

Informacje o wersji (fix) 1.14.0.11 z dn. 12-11-2024

Nowe i zmodernizowane funkcje

1. Skrypty migracji

Dodano możliwość definiowania skryptów SQL wykonywanych przed importem aplikacji na środowisko docelowe i po zakończeniu importu. Skrypty są uruchamiane w ramach transakcji importu; błąd wykonania skryptu o odpowiedniej istotności przerywa wykonanie transakcji. Skrypty można wpisać na nowo dodanych kartach w oknie definiowania aplikacji.

Przy użyciu skryptu przed importem można na przykład utworzyć w bazie nowe schematu używane przez importowaną aplikację, aby utworzyć kilka schematów można użyć w skrypcie komendy GO:

```
CREATE SCHEMA myAppSchema1;  
GO  
CREATE SCHEMA myAppSchema2;  
GO
```

Uwaga

Obsługa komendy GO została zaimplementowana w nAxiom punktowo tylko na potrzeby skryptów migracyjnych. W przypadku sprawdzania poprawności składni SQL dla skryptu jak w przykładzie powyżej, jest wyświetlany komunikat o błędzie, jednak skrypt można zapisać i jest on wykonywany poprawnie. Ten problem zostanie rozwiązany w kolejnej wersji nAxiom.

2. Zmienne aplikacji

Dodano możliwość wyłączenia nadpisywania wartości zmiennych aplikacji w środowisku docelowym podczas importu aplikacji. Funkcja działa osobno dla każdego rodzaju środowiska (dev/test/prod). Z funkcji można skorzystać w oknie definicji aplikacji na karcie **Zmienne**, gdzie dodano przycisk **Ustawienia migrowania zmiennych**. Kliknięcie przycisku wyświetla okno dialogowe z trzema przełącznikami dla indywidualnych rodzajów środowisk. Wyłączenie przełącznika spowoduje, że wartości zmiennych aplikacji w środowisku docelowym danego typu nie będą nadpisywane wartościami z importowanej aplikacji.

W przypadku zmiennych, które nie istnieją w środowisku docelowym, wyłączenie nadpisywania spowoduje, że nowa zmienna zostanie utworzona i będzie miała wartość NULL.

3. Migrator aplikacji

W migratorze zmieniono tryb importu procedur SQL w przypadku, gdy taka procedura już istnieje na środowisku docelowym. Obecnie istniejąca procedura jest aktualizowana za pomocą instrukcji ALTER. Wcześniej taka procedura była usuwana i tworzona od nowa (DROP/CREATE).

Poprawki dotyczące bezpieczeństwa i dobrych praktyk programistycznych

1. Biblioteki Javascript

Zaktualizowano używane w projekcie biblioteki Javascript:

- jquery 3.6.0 -> 3.7.1
- jquery-validate 1.19.5 -> 1.21.0
- jquery-validation-unobtrusive 3.2.11 -> 4.0.0

2. Usunięcie nadmiarowych informacji

Z komunikacji http między aplikacją (FrontSPA) i backendem usunięto informacje umożliwiające poznanie struktury bazy danych. Ma to na celu poprawę bezpieczeństwa, w tym między innymi uniemożliwienie identyfikacji miejsc podatnych na ataki typu SQL Injection.

3. nginx 1.27.1

W pakiecie do wdrożeń w architekturze kontenerów zaktualizowano używany serwer nginx do wersji 1.27.1.

4. Nagłówki odpowiedzi HTTP

W wysyłanych z nAxiom odpowiedziach HTTP na niektóre żądania uzupełniono brakujące nagłówki:

- Permissions-Policy (dawn. Feature-Policy): umożliwia szczegółową kontrolę nad zakresem wykorzystania przez przeglądarkę klienta dostępnych funkcjonalności oraz API aplikacji.
- Content-Security-Policy: zawiera informacje o typach zawartości zamieszczonych na stronie.
- Referrer-Policy; pozwala na zarządzanie postacią nagłówka Referer w przypadku żądań kierowanych do innych witryn z aplikacji nAxiom.
- X-Content-Type-Options (nosniff): znacznik używany przez serwer do wskazania, że typy MIME ogłaszane w nagłówkach Content-Type nie powinny być zmieniane, oraz że należy ich przestrzegać.
- X-Frame-Options: pozwala zapobiegać atakom typu clickjacking, polegającym na doprowadzeniu użytkownika do nieświadomego wykonania operacji na stronie.

