mMedica

Moduł Repozytorium P1 – instalacja i konfiguracja

Spis treści

1. WSTĘP 4

1.1. OPIS KOMPONENTU 4
1.2. WYMAGANIA 4
1.3. ZASADA DZIAŁANIA 5

2. INSTALACJA WINDOWS 6

2.1. INSTALACJA ZA POMOCĄ INSTALATORA 6
2.1.1. Czysta instalacja za pomocą instalatora 7
2.1.2. Doinstalowanie komponentu za pomocą instalatora 8
2.2. INSTALACJA MANUALNA 10
2.2.1. Dodawanie certyfikatów 11
2.2.2. Instalacja i konfiguracja komponentu 12
2.2.3. Ustawienie protokołu SSL 19
2.2.4. Konfiguracja nazwy aplikacji 20
2.3. WERYFIKACJA INSTALACJI 21
2.4. DODATKOWA KONFIGURACJA IIS 22
2.4.1. Zaawansowana konfiguracja witryn 22
2.4.2. Zaawansowana konfiguracja aplikacji 23
2.4.3. Konfiguracja wielu aplikacji na jednym porcie 25
2.5. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW 26
2.6. POWIĄZANIE INSTALACJI Z ISTNIEJĄCĄ APLIKACJĄ REPOZYTORIUM P1 27
2.7. AKTUALIZACJA MODUŁU 28

3. INSTALACJA W DYSTRYBUCJACH LINUX 29

3.1. INSTALACJA 29
3.2. KONFIGURACJA SERWERA ORAZ INSTALACJA MODUŁU 29
3.3. KONFIGURACJA NAZWY APLIKACJI 33
3.4. KONFIGURACJA ADRESU APLIKACJI 34
3.5. WERYFIKACJA INSTALACJI 34
3.6. KONFIGURACJA DODATKOWA APACHE 35
3.6.1. Zaawansowana konfiguracja witryn 35
3.7. KONFIGURACJA WIELU REPOZYTORIUM P1 NA JEDNYM SERWERZE 36
3.8. RESTARTOWANIE I ZATRZYMYWANIE KOMPONENTÓW 36
3.9. AKTUALIZACJA MODUŁU 37
3.10. POMOC 37

4. KONFIGURACJA APLIKACJI 38

4.1. KONFIGURACJA POŁĄCZENIA Z BAZAMI DANYCH 38
4.2. KONFIGURACJA NAZWY ORAZ ADRESU APLIKACJI 38

4.3. Przekierowanie nagłówków z proxy 38

5. OPERACJA ZWIĄZANE Z REPOZYTORIUM 40

5.1. Rejestracja repozytorium w P1 40
5.2. Zmiana adresu repozytorium w P1 41
5.3. Aktualizacja certyfikatu TLS lub WSS 42

6. ZMIANY W EARCHIWUM 42

6.1. Konfiguracja 42
6.2. Repozytoria P1 43
6.3. Historia pobrań dokumentów 43
6.4. Logi ATNA 44
6.4.1. Opis logu ATNA 46

7. POBIERANIE DANYCH DIAGNOSTYCZNYCH 47

8. ROZWIĄZANIA CZĘSTYCH PROBLEMÓW 47

8.1. Błąd „Niepoprawne hasło lub certyfikat" podczas rejestrowania repozytorium w P1 47
8.2. Biała strona komponentu po instalacji na IIS 47
8.3. Błąd 403.4 na localhost lub na adresie komponentu na IIS 48
8.4. Błąd 500.21 w IIS 48
8.5. Błąd 502.5 w IIS 48
8.6. Polecenie dotnet nie jest rozpoznawalne – Linux 48
8.7. Status serwisu Main process exited – Linux 48
8.8. Brak portu w statusie usługi – Linux 49
8.9. Strona jest widoczna wyłącznie z komputera lokalnego 49
8.10. Przekroczenie czasu realizacji operacji na bazie danych (timeout) 49
8.11. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows 50

1. Wstęp

1.1. Opis komponentu

RepozytoriumP1 służy do integracji modułu Archiwum z systemem wymiany dokumentów EDM P1. RepozytoriumP1 dostarcza repozytorium dokumentów z usługą IHE ITI-43 Retrieve Document Set, przez którą inne jednostki skomunikowane z systemem P1 mogą pobierać dokumenty medyczne w formie plików PIK HL7 CDA. Komunikacja pomiędzy RepozytoriumP1 a komponentem innej jednostki medycznej jest zabezpieczona za pomocą certyfikatów TLS oraz WSS dostarczonych przez system P1.

Zainstalowane i skonfigurowane RepozytoriumP1 należy zarejestrować w systemie P1 z poziomu mMedica (patrz: rozdział 5). W procesie rejestracji jednostka wysyła adres swojego repozytorium (stały oraz publiczny adres IP lub adres domenowy) a w odpowiedzi otrzymuje unikalny identyfikator (OID) repozytorium nadany przez system P1.

RepozytoriumP1 podczas żądania pobierania dokumentu weryfikuje w P1, czy została wyrażona zgoda przez pacjenta w systemie IKP (z wyjątkiem trybu ratowania życia) na pobranie dokumentu, a każda próba pobrania dokumentu jest zapisywana w systemie P1 za pomocą logu ATNA (IHE ITI-20 ATNA). Informacje o pobraniu dokumentu znajdują się również w panelu administracyjnym Archiwum.

1.2. Wymagania

Poniżej przedstawiono listę ogólnych warunków do uruchomienia i prawidłowego działania komponentu:

1. RepozytoriumP1 wymaga stałego oraz publicznego adresu IP (adres domenowy jest opcjonalny).
2. Zainstalowany i skonfigurowany moduł Archiwum wersji 6.9.0 lub wyższej.
3. Moduł Archiwum w wersji równej wersji RepozytoriumP1.
4. Zapewnione połączenie pomiędzy bazą danych Archiwum i komponentem RepozytoriumP1. Komunikacja do bazy danych powinna być bezpieczna tj. w ramach jednego komputera lub w ramach bezpiecznej sieci Intranet bądź za pomocą bezpiecznego VPN.
5. Dla funkcjonalności indeksowania dokumentów w P1 aplikacja Archiwum nie musi zostać udostępniona do sieci Internet. Ważne, aby aplikacja RezpozytoriumP1 była widoczna z sieci Internet.
6. Posiadanie certyfikatu TLS oraz WSS (inna nazwa WSSE) wydanych przez Centrum e-Zdrowia (w skrócie CeZ) do integracji z Platformą P1 (certyfikaty wykorzystywane dla eRecept). RepozytoriumP1 nie może zostać wystawione na innym certyfikacie TLS niż tym, który został dostarczony na potrzeby integracji z Platformą P1.

7. Możliwość komunikacji z systemu, gdzie zainstalowane jest RepozytoriumP1 na adres sus.ezdrowie.gov.pl na porcie 6514 przez TCP. Innymi słowy, aplikacja RepozytoriumP1 musi mieć możliwość – niezablokowanej przez firewall – komunikacji do adresu sus.ezdrowie.gov.pl na wskazanym porcie.
8. Zapewnione połączenie pomiędzy aplikacją eArchiwum a RepozytoriumP1.

Wymagania techniczne dotyczące m.in. systemu operacyjnego oraz oprogramowania są takie same jak w przypadku eArchiwum.

1.3. Zasada działania

Opis wymiany dokumentów w ramach P1 w wykorzystaniem RepozytoriumP1 przedstawia się następująco:

1. Podmiot A wykonuje jednorazową rejestrację swojego repozytorium w P1. P1 w tym procesie zwraca unikalny OID repozytorium. P1 udostępnia zintegrowanym podmiotom usługę, która pozwala za pomocą podanego OID pobrać fizyczny adres URL repozytorium.
2. Podmiot A wysyła dokument do swojego repozytorium, które zostało zarejestrowane w P1 (ma własny OID).
3. Podmiot A indeksuje dokument w systemie P1, w tym procesie przesyła informacje o dokumencie (ale bez samego dokumentu) oraz OID repozytorium, gdzie został dokument wysłany.
4. Podmiot B wyszykuje w systemie P1 dokumentu (informację o samym dokumencie, które opisane w punkcie 3), który został zindeksowany przez podmiot A. Operacja zgodna z IHE ITI-18.
5. Podmiot B odpytuje system P1 o adres repozytorium, gdzie znajduje się interesujący go dokument. Innymi słowy, podmiot B wysyła do usługi P1 OID repozytorium (który jest w informacjach o dokumencie), a system P1 zwraca fizyczny adres repozytorium.
6. Podmiot B wykonuje pobranie dokumentu z zarejestrowanego repozytorium podmiotu A (za pomocą fizycznego adres repozytorium). Operacja zgodna z IHE ITI-43.
7. Aplikacja RepozytoriumP1 podmiotu A otrzymuje żądanie pobrania dokumentu od podmiotu B i sprawdza, czy:
    a) Żądanie pobrania dokumentu zostało odpowiednio zabezpieczone m.in. czy certyfikaty TLS i WSSE są ważne (w czasie), nie zostały unieważnione i pochodzą z P1 (weryfikacja, czy pasują do pośrednich i nadrzędnych certyfikatów wydanych przez CeZ).
    b) Aplikacja RepozytoriumP1 łączy się do systemu P1, który sprawdza, czy pacjent w IKP wyraził zgodę na pobranie dokumentu przez placówkę B, jeśli tak dokument zostaje zwrócony; jeśli nie, dokument nie zostaje zwrócony. Uwaga, jeśli operacja jest wykonywana w trybie ratowania życia to system P1 pomija sprawdzanie zgody i zezwala na jego pobranie.

c) Aplikacja RepozytoriumP1 po każdej próbie pobrania dokumentu (udanej bądź nie) wysyła do systemu P1 log ATNA (operacja IHE ITI-20) z informacją jaki podmiot i osoba próbowała pobrać/pobrała dany dokument.

d) Aplikacja RepozytoriumP1 po każdej udanej próbie pobrania dokumentu zapisuje w bazie eArchiwum informacje, który podmiot i osoba pobrała dokument (widoczne jest to w Pobranych dokumentach w eArchiwum). Jeśli dokument nie mógł zostać udostępniony, aplikacja Repozytorium zapisuje informację do Dziennika Systemowego eArchiwum (zakładka API).

2. Instalacja Windows

Uwaga: RepozytoriumP1 wymaga publicznego oraz stałego adresu IP.

Uwaga: Funkcjonalności związane z RepozytoriumP1 wymagają zainstalowanego modułu Archiwum.

Uwaga: Proces instalacji środowiska uruchomieniowego .NEToraz IIS jest zamieszczony w instrukcji instalacji oraz konfiguracji Archiwum.

2.1. Instalacja za pomocą instalatora

Pełen proces instalacji za pomocą instalatora można przedstawić za pomocą następujących podpunktów:

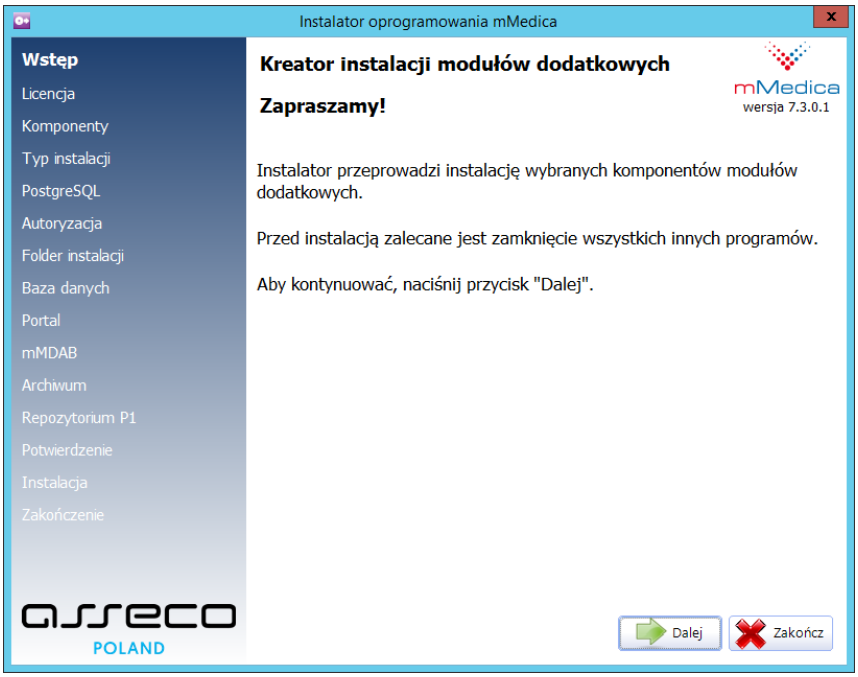
1. Instalacja serwera WWW.
2. Instalacja środowiska uruchomieniowego ASP .NET Core 6.0 oraz IIS (patrz: instrukcja instalacji i konfiguracji Archiwum).
3. Instalacja aplikacji przez instalator.
4. Weryfikacja instalacji.

Uwaga: Instalator może zainstalować wyłącznie jeden komponent danego typu. W przypadku chęci zainstalowania większej liczby komponentów należy wykonać instalację manualną.

Przykładowy proces instalacji opisuje instalacje wyłącznie RepozytoriumP1 przy założeniu, że moduł Archiwum został już zainstalowany. W przypadku, jeśli na tym samym komputerze, gdzie ma zostać zainstalowane Repozytorium P1 został zainstalowany jakikolwiek komponent mModułów należy przejść do punktu doinstalowania Repozytorium P1 za pomocą instalatora. W innym przypadku należy przejść do punktu czystej instalacji za pomocą instalatora

2.1.1. Czysta instalacja za pomocą instalatora

1. Uruchomić jako administrator plik instalatora modułów mMedica, który wyświetli formatkę powitalną. Przycisk strzałki w prawo pozwala przejść dalej (dotyczy to wszystkich kroków instalacji).



Rysunek 1: Formatka powitalna instalatora modułu

2. Zapoznać się z Umową Licencyjną. Aby ją zaakceptować należy zaznaczyć „Tak, zgadzam się z warunkami niniejszej Umowy Licencyjnej”.

Rysunek 2: Akceptacja umowy licencyjnej w instalatorze

3. Dalszą część kroków należy wykonać z Doinstalowanie komponentu za pomocą instalatora rozpoczynając od punktu 4.

2.1.2. Doinstalowanie komponentu za pomocą instalatora

1. Uruchomić jako administrator instalator modułów mMedica, który wyświetli tryb serwisowy.

Rysunek 3: Tryb serwisowy instalatora

2. Wybrać opcję „Zarządzaj modułami dodatkowymi”.
3. W oknie wybory zaznaczyć komponent Repozytorium P1 z sekcji „Moduł eArchiwum”.
4. Wybrać ścieżkę instalacji komponentu.

Rysunek 4: Wybór ścieżki instalacji komponentu

5. W oknie konfiguracji komponentu Repozytorium P1 należy skonfigurować połączenie do bazy danych Archiwum. Dodatkowo należy skonfigurować aplikację w IIS, w tym celu należy podać nazwę puli aplikacji, nazwę witryny IIS, port, pod którym zostanie udostępniona witryna, a także plik certyfikatu TLS oraz hasło do niego. W tym kroku należy podać końcowy certyfikat TLS, który został wydany przez CeZ. Na podstawie przekazanych danych instalator sam skonfiguruje aplikację Repozytorium P1 na serwerze IIS, a także zainstaluje niezbędne certyfikaty w systemie operacyjnym. System P1 nie wymaga, aby komponent RepozytoriumP1 był udostępniany na porcie 443.

   Uwaga, w przypadku doinstalowania komponentu nie należy zaznaczać opcji „Powiąż instalację z istniejącym na tym komputerze Repozytorium P1”.

