczytu bez posiadania klucza.

Quota – limit przypisany użytkownikowi, który może dotyczyć przestrzeni lub ilości przetrzymywanych obiektów.

Endpoint – punkt końcowy, punkt dostępowy interfejsu programu aplikacyjnego (czyli API usługi S3 Ceph), poprzez który użytkownikowi ma zapewniony bezpośredni dostęp do zasobów przetrzymywanych w chmurze.

Zarządzanie czasem życia danych (Data Lifecycle Management) – mechanizm wewnętrzny usługi Ceph S3. Jego zadaniem jest zarządzanie przepływem danych w bucketach użytkowników w oparciu o zdefiniowane – odgórnie lub przez samych użytkowników – polityki celem optymalizacji wykorzystania zasobów.

Polityka czasu życia - to zestaw reguł określający: których plików w buckecie dotyczy polityka, rodzaju plików tj. można określić czy ma dotyczyć aktualnych, czy starszych wersji, a także ich wiek w dniach oraz akcji do przeprowadzenia na tych plikach.

3. Instalacja programu

Program dostarczany jest w formie auto-instalatora. Po pobraniu i uruchomieniu instalatora należy zatwierdzić instalację, gdy zabezpieczenia systemu Windows wyświetlą monit bezpieczeństwa.
Zalecane jest pozostawienie domyślnych ustawień instalacji. Po zakończeniu procesu w Menu Start systemu Windows pojawi się folder Kielman ze skrótem do uruchamiania programu -> KielmanS3Luncher.exe oraz skrótem do deinstalacji programu. Program można również usunąć poprzez aplet *Programy i funkcje* z Panelu Sterowania Windows.

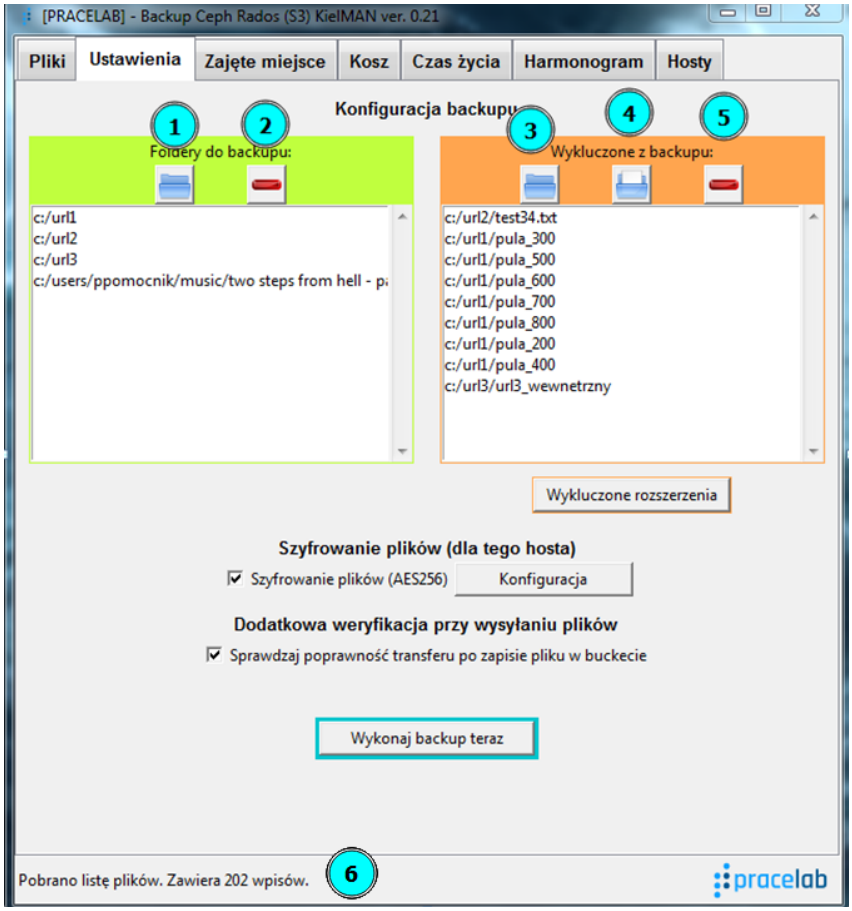
4. Pierwsze uruchomienie i konfiguracja

Aby rozpocząć użytkowanie usługi kopii zapasowej (zwanej też backupem) należy w pierwszym kroku przeprowadzić podstawową konfigurację programu.

1. Uruchomić program KielmanS3Luncher.exe. Instalator programu dodaje skrót w Menu Start systemu Windows.
2. Wejść na portal Prace-Lab (odnośnik: https://pracelab.s3.kielce.pl/backup/index/)
3. Uwierzytelnić się*
4. Wybrać z listy bucket dla usługi i kliknąć przycisk *Generuj poświadczenia*.
5. Wygenerowany ciąg znaków skopiować - za pomocą przycisku *Skopiuj poświadczenia*
6. Wkleić poświadczenia do okna programy (ctr+v lub prawy przycisk myszy na polu tekstowym), po czym kliknąć przycisk Zatwierdź.
7. Program wykonuje inicjację i zapisuje konfigurację dostępu. Aplikacja jest gotowa do użytku. Po pomyślnym zapisaniu danych dostępowych do bucketu otworzy się główne okno programu.

