Metadata-Bound Libraries w SAS 9.3M2

Zespół Wsparcia Technicznego, SAS Institute Polska *październik 2012*

Szanowni Państwo !

Niniejszy dokument stanowi wprowadzenie i omówienie podstawowych funkcjonalności mechanizmu zabezpieczania bibliotek, wprowadzonego w SAS 9.3M2. Mechanizm ten polega na powiązaniu bibliotek z metadanymi (Metadata-Bound Libraries). Pełny opis przedstawianego mechanizmu znajduje się w dokumencie SAS 9.3 Guide to Metadata-Bound Libraries.

Dokument ten i inne informacje związane z tematem będą publikowane na naszych stronach WWW pod adresem http://www.sas.com/poland/services

W razie dodatkowych pytań prosimy o kontakt z naszym Zespołem, telefonicznie na numer **(22) 5604666** lub elektronicznie pod adresem **support@spl.sas.com**.

Prosimy o uwagi i spostrzeżenia, które pomogą nam w przygotowaniu następnych wersji tego dokumentu.

Zawsze służąc Państwu pomocą,
Zespół Pomocy Technicznej
Centrum Technologii SAS Polska

Spis treści

1. Wstęp ... 3
2. Wymagania i ograniczenia ... 3
3. Tworzenie zabezpieczonej biblioteki ... 3
4. Używanie zabezpieczonej biblioteki ... 4
   - 4.1. Wymagane uprawnienia ... 4
   - 4.2. Dostęp do zabezpieczonej biblioteki z poziomu aplikacji klienckich ... 5
   - 4.3. Zdejmowanie zabezpieczeń z biblioteki ... 5
   - 4.4. Hasło do obiektów Secured library oraz Secured table ... 5
   - 4.5. Dodawanie, usuwanie zabezpieczonych tabel i bibliotek ... 6
   - 4.6. Wykrywanie niespójności ... 6
   - 4.7. Audytowanie dostępu do danych ... 7

1. Wstęp

Głównym zadaniem mechanizmu Metadata-Bound Libraries jest zabezpieczenie bibliotek SAS-owych przed niepowołanym dostępem przez użytkowników takich narzędzi jak SAS BASE czy SAS Enterprise Guide. Do tej pory, jeżeli użytkownik znał lokalizację biblioteki SAS-owej na dysku twardym, był w stanie dostać się do niej używając instrukcji libname, niezależnie od ustawień dostępu w metadanych. Jedynym zabezpieczeniem biblioteki przed takim dostępem było odpowiednie ustawienie praw do odczytu i zapisu na poziomie systemu plików.

Od wersji 9.3M2, biblioteka SAS-owa może zostać zmodyfikowana w taki sposób, że nawet przy próbie bezpośredniego podłączenia instrukcją libname, wymagane jest połączenie do serwera metadanych i uwierzytelnienie się jako użytkownik uprawniony do takiej czynności.

2. Wymagania i ograniczenia

Mechanizm Metadata-Bound Libraries wymaga posiadania SAS w wersji 9.3M2 oraz działającego serwera metadanych.

Korzystanie z mechanizmu zabezpieczania bibliotek wprowadza następujące ograniczenia:

- Mechanizm można zastosować jedynie do tabel (data set) oraz widoków (view). Obecnie jedyną wspieraną metodą dostępu jest silnik BASE.
- Zabezpieczone tabele i biblioteki w dalszym ciągu mogą być usuwane oraz modyfikowane z poziomu systemu plików. Wszelkie zmiany wprowadzone tą metodą są wykrywane i zapisywane.
- W chwili obecnej nie ma możliwości zdefiniowania uprawnień dostępu na poziomie kolumn. Aby zrealizować takie zachowanie należy użyć widoków.
- Zabezpieczona biblioteka jest niedostępna z poziomu klientów starszych niż 9.3M2.

3. Tworzenie zabezpieczonej biblioteki

Do stworzenia zabezpieczonej biblioteki potrzebne są następujące elementy: biblioteka do zabezpieczenia oraz folder w metadanych, w którym zostaną zapisane definicje zabezpieczonych obiektów (biblioteki oraz tabele).