Rysunek 5: Konfiguracja komponentu Repozytorium P1 przez instalator

6. Po pomyślnej instalacji pojawi się okno informacyjne.

2.2. Instalacja manualna

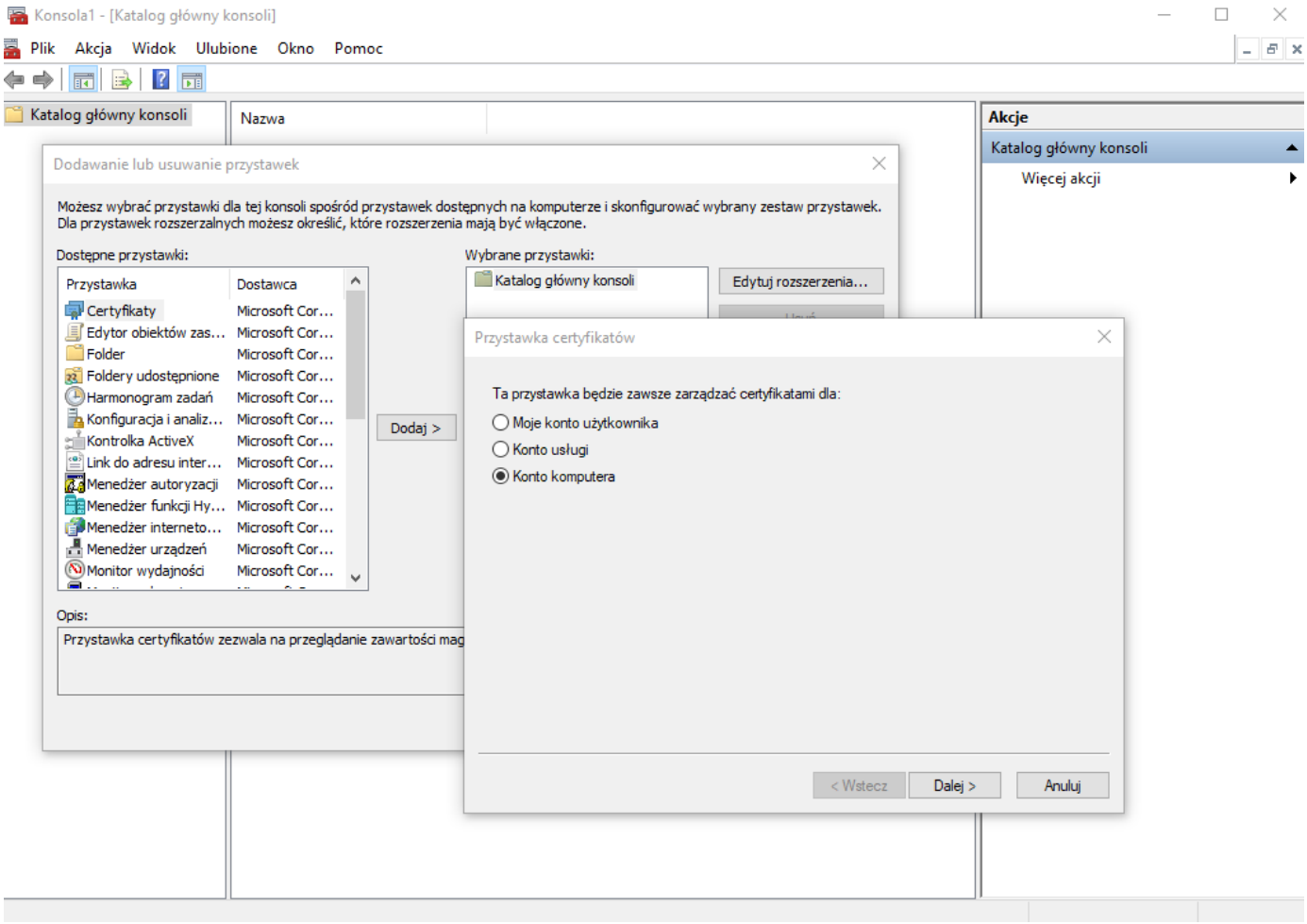
Instalacja manualna to proces, który można sprowadzić do następujących kroków:

1. Instalacja serwera WWW.
2. Instalacja środowiska uruchomieniowego ASP .NET Core 6.0 oraz IIS (patrz: instrukcja instalacji i konfiguracji Archiwum).
3. Dodawanie i konfiguracja certyfikatów.
4. Konfiguracja podstawowa serwera WWW (patrz: Instalacja i konfiguracja komponentu).
5. Skopiowanie plików poszczególnych komponentów (patrz: Instalacja i konfiguracja komponentu).
6. Konfiguracja połączenia z bazą danych Archiwum (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja).
7. Konfiguracja nazw aplikacji.
8. Weryfikacja instalacji.
9. Dodatkowa konfiguracja serwera WWW.

2.2.1. Dodawanie certyfikatów

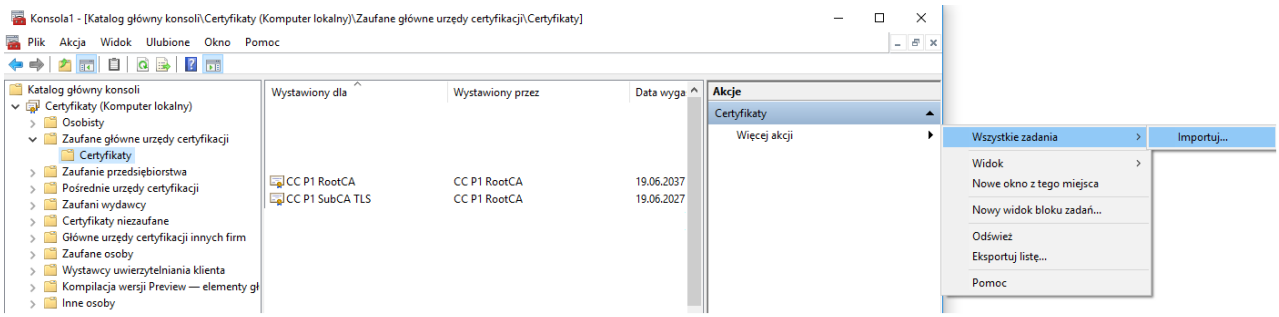
2.2.1.1. Certyfikaty nadrzędne

Do prawidłowej komunikacji należy pobrać certyfikaty nadrzędne P1 – odnośnik, a następnie skonfigurować je w systemie operacyjnym. W celu skonfigurowania certyfikatów nadrzędnych wykorzystywanych podczas weryfikacji certyfikatu klienta TLS, należy w wierszu poleceń wprowadzić komendę „MMC" i wcisnąć na klawiaturze klawisz „Enter". Operacja wymaga praw administratora. Po chwili powinno zostać otwarte okno. W oknie w menu „Plik" wybrać opcję „Dodaj/Usuń przystawkę…". Wybrać przystawkę „Certyfikaty" i ją dodać. Przy dodawaniu przystawki należy wybrać opcje „Konto komputera", a następnie opcję „Komputer lokalny".



Rysunek 6: Dodawanie certyfikatów nadrzędnych

Po dodaniu przystawki kliknąć przycisk „Ok". Rozwinąć katalog Certyfikaty i otworzyć katalog „Zaufane główne urzędy certyfikacji" > „Certyfikaty". Po otwarciu katalogu wybrać z prawej strony opcję „Więcej akcji" > „Wszystkie zadania" > „Importuj".



Rysunek 7: Importowanie certyfikatów nadrzędnych

Należy zaimportować dwa certyfikaty „CCP1RootCA” oraz „CCP1SubCATLS”, które należy umieścić w magazynie „Zaufane główne urzędy certyfikacji”. Oba certyfikaty są dostępne na stronie pobierania oprogramowania mMedica.

2.2.1.2. Certyfikat TLS

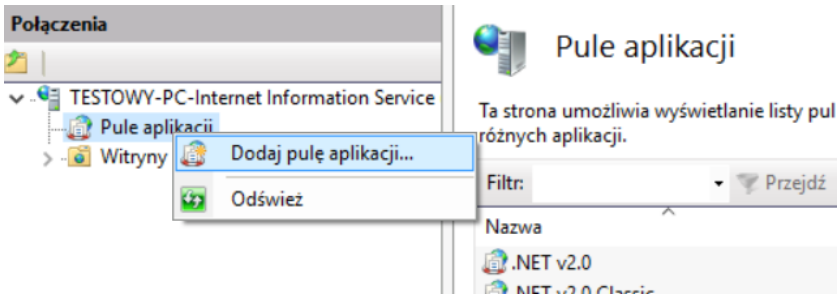
W celu skonfigurowania certyfikatu TLS wykorzystywanym do komunikacji z Repozytorium P1, należy w wierszu poleceń wprowadzić komendę „mmc” i wcisnąć na klawiaturze klawisz „Enter”. Operacja wymaga praw administratora. Po chwili powinno zostać otwarte okno. W oknie w menu „Plik” wybrać opcję „Dodaj/Usuń przystawkę…”. Wybrać przystawkę „Certyfikaty” i ją dodać. Przy dodawaniu przystawki należy wybrać opcje „Konto komputera”, a następnie opcję „Komputer lokalny”. Podobnie jak ma to miejsce przy konfiguracji certyfikatów nadrzędnych.

Rozwinąć katalog Certyfikaty i otworzyć katalog „Osobiste” > „Certyfikaty”. Po otwarciu katalogu wybrać z prawej strony opcję „Więcej akcji” > „Wszystkie zadania” > „Importuj”. Należy zaimportować certyfikat TLS dostarczony przez CeZ na potrzeby integracji z systemem P1. W przypadku braku widoczności certyfikatu należy w oknie wybierania zmienić zakres wyświetlanych rozszerzeń plików.

2.2.2. Instalacja i konfiguracja komponentu

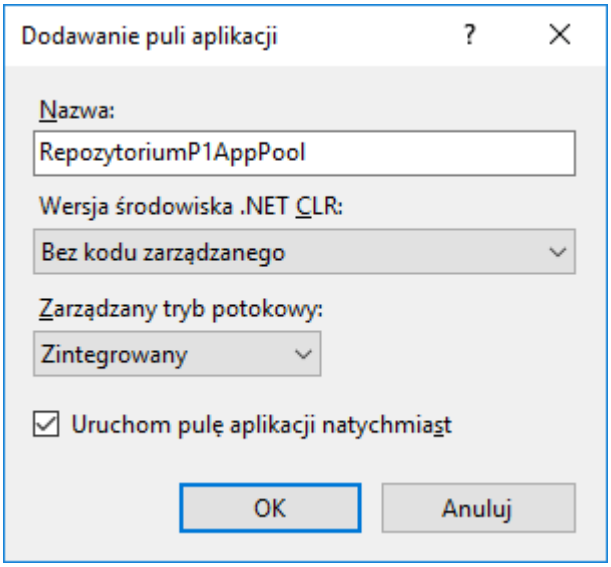
Proces instalacji:

1. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
    a) Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr” i zatwierdzić klawiszem Enter,
    b) Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
2. Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera, następnie kliknąć prawym przyciskiem myszy na ikonę podpisaną „Pule aplikacji” i wybrać opcję „Dodaj pulę aplikacji…”.



Rysunek 8: Tworzenie nowej puli aplikacji w programie IIS

3. Po wybraniu powyższej opcji powinno pojawić się okno, które należy uzupełnić jak poniżej. Nazwa puli aplikacji może być dowolna.

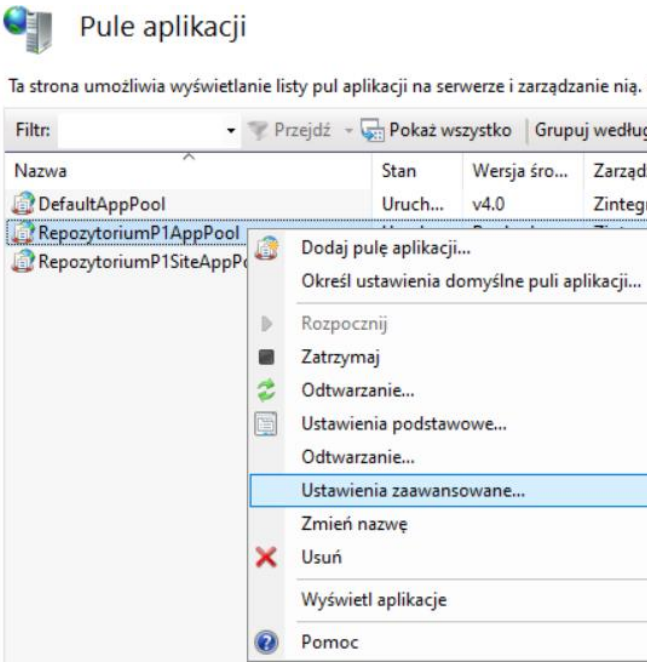


Rysunek 9: Tworzenie nowej puli aplikacji – ustawienia

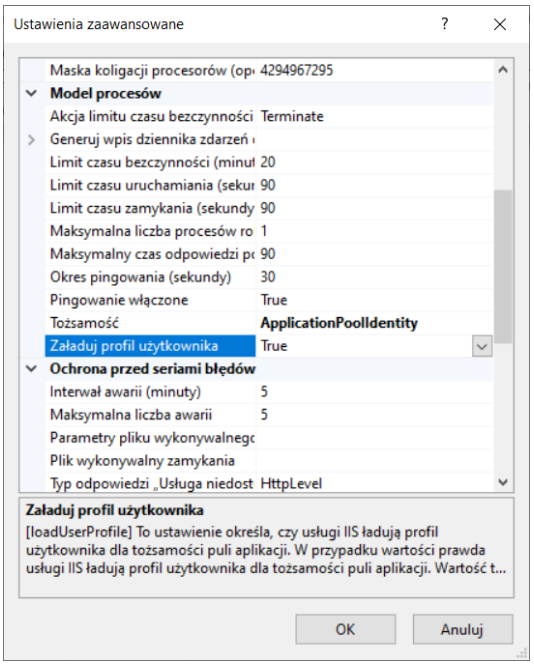
Krok można ponowić dodając drugą pulę aplikacji (takie same ustawienia, ale inną nazwą np. RepozytoriumP1SiteAppPool), która będzie dedykowana witrynie IIS, w której zostanie dodana aplikacja RepozytoriumP1. Pominięcie tego kroku spowoduje, że pula aplikacji powstanie automatycznie przy tworzeniu witryny IIS.

4. Na liście puli aplikacji kliknąć prawym przyciskiem myszy na utworzoną pulę dla Repozytorium P1 (w przykładzie RepozytoriumP1AppPool), a następnie z menu kontekstowego wybrać opcję „Ustawienia zaawansowane…”. W oknie ustawień odszukać pozycję „Załaduj profil użytkownika” (grupa „Model procesów”) i upewnić, się, że ma ustawioną wartość na „True” Jeśli opcja ustawiona jest na „False” należy ją przestawić i zapisać ustawienia. Dodatkowo, należy upewnić się, że dla puli aplikacji dla aplikacji mMedica Archiwum również wartość parametru „Załaduj profil użytkownika” jest ustawiona na „True”.

Uwaga: Brak ustawienia wartości „Załaduj profil użytkownika” na „True” dla puli aplikacji Archiwum w IIS może powodować błąd informujący o błędnym certyfikacie lub haśle podczas rejestracji repozytorium w systemie P1.