Po inicjacji program pobiera listę plików przetrzymywanych w buckecie i wyświetla je w formie drzewa. Przy dużej ilości plików operacja ta może zająć nieco czasu. Przy pierwszym uruchomieniu programu na danym komputerze lista plików będzie pusta.

W pierwszej kolejności należy przejść do zakładki *Ustawienia.*



O statusie lub postępie wykonywanego zadania, aplikacja informuje użytkownika za pomocą belki zlokalizowanej w dolnej części okna *(6)*.

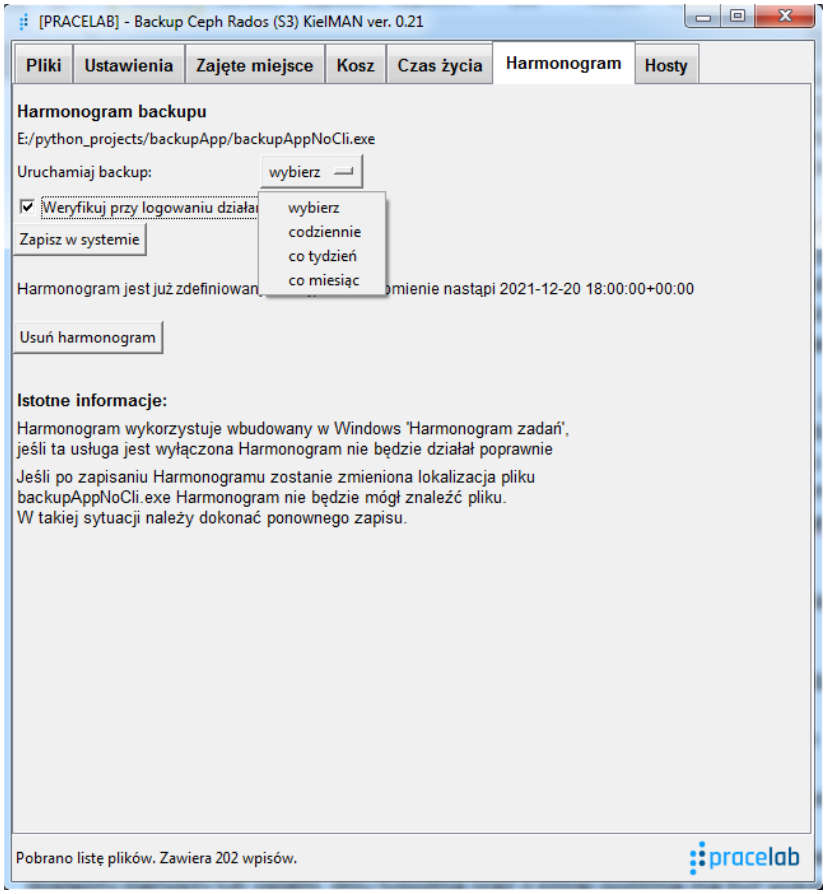
* - dla pracowników PŚk dane logowanie są tożsame z danymi do skrzynki pocztowej

W lewej kolumnie definiuje się foldery, które mają być zabezpieczone przez usługę. Służą do tego dwa przyciski: *Dodaj folder do backupu (1)* oraz *Usuń zaznaczony folder z backupu (2)*. Można wskazać dowolny folder, który znajduje się na komputerze. Użytkownik musi mieć dostęp (co najmniej prawo odczytu) do wskazanego folderu, by aplikacja mogła odczytywać jego zawartość.

W prawej kolumnie definiuje się folder lub pojedyncze pliki, które mają być pominięte przy przenoszeniu zawartości do bucketu. Takimi niepożądanymi plikami mogą być np. pliki robocze albo pliki tymczasowe innych aplikacji. Służą do tego trzy przyciski: *Dodaj cały folder (3), Dodaj pojedynczy plik (4)* oraz *Usuń zaznaczoną pozycję z listy (5)*. Aby dodać folder bądź plik do wykluczeń musi się on znajdować wewnątrz folderów wskazanych w lewej kolumnie, czyli w lokalizacji podlegającej zabezpieczeniu. Wykluczyć można też pliki na podstawie konkretnego rozszerzenia – typu pliku. Opcja ta jest dostępna po kliknięciu przycisku *Wykluczone rozszerzenia*. W nowym oknie widoczna jest lista aktualnie wykluczonych rozszerzeń. Można dodać tu kolejne typy plików do wykluczeń lub usunąć pozycję z listy. Akceptowalny jest zapis rozszerzenia zarówno w formie ‘.tmp’ jak i w formie ‘tmp’. Wykluczenie to będzie obowiązywać we wszystkich zabezpieczonych folderach.

Po zdefiniowaniu zabezpieczonych lokalizacji można już wykonać kopię zapasową na żądanie za pomocą przycisku *Wykonaj backup teraz*. Jest to zalecany scenariusz postępowania. W tle pojawi się czarne okienko terminala linii komend systemu Windows, w którym działa moduł backapujący aplikacji – jest to normalne zachowanie. Pierwsze wykonanie kopii zapasowej może zająć najwięcej czasu – przesłane zostaną wszystkie pliki znajdujące się we wskazanych lokalizacjach. Czas przesyłu zależy od ilości plików, ich łącznego rozmiaru oraz prędkości łącza użytkownika.

Opcjonalnym, lecz mocno zalecanym punktem konfiguracji jest zdefiniowanie harmonogramu wykonywania kopii zapasowej. Służy do tego celu zakładka *Harmonogram*.



