Urząd Komunikacji Elektronicznej | UKE

Załącznik F. Opis środowiska bazodanowego PLICBD

Warszawa, 2023

Spis treści

Opis środowiska bazodanowego PLICBD

W niniejszym dokumencie opisane zostały główne elementy wchodzące w skład środowiska bazodanowego

1. Bazy Danych

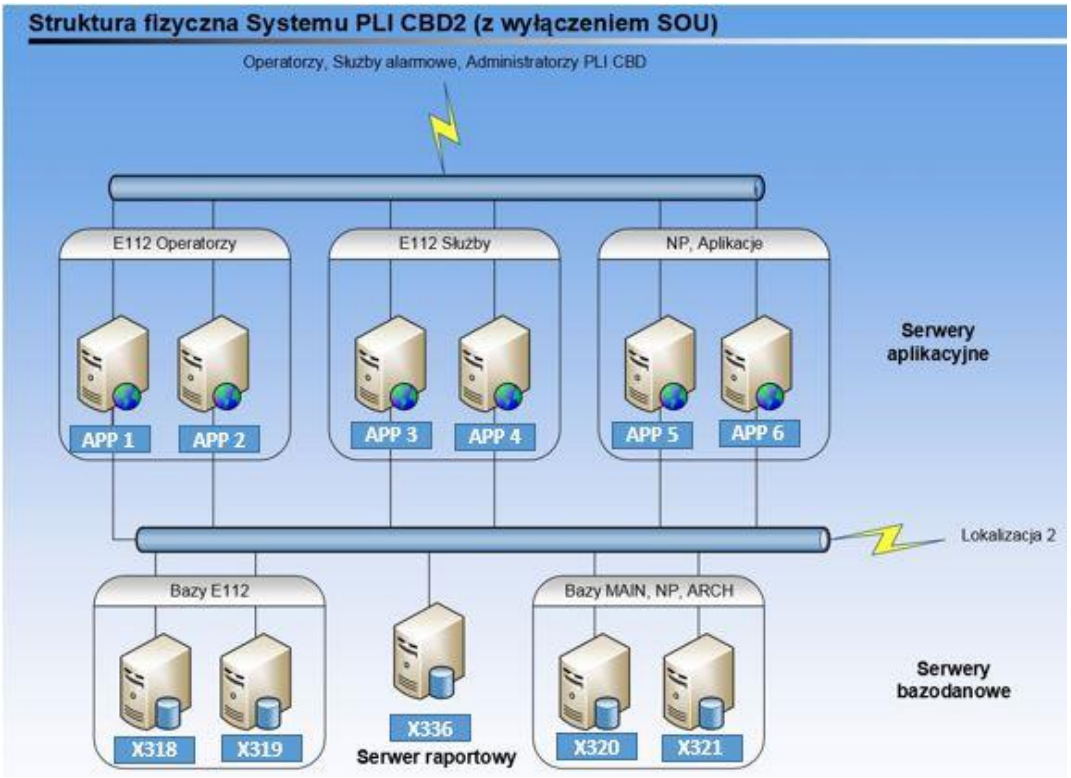
Całość danych PLI CBD można podzielić na siedem osobnych kategorii baz:

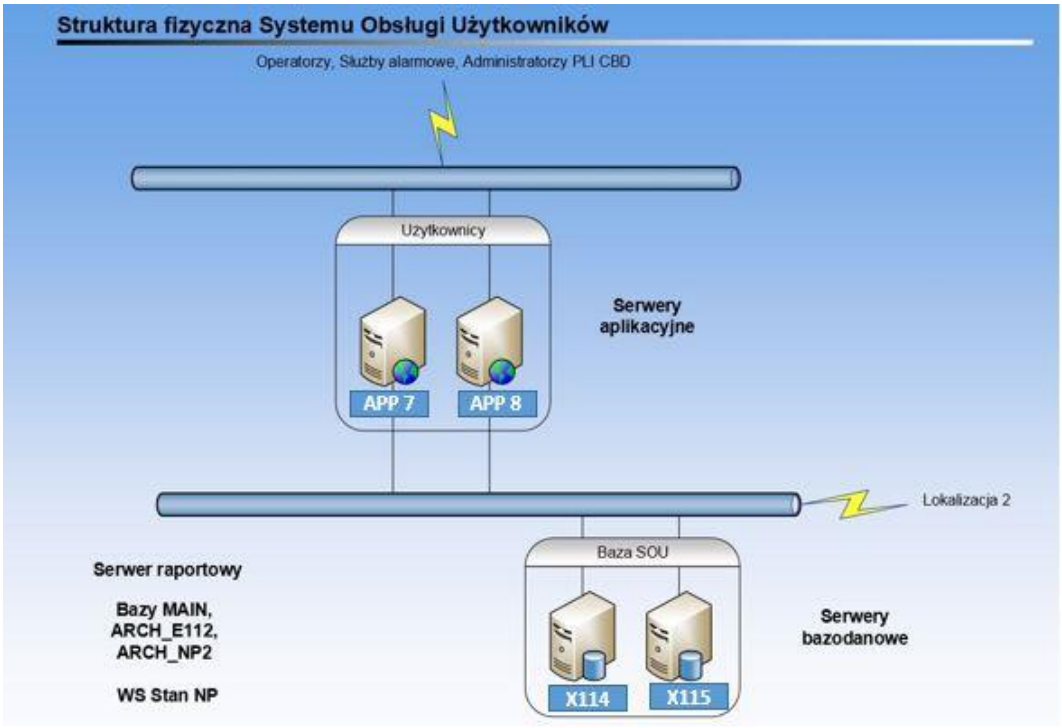
- E112 – operacyjna baza danych obsługująca wywołania i zapytania lokalizacyjne. W każdej lokalizacji są dwie równoległe instancje tej bazy uruchamiane na osobnych serwerach bazodanowych. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Dane zarówno w obrębie danej lokalizacji, jak i pomiędzy są synchronizowane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.
- NP2 – operacyjna baza danych obsługująca komunikaty i procesy przenoszenia numerów. W każdej lokalizacji jest jedna aktywna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i dodatkowo jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer w tej samej lokalizacji. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Pomiędzy lokalizacjami dane są uspójniane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.
- MAIN – referencyjna baza danych utrzymująca konfigurację, słowniki i aktualne tabele z bieżącym obrazem numerów przeniesionych, umowy o udostępnianie numeracji i zakresy numeracji przydzielone przez UKE. W każdej lokalizacji jest jedna aktywna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i dodatkowo jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer w tej samej lokalizacji. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Pomiędzy lokalizacjami dane są uspójniane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.
- ARCH_E112 – baza archiwizacyjna danych E112. W każdej lokalizacji jest jedna aktywna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i dodatkowo jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer w tej samej lokalizacji. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Pomiędzy lokalizacjami dane są uspójniane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.
- ARCH_NP2 – baza archiwizacyjna danych NP. W każdej lokalizacji jest jedna aktywna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i dodatkowo jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer w tej samej lokalizacji. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Pomiędzy lokalizacjami dane są uspójniane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.

- REPORT – baza utrzymująca dane na potrzeby raportowe, na wydzielonych serwerach raportowych. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Baza w każdej lokalizacji występuje tylko w jednej instancji.
- SOU – baza Systemu Obsługi Użytkowników utrzymywana jest na osobnym serwerze bazodanowym. W każdej lokalizacji jest jedna aktywna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i dodatkowo jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer w tej samej lokalizacji. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Pomiędzy lokalizacjami dane są uspójniane za pomocą zewnętrznych modułów wchodzących w skład systemu PLI CBD.

1.1. Rozmieszczenie fizyczne baz

Poniżej przedstawiona jest struktura fizyczna systemu PLI CBD:





APP – serwery aplikacyjne.
X – serwery bazodanowe
gdzie X oznacza S-LAN-SRVDB-1 - Siemianowice, B-LAN-SRVDB-2 – Borucza.

1.2. Wykaz serwerów produkcyjnych

Poniżej przedstawiony jest wykaz serwerów produkcyjnych, na których umiejscowione są poszczególne bazy danych. Szczegółowa specyfikacja fizyczna poniższych maszyn przedstawiona jest w dokumencie „Opis środowiska serwerowego PLI CBD”.