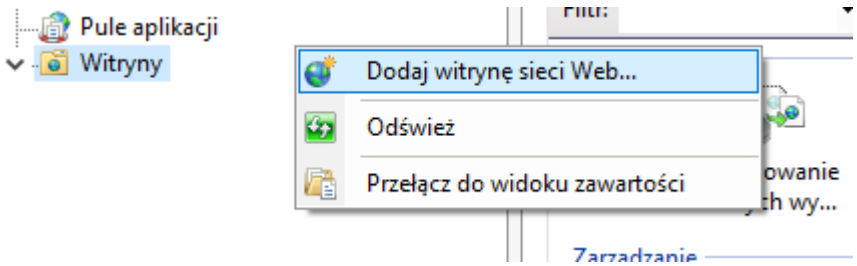


Rysunek 10 Uruchomienie ustawień zaawansowanych puli aplikacji na przykładzie puli aplikacji dla RepozytoriumP1



Rysunek 11: Ustawienia zaawansowane puli aplikacji

5. Kliknąć prawym przyciskiem myszy na „Witryny” i wybrać opcję „Dodaj witrynę sieci Web…”.

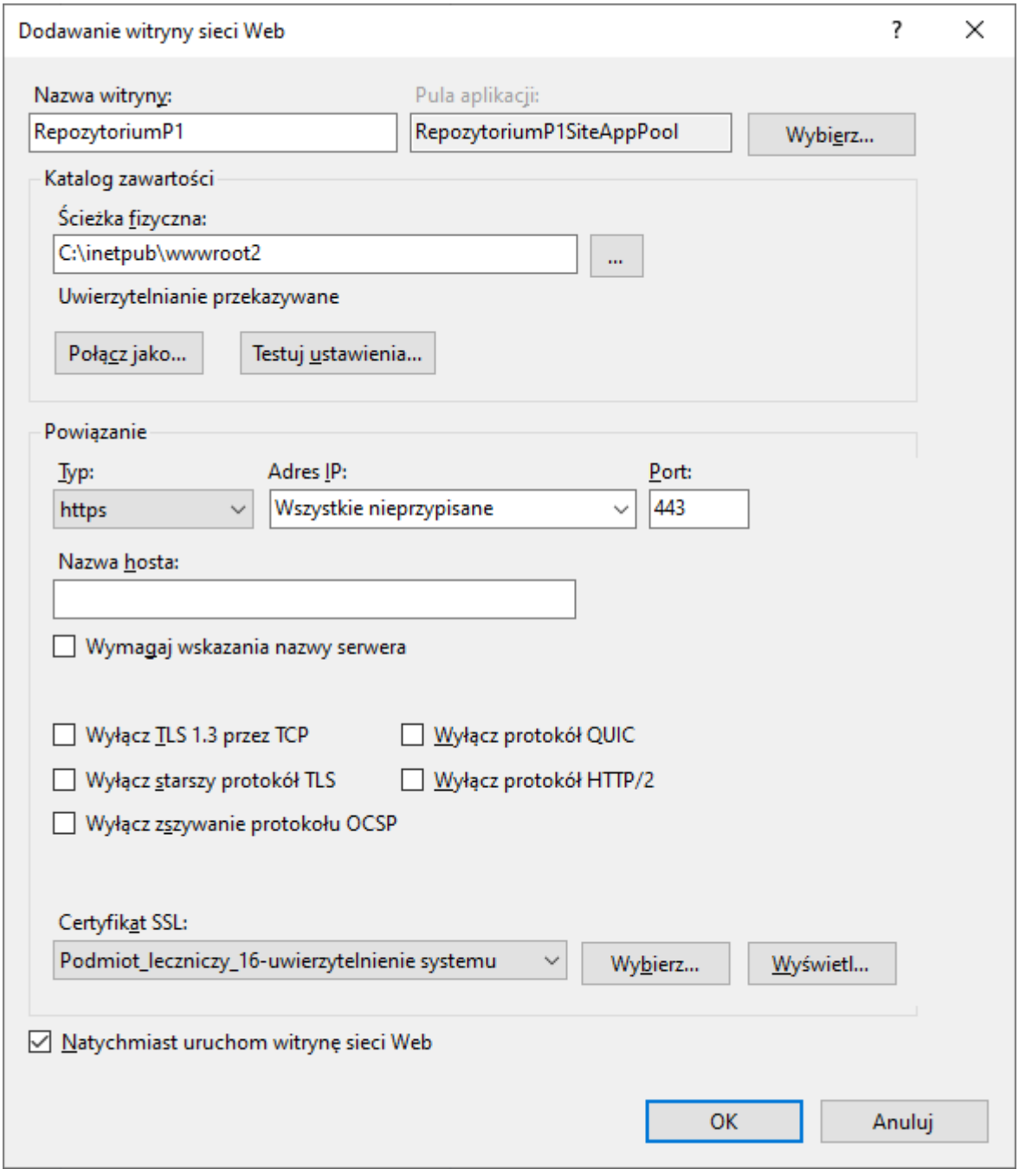


Rysunek 12: Dodawanie nowej witryny

6. Uzupełnić okno według zrzutu przedstawionego poniżej. Nazwa tworzonej witryny musi być unikalna (w przykładzie użyto nazwy RepozytoriumP1). Przy wybieraniu dowolnej fizycznej ścieżki do folderu, do którego w późniejszym etapie zostaną skopiowane pliki komponentu, można posłużyć się przyciskiem „…”. Zaleca się utworzenie osobnego folderu C:\inetpub (na potrzeby przykładu utworzono katalog wwwroot2). Za pomocą przycisku „Wybierz…” można wybrać zdefiniowaną wcześniej pulę aplikacji dla witryny IIS (jeśli nie zostanie wybrana, IIS utworzy pule aplikacji automatycznie). Przy konfiguracji Repozytorium P1 należy powiązanie typu https oraz wskazać certyfikat TLS (wydany przez

CeZ na potrzeby systemu P1). System P1 nie wymaga, aby komponent RepozytoriumP1 był udostępniany na porcie 443. Można wybrać niewykorzystany port. W przypadku posiadania wielu komponentów RepozytoriumP1 każdy z nich musi być udostępniany na unikalnym adresie usługi lub porcie.

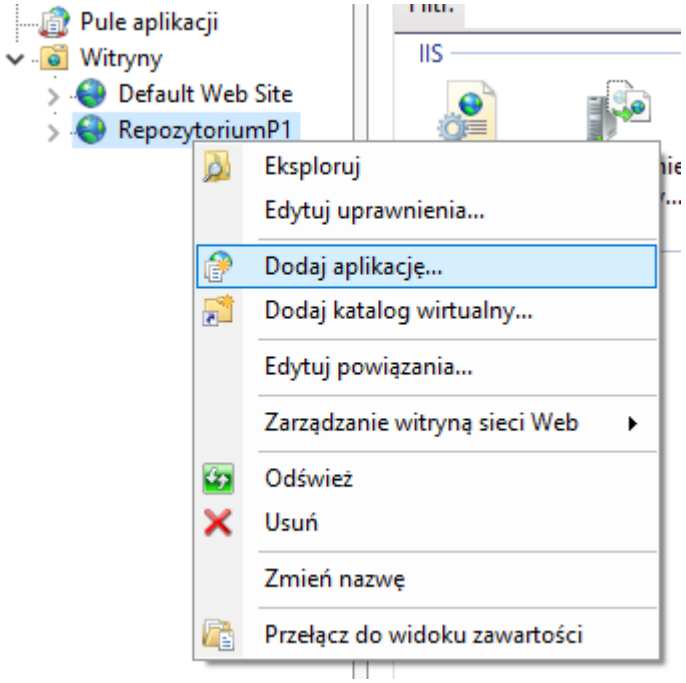
Uwaga: System P1 weryfikuje podczas rejestracji repozytorium w systemie P1, czy nie istnieje już zarejestrowane repozytorium pod danym adresem usługi i wskazanym porcie. Od dnia 30.06.2021 System P1 nie wymaga, aby RepozytoriumP1 było instalowane zawsze na unikalnym porcie przy korzystaniu z tego samego adresu usługi.



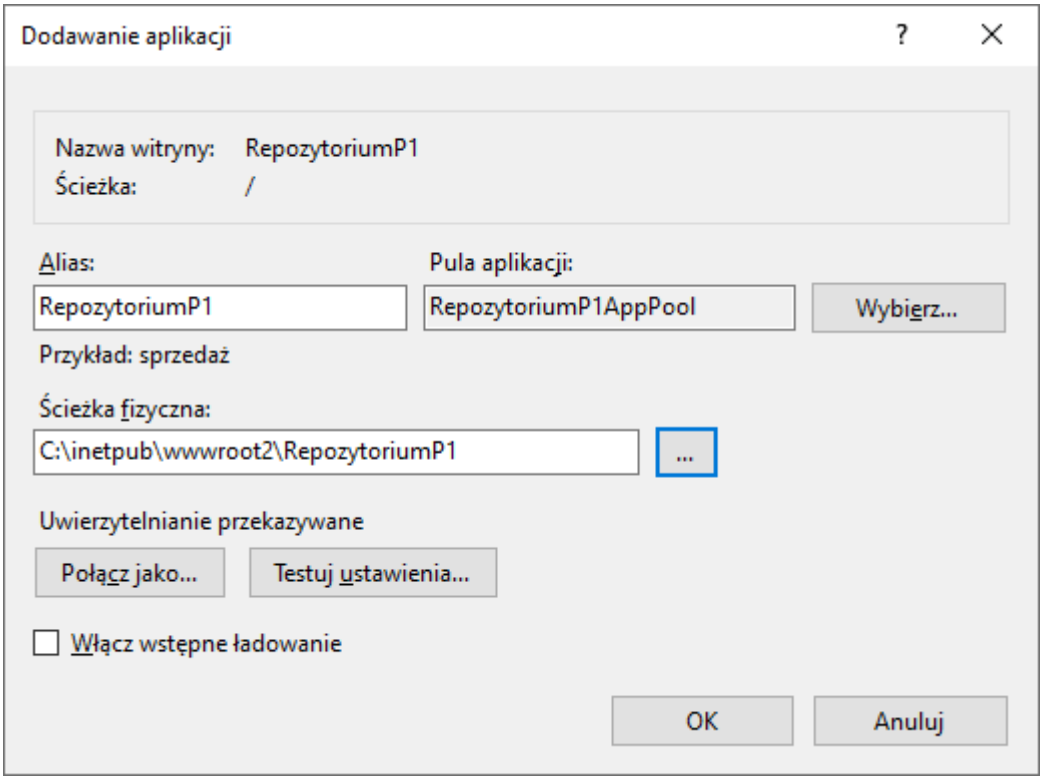
Rysunek 13: Dodawanie nowej witryny

7. Dodawanie aplikacji do witryny nie jest krokiem niezbędnym tj. aplikacja może działać bezpośrednio w witrynie bez konieczności dodawania dedykowanej puli aplikacji. Jednak na potrzeby procesu instalacji aplikacja zostanie utworzona. W tym celu należy z menu kontekstowego utworzonej witryny wybrać pozycję „Dodaj aplikację…”. Następnie w oknie dodawania aplikacji uzupełnić jej nazwę (alias)

oraz utworzoną wcześniej pulę aplikacji (przez przycisk „Wybierz”). Dodatkowo należy ustalić ścieżkę fizyczna do katalogu, w którym znajdą się pliki aplikacji (ścieżka może być taka sama jak w utworzonej witrynie).



Rysunek 14: Tworzenie aplikacji w witrynie

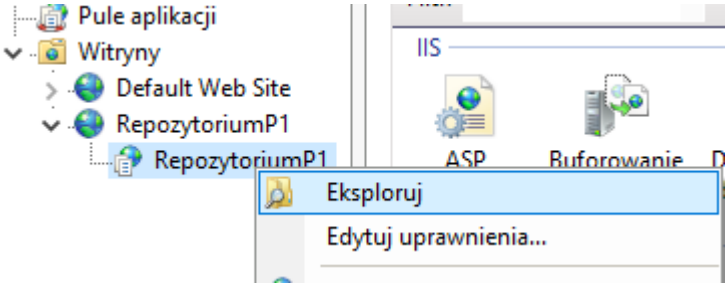


Rysunek 15: Dodawanie nowej aplikacji

8. Pobrać pliki komponentów – odnośnik. Skopiować z dostarczonego archiwum pliki (ścieżki dla przykładu z zrzutu powyżej):

   - Repozytorium P1 do: *C:\inetpub\wwwroot2\RepozytoriumP1*

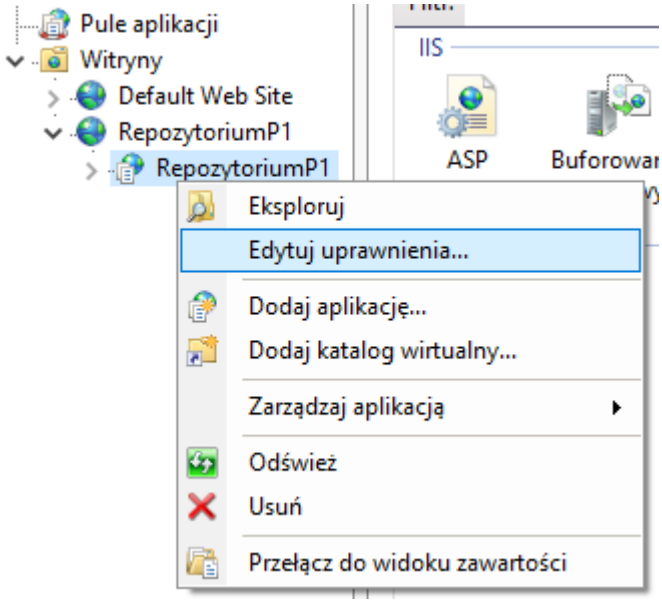
   Dla ułatwienia odszukania właściwego katalogu możliwe jest użycie opcji „Eksploruj”. Pojawia się ona do wyboru po naciśnięciu prawego przycisku myszy na dowolną aplikację (np. RepozytoriumP1) w oknie „Połączenia”.



Rysunek 16: Otworzenie katalogu aplikacji

9. Zaleca się umieszczanie plików komponentów w ścieżce C:\inetpub, gdyż jest to folder przeznaczony do przechowywania plików IIS. Jeśli pliki komponentów zostały skopiowane do innego katalogu, możliwe jest wyświetlenie w oknie przeglądarki błędu 502.5 w procesie weryfikacji instalacji. W takim przypadku wymagane jest dodatkowe nadanie uprawnień, które zezwolą puli aplikacji na odczyt plików z danej ścieżki. Proces nadawania:

   a) Przejść do ścieżki pliku lub folderu komponentu. Następnie kliknąć prawym przyciskiem myszy na plik lub folder i wybrać z menu kontekstowego „Właściwości”. Można również posłużyć się opcją „Edytuj uprawnienia…” dostępną w menu kontekstowym po wybraniu odpowiedniej aplikacji w IIS (patrz: *Rysunek 17: Edycja uprawnień do katalogu w IIS*).



Rysunek 17: Edycja uprawnień do katalogu w IIS

b) Przejść do górnej zakładki „Zabezpieczenia”.

c) Wybrać przycisk „Edytuj”.

d) W oknie nadawania uprawnień wybrać przycisk „Dodaj”.

e) W dolnym polu tekstowym wpisać nazwę IIS APPPOOL\[Nazwa puli aplikacji], czyli dla przykładu: „IIS APPPOOL\RepozytoriumP1AppPool” (dla katalogu Repozytorium P1 należy wybrać pulę aplikacji utworzoną dla Repozytorium P1).

f) Następnie kliknąć opcję sprawdzania nazwy „Sprawdź nazwy” oraz zatwierdzić przyciskiem „OK”. Jeśli nazwa została odnaleziona, zostanie podkreślona.

g) Zaznaczyć dodanego użytkownika (podaną wcześniej nazwę) kliknięciem myszy. W dolnym polu nadać użytkownikowi uprawnienia: „Odczyt i wykonywanie”, „Odczyt”. Zatwierdzić zmianę przyciskiem OK.

10. Nadać uprawnienia do zapisu dla plików:

a) Dla puli Repozytorium P1:

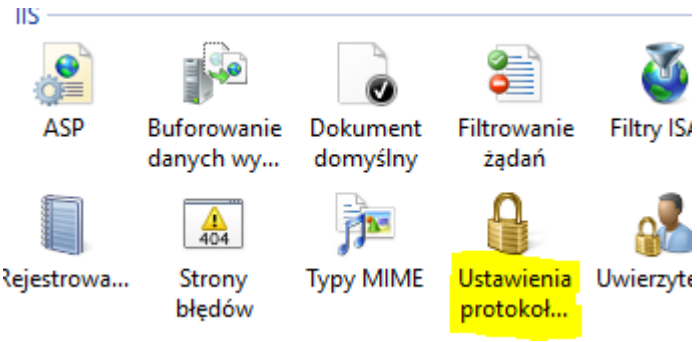
- [Ścieżka do Repozytorium P1]\application.log
  dla przykładowej instalacji: *C:\inetpub\wwwroot2\RepozytoriumP1*\application.log

2.2.3. Ustawienie protokołu SSL

Uwaga: Brak wykonania konfiguracji protokołu SSL spowoduje zagrożenie w bezpieczeństwie komunikacji oraz nieprawidłowe działanie aplikacji RepozytoriumP1.

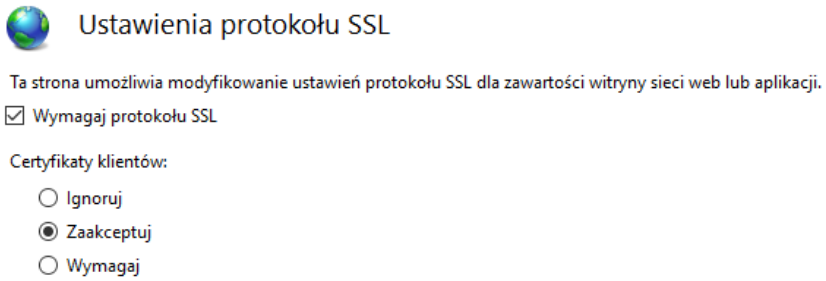
Ustawienie wymagalności protokołu SSL dokonuje się w następujący sposób:

1. Otworzyć Menedżer internetowych usług sieciowych (IIS).
2. W witrynie dedykowanej dla Repozytorium P1 wybrać z głównego okna opcję „Ustawienia protokołu SSL”.