Z listy rozwijalnej należy wybrać częstotliwość zadania. Dostępne opcje to: dzienny, tygodniowy, miesięczny. Wybranie opcji *codziennie* umożliwia wskazanie godziny, o której kopia zapasowa będzie wykonywana. Wybranie opcji, *co tydzień* umożliwia wskazanie dnia tygodnia oraz dokładnej godziny, o której kopia zapasowa będzie wykonywana. Wybranie opcji, *co miesiąc* pozwala z kolei na wskazanie w którym tygodniu miesiąca – dostępny pierwszy lub ostatni, dniu tego tygodnia oraz o której godzinie ma być wykonywana kopia zapasowa.

Ponadto dostępna jest opcja weryfikowania poprawności wykonania kopii zapasowej. Po jej zaznaczeniu przy każdym logowaniu użytkownika do systemu sprawdzana jest poprawność działania zadania harmonogramu w stosunku do określonej częstotliwości. Jeśli zostanie przekroczona krytyczna liczba opuszczonych lub zakończonych niepowodzeniem cykli zadania harmonogramu, stosowny komunikat zostanie wyświetlony w postaci notyfikacji – okienka pojawiającego się w prawym dolnym rogu nad zegarem Windows.

Harmonogram zapisuje się w systemie za pomocą przycisku *Zapisz w systemie*.

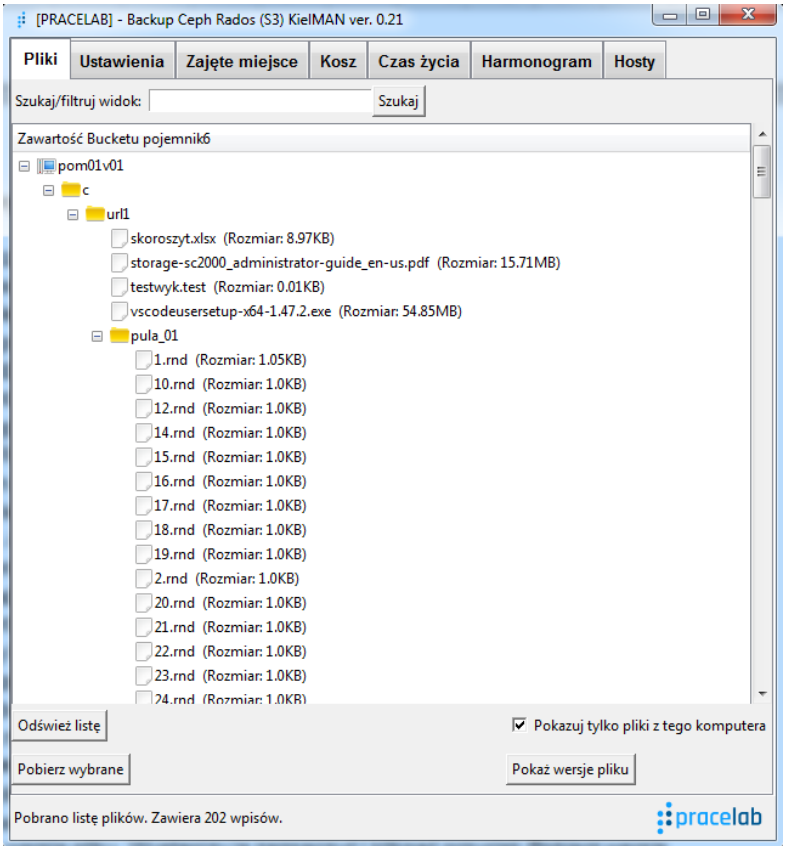
Definicja powyższych zadań opiera się na mechanizmie *Harmonogram zadań* systemu Windows. Jeśli ta usługa jest wyłączona lub działa niepoprawnie w systemie użytkownika zadanie kopii zapasowej nie będzie się wykonywało. W przypadku, gdy komputer użytkownika był wyłączony o godzinie ustalonej jako czas wykonania lub użytkownik był wylogowany, zadanie zostanie wykonane przy kolejnym uruchomieniu komputera i zalogowaniu się użytkownika do systemu. W takiej sytuacji zadanie uruchamiane jest przez *Harmonogram zadań* z pewnym opóźnieniem, zwykle 10-minutowym względem czasu zalogowania się do systemu.

Przeniesienie programu Backup S3 do innej lokalizacji już po zdefiniowaniu harmonogramu będzie skutkowało niemożliwością wykonywania zadania. W takiej sytuacji już po przeniesieniu programu należy za pomocą przycisku *Usuń harmonogram* usunąć zdefiniowane taski i jeszcze raz zdefiniować nowe zadanie.