Produkcyjne serwery bazodanowe, na których uruchomione są instancje bazy E112 (Hyper-V):

Lokalizacja Siemianowice		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
S-LAN-SRVDB-1318	Windows Server 2016 Standard	MS SQL Server 2014 Standard
S-LAN-SRVDB-1319	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-LAN-SRVDB-2318	Windows Server 2016 Standard	MS SQL Server 2014 Standard
B-LAN-SRVDB-2319	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Produkcyjne serwery bazodanowe, na których uruchomione są instancje baz: NP2,ARCH_NP2, MAIN, ARCH_E112:

Lokalizacja Siemianowice			
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**	**Rola**
S-LAN-SRVDB-1320	Windows Server 2016 Standard	MS SQL Server 2014 Standard	principal
S-LAN-SRVDB-1321	Windows Server 2016 Standard	MS SQL Server 2014 Standard	mirror

Lokalizacja Borucza			
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**	**Rola**
B-LAN-SRVDB-2320	Windows Server 2016 Standard	MS SQL Server 2014 Standard	principal
B-LAN-SRVDB-2321	Windows Server 2016 Standard	MS SQL Server 2014 Standard	mirror

Produkcyjne serwery bazodanowe, na których uruchomione są instancje bazy SOU (Hyper-V):

Lokalizacja Siemianowice			
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**	**Rola**
S-INETSRVDB1114	Windows Server 2016 Standard	MS SQL Server 2014 Standard	principal
S-INETSRVDB1115	Windows Server 2016 Standard	MS SQL Server 2014 Standard	mirror

Lokalizacja Borucza			
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**	**Rola**
B-INETSRVDB2114	Windows Server 2016 Standard	MS SQL Server 2014 Standard	principal
B-INETSRVDB2115	Windows Server 2016 Standard	MS SQL Server 2014 Standard	mirror

Produkcyjne serwery bazodanowe, na których uruchomione są instancje bazy REPORT:

Lokalizacja Siemianowice		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
S-LAN-SRVRA1336	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-LAN-SRVRA2336	Windows Server 2016 Standard	MS SQL Server 2014 Standard

1.3. Wykaz serwerów testowych

Poniżej przedstawiony jest wykaz serwerów testowych, na których umiejscowione są poszczególne bazy danych. Szczegółowa specyfikacja fizyczna poniższych maszyn przedstawiona jest w dokumencie „Opis środowiska serwerowego PLI CBD”.

Testowe serwery bazodanowe, na których uruchomione są instancje bazy E112 (Hyper-V):

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-DMZ-SRVTT2225	Windows Server 2016 Standard	MS SQL Server 2014 Standard
B-DMZ-SRVTT2226	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Testowe Serwery bazodanowe, na których uruchomione są instancje baz: NP2, ARCH_NP2, MAIN, ARCH_E112 (Hyper-V):

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-DMZ-SRVTT2223	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-DMZ-SRVTT2224	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Testowe Serwery bazodanowe, na których uruchomione są instancje baz SOU (Hyper-V):

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-INETSRVTT2120	Windows Server 2016 Standard	MS SQL Server 2014 Standard
B-INETSRVTT2121	Windows Server 2016 Standard	MS SQL Server 2014 Standard

Testowe Serwery bazodanowe, na których uruchomione są instancje baz Report (Hyper-V):

Lokalizacja Borucza		
Nazwa Serwera	**System operacyjny**	**Serwer Bazy Danych**
B-DMZ-SRVTT2228	Windows Server 2016 Standard	MS SQL Server 2014 Standard

1.4. Replikacja (mirroring)

Jak zostało wspomniane powyżej dla części baz danych w ramach danej lokalizacji wykorzystany został wewnętrzny mechanizm serwera SQL (mirroring) pozwalający na replikowanie danych na drugi zapasowy serwer. W rozwiązaniu zastosowany został tryb synchroniczny z wykorzystaniem świadka.