Rysunek 18: Ustawienia protokołu SSL

3. Zaznaczyć opcję „Wymagaj protokołu SSL” oraz w sekcji certyfikaty klientów wybrać opcję „Zaakceptuj”.

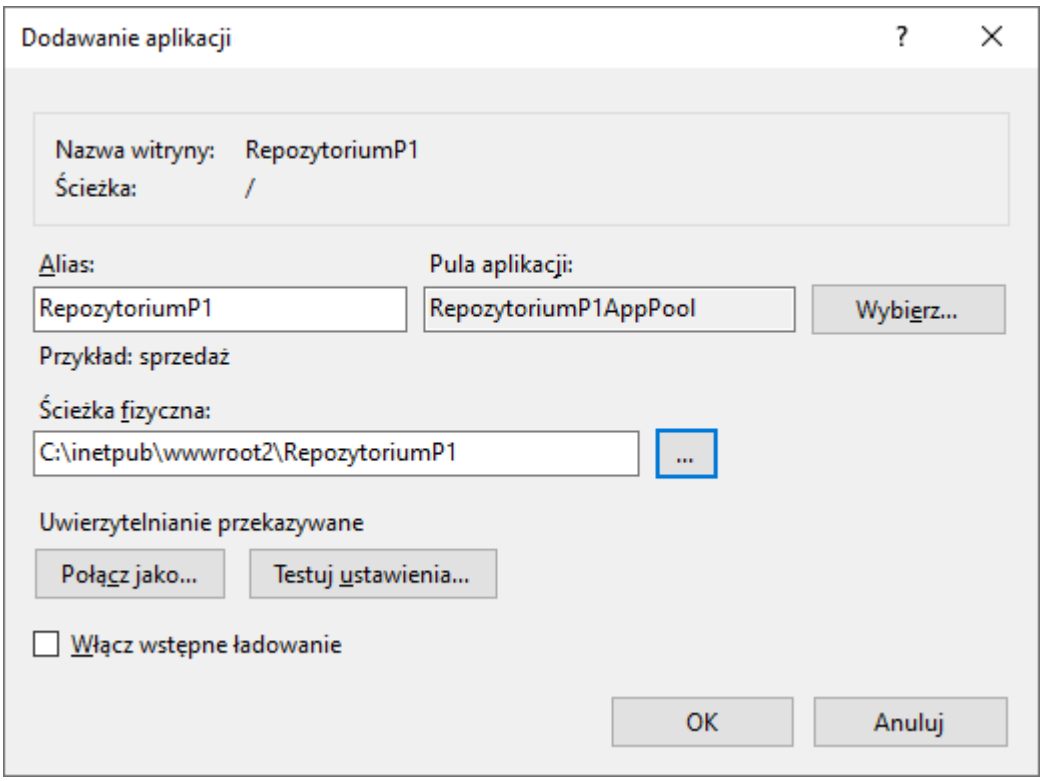


Rysunek 19: Parametry ustawienia protokołu SSL

2.2.4. Konfiguracja nazwy aplikacji

Uwaga: Konfiguracja nazw aplikacji odbywa się identycznie jak w module eRejestracja. Krok należy pominać jeśli nie utworzono dedykowanej aplikacji dla aplikacji Repozytorium P1.

Jeśli Repozytorium P1 nie ma swojego własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji, należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna. Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera IIS. Nazwa ta znajduje się w zaznaczonych miejscach:



Rysunek 20: Identyfikacja nazwy aplikacji

Nazwę tą należy umieścić w sekcji ApplicationName, dla przykładowej konfiguracji:

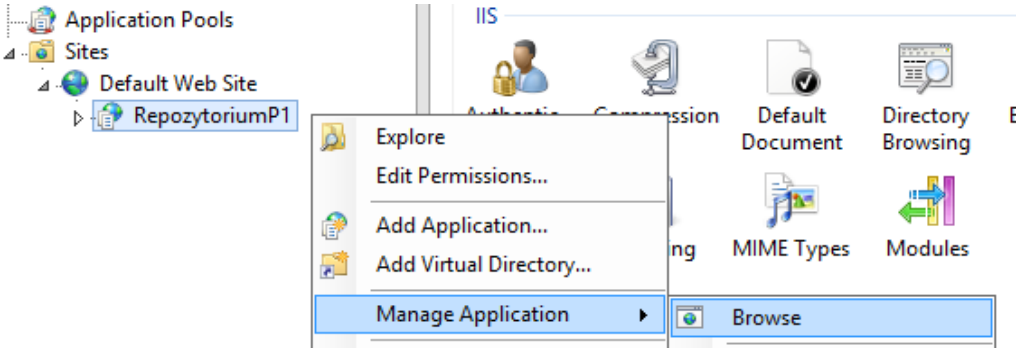
```
"ApplicationName": "RepozytoriumP1"
```

Nazwy powinny być unikalne w ramach jednego serwera WWW.

2.3. Weryfikacja instalacji

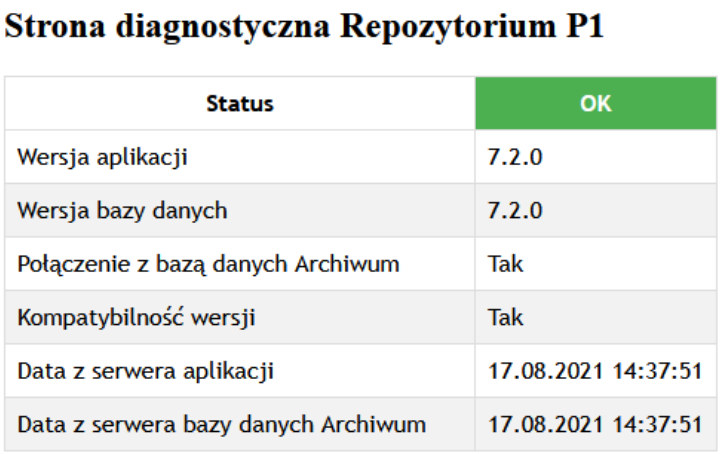
Po instalacji przez instalator jak i instalacji manualnej należy zweryfikować, czy instalacja została przeprowadzona poprawnie. Proces weryfikacji wygląda następująco:

1. Uruchomić Menedżer internetowych usług informacyjnych IIS (Internet Information Service Manager). Poniżej zamieszczono sposoby uruchomienia:
    a. Menu Start\Uruchom (skrót: klawisz Windows + r), wpisać „inetmgr" i zatwierdzić klawiszem Enter,
    b. Menu Start\Panel Sterowania\Narzędzia administracyjne\Menedżer internetowych usług informacyjnych (IIS).
2. Rozwinąć drzewo połączeń tak, aby widoczna była aplikacja, którą należy zweryfikować. Klikając prawym przyciskiem myszy na wybraną aplikację należy wybrać Zarządzaj aplikacją\Przeglądaj, co spowoduje uruchomienie aplikacji w przeglądarce internetowej.



Rysunek 21: Podgląd aplikacji z poziomu IIS

3. Weryfikacja usługi sieciowej Repozytorium P1 odbywa się poprzez wejście na stronę statusową usługi. Dla konfiguracji przykładowej adres wygląda następująco https://localhost/RepozytoriumP1. Jeśli nie utworzono dedykowanej aplikacji w IIS to adresem komponentu będzie: https://localhost. Uwaga, w przeglądarce internetowej po wejściu na stronę statusową aplikacji pojawi się ostrzeżenie o nieprawidłowej konfiguracji HTTPS. Jest to normlanej sytuacja, która wynika z faktu, że certyfikat TLS wydany przez CeZ nie jest powiązany z adresem domenowym aplikacji. Po akceptacji wyjątku wyświetlona zostanie strona statusowa dla aplikacji Repozytorium P1. Strona statusowa pozwala zweryfikować czy połączenie z bazą danych jest prawidłowe. Rezultat poprawnego działania Repozytorium P1 wygląda następująco:



Strona diagnostyczna Repozytorium P1

Status	OK
Wersja aplikacji	7.2.0
Wersja bazy danych	7.2.0
Połączenie z bazą danych Archiwum	Tak
Kompatybilność wersji	Tak
Data z serwera aplikacji	17.08.2021 14:37:51
Data z serwera bazy danych Archiwum	17.08.2021 14:37:51

Rysunek 22: Weryfikacja działania aplikacji Repozytorium P1

Błąd 500.21 oznacza problem z modułem .NET dla IIS – rozwiązanie zostało poruszone w rozdziale *4.3. Błąd 500.21*.

Z kolei w przypadku, w którym wymagane jest SSL i zostanie wyświetlona biała strona lub błąd 403.4, należy poprawić konfigurację SSL zgodnie z powyższą instrukcją.

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych Archiwum,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).

4. Po wejściu przeglądarką internetową na stronę statusową Repozytorium P1 należy również zweryfikować, czy aplikacja przedstawia się certyfikatem TLS wydanym przez CeZ, który został skonfigurowany dla witryny na serwerze www.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale 7.

2.4. Dodatkowa konfiguracja IIS

2.4.1. Zaawansowana konfiguracja witryn

Edycja powiązań (zmiana: portu, nazwy hosta, certyfikatu, powiązania IP):

1. Uruchomić manager IIS.
2. Na wybranej witrynie kliknąć prawym przyciskiem „Edytuj powiązania…”.
3. W oknie zaznaczyć istniejące powiązanie (domyślnie http na porcie 80) i wybrać przycisk „Edytuj…” lub przycisk „Dodaj…”.

4. W oknie „Edytowanie powiązań witryny” można zdefiniować typ, nazwę hosta oraz port. Dodatkowo istnieje możliwość przypisania konkretnego adresu IP, z którego będzie dostępna witryna (opcja „Wszystkie nieprzypisane” oznacza dostępność dla wszystkich dostępnych adresów IP).

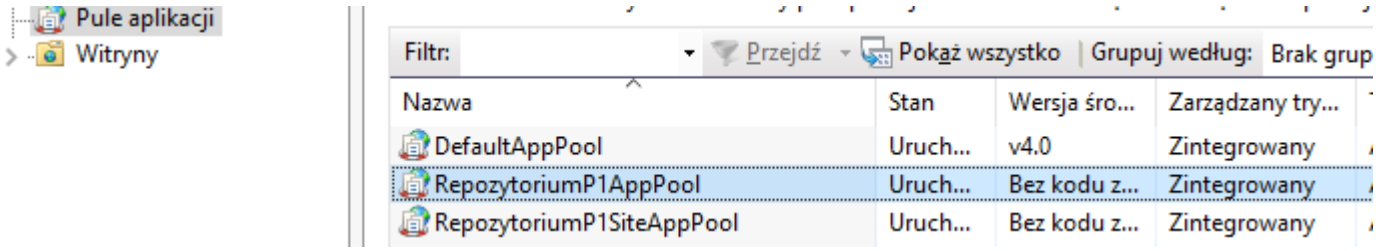
Uwaga: Każda z witryn, która nie posiada przypisanego adresu domenowego musi mieć unikalne numery portów.

Uwaga: W przypadku wykorzystywania innych portów niż 80 (dla http) oraz 443 (dla https) należy posługiwać się adresem zawierającym port np. http://localhost:81 (dla portu 81).

2.4.2. Zaawansowana konfiguracja aplikacji

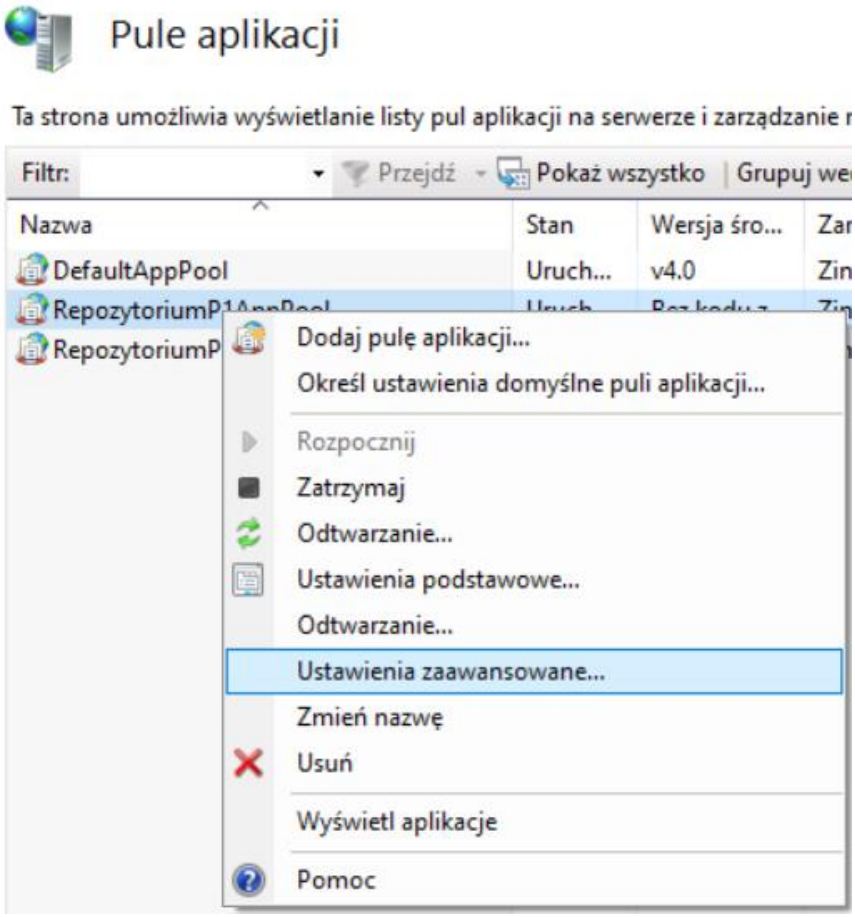
W celu wydłużenia czasu usypiania aplikacji w środowisku IIS należy uruchomić Menedżer internetowych usług informacyjnych.

Rozwinąć po lewej stronie drzewko „Połączenia” na nazwie komputera i wybrać opcję „Pule aplikacji”.



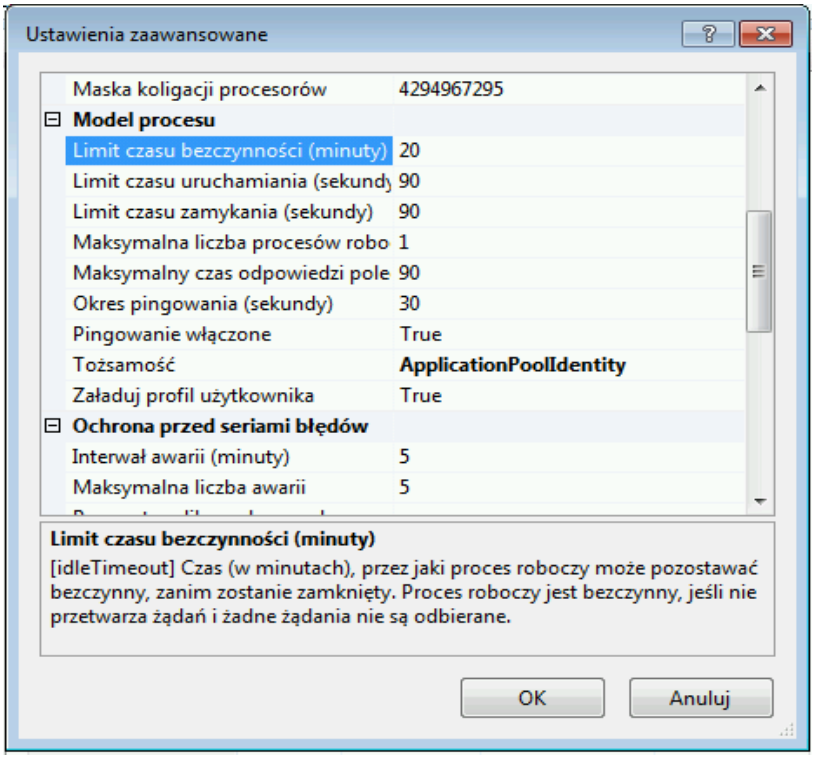
Rysunek 23: Drzewko "Połączenia" w aplikacji IIS Manager

Po wybraniu powyższej opcji po prawej stronie pojawi się okno do zarządzania pulami aplikacji. Z listy dostępnych pul należy wybrać interesującą nas pulę, kliknąć na nią prawym przyciskiem myszy i wybrać opcję „Ustawienia zaawansowane…”.