5. Szczegółowy opis dostępnych funkcji programu

5.1. Pliki

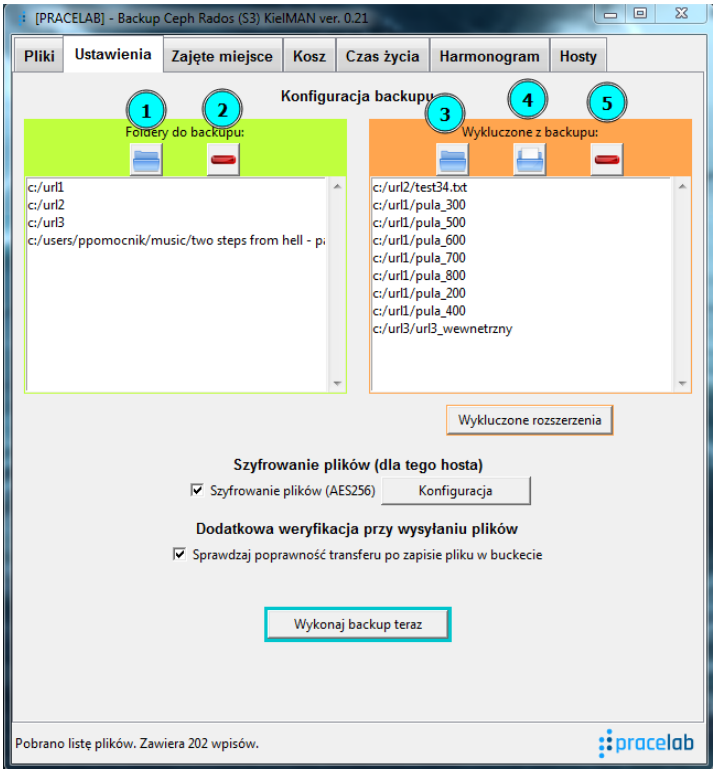
Główna część zakładki to przeglądarka plików umieszczonych w buckecie. Widok przedstawia pliki w formie listy-drzewa z zachowaniem struktury katalogów. Kliknięcie prawym przyciskiem myszy na gałęzi spowoduje rozwinięcie jej wraz z zagnieżdżonymi w niej gałęziami. Widok można zawęzić poprzez opcję Szukaj.



W polu edycyjnym *Szukaj/filtruj widok* należy wpisać nazwę lub ścieżkę (w całości lub fragment) pliku i kliknąć przycisk *Szukaj*. Widok zawartości zostanie zawężony tylko do plików spełniających zadane kryterium, czyli zawierających w sobie wpisany ciąg znaków.

Domyślnie wyświetlane są tylko pliki z hosta (komputera), na którym aktualnie uruchomiony jest program. Aby to zmienić, należy odznaczyć pole wyboru *Pokazuj tylko pliki z tego komputera,* a następnie kliknąć przycisk *Odśwież listę*. Można też pobierać dowolny plik. Wystarczy go zaznaczyć (lewy przycisk myszki) i kliknąć przycisk *Pobierz wybrane*. Można zaznaczyć więcej niż jeden plik trzymając wciśnięty lewy klawisz Ctrl i zaznaczając na liście kolejne pliki. Pobrane zostają najnowsze wersje zaznaczonych plików. Można również wyświetlić wszystkie dostępne w buckecie wersje danego pliku. Aby to zrobić, należy zaznaczyć plik na liście (lewy przycisk myszki) i kliknąć przycisk *Pokaż wersje pliku*. W przypadku zaznaczenia wielu plików zostaną wyświetlone wersje tylko dla pliku, który znajduje się na górze hierarchii. W nowym oknie w formie listy wyświetlone zostaną wszystkie dostępne wersje pliku. Można stąd pobrać wybraną wersję pliku. Wystarczy ją zaznaczyć i kliknąć przycisk *Pobierz wersje.*