Definicje zabezpieczonych obiektów domyślnie znajdują się w folderze ***/System/Secured Libraries***. Możliwe jest stworzenie dodatkowej struktury organizacyjnej, poprzez dodawanie podkatalogów. Najłatwiej jest to uczynić z poziomu programu SAS Management Console.

UWAGA. Domyślnie możliwość dostępu do folderu /System/Secured Libraries jest ograniczona do użytkowników z prawami administratora.

Po stworzeniu odpowiednich katalogów i zdefiniowaniu praw dostępu do nich, należy wykonać następujący kod SAS-owy:

```
libname testlib "C:\biblioteka";

proc authlib lib=testlib;
    create securedfolder="security_test"
        securedlibrary="test_secured"
        pw=secretpw;
    run;
quit;
```

Powyższy kod spowoduje zabezpieczenie biblioteki *testlib*. W metadanych w katalogu ***/System/Secured Libraries/security_test*** zostanie utworzony obiekt typu ***Secured library*** o nazwie *test_secured* oraz obiekty typu ***Secured table*** dla wszystkich tabel znajdujących się w bibliotece.

Podczas wykonywania powyższego kodu zostanie wyświetlone okno z prośbą o zdefiniowanie połączenia do serwera metadanych. Jeżeli wszystko zostało zdefiniowane poprawnie, w logu powinna pojawić się następująca nota:

```
NOTE: Successfully created a secured library object for the physical library TESTLIB and
      recorded its location as:
           SecuredFolder:      /System/Secured Libraries/security_test
           SecuredLibrary:     test_secured
           SecuredLibraryGUID: E05CA669-EE18-4F2A-A336-9037A5C32DA8
```

Komunikat ten oznacza utworzenie obiektu typu ***Secured library*** dla biblioteki. Dodatkowo dla każdej tabeli tworzony jest obiekt typu ***Secured table***. Jego utworzenie sygnalizowane jest następującym komunikatem w logu (przykład dla tabeli o nazwie *table_name*):

```
NOTE: Successfully added new secured table object "CARS.DATA" to the secured library object at
      path "/System/Secured Libraries/security_test/test_secured" for data set
      TESTLIB.TABLE_NAME.DATA.
NOTE: The passwords on TESTLIB.TABLE_NAME.DATA were successfully modified.
```

4. Używanie zabezpieczonej biblioteki

4.1. Wymagane uprawnienia

Po zabezpieczeniu biblioteki każda próba dostępu do niej za pomocą instrukcji libname, spowoduje nawiązanie połączenia do serwera metadanych w celu sprawdzenia uprawnień ***ReadMetadata*** na obiekcie zabezpieczonej biblioteki. Jeżeli takich uprawnień użytkownik nie będzie posiadał, próba zakończy się niepowodzeniem.

Uprawnienie ***ReadMetadata*** pozwala podpiąć bibliotekę przy użyciu instrukcji libname. Aby móc odczytywać dane potrzebne jest uprawnienie ***Select***. Modyfikacja danych wymaga zaś uprawnień ***Alter Table*** oraz kombinacji uprawnień ***Insert, Update*** oraz ***Delete*** na obiektach konkretnych tabel.

4.2. Dostęp do zabezpieczonej biblioteki z poziomu aplikacji klienckich

Aby użytkownik aplikacji klienckiej (Data Integration Studio, Enterprise Guide, Enterprise Miner itp.) mógł użyć zabezpieczonej biblioteki, musi zostać ona standardowo zarejestrowana w metadanych. Fakt powiązania z obiektami ***Secured library*** oraz ***Secured table*** nie zwalnia nas z tego obowiązku.

Zabezpieczona biblioteka jest używana w dokładnie taki sam sposób jak zwykła biblioteka. Prawa dostępu są wyznaczane na podstawie aktualnego profilu połączenia do serwera metadanych.