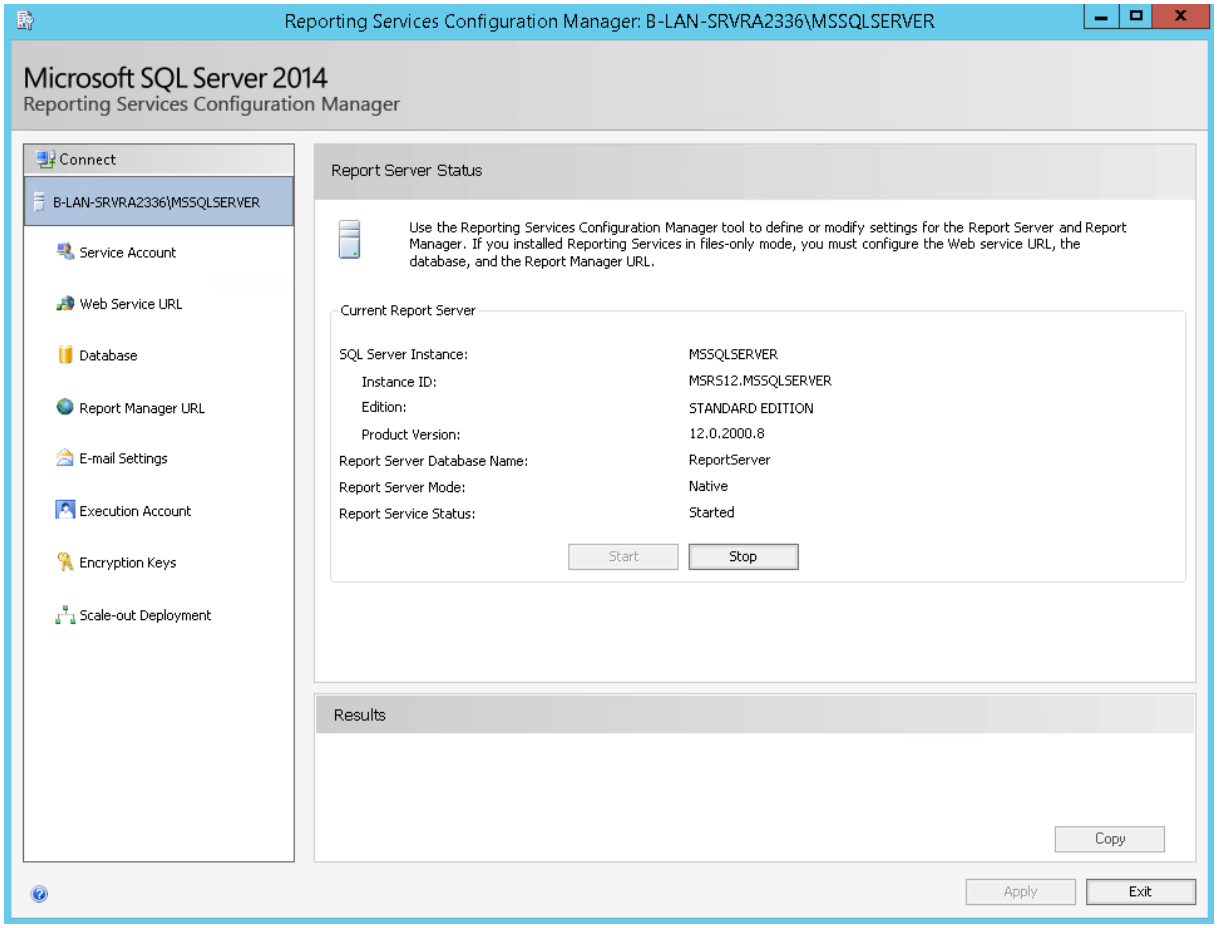
Dla serwerów bazodanowych, na których uruchomione są instancje baz MAIN, NP2, ARCH_NP2 ARCH_E112, świadkiem jest serwer bazodanowy uruchomiony na serwerze raportowym. Dla serwerów bazodanowych, na których uruchomione są instancje bazy SOU, świadkiem jest serwer bazodanowy uruchomiony na serwerze usługi WSUS (jest to serwer uruchomiony na potrzeby aktualizacji produktów Microsoft i nie jest on opisany w tym dokumencie).

2. Platforma Raportowa (Reporting Services)

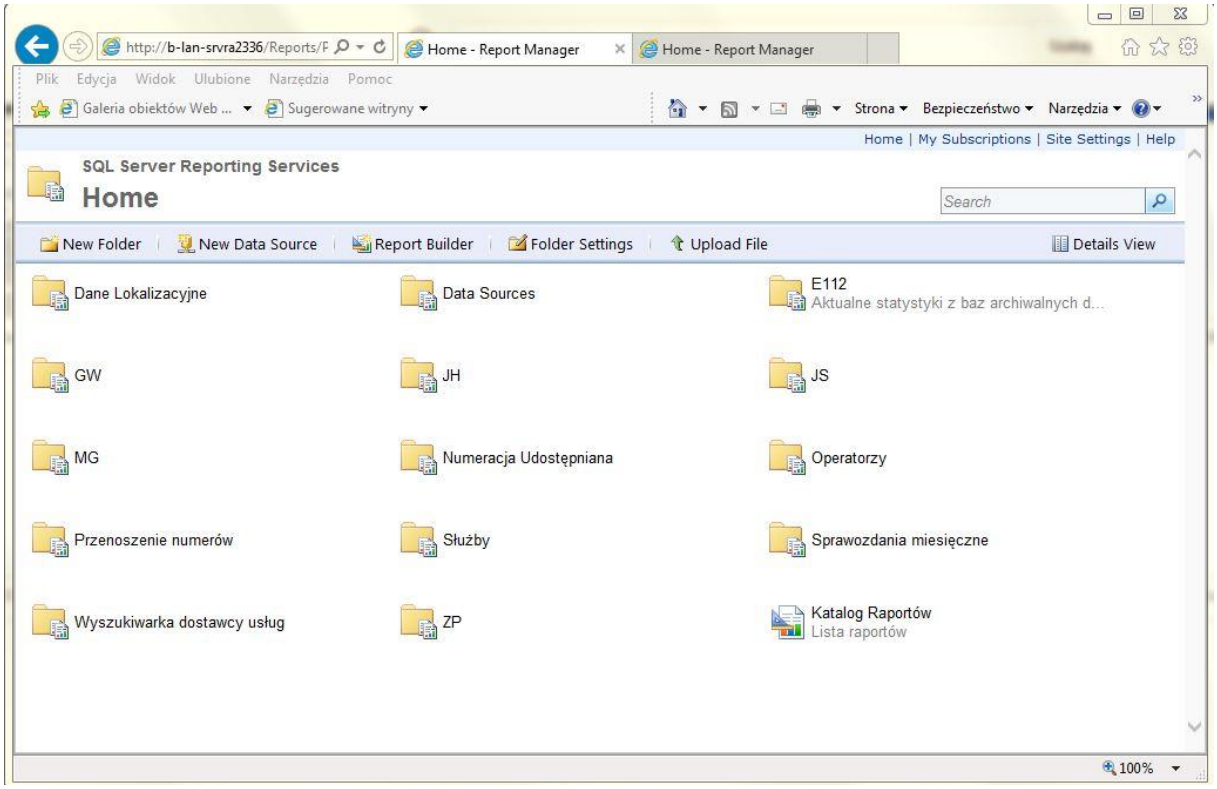
Na potrzeby wydziału PLI CBD wykonana została platforma generowania raportów oparta na usłudze Microsoft SQL Server Reporting Services. Platforma raportowa działa niezależnie od wbudowanego w aplikację PLI CBD modułu raportowego (ReportWeb). W każdej lokalizacji jest zainstalowany jeden serwer bazodanowy MS SQL Server z platformą raportową SQL Server Reporting Services.

Baza platformy raportowej zasilana jest danymi produkcyjnymi po wcześniejszym ich „zaciemnieniu", tak aby nie zawierała informacji wrażliwych. Zasilanie baz odbywa się raz dziennie za pomocą dedykowanych modułów przygotowanych przez wykonawcę systemu. Moduły te pracują opierając się na mechanizmie procedur zapamiętanych.

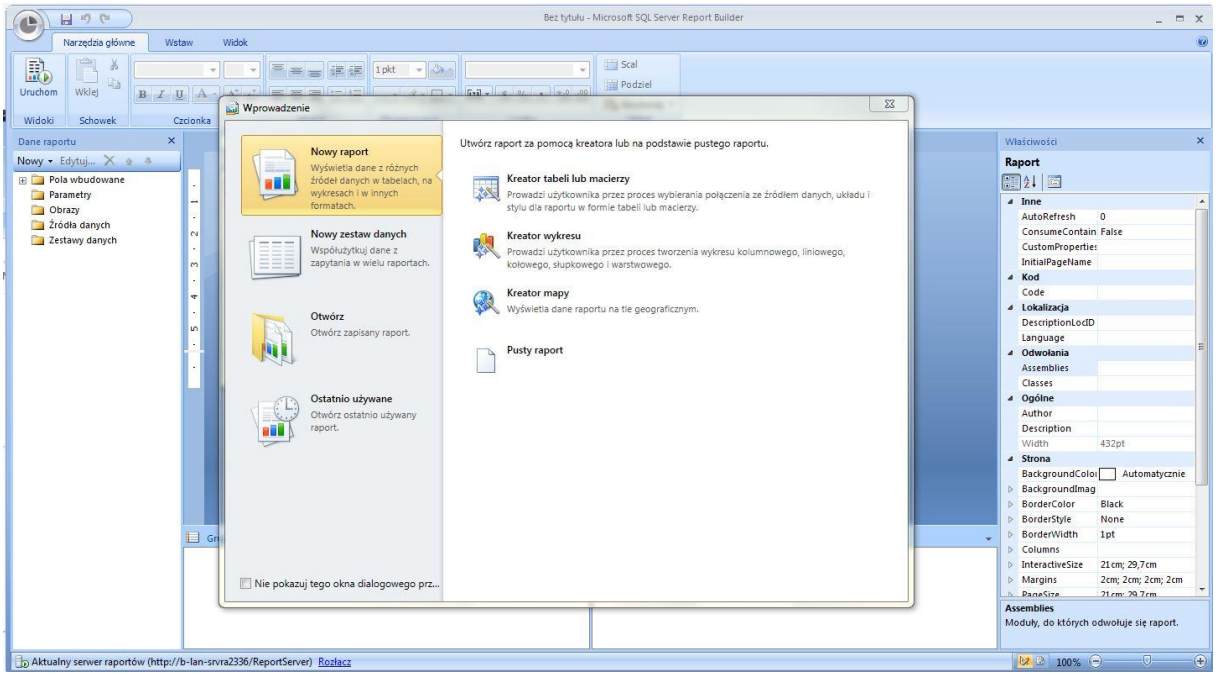
Zarządzanie usługą następuje poprzez Reporting Services Configuration Manager (dostępnej z poziomu systemu operacyjnego serwera):



Report Server uruchomiony został w trybie native. Dostęp (zarządzanie i przeglądanie) do raportów oraz pozostałych elementów (np. źródła danych) następuje poprzez aplikacje Report Manager.



Raporty tworzone są przy użyciu aplikacji ReportBuilder.



Lista serwerów raportowych:

Lokalizacja	Nazwa Serwera	Wersja
Siemianowice	S-LAN-SRVRA1336	MSSQL Reporting Services 2014

Lokalizacja	Nazwa Serwera	Wersja
Borucza	B-LAN-SRVRA2336	MSSQL Reporting Services 2014

3. System Centralnej kolekcji i korelacji zdarzeń

System PLI CBD jest zintegrowany z systemem RSA enVision klasy SIEM (Security Information and Event Management), który zbiera, zabezpiecza i archiwizuje logi zdarzeń z poszczególnych modułów.

Na system RSA składają się cztery urządzenia (po dwie na każda lokalizacje). Urządzenia działają niezależnie - każde urządzenie pobiera logi z serwerów aplikacyjnych (w jednej lokalizacji na dwóch serwerach enVision znajdują się te same logi z serwerów aplikacyjnych z danej lokalizacji). Każde z nich pobiera z serwerów aplikacji komplet danych.

Każdy serwer aplikacyjny udostępnia sieciowo logi (pliki tekstowe), które następnie są kopiowane przez agenta nicsftp zainstalowanego na serwerze enVision.

Serwery aplikacyjne udostępniają sieciowo katalog o nazwie „EnvLogs" dla każdego modułu aplikacji PLI CBD.

Pobieranie logów odbywa się w następujący sposób:

1. enVision (agent NICsftp) sprawdza czy na serwerze aplikacyjnym (połączenie do zasobu sieciowego) nie pojawił się nowy plik z logami lub też czy w istniejącym pliku tekstowym z zdarzeniami nie ma dodatkowych wpisów.

2. Nowe zdarzenia kopiowane są przez agenta NICsftp do enVision, które importuje je i realizuję analizę składni (parser).

Dla logów aplikacyjnych stworzono odpowiedni analizator składni (parser) (nowe logi wymagają modyfikacji wykonywanej przez ten analizator składni). Importowane logi są analizowane pod kątem składnik do odpowiednich pól wewnętrznej tabeli systemu RSA – „Windows Accounting". Konfiguracja analizatora składni znajduje się w systemie enVision w pliku:

E:\nic\4000\<nazwa_lokalizacji>\etc\devices\plicbd\plicbdmsg.xml.

Serwery aplikacyjne widoczne są jako urządzenia typu plicbd i do nich przyporządkowane są zdarzenia będące wynikiem działania analizatora składni.

Logi z serwerów aplikacyjnych składowane są w katalogu:

E:\nic\lsnode\data\<nazwa_lokalizacji>\plicbd.

Przykładowo logi z miesiąca marca 2023 znajdują się na jednym z serwerów enVision w katalogu:

E:\nic\lsnode\data\BLANENV2309-ES\plicbd\10.102.7.1\y2023\m03

3.1. Dostępy administracyjne

Dostęp do aplikacji RSA następuje poprzez przeglądarkę internetową z obsługą Java. Dostęp do systemu operacyjnego następuje poprzez zdalny pulpit.

Lista urządzeń RSA

Lokalizacja Siemianowice	
Nazwa Serwera	**Wersja**
SLANENV1309	RSA enVision 4.1.0 Build 0370
SLANENV1310	RSA enVision 4.1.0 Build 0370

Lokalizacja Borucza	
Nazwa Serwera	**Wersja**
BLANENV2309	RSA enVision 4.1.0 Build 0370
BLANENV2310	RSA enVision 4.1.0 Build 0370

4. IBM Guardium DAM (Database Activity Monitoring)

W sieci PLI CBD zainstalowano system monitorowania aktywności użytkowników w bazach danych w postaci 4 maszyn wirtualnych z oprogramowaniem SQL Guard 11.3.

W obu lokalizacjach zainstalowane są łącznie cztery (4) urządzenia (po dwa (2) urządzenia na lokalizację). W celu zwiększenia poziomu niezawodności i bezpieczeństwa wszystkie urządzania działają niezależnie i rejestrują ruch bazodanowy z lokalizacji, w której są uruchomione.

Na serwerach bazodanowych zainstalowane jest oprogramowanie (S-TAP) przechwytujące ruch (zapytania, parametry do procedury, działania administratorów) do baz danych. Każdy program S-TAP wysyła dane do dwóch serwerów Guardium w danej lokalizacji. S-TAP-y uruchomione są na serwerach BD na których zainstalowane są bazy E112, NP2,ARCH_NP2, MAIN, ARCH_E112. Dodatkowo S-TAP na serwerze na którym aktualnie bazy są w roli mirror zostaje wyłączony przez odpowiednie skrypty znajdujące się lokalnie na danym serwerze BD.

Do głównych zadań systemu należy monitorowanie dostępu do tabel zawierających dane wrażliwe oraz monitorowanie operacji DDL i DML.

4.1. Dostępy administracyjne

Dostęp do aplikacji Guadrium następuje poprzez przeglądarkę internetową z obsługą Java. Dostęp do systemu operacyjnego następuje poprzez protokół SSH.

Lista urządzeń GURDIUM

Lokalizacja Siemianowice		
Nazwa Serwera	**Typ urządzenie**	**Wersja**
SLANENV1307	Maszyna wirtualna	11.3
SLANENV1308	Maszyna wirtualna	11.3

Lokalizacja Borucza		
Nazwa Serwera	**Typ urządzenie**	**Wersja**
BLANENV2307	Maszyna wirtualna	11.3
BLANENV2308	Maszyna wirtualna	11.3