5.2. Ustawienia

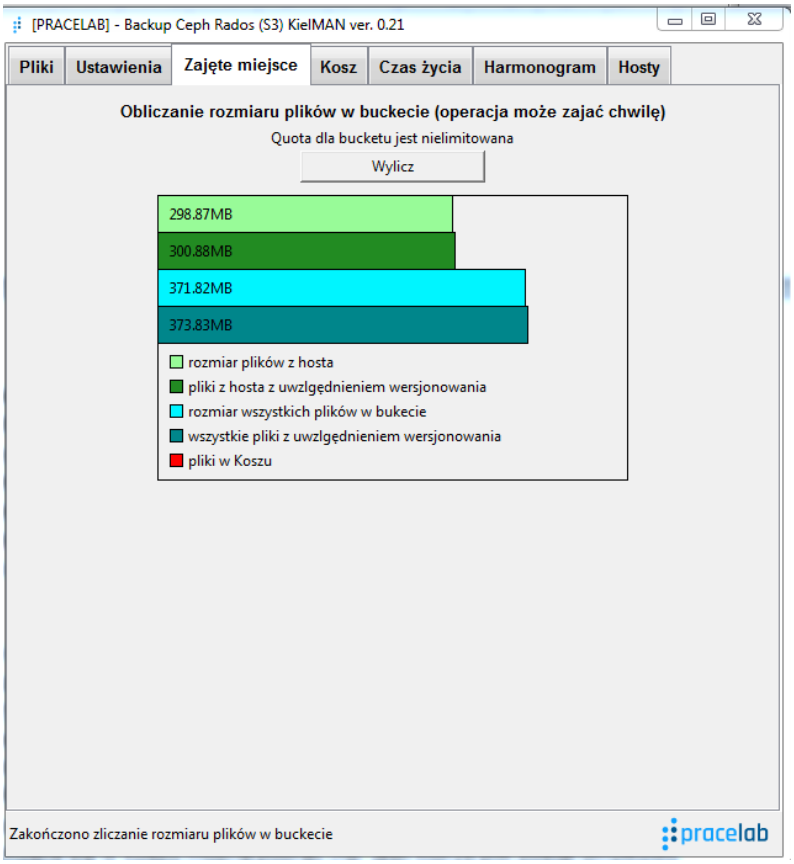


Można tu wyróżnić dwie sekcje ustawień. Pierwsza sekcja to ustawienia określające zasoby, które będą zabezpieczone w usłudze Backup S3.
W lewej (zielonej) kolumnie wyświetlone są foldery zabezpieczone. Foldery można dodać poprzez przycisk *Dodaj folder do backupu (1)*. Usunięcie niechcianego folderu z listy umożliwia przycisk *Usuń zaznaczony folder z backupu (2)*.
W prawej (pomarańczowej) kolumnie wyświetlone są z kolei foldery i pliki, które są wykluczone (czyli pomijane w trakcie operacji) z kopii zapasowej. Dodanie folderu do wykluczonych realizuje się za pomocą przycisku *Dodaj cały folder do wykluczeń (3)*. Dodanie pojedynczego pliku umożliwia przycisk *Dodaj pojedynczy plik do wykluczeń (4)*. Folder lub plik muszą znajdować się w lokalizacji, która podlega zabezpieczeniu, aby można je było zdefiniować jako wykluczenia. Usunięcie pozycji z listy wykluczeń umożliwia przycisk *Usuń zaznaczoną pozycję z wykluczeń (5)*.
Przycisk *Wykluczone rozszerzenia* wywołuje dodatkowe okno, w którym można zdefiniować rozszerzenia plików, które będą wykluczone z kopii zapasowej. W trakcie podawania rozszerzenia akceptowany jest zapis w formie ‘txt’ jak i ‘.txt’. Wykluczenie typu plików obowiązuje w całym zakresie zabezpieczonej przestrzeni.

Druga sekcja to dodatkowe ustawienia kopii zapasowej.
Zaznaczenie checkboxa *Szyfrowanie plików (AES256)* włącza szyfrowanie przy pomocy SEE (opis w słowniku) zapisywanych na buckecie plików. Po zaznaczeniu checkboxa pojawi się okno konfiguracji. W nim należy zdefiniować Klucz SSE, którym będą szyfrowane pliki. Można to zrobić na dwa sposoby. Pierwszy polega na podaniu bezpośrednio 32-znakowego ciągu znaków, który będzie kluczem. Drugi sposób to wpisanie hasła na podstawie którego generowany jest 32-znakowy ciąg znaków, czyli hash. Po kliknięciu przycisku *Zapisz* klucz SSE zostaje zapisany i włączona będzie funkcja szyfrowania plików. Od tego momentu każdy plik zapisany w buckecie będzie wymagał do odczytu posiadania klucza SSE. Nie dotyczy to jednak plików i starszych wersji plików zapisanych przed uruchomieniem opcji szyfrowania.
Klucz SSE należy zapisać i przechowywać w bezpiecznym miejscu – wskazane jest, aby była to lokalizacja poza zabezpieczaną maszyną.

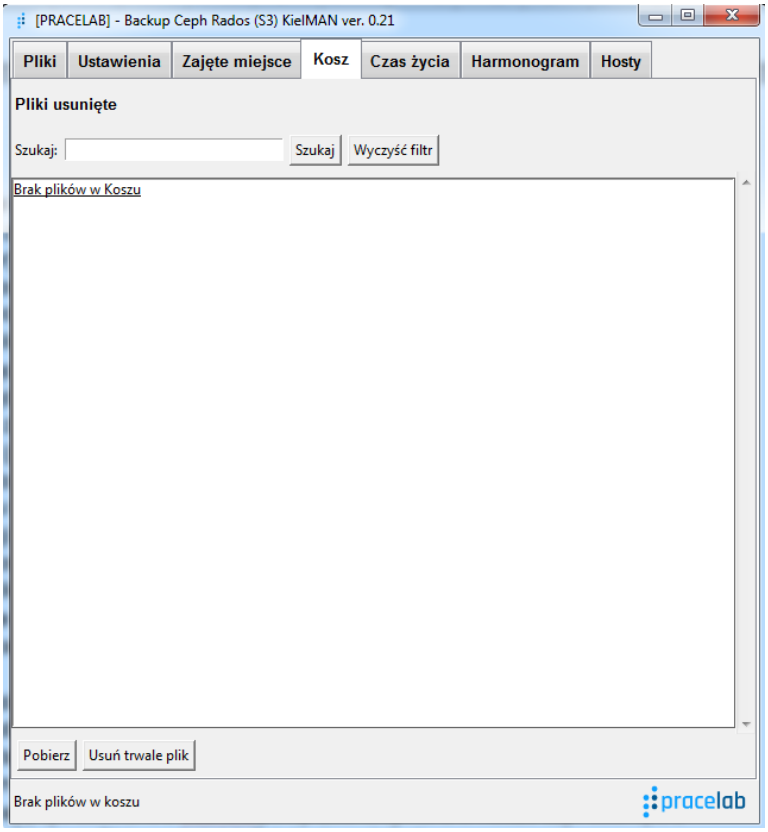
Drugi checkbox *Sprawdzaj poprawność transferu po zapisie pliku w buckecie* uruchamia opcję dodatkowej weryfikacji całego procesu zapisu z hosta użytkownika do zdalnego bucketu. Znalezione informacje o problemie są zapisywane w pliku backupAppAccess.log oraz wyświetlane na ekranie, jeśli moduł backupujący został uruchomiony z widokiem konsoli. Uruchomienie tej opcji wydłuża każdorazowo czas wykonywania kopii zapasowej.