- Strict-Transport-Security: informuje przeglądarki, że dostęp do danej witryny powinien zawsze odbywać się przez połączenie szyfrowane HTTPS, oraz że wszelkie przyszłe próby dostępu przez HTTP powinny być automatycznie konwertowane na HTTPS.

5. Protokoły TLS

W celu podniesienia poziomu bezpieczeństwa wyłączono obsługę protokołu TLS w wersji 1.0 i 1.1.

6. Algorytmy kryptograficzne

Z zestawu algorytmów kryptograficznych możliwych do wynegocjowania do ochrony transmisji szyfrowanej SSL/TLS usunięto te, których użycie nie jest już rekomendowane ze względów bezpieczeństwa. Dotyczy to między innymi algorytmów RSA używanych do wymiany kluczy, szyfrów blokowych pracujących w trybie CBC i algorytmów SHA używanych jako funkcja skrótu do uwierzytelniania wiadomości.

7. Pliki cookie sesji

Dodano atrybuty httponly i secure w plikach cookie sesji, których tworzenie wymusza serwer nAxiom podczas korzystania z wskazanych serwisów. Pierwszy z tych atrybutów blokuje dostęp do plików cookie z poziomu aktywnego kodu po stronie klienta (np. JavaScript), drugi pozwala na przesyłanie pliku cookie tylko przez połączenie szyfrowane.

8. Informacje o technologii

Z odpowiedzi HTTP rozsyłanych przez witrynę nAxiom wyeliminowano informację o wykorzystywanych komponentach (Server: nginx/1.23.4).

9. Przedrostek URL tenanta

W aplikacji TenantsAdminSPA, w konfiguracji przedrostka adresu URL tenanta dodano mechanizm walidacji wykluczający użycie znaku podkreślenia (_) w tym przedrostku w celu zapewnienia zgodności z obowiązującymi specyfikacjami i standardami oraz uniknięcia potencjalnych problemów z routingiem i identyfikacją tenanta.

Ponieważ domyślnie wartość tego ustawienia jest pobierana z ustawienia Kod, również w kodzie tenanta wykluczono możliwość stosowania podkreślenia.

Poprawki i usunięte błędy

1. Migrator aplikacji

W migratorze aplikacji wyłączono sprawdzanie, czy nazwa importowanej kolumny zaczyna się od wielkiej litery. Kolumny, które nie spełniały tego wymagania, nie były tworzone w środowisku docelowym. Problem dotyczył tabel tworzonych poza kreatorem modeli danych, w którym nawy kolumn muszą zaczynać się z wielkiej litery.

2. Raporty Telerik

Żądanie generowania raportu Telerik rozbudowano o obsługę błędów i automatyczne ponawianie w przypadku błędu połączenia.

3. Lista hierarchiczna

Usunięto błąd, który powodował, że odświeżenie strony powodowało usunięcie skonfigurowanych filtrów dla listy hierarchicznej.

4. Wartość ustalona

Zmieniono mechanizm pobierania danych dla listy wyboru z wartością ustaloną. W takich przypadkach w trybie tylko do odczytu wyłączono wczytywanie źródła danych kontrolki, aby zlikwidować niepotrzebne opóźnienia.

5. Akcja odświeżania uprawnień

W oknie dialogowym akcji odświeżania uprawnień przywrócono wyświetlanie opisu zapytania SQL pod edytorem SQL.

6. Sygnalizacja wymagalności

Poprawiono błąd, który powodował, że dla niektórych kontrolek formularza nie działała sygnalizacja wymagalności pól (czerwony napis Pole wymagane).

7. Akcja komunikatu

Poprawiono błąd, który powodował, że w przypadku zamknięcia okna komunikatu klawiszem Esc, pozostawała aktywna blokada ekranu z ikoną operacji w toku. Problem dotyczył komunikatów wyświetlanych akcją komunikatu.

8. Lista wyboru interesariuszy

Poprawiono błąd, który powodował, że po rozwinięciu listy wyboru interesariuszy, która znajdowała się u dołu ekranu, lista była niewidoczna (rozwijała się poza obszar widoczny na ekranie).

9. Bloczek akceptacji

Poprawiono błąd w działaniu bloku akceptacji w przypadku kilku akceptantów.