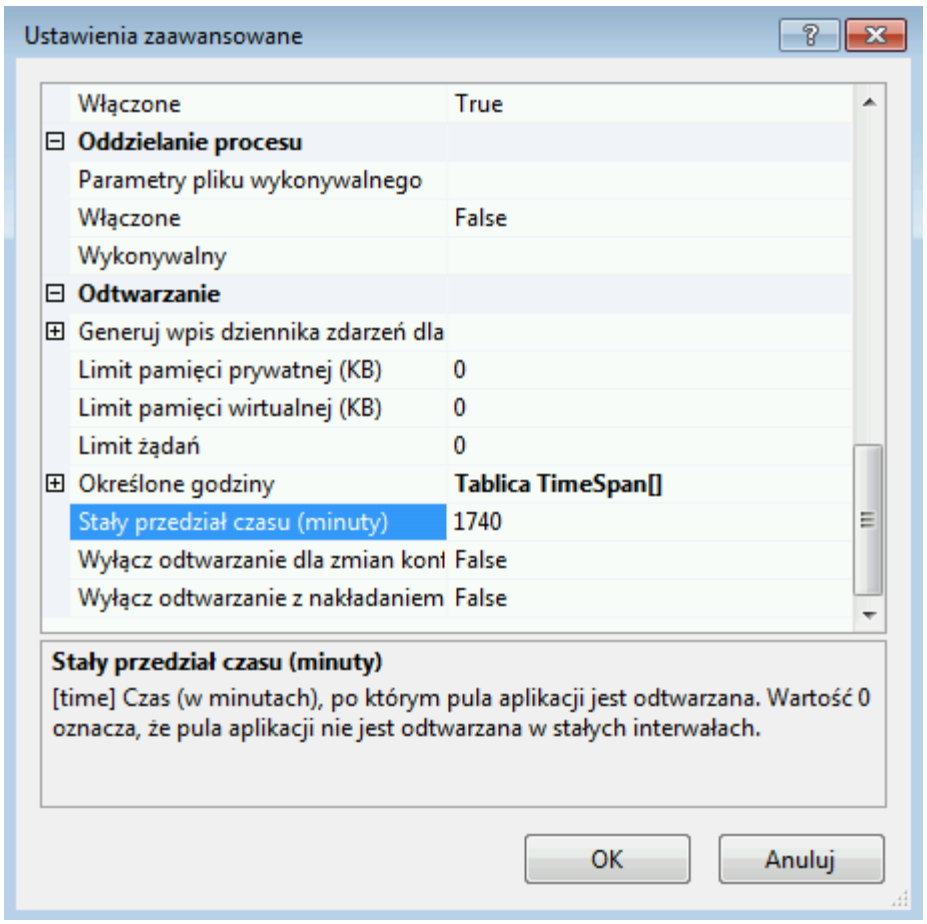
Rysunek 24: Okno zarządzania pulami aplikacji

Po wybraniu opcji pojawi się okno konfiguracji.



Rysunek 25: Okno konfiguracji - "Ustawienia zaawansowane": Limit czasu bezczynności (minuty)

Modyfikowanie wartości w polu „Limit czasu bezczynności (minuty)” pozwala na wydłużenie/skrócenie czasu, po którym aplikacja przejdzie w stan uśpienia. Ustawienie wartości 0 pozwala na skonfigurowania aplikacji tak, aby nie była ona usypiana.



Rysunek 26: Okno konfiguracji - "Ustawienia zaawansowane": Stały przedział czasu (minuty)

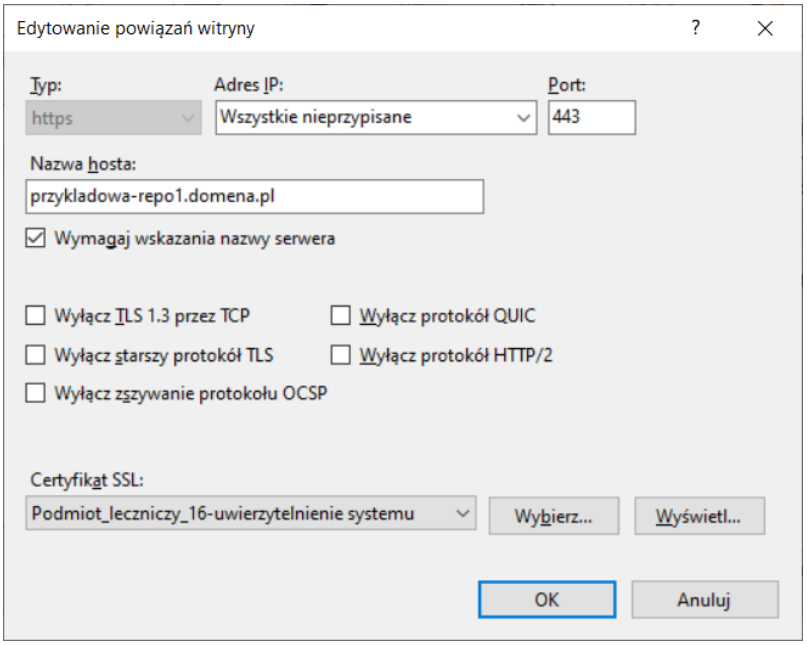
Kolejnym parametrem jest „Stały przedział czasu (minuty)”. Pozwala on na określenie czasu, po jakim pula aplikacji powinna ulec zrestartowaniu. Parametr ten również można ustawić na wartość 0. Spowoduje to, że pula aplikacji nie będzie restartowana. Nie jest to zalecane ze względu na zużywanie pamięci przez aplikację, gdyż w przypadku wykorzystania zbyt dużej ilości zasobów może dojść do błędów.

2.4.3. Konfiguracja wielu aplikacji na jednym porcie

Istnieje możliwość konfiguracji wielu aplikacji (np. eArchiwum, RepozytoriumP1) na jednym porcie (np. 443) pod warunkiem spełnienia wszystkich poniższych warunków:

1. Wszystkie witryny IIS (które mają działać na jednym porcie), gdzie są zainstalowane aplikacje muszą mieć nadany adres domenowy (mogą to być subdomeny). Wykorzystywanie wyłącznie adresu IP wyklucza taką konfigurację.

2. Wszystkie witryny IIS (które mają działać na jednym porcie), gdzie są zainstalowane aplikacje w oknie „Edycji powiązania witryny” w IIS (opcja „Edytuj powiązania…”, a następnie „Edytuj…” na zaznaczonym powiązaniu typu https) muszą mieć poprawnie wpisany adres domenowy w oknie „Nazwa hosta” oraz zaznaczoną opcję „Wymagaj wskazania nazwy serwera”.



Rysunek 27: Konfiguracja powiązania witryny do pracy z wieloma witrynami na jednym porcie

3. Wykonanie rejestracji repozytorium w P1 na adresie domenowym.

Taka konfiguracja pozwana m.in. na skonfigurowanie wielu aplikacji RepozytoriumP1 na jednym porcie w obrębie jednego serwera www.

2.5. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent jest odtworzenie kopii zapasowej bazy danych.

Możliwe jest pełne zrestartowanie komponentu na dwa sposoby:

1. Zatrzymać pracę usługi IIS. Opcja jest dostępna w IIS z menu „Akcje” (Zarządzanie serwerem) z poziomu przycisk „Zatrzymaj”. Ponowne uruchomienie serwera IIS możliwe jest również z poziomu menu „Akcje” wybierając przycisk „Rozpocznij”.
2. Zatrzymanie witryny w IIS, w której znajdują się komponenty do zatrzymania. Z poziomu IIS rozwinąć po prawej stronie z okna „Połączenia” katalog „Witryny” i zaznaczyć wybraną witrynę. Następnie z menu po prawej stronie (o nazwie „Zarządzanie witryną sieci Web”) należy wybrać przycisk „Zatrzymaj”. Aby ponownie uruchomić witryny należy wybrać opcję „Rozpocznij”.

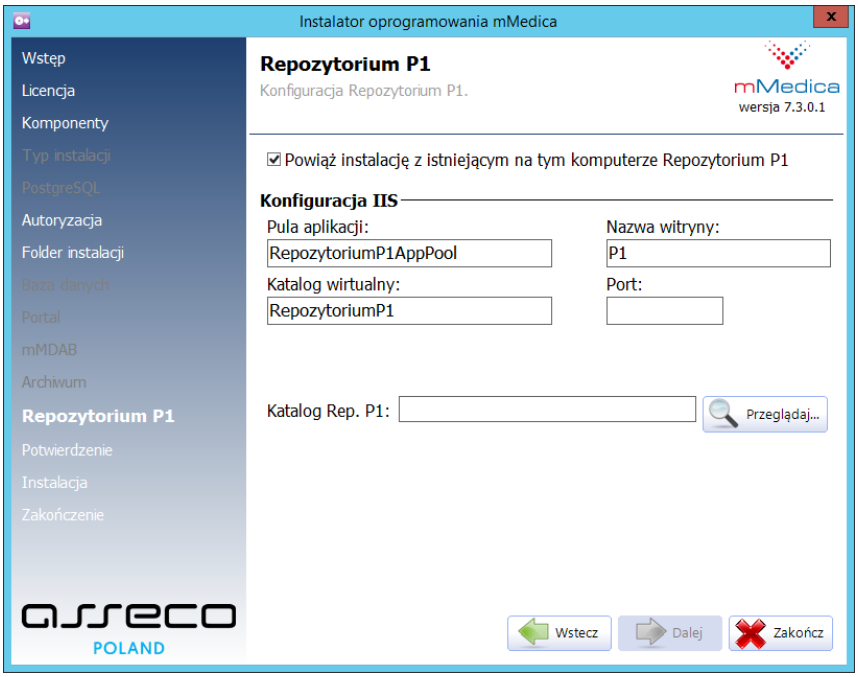
2.6. Powiązanie instalacji z istniejącą aplikacją Repozytorium P1

Jeśli komponent Repozytorium P1 został zainstalowany manualnie możliwe jest wykrycie takiej instalacji przez instalator modułów mMedica, dzięki czemu będzie możliwe wykonywanie aktualizacji aplikacji Repozytorium P1 za pomocą instalatora. Po poprawnym powiązaniu instalacji z istniejąca aplikacją Repozytorium P1 możliwe jest również jej odinstalowanie (usunięcie plików aplikacji oraz ustawień IIS) za pomocą instalatora modułów mMedica.

Proces powiązania wygląda następująco:

1. Uruchomić jako administrator instalator modułów mMedica.
2. W zależności od przypadku:
    a. Brak wcześniej zainstalowanych przez instalator komponentów mModułów: należy przejść w instalatorze do wyboru instalacji nowego komponentu Repozytorium P1.
    b. Zainstalowany jakikolwiek komponent przez instalator mModułów: instalator uruchamia się w trybie serwisowym, gdzie należy wybrać należy wybrać opcję „Zarządzaj modułami dodatkowymi”, a następnie oznaczyć komponent Repozytorium P1 do instalacji.
3. Na formatce konfiguracji komponentu Repozytorium P1 należy oznaczyć opcję „Powiąż instalację z istniejącym na tym komputerze Repozytorium P1”. Na formatce należy uzupełnić konfigurację IIS zgodnie z tym co zostało skonfigurowane dla Repozytorium P1 w IIS, a dodatkowo wskazać katalog z plikami aplikacji Repozytorium P1.

    Instalator nie sprawdza poprawności wprowadzonych danych w obszarze konfiguracji IIS. Jeśli parametry konfiguracji IIS nie zostaną poprawnie podane to w procesie odinstalowania komponentu przez instalator, elementy konfiguracji IIS nie zostaną usunięte. Z kolei, instalator weryfikuje podany katalog z plikami aplikacji dla Repozytorium P1.



Rysunek 28: Powiązanie instalacji z istniejącym na komputerze Repozytorium P1

4. Po poprawnym procesie powiązania zostanie wyświetlone okno z podsumowaniem procesu.

2.7. Aktualizacja modułu

W przypadku, w którym moduł został zainstalowany przez instalator lub poprawnie dokonano powiązania instalacji z istniejącym na komputerze Repozytorium P1 możliwa jest aktualizacja aplikacji z poziomu instalatora modułów mMedica. Instalator wykryje istniejącą instalację Repozytorium P1 i zaktualizuje pliki, które zostały wcześniej utworzone przez instalator. Instalator równocześnie zaktualizuje wszystkie zainstalowane komponenty mModułów.

W przypadku instalacji manualnej należy podmienić wszystkie pliki komponentów oraz przenieść ustawienia z wcześniej skonfigurowanych plików appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie. Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach modułów mMedica w IIS (całym serwerze lub witrynie, w której znajdują się instalacje). Po aktualizacji należy uruchomić ponownie komponent na serwerze WWW.

3. Instalacja w dystrybucjach Linux

3.1. Instalacja

Uwaga: RepozytoriumP1 wymaga publicznego oraz stałego adresu IP.

Uwaga: Funkcjonalności związane z RepozytoriumP1 wymagają zainstalowanego modułu Archiwum.

Uwaga: Proces instalacji środowiska uruchomieniowego .NET Core oraz Apache jest zamieszczony w instrukcji instalacji oraz konfiguracji Archiwum.

Proces instalacji dla przypadku instalacji wszystkich komponentów oraz serwera bazy danych na jednym komputerze można opisać za pomocą następujących kroków:

1. Instalacja środowiska uruchomieniowego ASP .NET Core 6.0 oraz Apache (patrz: instrukcja instalacji i konfiguracji Archiwum).
2. Skopiowanie plików komponentów.
3. Konfiguracja serwera Apache.
4. Konfiguracja nazw aplikacji.
5. Konfiguracja adresów aplikacji.
6. Konfiguracja połączenia z bazą danych Archiwum (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja).
7. Weryfikacja instalacji.
8. Konfiguracja dodatkowa serwera WWW.

3.2. Konfiguracja serwera oraz instalacja modułu

W niniejszym rozdziale omówiono najprostszą konfigurację serwera Apache. Procedura wygląda następująco:

1. Jeśli aplikacja mMedica Archiwum jest udostępniana za pomocą IIS to należy upewnić się, że dla puli aplikacji dla aplikacji Archiwum wartość parametru „Załaduj profil użytkownika” jest ustawiona na „True”.

   Uwaga: Brak ustawienia wartości „Załaduj profil użytkownika” na „True” dla puli aplikacji Archiwum w IIS może powodować błąd informujący o błędnym certyfikacie lub haśle podczas rejestracji repozytorium w systemie P1.

2. Pobrać pakiety plikowe - odnośnik.
3. Do katalogu /var/www (domyślny katalog stron dla Apache) należy przekopiować katalogi ze źródłami RepozytoriumP1.
4. Należy przeprowadzić wstępną konfigurację opisaną w późniejszych punktach.
5. Jeżeli w katalogu /var/www znajduje się plik index.html, należy go usunąć lub przenieść w inne miejsce.
6. Utworzyć nowy plik konfiguracyjny witryny:

```
sudo nano /etc/apache2/sites-available/RepozytoriumP1.conf
```

7. Do prawidłowej komunikacji należy pobrać certyfikaty P1 – odnośnik i scalić je przy pomocy komendy:

```
sudo bash -c 'cat CCP1RootCA.crt CCP1SubCATLS.crt >> CCP1Chain.crt'
```

8. Skonfigurować plik witryny /etc/apache2/sites-available/RepozytoriumP1.conf:

```
<VirtualHost *:443>
ServerName localhost
      ProxyPreserveHost On
      ProxyPass / http://localhost:5004/
      ProxyPassReverse / http://localhost:5004/


  SSLEngine on
  Header edit Set-Cookie ^(.*)$ $1;Secure
  SSLProtocol +TLSv1.2
  SSLCertificateFile /etc/ssl/certs/certyfikat_serwera_tls.pem

  RequestHeader set X-Forwarded-Proto https

  SSLCACertificateFile /etc/ssl/certs/CCP1Chain.crt
  SSLOptions +ExportCertData
  SSLVerifyClient optional
  SSLVerifyDepth 3
  RequestHeader set SSL_CLIENT_CERT "%{SSL_CLIENT_CERT}e"
 . . .
```

Uwaga: Używany port musi być unikatowy w ramach serwera.

- ServerName – nazwa lub adres serwera,
- ProxyPass oraz ProxyPassReverse zapewniają dwukierunkową komunikację. Pierwszym elementem jest adres routingu (jest on bezpośrednio powiązany z Konfiguracja nazwy aplikacji). Drugi element to adres aplikacji, na który przekierowany ma zostać ruch (parametr powiązany z Konfiguracja adresu aplikacji).

- SSLCertificateFile – Certyfikat TLS wystawiony przez CeZ w formacie o rozszerzeniu „*.pem”. W przypadku posiadania certyfikatu o rozszerzeniu „*.p12” można przekonwertować certyfikat za pomocą polecenia:

```
sudo openssl pkcs12 –in certyfikat.p12 –out certyfikat_serwera_tls.pem -nodes -clcerts
```

- SSLCACertificateFile – pobrane i scalone certyfikaty P1 (z poprzedniego punktu).