5.3. Zajęte miejsce



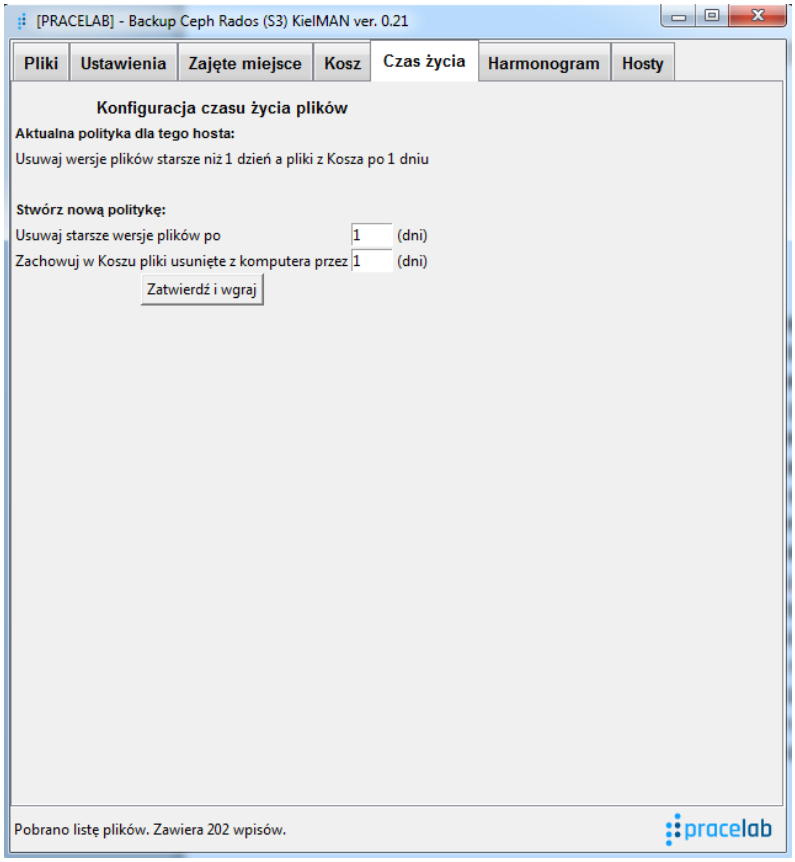
Ta zakładka pozwala sprawdzić użytkownikowi stan zajętego miejsca w buckecie, na który wysyłane są pliki z hosta. Po kliknięciu przycisku *Wylicz* program wylicza informacje o zajętości miejsca i prezentuje je w postaci wykresu słupkowego. Dodatkowo, jeśli na bucket nałożona jest quota pokazywany jest procent zajętego/dostępnego miejsca w postaci wykresu kołowego.

5.4. Kosz



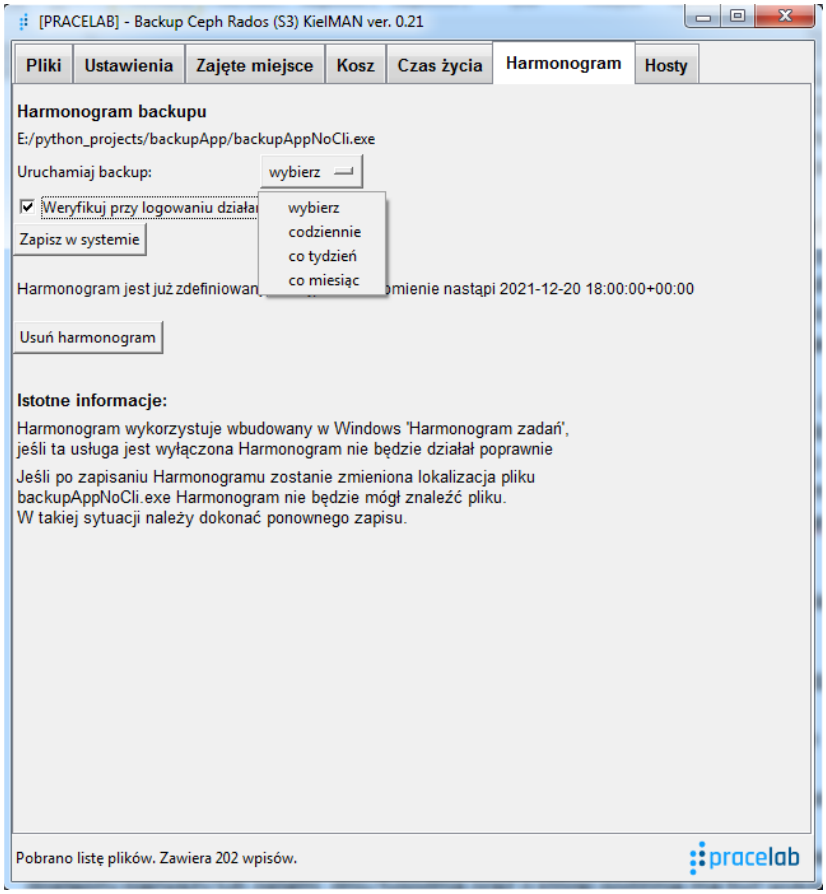
Zakładka Kosz wyświetla wszystkie pliki przeniesione do kosza tzn. oznaczone, jako usunięte z hosta źródłowego. Zasady, kiedy plik trafia do kosza opisane są w punkcie 5.8 tej instrukcji.
Pliki w koszu prezentowane są w postaci listy. Można zawęzić ilość wyświetlanych pozycji poprzez wpisanie w pole edycyjne *Szukaj* nazwy bądź części nazwy lub ścieżki pliku i wciśnięcie przycisku *Szukaj*. Wyświetloną zostaną wtedy tylko pozycje spełniające kryterium tj. zawierające w sobie wpisany ciąg znaków.
Pliki znajdujące się w koszu można pobrać (np. jeśli któryś plik został omyłkowo usunięty z hosta źródłowego lub uszkodzony). Aby to zrobić, należy zaznaczyć pliki na liście (jeden na raz) i kliknąć przycisk *Pobierz*. Otworzy się nowe okno, w którym wyświetlone zostaną wszystkie dostępne wersje danego pliku. Po wybraniu wersji i kliknięciu na przycisk *Pobierz wersję* rozpocznie się pobieranie pliku do wskazanej lokalizacji.
Pliki w koszu można również trwale usunąć z bucketu. Po zaznaczeniu pliku na liście należy kliknąć przycisk *Usuń trwale plik*. Po zatwierdzeniu operacji plik (wszystkie istniejące wersje) zostanie całkowicie usunięty z bucketu bez możliwości jego przywrócenia.

5.5. Czas życia



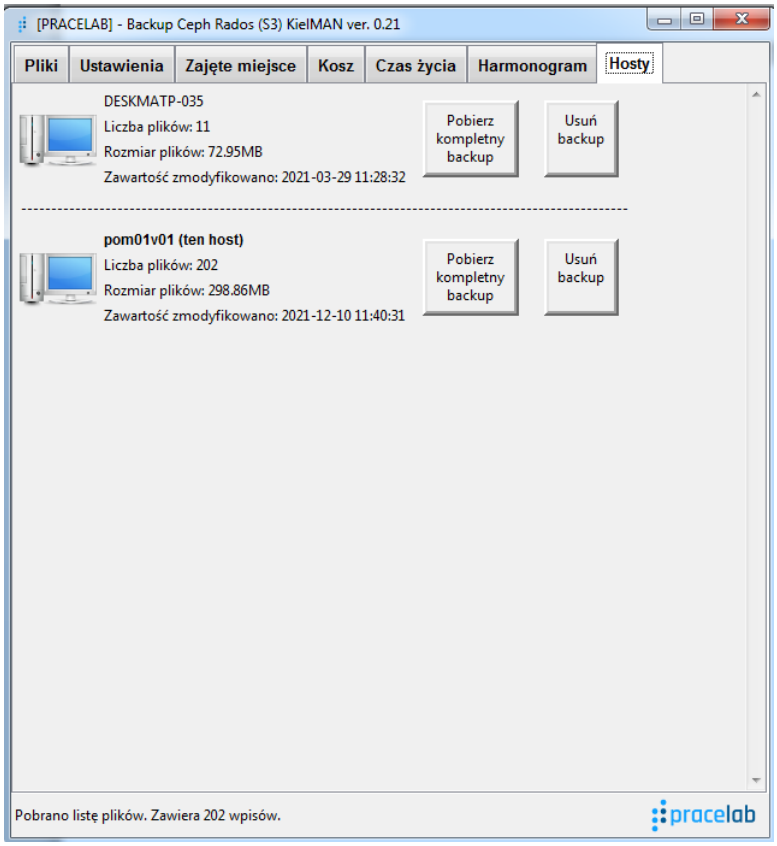
Ta zakładka pozwala zdefiniować politykę czasu życia plików (patrz słownik) w buckecie.
Polityka taka składa się z dwóch elementów. Pierwszy definiuje wiek po osiągnięciu, którego mają być usuwane starsze wersje plików (wszystkie poza najnowszą). Drugi element definiuje, po jakim czasie mają być usuwane z bucketu pliki przechowywane w Koszu, czyli usunięte z hosta źródłowego (komputer backupowany). Obie wartości definiuje się w dniach gdzie minimalna wartość to 1 dzień.
Zdefiniowanie (lub nie) polityk czasu życia wpływa na funkcjonowanie usługi. Brak definicji sprawia, że pliki w buckecie nie są usuwane, co w przyszłości może skutkować zapełnieniem bucketu i brakiem możliwości wgrywania kolejnych plików lub nowszych wersji plików.
Zaznaczyć należy, że użytkownik nie może samodzielnie usunąć pojedynczo plików zapisanych w buckecie, aby zwolnić miejsce, gdyż taka akcja łamałaby przyjętą zasadę synchronizacji zawartości host źródłowy – bucket. Z zakładki Hosty dostępna jest opcja pozwalająca usunąć całą kopię zapasową danego hosta.
Z kolei zdefiniowanie polityk ze zbyt krótkim czasem życia może skutkować zbyt szybkim usuwaniem zawartości, co może negatywnie odbić się na bezpieczeństwie przechowywanych danych. Na przykład czas życia dla plików w koszu ustawiony na jeden dzień może być czasem za krótkim na reakcję użytkownika, by odzyskać pliki, które na hoście źródłowym zostały omyłkowo usunięte lub uległy uszkodzeniu.
Zapisanych zasad nie można już usunąć, ale można je modyfikować.

5.6. Harmonogram



Ta zakładka pozwala stworzyć w systemowym Harmonogramie zadań Windows zadanie regularnego wykonywania kopii zapasowej.
Z listy rozwijalnej należy wybrać częstotliwość zadania. Dostępne opcje to: dzienny, tygodniowy, miesięczny. Wybranie opcji *codziennie* umożliwia wskazanie godziny, o której kopia zapasowa będzie wykonywana. Wybranie opcji, *co tydzień* umożliwia wskazanie dnia tygodnia oraz dokładnej godziny, o której kopia zapasowa będzie wykonywana. Wybranie opcji, *co miesiąc* pozwala z kolei na wskazanie w którym tygodniu miesiąca – dostępny pierwszy lub ostatni, dniu tego tygodnia oraz o której godzinie ma być wykonywana kopia zapasowa.
Ponadto dostępna jest opcja weryfikowania działania zadania kopii zapasowej. Po jej zaznaczeniu przy każdym logowaniu użytkownika do systemu sprawdzana jest poprawność działania zadania kopii zapasowej w stosunku do określonej częstotliwości. Jeśli zostanie przekroczona krytyczna liczba opuszczonych lub zakończonych niepowodzeniem cykli zadania, stosowny komunikat zostanie wyświetlony w postaci notyfikacji – okienka pojawiającego się w prawym dolnym rogu nad zegarem Windows.
Harmonogram zapisuje się w systemie za pomocą przycisku *Zapisz w systemie*.
Przycisk *Usuń harmonogram* pozwala na usunięcia zadania z systemu.
W tej funkcjonalności wykorzystywany jest mechanizm Harmonogramów zadań systemu Windows. Jeśli ta usługa jest wyłączona w systemie lub nie działa prawidłowo zdefiniowanie zadania backupu będzie niemożliwe, lub zadanie nie będzie się wykonywało.

5.7. Hosty



W zakładce Hosty wyświetlane są wszystkie komputery, z których kopie zapasowe są wykonywane w buckecie.
Dla każdego hosta dostępne są ogólne statystki oraz dwie możliwe akcje do wykonania.
Za pomocą przycisków *Pobierz kompletny backup* można pobrać wszystkie pliki z danego hosta na komputer, na którym aktualnie się pracuje. Po wskazaniu folderu do zapisu wewnątrz niego odtwarzana jest cała struktura katalogów z hosta źródłowego poczynając od dysków (czyli struktura będzie miała hierarchię: *wskazany_folder/c/zabezpieczonyPlik.txt*). Pobieranie nie rozpocznie się, jeśli we wskazanej lokalizacji nie ma wystarczająco dużo miejsca by zapisać wszystkie pliki.
Za pomocą przycisków *Usuń backup* można usunąć zawartość całej kopii zapasowej. **Ta operacja jest nieodwracalna i należy jej używać z rozwagą**. W trakcie operacji dla wybranego hosta usuwane są wszystkie pliki, wszystkie ich wersje, wszystkie pliki w Koszu pochodzące z tego Hosta, polityki czasu życia oraz plik systemowy manifest zawierający informacje o kopii zapasowej z danego hosta.

5.8. Zasady synchronizacji

Zasada działania programu polega na idei synchronizacji zawartości folderów lokalnych do zdalnej lokalizacji - bucketu tworzonego dla tej konkretnej usługi z włączonymi wersjonowaniem. Pliki zapisywane są w buckecie użytkownika przez moduł backupApp.exe (oraz jego wersję NoCli) w określonych, zdefiniowanych interwałach lub przy pierwszej możliwej okazji, jeśli nie można była tego dokonać w oryginalnym czasie lub na żądanie użytkownika. Pliki przesyłane są protokołem https, czyli szyfrowanym kanałem na standardowym porcie 443.
Program wykorzystuje wersjonowanie. Ilość wersji plików zabezpieczonych na buckecie jest zależna od czasu życia poprzednich wersji, częstotliwości wykonywania

backupu oraz częstotliwości zmian zawartości pliku na komputerze źródłowym. Ilość starszych wersji dla każdego pliku może być, zatem inna.
Zasada synchronizacji wyklucza usuwanie plików z bucketu, jeśli ich odpowiednik istnieje na komputerze źródłowym dlatego też nie ma takiej opcji w zakładce *Pliki*.
Plik zostaje usunięty w przypadku, gdy jego odpowiednik na komputerze lokalnym zostanie usunięty (lub jego nazwa zostanie zmieniona). Plik w buckecie nie zostaje jednak od razu permanentnie usunięty a jedynie zostaje oznaczony tzw. tagiem i wciąż jest dostępny dla Użytkownika, przy czym widoczny jest już tylko w zakładce Kosz. Plik zostaje trwale usunięty, jeśli zdefiniowana jest polityka czasu życia plików usuniętych. Będący w Koszu plik można również usunąć za pomocą odpowiedniego przycisku ręcznie.
Plik znajdzie się w Koszu również w następujących sytuacjach:
- plik lub jego lokalizację dodano do wykluczeń,
- usunięto lokalizację pliku z zabezpieczanej lokalizacji,
- typ pliku został wykluczony z kopii zapasowej.

Można usunąć też wszystkie pliki z danego hosta tak jak opisano to w sekcji 5.7.
Program przy pierwszym wykonaniu kopii zapasowej z komputera źródłowego tworzy w buckecie specjalny plik o nazwie nazwaHost-manifest.csv. W pliku tym zapisywane są informacje o wszystkich plikach wgranych z danego hosta i plik ten nie jest w ogóle wyświetlany użytkownikowi, gdy przegląda zawartość bucketu używając oferowanego w ramach usługi programu. W razie przeglądania zawartości bucketu programem trzecim plik będzie normalnie widoczny. W takiej sytuacji nie jest zalecane usuwanie go, gdyż taka akcja zachwieje stabilnością rozwiązania. Nie będzie to jednak skutkować utratą danych wgranych na bucket.