4.3. Zdejmowanie zabezpieczeń z biblioteki

Aby usunąć powiązanie biblioteki z metadanymi, tym samym wyłączając mechanizm zabezpieczeń, należy wykonać następujące polecenie:

```
proc authlib lib=testlib;
    remove pw=secretpw/;
    run;
quit;
```

UWAGA. Powyższy kod powoduje całkowite usunięcie zabezpieczeń z tabel, wraz z hasłami Jeżeli chcemy pozostawić hasła, należy użyć kluzuli remove pw=secretpw;

4.4. Hasło do obiektów Secured library oraz Secured table

Podczas wykonywania procedury **authlib**, w momencie tworzenia, modyfikacji oraz usuwania powiązań z metadanymi, konieczne jest podanie hasła do wykonania zadanej operacji. Dla danego obiektu mogą zostać zdefiniowane 3 różne hasła: do operacji odczytu (READ), zapisu (WRITE) oraz modyfikacji (ALTER). Hasła te mogą mieć długość co najwyżej 8 znaków.

UWAGA. Przedstawione hasła służą do zabezpieczenia dostępu do obiektów w metadanych i powinny być znane jedynie administratorom.

W przedstawionych przykładach używana była opcja **pw=<hasło>.** Można z niej skorzystać, jeżeli wszystkie hasła dla danego obiektu są takie same.

Hasła mogą być ustalane indywidualnie dla każdej biblioteki oraz tabeli. Przykładowo, jeżeli chcemy aby dostęp do obiektów zabezpieczeń wymagał różnych haseł, należy przy zabezpieczaniu biblioteki zamiast opcji **pw** użyć **read**, **write** bądź **alter**. Przykładowy kod wygląda następująco.

```
proc authlib lib= testlib;
    create securedfolder="security_test"
        securedlibrary="test_secured"
        read=readpw
        write=writepw
        alter=alterpw;
    run;
quit;
```

Aby zmienić hasło należy dla danej biblioteki/tabeli wykonać procedurę **authlib** z opcją **modify**. Hasło, które chcemy zmienić należy podać w następujący sposób: ***<typ hasła>=<stare hasło>/<nowe hasło>.*** Przykład zmiany hasła dla całej biblioteki z wszystkimi tabelami prezentuje poniższy kod:

```
proc authlib lib=testlib;
    modify
        read=readpw/secretpw
        write=writepw/secretpw
        alter=alterpw/secretpw;
    run;
quit;
```

4.5. Dodawanie, usuwanie zabezpieczonych tabel i bibliotek

Zalecaną metodą dodawania i usuwania tabel w zabezpieczonej bibliotece jest korzystanie z procedury **datasets**. Operacje na tabelach wykonane za jej pomocą są automatycznie uwzględniane w obiektach metadanowych.

W przypadku ręcznego dodania tabeli do biblioteki (np. poprzez dodanie pliku do folderu) w momencie jej odczytu otrzymujemy następujące ostrzeżenie w logu:

```
WARNING: Data set TESTLIB.TABLE_NAME.DATA is not bound to a secured table object, but it resides
         in a directory that is bound to a secured library object. The data set might have
         existed in this directory before the library was bound, or the data set might have been
         copied to this directory with a host copy utility.
WARNING: Metadata permissions are not enabled.
```

4.6. Wykrywanie niespójności

Do wykrywania niespójności pomiędzy fizycznymi plikami na dysku a odpowiadającymi im obiektami w metadanych służy klauzula report. Sprawdza ona wszystkie tabele znajdujące się w bibliotece i produkuje dla każdej z nich krótkie podsumowanie. Przykładowe uruchomienie:

```
proc authlib lib=testlib;
    report;
    run;
quit;
```

4.7. Audytowanie dostępu do danych

Zdarzenia związane z mechanizmem Metadata-Bound Libraries można zapisywać wykorzystując podane poniżej loggery:

Kategoria (logger)	Logowane zdarzenia
Błąd autoryzacji (Audit.Data.MetaboundLib.PermDenied)	Użytkownik próbował uzyskać dostęp do biblioteki, nie mając do niej wystarczających uprawnień
Niespójność danych (Audit.Data.MetaBoundLib.AuthAudit)	Dostęp do zabezpieczonej tabeli znajdującej się w niezabezpieczonej bibliotece i vice versa itp.

Szczegóły definiowania logowania dla serwerów SAS-owych opisane są w dokumencie SAS Intelligence Platform: System Administration Guide w rozdziale ***„System Monitoring and Logging” → „Administering Logging for SAS Servers”.***