Powyższy plik konfiguracyjny (dla protokołu https) definiuje wykorzystanie domyślnego portu 443 do komunikacji oraz wskazuje aplikacje na jakie przekierowywany ma być ruch. Konfiguracja ta pozwala na przesłanie przez klienta certyfikatu TLS. Apache pełni tu rolę serwera pośredniczącego, dlatego konieczne jest zezwolenie serwerowi na tego typu operacje:

```
sudo a2enmod ssl
sudo a2enmod proxy
sudo a2enmod proxy_balancer
sudo a2enmod proxy_http
sudo a2enmod headers
```

Apache domyślnie przekierowuje oryginalny adres IP żądania do aplikacji. Automatyczne przekierowanie protokołu z (http lub https) możliwe jest po dodaniu do pliku konfiguracji witryny wpisu:

```
RequestHeader set "X-Forwarded-Proto" expr=%{REQUEST_SCHEME}
```

System P1 nie wymaga, aby komponent RepozytoriumP1 był udostępniany na porcie 443. Można wybrać niewykorzystany port. W przypadku posiadania wielu komponentów RepozytoriumP1 każdy z nich musi być udostępniany na unikalnym adresie usługi lub porcie.

Uwaga: System P1 weryfikuje podczas rejestracji repozytorium w systemie P1, czy nie istnieje już zarejestrowane repozytorium pod danym adresem IP i wskazanym porcie. Od dnia 30.06.2021 System P1 nie wymaga, aby RepozytoriumP1 było instalowane zawsze na unikalnym porcie przy korzystaniu z tego samego adresu usługi.

W przypadku wykorzystania innego portu niż 443 konieczne jest dodanie portu do listy portów nasłuchiwanych w pliku /etc/apache2/ports.conf.

9. Udostępnić nowo utworzoną witrynę komendą:

```
sudo a2ensite RepozytoriumP1.conf
```

10. Skonfigurować połączenie komponentów z bazami danych według opisu (Uwaga: proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja.
11. Zrestartować serwer Apache:

```
sudo service apache2 restart
```

W przypadku problemów z uruchomieniem apache ze względu na długość klucza certyfikatu konieczna jest zmiana domyślnej konfiguracji SSL. Powód błędnego uruchamiania usługi apache można sprawdzić poprzez wylistowanie pliku błędów komendą:

```
cat /var/log/apache2/error.log
```

Jeżeli w pliku na końcu znajduje się podobny wpis „SSL Library Error: error:140AB18F:SSL routines:SSL_CTX_use_certificate:ee key too small" oznacza to, że konieczna jest edycja pliku /etc/ssl/openssl.cnf. Dopisując wskazane fragmenty na początku oraz na końcu pliku.

```
# This definition stops the following lines choking if HOME isn't
# defined.
HOME                    = .

# Extra OBJECT IDENTIFIER info:
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids
#Poczatek
#System default
openssl_conf = default_conf
. . .
#Koniec
[ default_conf ]
ssl_conf = ssl_sect
[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = TLSv1.2
CipherString = DEFAULT:@SECLEVEL=1
```

12. Utworzyć skrypty uruchomieniowe:
    a) plik RepozytoriumP1.sh o zawartości:

```
#!/bin/sh
cd /var/www/RepozytoriumP1
dotnet ./RepozytoriumP1.dll
```

    b) Nadać plikowi uprawnienia do wykonywania:

```
sudo chmod +x RepozytoriumP1.sh
```

13. Dodać aplikację do serwisu:
    a) Utworzyć plik mMedica.RepozytoriumP1.service w katalogu /etc/systemd/system o zawartości:

```
[Unit]
Description = mMedica Repozytorium P1
[Service]
ExecStart=/var/www/RepozytoriumP1.sh
WorkingDirectory=/var/www/RepozytoriumP1
Restart=always
RestartSec=10
SyslogIdentifier=mMedica-RepozytoriumP1
User=user
Environment=ASPNETCORE_ENVIRONMENT=Production

[Install]
WantedBy=Multi-user.target
```

W pole User należy wprowadzić nazwę istniejącego w systemie użytkownika, na którym uruchomiony zostanie serwis (nie zaleca się stosowanie użytkownika root).

b) Udostępnić serwisy:

```
sudo systemctl enable mMedica.RepozytoriumP1.service
```

c) Uruchomić serwisy:

```
sudo systemctl start mMedica.RepozytoriumP1.service
```

14. Nadać uprawnienia do plików i folderów:

a) Nadać uprawnienia do zapisu pliku application.log w Repozytorium P1:

```
sudo chmod +w /var/www/RepozytoriumP1/application.log
```

3.3. Konfiguracja nazwy aplikacji

Jeśli Repozytorium P1 nie posiada własnego adresu domenowego, to w pliku appsettings.json znajdującym się w katalogu każdej z aplikacji należy wprowadzić nazwę aplikacji. Nazwa ta nie jest dowolna. Należy wprowadzić dokładnie tę samą nazwę, która zostanie wykorzystana do konfiguracji serwera Apache. Nazwa ta znajduje się w zaznaczonych miejscach:

```
<VirtualHost *:443>
      ServerName localhost
      ProxyPreserveHost On
      ProxyPass /RepozytoriumP1 http://localhost:5004/
      ProxyPassReverse /RepozytoriumP1 http://localhost:5004/
</VirtualHost>
```

Nazwę tą należy umieścić w sekcji ApplicationName:

a) w pliku konfiguracyjnym w Repozytorium P1 (dla przykładowej konfiguracji):

```
"ApplicationName": "RepozytoriumP1"
```

Nazwy powinny być unikalne w ramach jednego serwera www.

3.4. Konfiguracja adresu aplikacji

Poprzez konfigurację sekcji ApplicationUrl w pliku appsettings.json zmieniać można adres pod jakim widoczna będzie aplikacja. Adres dla przykładowej konfiguracji:

```
"ApplicationUrl": "http://localhost:5004"
```

Port powinien być unikalny w ramach całego serwera.

3.5. Weryfikacja instalacji

W przypadku wykorzystywania systemu bez środowiska graficznego pomocne jest skorzystanie z drugiego komputera w celu wyświetlenia zawartości komponentów w przeglądarce internetowej (należy wtedy pamiętać o wpisaniu odpowiedniego adresu IP zamiast localhost).

1. Weryfikacja usługi sieciowej Repozytorium P1 odbywa się poprzez wejście na stronę usługi, dla konfiguracji przykładowej adres wygląda następująco http://localhost/RepozytoriumP1. Uwaga, w przeglądarce internetowej po wejściu na stronę statusową aplikacji pojawi się ostrzeżenie o nieprawidłowej konfiguracji HTTPS. Jest to normlanej sytuacja, która wynika z faktu, że certyfikat TLS wydany przez CeZ nie jest powiązany z adresem domenowym aplikacji. Po akceptacji wyjątku zostanie strona statusowa dla aplikacji Repozytorium P1. Strona statusowa pozwala zweryfikować czy połączenie z bazą danych jest prawidłowe. Rezultat poprawnego działania Repozytorium P1 wygląda następująco:

Strona diagnostyczna Repozytorium P1

Status	OK
Wersja aplikacji	6.9.0
Wersja bazy danych	6.9.0
Połączenie z bazą danych Archiwum	Tak
Uwagi dotyczące kompatybilności	Tak
Data z serwera aplikacji	28.09.2020 10:04:59
Data z serwera bazy danych Archiwum	28.09.2020 10:04:59

Rysunek 29: Weryfikacja działania aplikacji Repozytorium P1

W przypadku problemów zostanie wyświetlony komunikat o błędzie. Możliwe problemy:

- nieprawidłowy adres serwera bazy danych, port lub nieprawidłowa nazwa bazy danych mMedica,
- brak komunikacji z serwerem bazy danych (zapora ogniowa lub konfiguracja serwera PostgreSQL).

- baza danych mMedica w stanie aktualizacji.

Jeśli strona Repozytorium P1 się nie otwiera, należy sprawdzić czy usługa Apache działa:

```
service apache2 status
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługa nie jest uruchomiona należy ją uruchomić:

```
sudo service apache2 start
```

Jeżeli strona nadal się nie wyświetla, a status Apache jest poprawny, należy sprawdzić status serwisu:

- Dla Repozytorium P1:

```
sudo systemctl status mMedica.RepozytoriumP1.service
```

W wyniku powinien zostać wyświetlony status jako „active (running)”. Jeżeli usługi nie są uruchomione, należy je uruchomić i ponownie sprawdzić ich status. W przypadku, gdy status się nie zmieni, należy sprawdzić czy pliki konfiguracyjne zawierają dobre dane, pliki skryptowe oraz konfiguracje serwisów zawierają odpowiednią treść.

2. Po wejściu przeglądarką internetową na stronę statusową Repozytorium P1 należy również zweryfikować, czy aplikacja przedstawia się certyfikatem TLS wydanym przez CeZ, który został skonfigurowany dla witryny na serwerze www.

Uwaga: Najczęściej pojawiające się problemy zostały opisane w rozdziale 7.

3.6. Konfiguracja dodatkowa Apache

3.6.1. Zaawansowana konfiguracja witryn

Możliwe jest dodawanie nowych witryn do usługi Apache. Na poziomie witryny konfigurowany jest m.in. port komunikacji, adres domenowy, alias, certyfikat SSL, zakres IP z jakiego jest widoczna witryna. Możliwe jest działanie wielu witryn na tym samym porcie komunikacji. Pojedyncza witryna jest definiowana w pliku o rozszerzeniach „conf” w ścieżce /etc/apache2/sites-available/.

Przykładowa zawartość dla pliku s1.conf:

```
<VirtualHost *:80>
  ServerName www.p1.domena.pl
  ServerAlias p1.domena.pl
  ProxyPreserveHost On
  ProxyPass /RepozytoriumP1 http://localhost:5004/
  ProxyPassReverse /RepozytoriumP1 http://localhost:5004/
</VirtualHost>
```

Powyższa konfiguracja posiada przypisany adres domenowy www.p1.domena.pl oraz alias.

Przykładowa zawartość plik s2.conf:

```
<VirtualHost 10.10.10.2:1099>
  ServerName 10.10.10.2
  <Location /RepozytoriumP1>
    Deny from all
    Allow from 10.10.10.1/24
    ProxyPass http://localhost:5004/
    ProxyPassReverse http://localhost:5004
  </Location>
</VirtualHost>
```

W pliku s2.conf witryna jest przypisana do adresu 10.10.10.2 i tylko pod takim będzie widoczna. Z kolei „Allow from" pozwala zdefiniować zakres adresów IP, z których jest widoczna strona. Domyślnie ma on wartość „all" oznaczającą brak ograniczeń.

Po utworzeniu pliku z konfiguracją witryny w ścieżce /etc/apache2/sites-available/, należy wykonać polecenie:

```
sudo a2ensite NAZWA_PLIKU_KONFIGURACJI.conf
```

Przykład:

```
sudo a2ensite s1.conf
```

Następnie należy przeładować konfigurację usługi Apache:

```
sudo service apache2 reload
```

3.7. Konfiguracja wielu Repozytorium P1 na jednym serwerze

W przypadku, kiedy na jednym serwerze Apache udostępniony jest więcej niż jeden moduł Repozytorium P1, należy poczynić dodatkowe kroki konfiguracyjne. Utworzyć dla każdego z komponentów osobny katalog, w którym znajdować się będą pliki aplikacji. Wymagana jest zmiana portu, na którym dana aplikacja będzie udostępniona, dlatego należy w pliku appsettings.json każdej aplikacji zmienić adres aplikacji.

Uwaga: Ważne, aby każda z instancji Repozytorium P1 miała unikalny atrybut „ApplicationUrl" oraz „ApplicationName" w ramach jednego serwera www.

Konieczne jest ponowne dokonanie kroków opisanych w tym dokumencie.

3.8. Restartowanie i zatrzymywanie komponentów

Komponenty zawierają wewnętrzną pamięć podręczną i może istnieć potrzeba jej wyczyszczenia za pomocą zrestartowania komponentu. Takim przypadkiem, w którym należy zrestartować komponent jest odtworzenie kopii zapasowej bazy danych. Możliwe jest zrestartowanie komponentów w następujący sposób:

1. Przykład dla Repozytorium P1:
   a) Wyłączyć usługę Repozytorium P1 w serwisach:

```
sudo systemctl stop mMedica.RepozytoriumP1.service
```

b) Uruchomić usługę ponownie po odczekaniu około 1 min. wykorzystując polecenie:

```
sudo systemctl start mMedica.RepozytoriumP1.service
```

3.9. Aktualizacja modułu

Należy podmienić wszystkie pliki komponentu oraz przenieść ustawienia z wcześniej skonfigurowanego pliku appsettings.json do nowych. Nie zaleca się podmiany plików na wcześniej skonfigurowane, gdyż struktura pliku konfiguracyjnego może ulegać zmianie.

Proces aktualizacji powinien być wykonywany na zatrzymanych komponentach modułów w dystrybucjach Linux. Po aktualizacji należy uruchomić ponownie komponent w systemie. Do aktualizacji komponentów należy posłużyć się opisem znajdujących się w rozdziale *2.11. Restartowanie i zatrzymywanie komponentów.*

3.10. Pomoc

W razie problemów można skorzystać z pomocy pod następującymi adresami internetowymi:

1. http://httpd.apache.org/docs/
2. http://httpd.apache.org/docs/current/mod/mod_ssl.html
3. https://docs.microsoft.com/en-us/dotnet/core/linux-prerequisites?tabs=netcore1x
4. https://docs.microsoft.com/en-us/aspnet/core/publishing/apache-proxy

4. Konfiguracja aplikacji

Uwaga: Proces konfiguracji baz danych jest taki sam jak w przypadku modułu eRejestracja.

4.1. Konfiguracja połączenia z bazami danych

W przypadku instalacji manualnej w systemach operacyjnych Microsoft Windows, dystrybucjach systemów opartych o jądro Linux oraz w przypadku doinstalowania komponentów konieczna jest konfiguracja połączenia z bazami danych w komponentach. Możliwa jest również edycja parametrów połączeń, które zostały utworzone przez instalator. Każdy z komponentów posiada plik appsettings.json, w którym znajdują się parametry połączenia z bazą danych (adres serwera bazy danych, port oraz nazwa bazy danych).
Konfiguracja połączenia z bazą danych wygląda następująco:

1. Otworzyć plik appsettings.json z prawami administratora do edycji.
2. Wyszukać fragment (identyczny lub podobny) dla:

```
"ConnectionString": "Server=localhost,5432;Database=ARCHMMEDICA;"
```

3. Zmienić według wzoru: „Server=localhost,5432;Database=NAZWA_BAZY" – baza danych o nazwie NAZWA_BAZY znajduje się na komputerze, na którym działa komponent (localhost) na porcie 5432. W przypadku innej nazwy bazy danych należy zmienić właściwość „Database" na odpowiednią. Dla innego adresu, na którym znajduje się baza, należy zmienić parametr Server.

Zapisać plik i zrestartować komponent zgodnie z *1.8. Restartowanie i zatrzymywanie komponentów* (Windows) lub *2.11. Restartowanie i zatrzymywanie komponentów* (Linux).

4.2. Konfiguracja nazwy oraz adresu aplikacji

Konfiguracja ta została opisana osobno dla systemu Windows (w rozdziale *1.4 Konfiguracja nazwy aplikacji*) oraz Linux (w rozdziałach *2.5 Konfiguracja nazwy aplikacji* oraz *2.6* Konfiguracja adresu aplikacji).

4.3. Przekierowanie nagłówków z proxy

W przypadku, w którym komponent Repozytorium P1 zainstalowany jest na IIS (system rodziny Windows) dostępny jest poprzez proxy lub reverse-proxy, należy odpowiednio skonfigurować plik appsettings.json. Uruchomienie obsługi proxy polega na edycji sekcji w pliku appsettings.json danego komponentu poprzez zmianę wartości klucza *ProxyWindowsEnable*:
Ustawienie domyślne (proxy wyłączone):

```
"ProxyWindowsEnable": false
```

Włączona obsługa proxy:

```
"ProxyWindowsEnable": true
```

Mechanizm automatycznie obsługuje proxy, które jest uruchomione na tym samym systemie co komponent (adres lokalny). Jeśli proxy znajduje się pod innym adresem niż adres lokalny, należy jego adres IP wpisać w kluczu *ProxyIPs* (w przypadku wielu proxy należy wpisać adresy po średniku), przykład:

```
"ProxyIPs": "192.168.137.1;192.168.137.2;192.168.137.3"
```

Na środowisku opartym o jądro Linux ruch do komponentów przekierowywany z Apache do odpowiednich usług komponentów. Jednak Repozytorium P1 automatycznie obsługują odpowiednie nagłówki z proxy dla Linux. Podobnie jak w przypadku komponentów zainstalowanych w systemie Windows, o ile proxy jest na adresie lokalnym, nie wymaga on dodatkowej konfiguracji. W innym przypadku konfiguracja odbywa się na takich samych zasadach jak dla instalacji pod Windows (edycja klucza *ProxyIPs*).

Do prawidłowego działania mechanizmu przekazywania nagłówków http z proxy konieczne jest, aby proxy obsługiwało nagłówek HTTP X-Forwarded-For, w którym przekazywany jest oryginalny adres IP pochodzący z żądania.

Brak odpowiedniej konfiguracji proxy będzie skutkowało odczytem nieprawidłowych adresów IP z żądań, co z kolei może spowodować nieprawidłowe działanie mechanizmu blokad IP przez mechanizmy blokad dostępowych do komponentów.

5. Operacja związane z repozytorium

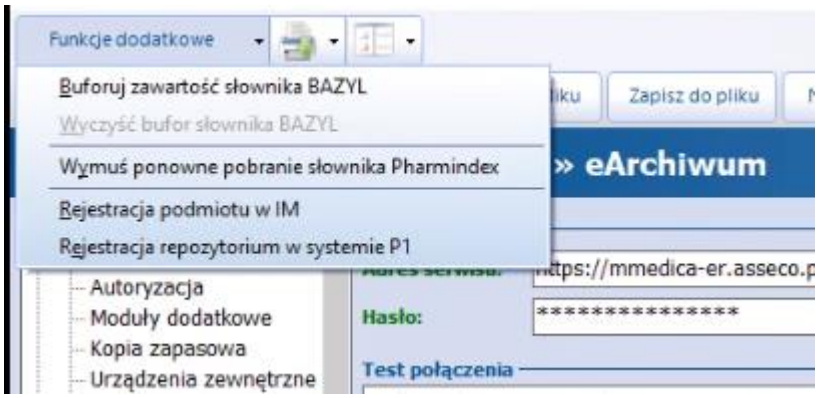
5.1. Rejestracja repozytorium w P1

Proces rejestracji repozytorium w P1 odbywa się w aplikacji mMedica. Przed procesem rejestracji repozytorium w P1 należy upewnić się, czy:

1. Istnieje prawidłowo skonfigurowane połączenie z mMedica do Archiwum (zalecane jest wykonanie testu połączenia z poziomu Konfiguratora mMedica).
2. Zostały dodane aktualne certyfikaty P1 WSSE oraz P1 TLS w Konfigurator\Autoryzacja w programie mMedica.

Po spełnieniu wyżej wymienionych warunków można przejść do etapu rejestracji repozytorium w systemie P1:

1. W mMedica przejść do Konfiguratora, następnie wybrać Funkcje dodatkowe\Rejestracja repozytorium w systemie P1.

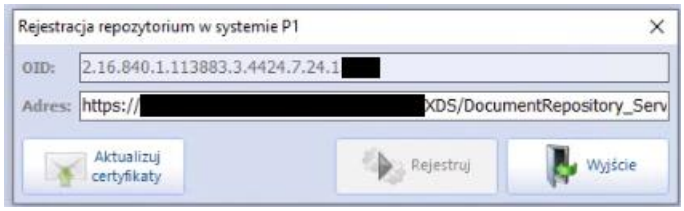


Rysunek 30: Rejestracja repozytorium w systemie P1

2. W oknie rejestracji należy podać publiczny adres usługi repozytorium, który musi się kończyć frazą „XDS/DocumentRepository_Service”. Jeśli komponent RepozytoriumP1 ma adres: „https://adres-repo/RepozytoriumP1” to w polu „Adres” należy podać „https://adres-repo/RepozytoriumP1/XDS/DocumentRepository_Service”, a następnie wybrać przycisk „Rejestruj”.

Rysunek 31: Okno rejestracji w systemie P1

3. W przypadku pomyślnej rejestracji, w polu „OID” pojawi się unikalny identyfikator nadany przez system P1 dla zarejestrowanego repozytorium.



Rysunek 32: Okno z zarejestrowanym repozytorium w systemie P1

W czasie procesu rejestracji repozytorium w P1, aplikacja eArchiwum komunikuje się z aplikacją RepzytoriumP1 i weryfikuje, czy pod podanym adresem znajduje się działająca aplikacja RepozytoriumP1 oraz czy skonfigurowany w mMedica certyfikat TLS dla P1 odpowiada certyfikatowi, którym przedstawia się aplikacja RepozytoriumP1. Funkcjonalność weryfikacji konfiguracji RepozytoriumP1 przez wykonanie komunikacji z aplikacji Archiwum do RepozytoriumP1 można wyłączyć w eArchiwum (parametr „Walidacja konfiguracji aplikacji Repozytorium P1” w Konfiguracji).

Jeśli po rejestracji repozytorium w systemie P1 baza danych mMedica utraci informację o rejestracji (np. przez odtworzenie kopii bazy danych sprzed faktu rejestracji), stan rejestracji można odzyskać przez ponowną rejestrację repozytorium na ten sam adres (OID jest odzyskiwany z bazy danych eArchiwum).

Uwaga: Brak ustawienia wartości „Załaduj profil użytkownika” na „True” dla puli aplikacji Archiwum w IIS może powodować błąd informujący o błędnym certyfikacie lub haśle podczas rejestracji repozytorium w systemie P1.

Uwaga: System P1 weryfikuje podczas rejestracji repozytorium w systemie P1, czy nie istnieje już zarejestrowane repozytorium pod danym adresem IP i wskazanym porcie. Od dnia 30.06.2021 System P1 nie wymaga, aby RepozytoriumP1 było instalowane zawsze na unikalnym porcie przy korzystaniu z tego samego adresu usługi.

5.2. Zmiana adresu repozytorium w P1

Po zarejestrowaniu repozytorium w P1 istnieje możliwość zmiany jego adresu. W pierwszej kolejności należy wykonać działania związane ze zmianą konfiguracji aplikacji RepozytoriumP1 na serwerze www. W kolejnym kroku, z poziomu okna „Rejestracja repozytorium w P1” w mMedica istnieje możliwość zmiany adresu repozytorium i zatwierdzenie zmian.

Podczas operacji zmiany adres repozytorium w P1, aplikacja eArchiwum komunikuje się z aplikacją RepzytoriumP1 i weryfikuje, czy pod podanym adresem znajduje się działająca aplikacja. Funkcjonalność weryfikacji konfiguracji RepozytoriumP1 przez wykonanie komunikacji z aplikacji Archiwum do RepozytoriumP1 można wyłączyć w eArchiwum (parametr „Walidacja konfiguracji aplikacji Repozytorium P1" w Konfiguracji).

5.3. Aktualizacja certyfikatu TLS lub WSS

W przypadku zmiany certyfikatu TLS dla RepozytoriumP1 należy w pierwszej kolejności wykonać zmianę certyfikatu na serwerze www, gdzie jest zainstalowana aplikacja. Następnie należy wykonać sprawdzenie czy zmiana certyfikatu została przeprowadzona poprawnie. Weryfikację można wykonać przez wejście na stronę statusową RepozytoriumP1 przez przeglądarkę internetową, a następnie wyświetlenie informacji o certyfikacie.

Zmianę certyfikatów TLS lub/i WSS w aplikacji mMedica należy wykonać dwuetapowo. Najpierw wczytać nowe certyfikatu TLS lub/i WSS dla systemu P1 w konfiguratorze, a następnie z poziomu okna rejestracji repozytorium w systemie P1 wykonać aktualizację certyfikatów.

Podczas procesu aktualizacji certyfikatu TLS dla RepozytroiumP1, aplikacja eArchiwum komunikuje się z RepozytroiumP1 celem weryfikacji, czy skonfigurowany w mMedica certyfikat TLS odpowiada certyfikatowi TLS, którym przedstawia się aplikacja RepozytoriumP1. Funkcjonalność weryfikacji konfiguracji RepozytoriumP1 przez wykonanie komunikacji z aplikacji Archiwum do RepozytoriumP1 można wyłączyć w eArchiwum (parametr „Walidacja konfiguracji aplikacji Repozytorium P1" w Konfiguracji).

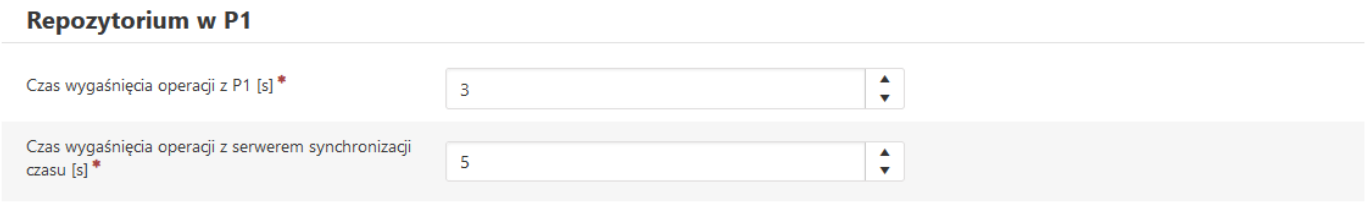
Nieaktualne certyfikaty będą skutkować brakiem komunikacji RepozytoriumP1 oraz eArchiwum z systemem P1.

6. Zmiany w eArchiwum

6.1. Konfiguracja

W konfiguracji eArchiwum znajdują się dwa parametry odpowiedzialne za komunikacje RepozytoriumP1 z systemem P1:

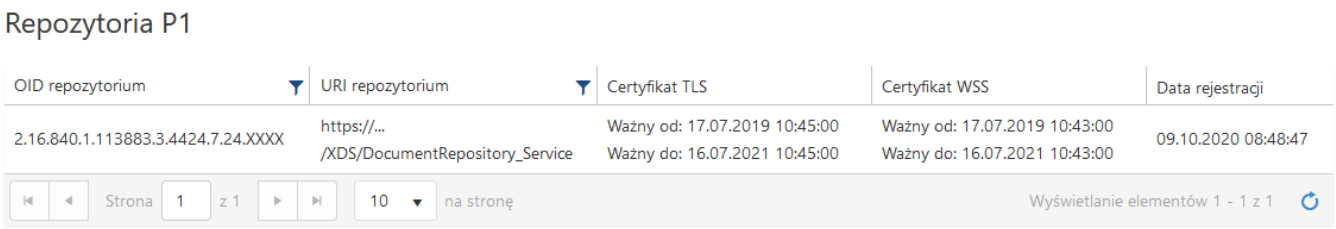
- Czas wygaśnięcia operacji z P1 [s] – maksymalny dopuszczalny czas operacji z systemem P1 (timeout) wyrażony w sekundach.
- Czas wygaśnięcia operacji z serwerem synchronizacji czasu [s] – maksymalny dopuszczalny czas operacji z serwerem synchronizacji czasu (timeout) wyrażony w sekundach.



Rysunek 33: Parametry konfiguracyjne dotyczące komunikacji z P1

6.2. Repozytoria P1

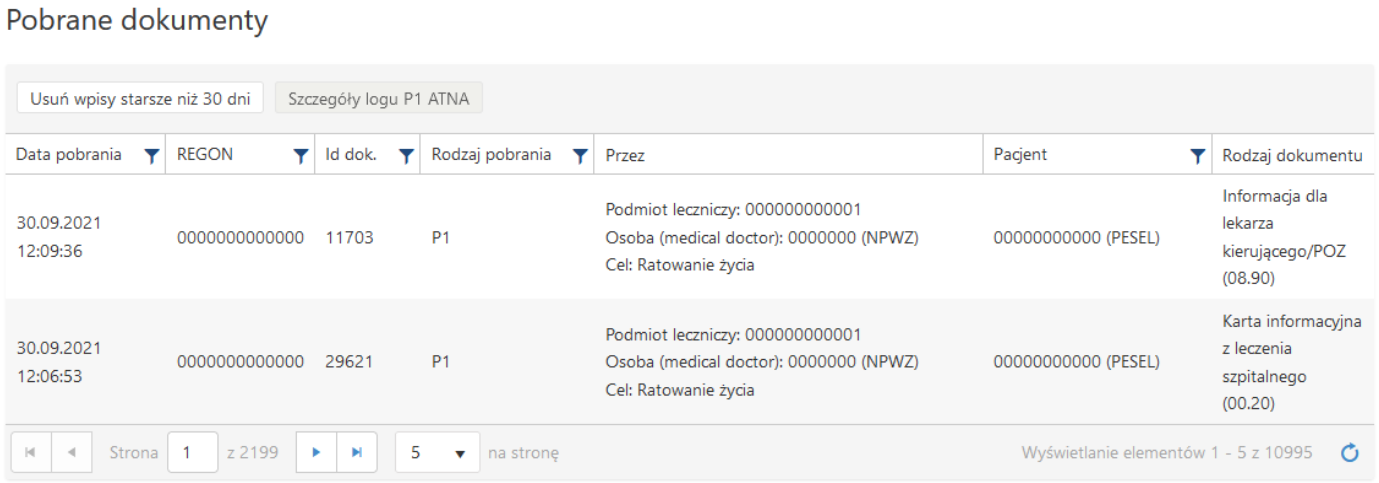
Administrator ma możliwość podglądu danych zarejestrowanego repozytorium w systemie P1 za pomocą strony „Repozytoria P1”. Poza identyfikatorem (OID) oraz adresem repozytorium, znajdują się również tam informacje o datach ważności certyfikatów TLS oraz WSS wysłanych przez mMedica do Archiwum. Nieaktualne certyfikaty będą skutkować brakiem komunikacji RepozytoriumP1 oraz eArchiwum z systemem P1.



Rysunek 34: Strona Repozytoria P1 w Archiwum

6.3. Historia pobrań dokumentów

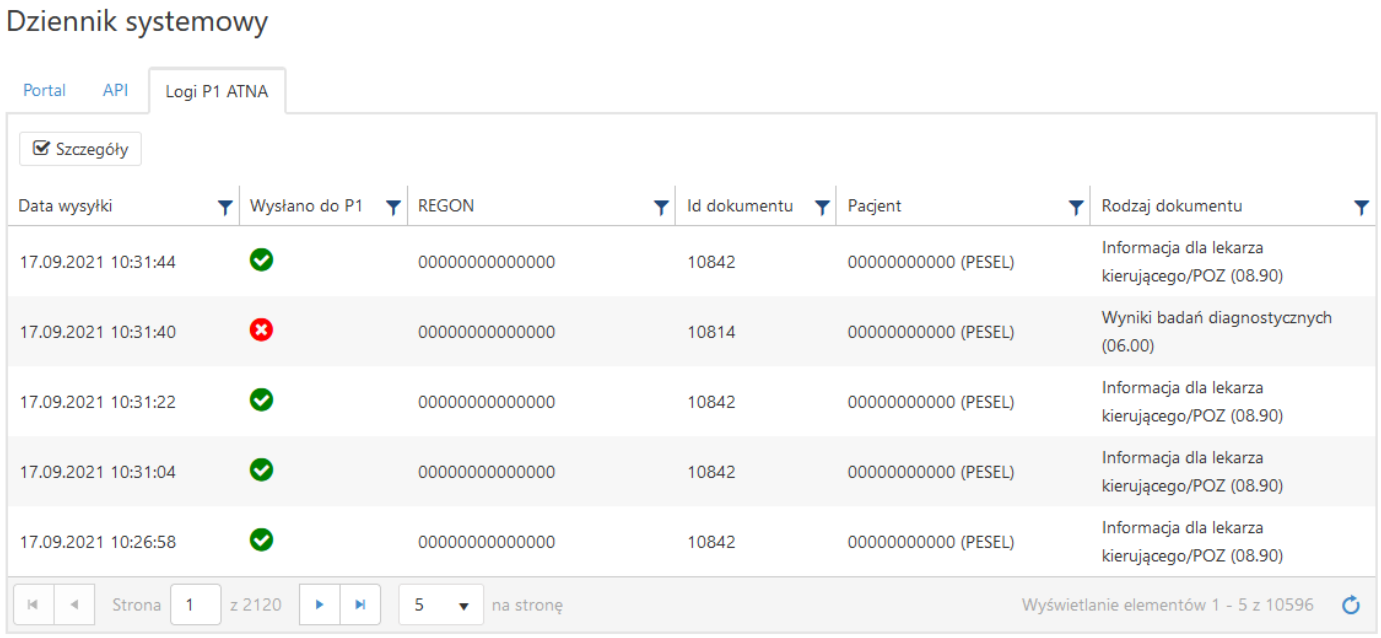
Na potrzeby integracji Archiwum z RepozytoriumP1 strona „Pobrane dokumenty” została rozbudowana o dane dotyczące pobrań z systemu P1 wraz z informacją o jednostce oraz personelu medycznym, który dokonał pobrania. Od wersji 7.2.0 rozszerzono zakres zapisywanych informacji o cel pobrania dokumentu.



Rysunek 35: Historia pobrań dokumentów w Archiwum

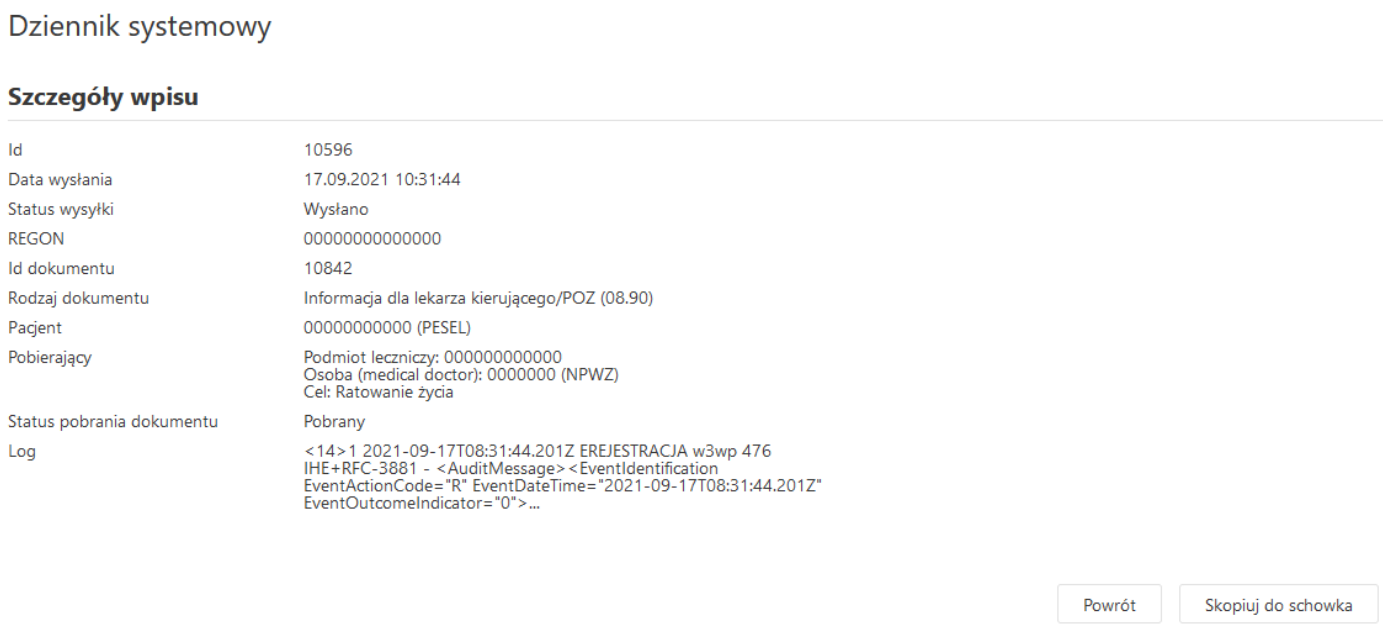
6.4. Logi ATNA

Administrator z poziomu „Dziennika systemowego” w zakładce „Logi P1 ATNA” może wyświetlić listę logów ATNA z informacjami m.in. jakiego dokumentu oraz pacjenta dotyczy log oraz czy został poprawnie wysłany do P1.



Rysunek 36: Tabela z listą wpisów logu P1 ATNA

Po zaznaczeniu pozycji w tabeli można przejść do szczegółów wpisu. Informacje o wpisie są również dostępne z poziomu „Pobranych dokumentów” po zaznaczeniu dokumentu i wybraniu opcji „Szczegóły logu P1 ATNA”. W szczegółach znajdują się dodatkowe informacje m.in. o pobierającym dokument, statusie pobrania dokumentu oraz samą treść logu.



Rysunek 37: Szczegółu wpisu logu P1 ATNA

W przypadku błędu wysłania logu do P1 lub błędu pobrania dokumentu, w szczegółach wpisu wyświetlany jest identyfikator błędu z Dziennika systemowego, który jest odnośnikiem przenoszącym do szczegółów błędu.

6.4.1. Opis logu ATNA

Poniżej przedstawiono przykładowy log ATNA z opisem najważniejszych parametrów:

```
<14>1 [Data i czas zdarzenia UTC] [nazwa hosta] [nazwa procesu] [identyfikator procesu] IHE+RFC-3881 -
<AuditMessage>
    <EventIdentification EventActionCode="R"
                         EventDateTime="[Data i czas zdarzenia UTC]"
                         EventOutcomeIndicator="[0 dla sukcesu pobrania, 4 dla błędu pobrania]">
        <EventID csd-code="110106"
                 codeSystemName="DCM"
                 originalText="Export"/>
        <EventTypeCode csd-code="ITI-43"
                       codeSystemName="IHE Transactions"
                       originalText="Retrieve Document Set"/>
    </EventIdentification>
    <ActiveParticipant UserID="[Pełny URI repozytorium]"
                       AlternativeUserID="[Identyfikator procesu]"
                       UserIsRequestor="false"
                       NetworkAccessPointID="[Adres IP lub adres domenowy repozytorium]"
                       NetworkAccessPointTypeCode="[1 dla adres domenowego, 2 dla adresu IP]">
        <RoleIDCode csd-code="110153"
                    codeSystemName="DCM"
                    originalText="Source"/>
    </ActiveParticipant>
    <ActiveParticipant UserID="http://www.w3.org/2005/08/addressing/anonymous"
                       AlternativeUserID="[Identyfikator podmiotu pobierającego]"
                       UserIsRequestor="true"
                       NetworkAccessPointID="[Adres IP podmiotu pobierającego]"
                       NetworkAccessPointTypeCode="2">
        <RoleIDCode csd-code="110152"
                    codeSystemName="DCM"
                    originalText="Destination"/>
    </ActiveParticipant>
    <AuditSourceIdentification AuditSourceID="[Identyfikator podmiotu, do którego należy repozytorium]">
        <AuditSourceTypeCode csd-code="4"
                             codeSystemName="DCM"
                             originalText="Application Server Process or Thread"/>
    </AuditSourceIdentification>
    <ParticipantObjectIdentification ParticipantObjectID="[Identyfikator pobieranego dokumentu]"
                                     ParticipantObjectTypeCode="2"
                                     ParticipantObjectTypeCodeRole="3">
        <ParticipantObjectIDTypeCode csd-code="9"
                                     codeSystemName="RFC-3881"
                                     originalText="Report Number"/>
        <ParticipantObjectDetail type="Repository Unique Id"
                                 value="[OID repozytorium zapisany w formie Base64]"/>
        <ParticipantObjectDetail type="ihe:homeCommunityID"
                                 value="[Identyfikator domeny krajowej zapisany w formie Base64]"/>
    </ParticipantObjectIdentification>
</AuditMessage>
```

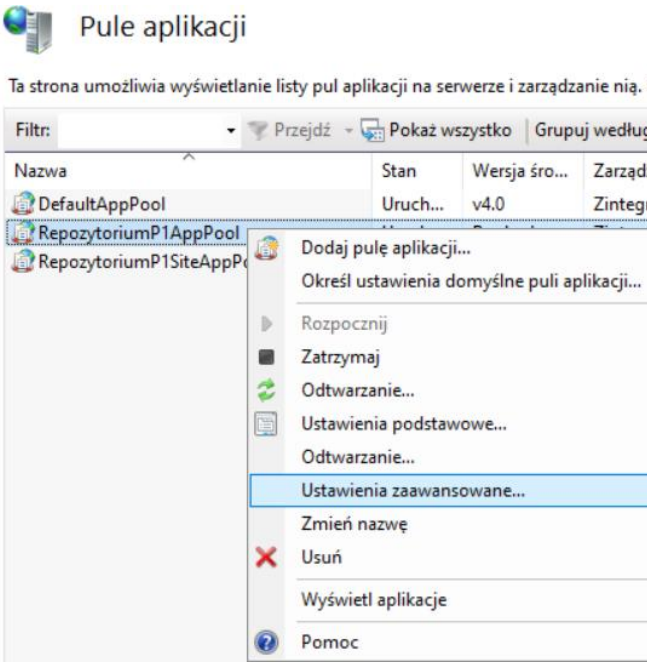
7. Pobieranie danych diagnostycznych

Możliwe jest pobieranie danych diagnostycznych w formie XML lub JSON dotyczących działania komponentów mModułów. Zakres danych do pobrania jest tożsamy z danymi wyświetlanymi na stronach statusowych. Opis techniczny znajduje się w dokumencie pod odnośnikiem.

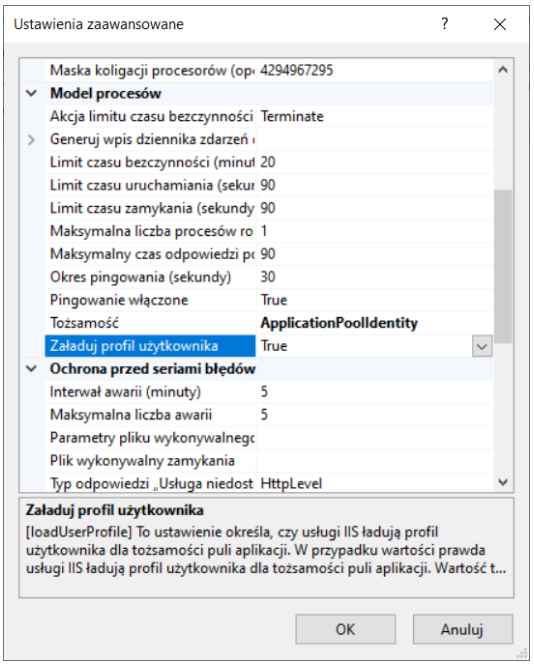
8. Rozwiązania częstych problemów

8.1. Błąd „Niepoprawne hasło lub certyfikat” podczas rejestrowania repozytorium w P1

Brak ustawienia wartości „Załaduj profil użytkownika” na „True” dla puli aplikacji Archiwum w IIS może powodować błąd informujący o błędnym certyfikacie lub haśle podczas rejestracji repozytorium w systemie P1.



Rysunek 38 Uruchomienie ustawień zaawansowanych puli aplikacji



Rysunek 39: Ustawienia zaawansowane puli aplikacji

8.2. Biała strona komponentu po instalacji na IIS

Powodem takiej sytuacji jest zaznaczenie dla komponentu wymagania korzystania z SSL bez konfiguracji certyfikatu w IIS. Jeżeli wymaganie SSL zostało zaznaczone rozmyślnie, należy skonfigurować SSL zgodnie z *1.6.1. Konfiguracja certyfikatu SSL*. W innym przypadku istnieje możliwość wyłączenia opcji. W tym celu należy uruchomić Menedżer internetowych usług informacyjnych, następnie wybrać witrynę, w której zostały

zainstalowane aplikacje (domyślnie „Default Web Site”). Z panelu środkowego wybrać „Ustawienia protokołu SSL” i odznaczyć pole „Wymagaj protokołu SSL”. Następnie kliknąć prawym przyciskiem myszy na witrynę (domyślnie „Default Web Site”) i wybrać opcję „Edytuj powiązania…”. Jeżeli w oknie brak jest typu „http”, należy go dodać opcją „Dodaj…” z portem 80. Jeżeli na liście powiązań widnieje typ „https”, to można go usunąć zaznaczając wiersz i wybierając opcję „Usuń”. Dodatkowo należy zaznaczyć witrynę i w menu „Zarządzaj witryną sieci Web” wybrać opcję „Rozpocznij” (jeśli witryna jest zatrzymana). Istnieje również możliwość późniejszej konfiguracji SSL zgodnie z podrozdziałem *1.6.1. Konfiguracja certyfikatu SSL*.

8.3. Błąd 403.4 na localhost lub na adresie komponentu na IIS

Rozwiązanie problemu zostało opisane w podrozdziale *3.1. Biała strona komponentu po instalacji IIS.*

8.4. Błąd 500.21 w IIS

Powodem błędu jest brak zainstalowanego modułu AspNetCoreModuleV2 dla IIS. Konieczne jest zainstalowanie lub zainstalowanie ponowne pakietu DotNetCore WindowsHosting.

8.5. Błąd 502.5 w IIS

Błąd najczęściej jest spowodowany brakiem zrestartowania usługi IIS po instalacji DotNetCore WindowsHosting. Problem może również być wynikiem braku instalacji pakietu KB2533623 dla systemów Windows 7 SP1 oraz Windows Server 2008 R2 SP1. Innym powodem błędu może być brak uprawnień do odczytu folderu komponentu przez pulę aplikacji.

8.6. Polecenie dotnet nie jest rozpoznawalne – Linux

Do poprawnego uruchomienia aplikacji wymagana jest instalacja środowiska ASP .NET Core. Jeżeli po dodaniu certyfikatu Microsoft, podczas próby zaktualizowania listy pakietów pojawi się problem związany z brakiem możliwości zweryfikowania podpisu, to pobierany jest certyfikat dla nieodpowiedniej wersji systemu. Przykładowy certyfikat dla Linux Ubuntu 20.04:

```
wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-
prod.deb -O packages-microsoft-prod.deb
sudo dpkg -i packages-microsoft-prod.deb
```

Na stronie https://docs.microsoft.com/pl-pl/dotnet/core/install/linux znajdują się instrukcje dla innych popularnych wersji systemu.

8.7. Status serwisu Main process exited – Linux

Błąd ten może wynikać z wielu przyczyn:

a) Brak uprawnień wykonywania dla pliku z rozszerzeniem .sh. Należy je wtedy dodać poprzez polecenie:

```
sudo chmod +x nazwa_pliku.sh
```

b) W pliku */etc/systemd/system/[*nazwa_serwisu*].service* została umieszczona błędna ścieżka do pliku wykonywalnego. Należy ja poprawić zgodnie z umieszczonym wcześniej opisem.

c) W pliku *nazwa_pliku.sh* umieszczona została błędna ścieżka do pliku wykonywalnego. Należy ja poprawić.

8.8. Brak portu w statusie usługi – Linux

Jeśli podczas sprawdzania statusu serwisu poprzez polecenie:

```
sudo systemctl status nazwa_serwisu.service
```

pojawił się komunikat o uruchomieniu aplikacji, ale brak informacji o tym na jakim porcie aplikacja została wystawiona, to najprawdopodobniej jest to związane z błędną konfiguracją komponentów. Więcej informacji można uzyskać uruchamiając plik wykonywalny *nazwa_pliku.sh* ręcznie. Poprzez komendę:

```
./nazwa_pliku.sh
```

W razie potrzeby należy poprawić konfigurację w pliku appsettings.json komponentu zgodnie z instrukcją. Możliwe jest również, że błąd wynika z braku odpowiedniego pakietu. Jeżeli podczas ręcznego uruchomienia wyświetlony zostanie komunikat o błędzie związanym z libunwind, należy go zainstalować zgodnie z instrukcją.

8.9. Strona jest widoczna wyłącznie z komputera lokalnego

Należy sprawdzić, czy strona została właściwie powiązana z adresem, a także czy zapora ogniowa akceptuje ruch przychodzący na porcie działania usługi WWW.

8.10. Przekroczenie czasu realizacji operacji na bazie danych (timeout)

Możliwa jest edycja maksymalnego czasu wykonywania operacji na bazie danych dla każdego komponentu. W tym celu należy wpisać „CommandTimeout=WARTOSC” w pliku appsettings.config komponentu (sekcja „ConnectionString”). WARTOSC jest podawana w sekundach. Przykład dla 250 sekund i bazy danych Archiwum:

```
"ConnectionString": "Server=localhost,5432;Database=ARCHMMEDICA;CommandTimeout=250;"
```

8.11. Brak pliku api-ms-win-crt-runtime-l1-1-0 – Windows

W przypadku błędu informującego o braku pliku api-ms-win-crt-runtime-l1-1-0 podczas uruchomienia Archiwum należy zainstalować lub zaktualizować pakiet „Universal C Runtime in Windows”. Więcej informacji na stronie: https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows.