

IBM Business Monitor



Podręcznik instalowania programu IBM Business Monitor

Wersja 7.5.0

IBM Business Monitor



Podręcznik instalowania programu IBM Business Monitor

Wersja 7.5.0

Spis treści

Rozdział 1. Instalowanie produktu IBM Business Monitor. 1

Rozdział 2. Planowanie instalacji produktu IBM Business Monitor 3

| | |
|--|----|
| Wybór odpowiednich topologii | 3 |
| Topologia pojedynczego serwera | 3 |
| Topologia wysokiej dostępności (wdrażanie sieciowe) | 3 |
| Korzystanie z istniejącego wstępnie wymaganego oprogramowania | 9 |
| Profile. | 9 |
| Wybór typu profilu | 10 |
| Zagadnienia dotyczące bazy danych | 12 |
| Uwagi dotyczące bazy danych MONITOR dla produktu DB2 | 14 |
| Uwagi dotyczące bazy danych COGNOSCS dla produktu DB2 | 15 |
| Uwagi dotyczące bazy danych MONITOR dla produktu DB2 for z/OS | 16 |
| Uwagi dotyczące bazy danych MONITOR dla produktu Oracle | 18 |
| Uwagi dotyczące bazy danych COGNOSCS dla produktu Oracle | 19 |
| Uwagi dotyczące bazy danych MONITOR dla produktu Microsoft SQL Server | 21 |
| Uwagi dotyczące bazy danych COGNOSCS dla produktu Microsoft SQL Server. | 23 |
| Uprawnienia do bazy danych | 24 |
| Zagadnienia dotyczące rejestru użytkowników | 25 |
| Uwagi dotyczące użytkownika bez uprawnień administratora | 26 |
| Przykładowe ścieżki instalacji | 27 |
| Ścieżka instalacyjna dla topologii pojedynczego serwera | 27 |
| Ścieżka instalacji dla topologii wdrożenia sieciowego korzystającej ze wzorców środowiska wdrażania. | 27 |
| Ścieżka instalacji na potrzeby topologii niestandardowego wdrożenia sieciowego | 28 |
| Ścieżki instalacji środowiska wdrażania zarządzanego dla programu WebSphere Business Modeler | 29 |
| Przegląd zadania: instalacja i konfiguracja | 30 |

Rozdział 3. Przygotowywanie instalacji produktu 33

| | |
|--|----|
| Wymagania dotyczące sprzętu i oprogramowania | 33 |
| Przygotowywanie systemów operacyjnych do instalacji produktu | 33 |
| Przygotowywanie systemów AIX do instalacji | 33 |
| Przygotowywanie systemów HP-UX do instalacji | 34 |
| Przygotowywanie systemów Linux do instalacji | 35 |
| Przygotowywanie systemów Solaris do instalacji | 37 |
| Przygotowywanie systemów Windows do instalacji | 38 |

Rozdział 4. Instalowanie produktu IBM Business Monitor 39

| | |
|--|----|
| Instalowanie oprogramowania IBM Business Monitor | 39 |
| Instalowanie z poziomu startera produktu | 39 |
| Instalacja cicha produktu IBM Business Monitor. | 44 |
| Praca z programem IBM Installation Manager | 46 |
| Instalowanie Centrum informacyjnego. | 49 |

Rozdział 5. Tworzenie baz danych 53

| | |
|---|----|
| Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych | 54 |
| Ręczne konfigurowanie skryptów bazy danych | 56 |
| Ręczne instalowanie baz danych | 59 |
| Ręczne tworzenie tabel mechanizmu przesyłania komunikatów | 60 |

Rozdział 6. Tworzenie i rozszerzanie profili 63

| | |
|--|----|
| Tworzenie i rozszerzanie profili przy użyciu narzędzia Profile Management Tool | 63 |
| Tworzenie profili autonomicznych | 64 |
| Tworzenie profili menedżera wdrażania | 71 |
| Rozszerzanie profili menedżera wdrażania | 77 |
| Tworzenie profili niestandardowych dla węzłów | 82 |
| Rozszerzanie profili niestandardowych dla węzłów | 84 |
| Tworzenie i rozszerzanie profili za pomocą komendy manageprofiles. | 86 |

Rozdział 7. Weryfikowanie instalacji 89

Rozdział 8. Określanie numerów portów 91

Rozdział 9. Konfigurowanie środowiska 93

| | |
|---|-----|
| Tworzenie środowiska wdrażania za pomocą wzorca | 93 |
| Importowanie definicji środowisk wdrażania opartych na dokumentach projektu | 100 |
| Tworzenie środowiska wdrażania przy użyciu topologii niestandardowej | 106 |
| Tworzenie klastrów programu IBM Business Monitor | 106 |
| Konfigurowanie usług zdarzeń infrastruktury CEI | 108 |
| Konfigurowanie środowiska przy użyciu kreatora konfiguracji | 109 |
| Konfigurowanie środowiska przy użyciu komend narzędzia wsadmin | 116 |
| Ręczne konfigurowanie środowiska | 118 |

Rozdział 10. Konfigurowanie komponentów programu IBM Business Monitor. 131

| | |
|---|-----|
| Konfigurowanie produktu IBM Cognos BI | 131 |
| Konfigurowanie nowej usługi IBM Cognos BI | 131 |
| Konfigurowanie istniejącej usługi IBM Cognos BI | 132 |

| | |
|--|-----|
| Konfigurowanie produktu IBM Cognos BI przy użyciu produktu WebSphere Portal | 133 |
| Konfigurowanie widgetów programu IBM Business Monitor dla produktu WebSphere Portal | 135 |
| Konfigurowanie sposobu odbierania zdarzeń | 135 |
| Uwagi dotyczące zdarzeń asynchronicznych. | 135 |
| Odbieranie zdarzeń z infrastruktury CEI | 137 |
| Konfigurowanie produktu Business Space | 143 |
| Konfigurowanie produktu Business Space | 143 |
| Migrowanie produktu Business Space (czynności po migracji produktu) | 272 |
| Konfigurowanie produktu Business Space do pracy z produktem Mashup Center | 273 |
| Konfigurowanie widgetów do pracy z produktem WebSphere Portal | 275 |
| Konfigurowanie monitorowania czynności personelu | 284 |
| Ręczne instalowanie modelu monitorowania czynności personelu | 284 |
| Włączanie zdarzeń dla monitorowania czynności personelu | 284 |
| Konfigurowanie połączeń produktu Business Space w programie WebSphere Portal | 285 |

| | |
|--|-----|
| Konfigurowanie połączeń dla portletowych paneli kontrolnych | 285 |
| Konfigurowanie modelu monitorowania procesu globalnego | 286 |
| Ręczne instalowanie modelu monitorowania procesu globalnego | 286 |
| Włączanie zdarzeń dla modelu monitorowania procesu globalnego | 287 |
| Konfigurowanie paneli kontrolnych dla modelu monitorowania procesu globalnego | 287 |

Rozdział 11. Instalowanie przykładu modelowego. 291

| | |
|---|------------|
| Rozdział 12. Deinstalowanie produktu IBM Business Monitor. 293 | 293 |
| Deinstalowanie produktu IBM Business Monitor | 293 |
| Usuwanie przykładu modelowego. | 294 |

Rozdział 1. Instalowanie produktu IBM Business Monitor

Program IBM® Business Monitor można zainstalować w wielu topologiach. Istnieje możliwość zainstalowania wszystkich komponentów na pojedynczym serwerze lub rozmieszczenia ich w wielu systemach. Aby uzyskać środowisko wysokiej dostępności z obsługą przełączania awaryjnego, produkt IBM Business Monitor można zainstalować w środowisku klastrowym, w którym używana jest technologia klastrowa produktu WebSphere Application Server lub Process Server.

Ważne: Produkt IBM Business Monitor działa na wielu platformach. Szczegółowe informacje o obsługiwanych systemach operacyjnych oraz sprzęcie, a także wymagania dotyczące pamięci i wolnego miejsca na dysku można znaleźć w serwisie WWW IBM Business Monitor System requirements (Wymagania systemowe produktu IBM Business Monitor).

Rozdział 2. Planowanie instalacji produktu IBM Business Monitor

Program IBM Business Monitor ma wiele komponentów, które można zainstalować na jednym serwerze lub na wielu serwerach w sieci. Podczas procesu instalacyjnego dostępnych jest wiele opcji, które należy wziąć pod uwagę. Podczas planowania instalacji programu IBM Business Monitor należy wziąć pod uwagę dostępne opcje oraz przyjęty sposób wdrożenia komponentów w sieci.

Dostępne są informacje ułatwiające określenie najbardziej odpowiedniej topologii dla danego środowiska i poznanie opcji dostępnych podczas instalacji.

Przed rozpoczęciem instalacji produktu IBM Business Monitor należy zapoznać się z następującymi informacjami:

Wybór odpowiednich topologii

Program IBM Business Monitor może zostać zainstalowany w wielu różnych konfiguracjach. Udostępniono kilka podstawowych topologii. Konieczne może być ich dostosowanie do konkretnego środowiska.

Aby pomóc w zrozumieniu niektórych możliwych wdrożeń instalacji, przedstawiono topologie ilustrujące kilka typowych instalacji:

Topologia pojedynczego serwera

Jeśli używana jest topologia pojedynczego serwera, wszystkie dodatkowe produkty oraz wszystkie komponenty produktu IBM Business Monitor są instalowane na tym samym serwerze fizycznym.

Zainstalowanie produktu IBM Business Monitor na pojedynczym serwerze doskonale nadaje się do projektowania środowisk testowych, środowisk koncepcyjnych i prostych wdrożeń, które nie wymagają przełączania awaryjnego ani wysokiej dostępności.

Przy użyciu programu instalacyjnego produktu IBM Business Monitor można zainstalować produkty IBM Business Monitor i WebSphere Application Server. Kiedy produkt IBM Business Monitor jest instalowany na pojedynczym serwerze, instalowana jest również usługa Cognos. Do wyświetlenia monitorowanych danych można użyć obszaru Business Space lub portletowych paneli kontrolnych.

Po zainstalowaniu produktu IBM Business Monitor należy utworzyć profil autonomiczny w celu zdefiniowania środowiska wykonawczego. Wszystkie wymagane komponenty programu IBM Business Monitor są tworzone podczas tworzenia lub rozszerzania profilu autonomicznego.

Topologia wysokiej dostępności (wdrażanie sieciowe)

Program IBM Business Monitor wykorzystuje możliwości funkcji wysokiej dostępności w środowiskach WebSphere Application Server lub Process Server Network Deployment (ND). Wdrożenie sieciowe (Network Deployment) udostępnia moc obliczeniową, skalowalność i stabilność, które są ogólnie wymagane w środowisku produkcyjnym. W środowiskach wdrożenia sieciowego grupa serwerów może współpracować, aby udostępniać funkcję równoważenia obciążenia oraz przełączania awaryjnego. Jedna Konsola administracyjna umożliwia scentralizowane zarządzanie serwerami.

Program IBM Business Monitor korzysta z tego samego modelu architektury co produkty WebSphere Application Server oraz Process Server. Korzystając z tego modelu, użytkownik tworzy środowiska, które mają komórki, węzły, serwery i (opcjonalnie) klastry.

Jeśli został wybrany jeden z dostępnych wzorców środowiska wdrożenia sieciowego (jeden klastr lub cztery klastry), kreator środowiska wdrożenia pomaga w skonfigurowaniu wymaganych klastrów, serwerów i komponentów.

Komórka jest główną domeną administracyjną. Można ją sobie wyobrazić jako logiczną grupę serwerów, klastrów lub ich kombinacji. (Klastr jest grupą serwerów aplikacji, które współpracują ze sobą w celu równoważenia obciążenia i przełączania awaryjnego). Korzystając z serwerów i klastrów, można zainstalować program IBM Business Monitor w pojedynczej komórce, która jest zarówno wysoce dostępna, jak i skalowalna.

Węzeł zarządzany (czyli węzeł w komórce) zawiera jeden lub kilka serwerów. Każdy serwer udostępnia środowisko wykonawcze. Serwery zarządzane tworzone są w węźle zarządzanym, który jest definiowany przez profil niestandardowy. Każdy z węzłów zarządzanych jest stowarzyszony z tym samym menedżerem wdrażania, a menedżer wdrażania zarządza wszystkimi węzłami zarządzanymi w komórce. Serwery mogą być grupowane w klastry, które są również zarządzane przez menedżer wdrażania. W przypadku środowiska wdrożenia sieciowego programu należy zgrupować aplikacje w klastrze w celu ich zabezpieczenia przed awarią pojedynczego serwera (wysoka dostępność) i/lub w celu rozłożenia obciążenia aplikacji na większą liczbę równorzędnych serwerów (równoważenie obciążenia).

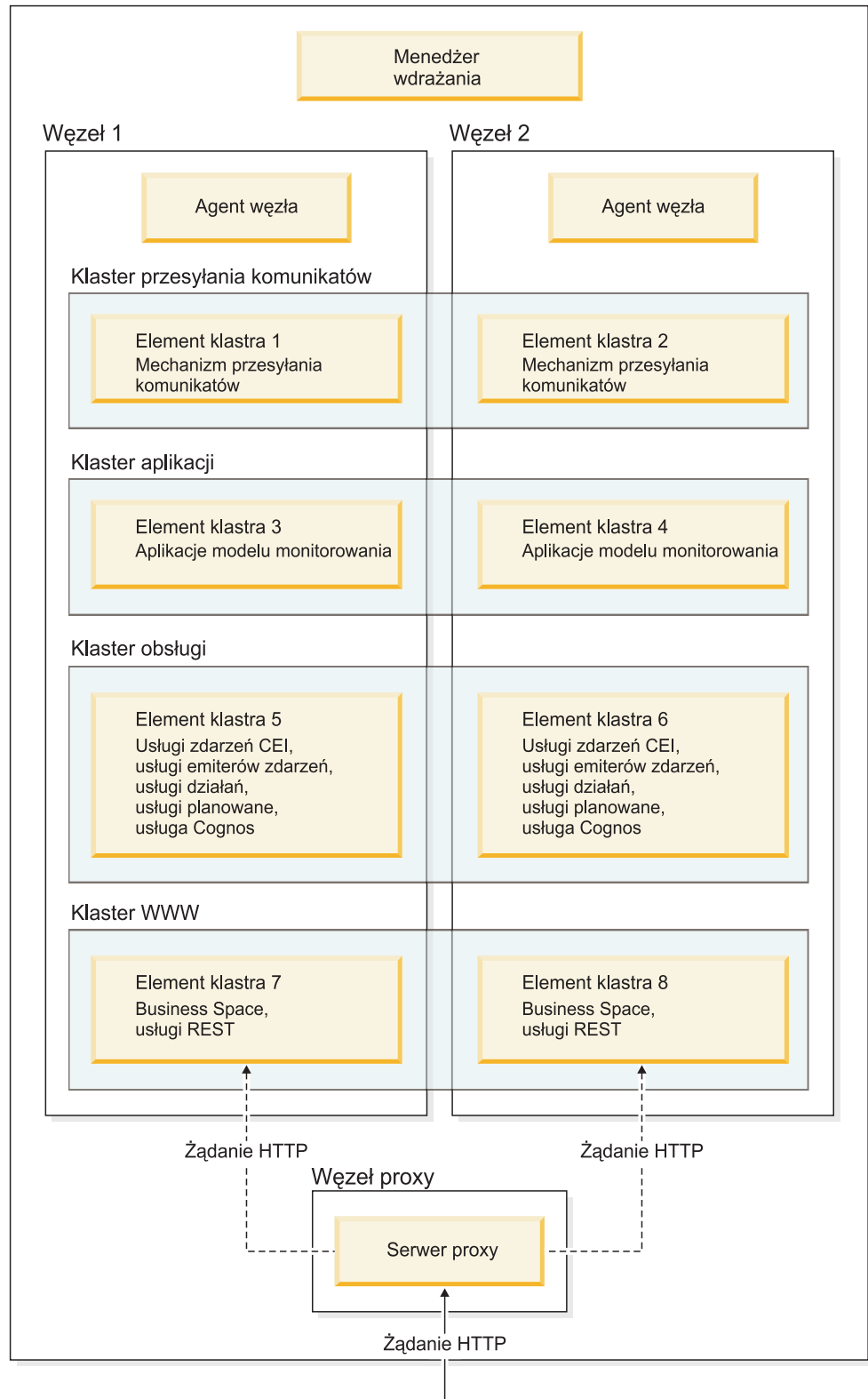
Więcej informacji o wysokiej dostępności zawiera temat Wysoka dostępność i równoważenie obciążenia dostępny w sekcji stron pokrewnych.

W środowisku wdrożenia sieciowego zazwyczaj konfigurowany jest serwer proxy lub serwer HTTP ze względów bezpieczeństwa i w celu równoważenia obciążenia. Więcej informacji dotyczących serwera proxy zawiera temat Skalowalność.

Skalowalność

Instalowanie komponentów i modeli monitorowania programu IBM Business Monitor zwiększa możliwości użytkownika w zakresie zarządzania ich obciążeniem. Rozpraszanie komponentów i modeli monitorowania między wiele klastrów i grupowanie komponentów według wspólnych wzorców użycia zasobów umożliwia użytkownikowi zarządzanie obciążeniem poszczególnych klastrów na podstawie wzorców użycia zasobów zainstalowanych komponentów. Sugestie na temat punktu początkowego planowania skalowalnej topologii zawiera temat Topologia czteroklastrowa.

Na poniższym diagramie przedstawiono komórkę z dwoma węzłami zarządzanymi.



Mechanizmy przesyłania komunikatów

Jeśli mechanizm przesyłania komunikatów utworzony na potrzeby magistrali integracji usług programu IBM Business Monitor został wdrożony w klastrze, jednocześnie tylko jeden taki

mechanizm może być aktywny w jednym elemencie klastra. To zachowanie wynika z domyślnej strategii magistrali integracji usług. Domyślną strategią magistrali integracji usług można co prawda konfigurować, jednak zawsze należy stosować strategię typu 1 z N. Strategia 1 z N umożliwia zaledwie jednej instancji mechanizmu przesyłania komunikatów zostanie instancją aktywną w klastrze, co przekłada się na wysoką dostępność (chroniąc komponenty i modele przed awarią pojedynczego serwera), ale nie gwarantuje skalowalności (zdolności do rozszerzania wraz z dodawaniem zasobów).

Zakres stosowania mechanizmu przesyłania komunikatów można zminimalizować, a wydajność można podnieść, korzystając z opcji umożliwiającej usłudze zdarzeń infrastruktury CEI wprowadzanie zdarzeń bezpośrednio do bazy danych programu IBM Business Monitor, a więc z pominięciem kolejek JMS (Java Messaging Service). Więcej informacji zawiera sekcja Odbieranie zdarzeń przy użyciu metody skalowalnej lub opartej na tabeli na stronach pokrewnych.

Komponenty obsługi

Do komponentów obsługi zalicza się usługę zdarzeń infrastruktury CEI, usługę IBM Cognos Business Intelligence, usługi działań, usługi emitera zdarzeń oraz usługi planowane. Dla wszystkich tych typów usług (oprócz usługi planowanej) należy dodać nowe elementy klastra zwiększające pojemność.

Usługi planowane w największym stopniu obciążają serwer bazy danych. Wzrost obciążenia usług planowanych wymaga więc monitorowania, oceny i właściwego strojenia serwera bazy danych. Obciążeniem usług planowanych można też sterować, włączając lub wyłączając różne usługi planowane bądź edytując odstępy czasu powiązane z poszczególnymi usługami planowanymi. Więcej informacji na ten temat zawiera sekcja Zarządzanie usługami planowanymi programu Monitor dostępna wśród odsyłaczy do zadań pokrewnych.

Komponenty WWW

Do komponentów WWW zalicza się produkt Business Space, widżety oraz usługę REST API produktu IBM Business Monitor. Użytkownik powinien dodać nowe elementy klastra zwiększające pojemność.

W środowisku wdrożenia sieciowego zazwyczaj konfigurowany jest serwer proxy lub serwer HTTP ze względów bezpieczeństwa i w celu równoważenia obciążenia. Przychodzące żądania HTTP nie są kierowane bezpośrednio do produktu WebSphere Application Server, zamiast tego są kierowane do serwera proxy, który może je rozesłać do wielu serwerów aplikacji obsługujących żądanie. Serwer proxy należy utworzyć w produkcie WebSphere Application Server. Zamiast serwera proxy lub „przed” nim można używać innych serwerów kierujących, na przykład serwera IBM HTTP Server. Zaletą używania serwera proxy jest jego integracja z produktem WebSphere Application Server i wynikająca z niej łatwość użytkowania i obsługi.

Ważne: Serwer proxy (lub alternatywny serwer kierujący) jest wymagany do równoważenia obciążenia przez rozdzielanie żądań HTTP między dwa lub więcej elementów klastra. Serwer proxy umożliwia klientom uzyskiwanie dostępu do aplikacji w obrębie tej topologii.

Aplikacje modelu monitorowania

Aplikacje modelu monitorowania są umieszczane w standardowych archiwach aplikacji korporacyjnej (EAR) języka Java. Aplikacja modelu monitorowania skaluje liczbę elementów w klastrze.

Zagadnienia dotyczące pamięci

Ilość pamięci dostępnej dla pojedynczego elementu klastra zależy od układu przestrzeni adresowej systemu operacyjnego oraz tego, czy maszyna JVM, w której działa ten element klastra, ma postać procesu 32-, czy 64-bitowego. O ile 64-bitowa maszyna JVM może uzyskiwać dostęp do dowolnych danych w pamięci zajmującej od 500 GB do 4 EB, o tyle 32-bitowa maszyna JVM może uzyskiwać dostęp do zaledwie 2 GB pamięci (tak jest na przykład w 32-bitowym systemie Windows).

Ogólnie, dodanie drugiego klastra na potrzeby wdrażanych aplikacji modelu monitorowania należy rozważyć w sytuacji, gdy liczba aplikacji modelu monitorowania do wdrożenia przekracza dziesięć i gdy elementy klastra działają na 32-bitowej maszynie JVM. To tylko wskazówka - w każdym przypadku obciążenie i liczby modeli mogą się różnić.

Topologia czteroklastrowa

Produkt IBM Business Monitor można zainstalować w wielu topologiach. Topologii czteroklastrowej można użyć w celu skonfigurowania środowiska o wysokiej wydajności.

Poniższa topologia czteroklastrowa używa wzorca środowiska wdrażania Zdalne przesyłanie komunikatów, zdalna obsługa i sieć WWW. Ten wzorzec grupuje aplikacje produktu IBM Business Monitor w ramach czterech klastrów w pojedynczej komórce.

Klaster mechanizmu przesyłania komunikatów
Magistrale produktu WebSphere Business Monitor i infrastruktury CEI

Klaster obsługi
Usługi zdarzeń CEI, usługi działań, program planujący usługi, usługi emiterów zdarzeń, usługa Cognos

Klaster aplikacji
Aplikacje modelu monitorowania

Klaster WWW
Aplikacja produktu Business Space, widgety produktu Business Space, aplikacja usług REST

Klaster mechanizmu przesyłania komunikatów

Mechanizm przesyłania komunikatów dla magistrali programu IBM Business Monitor

Mechanizm przesyłania komunikatów na potrzeby magistrali infrastruktury CEI (Common Event Infrastructure)

Klaster obsługi

Usługa zdarzenia infrastruktury CEI

- Usługi emitera zdarzeń
- Usługi działań
- Usługi planowane programu Monitor
- Usługa IBM Cognos Business Intelligence

Klaster aplikacji

- Aplikacje modelu monitorowania

Klaster WWW

- Aplikacja Business Space
- Widżety produktu Business Space
- Aplikacja usług REST (Representational State Transfer)

Uwaga: Aby zwiększyć wydajność, należy umieścić usługi emitatorów zdarzeń i usługę zdarzeń infrastruktury CEI w tym samym klastrze. Usługi emitatorów zdarzeń obejmują zarówno emitery zdarzeń REST, jak i zdarzeń JMS.

Topologia czteroklastrowa z produktem IBM Business Process Manager

Użytkownik może utworzyć złożone środowisko wdrażania produktów IBM Business Process Manager i IBM Business Monitor za pomocą wzorca zdalnego przesyłania komunikatów, zdalnej obsługi i sieci WWW (topologia czteroklastrowa). Ponieważ jedno środowisko wdrażania produktu IBM Business Monitor może monitorować wszystkie aplikacje w komórce, w bieżącej komórce należy utworzyć tylko jedno takie środowisko.

Topologia czteroklastrowa łączy klastry mechanizmów przesyłania komunikatów produktów IBM Business Monitor i IBM Business Process Manager w ramach pojedynczego klastra. Poniższa topologia czteroklastrowa używa wzorca środowiska wdrażania Zdalne przesyłanie komunikatów, zdalna obsługa i sieć WWW.

Klaster mechanizmu przesyłania komunikatów

- Mechanizm przesyłania komunikatów dla magistrali produktu IBM Business Monitor

- Mechanizm przesyłania komunikatów na potrzeby magistrali infrastruktury CEI (Common Event Infrastructure)

- Mechanizm przesyłania komunikatów dla magistrali produktu Process Server

- Mechanizm przesyłania komunikatów dla magistrali hurtowni danych wydajności

- (Tylko produkt BPM Advanced) Mechanizm przesyłania komunikatów na potrzeby magistrali architektury SCA (Service Component Architecture)

- (Tylko produkt BPM Advanced) Mechanizm przesyłania komunikatów na potrzeby magistrali BPEL (Business Process Execution Language)

Klaster obsługi

- Usługa zdarzenia infrastruktury CEI
- Usługi emitera zdarzeń
- Usługi działań
- Usługi planowane programu Monitor
- Usługa IBM Cognos Business Intelligence
- Hurtownia danych wydajności
- (Tylko produkt BPM Advanced) Menedżer reguł biznesowych

Klaster aplikacji

Aplikacje modelu monitorowania

Aplikacje procesów

(Tylko produkt BPM Advanced) Aplikacje BPEL

Klaster WWW

Aplikacja Business Space

Widżety produktu Business Space

Aplikacja usług REST (Representational State Transfer)

(Tylko produkt BPM Advanced) Narzędzia produktu Business Process Choreographer

Korzystanie z istniejącego wstępnie wymaganego oprogramowania

Produkt IBM Business Monitor można instalować na serwerach, na których zainstalowano wstępnie wymagane oprogramowanie.

Istniejące serwery aplikacji

Serwer produktu IBM Business Monitor można zainstalować na serwerze fizycznym, na którym jest obecnie zainstalowana platforma serwera aplikacji. Dla produktu IBM Business Monitor obsługiwane są następujące platformy serwera aplikacji:

- WebSphere Application Server
- Process Server
- WebSphere Enterprise Service Bus

Istnieje możliwość rozszerzenia istniejącego profilu lub utworzenia nowego profilu, który ma zawierać serwer produktu IBM Business Monitor.

Istniejący produkt WebSphere Portal

Program IBM Business Monitor nie udostępnia już portletowych paneli kontrolnych. Widżety programu IBM Business Monitor mogą być nadal wyświetlane w produkcie WebSphere Portal. Więcej informacji udostępnia odsyłacz do zadań pokrewnych.

Profile

Profil definiuje środowisko wykonawcze i obejmuje wszystkie pliki przetwarzane przez serwer w środowisku wykonawczym. W środowisku o wysokiej dostępności należy utworzyć wiele profili, aby w odpowiedni sposób zarządzać złożonym systemem. Użytkownik może utworzyć nowe profile lub rozszerzyć istniejące profile.

Produkt IBM Business Monitor zawiera szablony profili, które włączają konkretne funkcjonalności produktu IBM Business Monitor. Po zainstalowaniu produktu można tworzyć i rozszerzać profile za pomocą kreatora Profile Management Tool lub komendy manageprofiles. (Jeśli jest używana 64-bitowa wersja produktu IBM Business Monitor, należy użyć komendy manageprofiles).

Typy profili produktu IBM Business Monitor są rozszerzeniami podobnie nazwanych typów profili dostępnych w produkcie WebSphere Application Server. Typy profili dostępne w produkcie IBM Business Monitor nie są takie same, jak te dostępne w produkcie WebSphere Application Server.

Używanie nowych profili jest bardziej wydajne i mniej podatne na błędy niż wielokrotne instalowanie produktu. Programiści mogą używać oddzielnych profili na potrzeby programowania i testów. Korzystanie z profili zamiast kilku instalacji produktu pozwala uzyskać następujące korzyści:

- Niezbędna jest konserwacja tylko jednego zestawu podstawowych plików produktu.
- Oszczędność miejsca na dysku.
- Łatwiejsze aktualizowanie produktu.

Wybór typu profilu

Profil definiuje unikalne środowisko wykonawcze z oddzielnymi plikami komend, plikami konfiguracyjnymi i plikami dzienników. Profile definiują trzy typy środowisk: pojedynczy serwer autonomiczny, menedżer wdrażania oraz węzeł zarządzany. Profile pozwalają na uzyskanie w systemie więcej niż jednego środowiska wykonawczego bez konieczności instalowania kilku kopii produktu.

W przypadku środowiska jednoserwerowego należy utworzyć profil autonomiczny.

W przypadku środowiska wdrażania sieciowego wykonaj następujące kroki:

1. Przed utworzeniem innych profili należy utworzyć profil menedżera wdrażania. Jeśli profil menedżera wdrażania utworzono przed zainstalowaniem produktu IBM Business Monitor (na przykład dla produktu WebSphere Application Server lub Process Server) i jeśli planowane jest używanie tego samego profilu menedżera wdrażania do zarządzania węzłami produktu IBM Business Monitor, należy rozszerzyć profil przy użyciu szablonu udostępnionego w produkcie IBM Business Monitor.
2. Profil niestandardowy należy utworzyć dla każdego węzła, który ma zostać dodany do klastra serwerów. Można również rozszerzyć istniejący profil niestandardowy dla każdego węzła, który ma zostać dodany.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

Szablony każdego profilu znajdują się w katalogu `katalog_główny_serwera_aplikacji/profileTemplates`. Dostępne są następujące szablony profili:

| Profil | Wykorzystanie |
|---|--|
| Autonomiczny serwer programu Monitor | W jednoserwerowych środowiskach programu IBM Business Monitor |
| Menedżer wdrażania serwera programu Monitor | Jeśli jest konfigurowane środowisko wdrożenia sieciowego, należy najpierw utworzyć lub rozszerzyć ten profil. Jeśli menedżer wdrażania utworzono przed zainstalowaniem programu IBM Business Monitor i jeśli planowane jest używanie tego samego profilu menedżera wdrażania na potrzeby zarządzania węzłami programu IBM Business Monitor, należy rozszerzyć profil przy użyciu szablonu udostępnionego w programie IBM Business Monitor. |

| Profil | Wykorzystanie |
|--|---|
| Profil niestandardowy serwera programu Monitor | Jeśli jest skonfigurowane środowisko wdrożenia sieciowego, należy utworzyć lub rozszerzyć węzły niestandardowe, a następnie użyć Konsoli administracyjnej w celu zainstalowania konkretnych aplikacji w różnych węzłach niestandardowych. |

Profile autonomiczne

W przypadku produktu IBM Business Monitor należy użyć profilu autonomicznego, znanego również jako profil autonomicznego serwera aplikacji dla środowisk jednoserwerowych.

Każdy węzeł autonomicznego serwera aplikacji ma własną Konsolę administracyjną, za pomocą której można nim zarządzać. Węzeł autonomiczny może zawierać więcej niż jeden serwer.

Serwer autonomiczny można łatwo skonfigurować i jest on wyposażony w konsolę Pierwsze kroki, za pomocą której można go uruchamiać i zatrzymywać oraz zainstalować przykład modelowy. Po zainstalowaniu przykładu na serwerze autonomicznym za pomocą Konsoli administracyjnej można przeglądać zasoby użyte w tym przykładzie.

Własne rozwiązania można wdrażać na serwerze autonomicznym, ale nie udostępnia on takiej mocy obliczeniowej, skalowalności i stabilności, które są ogólnie wymagane w środowisku produkcyjnym. W przypadku środowisk produkcyjnych lepszym rozwiązaniem jest użycie środowiska wdrożenia sieciowego.

Profile menedżera wdrażania

Menedżer wdrażania jest serwerem zarządzającym operacjami dla grupy logicznej lub komórki innych serwerów. W środowiskach wdrożenia sieciowego grupa serwerów może współpracować, aby udostępniać funkcję równoważenia obciążenia oraz przełączania awaryjnego. Menedżer wdrażania stanowi centrum administrowania serwerami i klastrami w komórce.

Profil menedżera wdrażania jest pierwszym profilem, który należy utworzyć lub rozszerzyć w celu utworzenia środowiska wdrożenia. Menedżer wdrażania zawiera konsolę Pierwsze kroki, za pomocą której można uruchomić i zatrzymać menedżer wdrażania, a także uruchomić jego Konsolę administracyjną. Konsola administracyjna menedżera wdrażania służy do zarządzania serwerami i klastrami w komórce. Umożliwia ona konfigurowanie serwerów i klastrów, dodawanie serwerów do klastrów, uruchamianie i zatrzymywanie serwerów i klastrów oraz wdrażanie ich modułów.

Choć menedżer wdrażania jest pewnego rodzaju serwerem, nie można instalować modułów bezpośrednio w menedżerze wdrażania.

Po utworzeniu lub rozszerzeniu menedżera wdrażania dla programu IBM Business Monitor w środowisku wdrożenia sieciowego można tworzyć lub rozszerzać węzły niestandardowe i stowarzyszać je w menedżerze wdrażania lub czynić je jego częścią w celu utworzenia komórki, czyli grupy centralnie administrowanych węzłów lub klastrów.

Przed utworzeniem lub rozszerzeniem profili niestandardowych należy utworzyć lub rozszerzyć profil menedżera wdrażania. Jeśli profil menedżera wdrażania utworzono przed zainstalowaniem programu IBM Business Monitor i jest planowane używanie tego samego profilu menedżera wdrażania na potrzeby zarządzania węzłami programu IBM Business Monitor, należy rozszerzyć profil przy użyciu szablonu udostępnionego w programie IBM Business Monitor.

Profile niestandardowe

Aby skonfigurować środowisko wdrożenia sieciowego dla produktu IBM Business Monitor, należy utworzyć węzły niestandardowe i stowarzyszyć je w komórce menedżera wdrażania lub uczynić te węzły jej częścią. Komórka menedżera wdrażania będzie zarządzać tymi węzłami. Można również rozszerzyć istniejący profil niestandardowy dla każdego węzła, który ma zostać dodany do komórki. Następnie należy użyć Konsoli administracyjnej do zainstalowania konkretnych aplikacji w różnych węzłach niestandardowych.

Profil niestandardowy jest pustym węzłem, który nie zawiera domyślnych aplikacji, lub serwerem uwzględnionym w profilu serwera autonomicznego. W trakcie tworzenia lub rozszerzania profilu niestandardowego należy stowarzyszyć węzeł w celu zidentyfikowania profilu menedżera wdrażania, który ma być używany do zarządzania węzłem. Po stowarzyszeniu profilu niestandardowego w menedżerze wdrażania węzeł staje się *węzłem zarządzanym*.

Węzeł zarządzany zawiera agent węzła, a także może zawierać serwery zarządzane. W węźle zarządzanym można konfigurować i uruchamiać serwery zarządzane. Serwery skonfigurowane w węźle zarządzanym tworzą zasoby środowiska wdrażania. Te serwery są tworzone, konfigurowane, uruchamiane, zatrzymywane, zarządzane i usuwane za pomocą Konsoli administracyjnej menedżera wdrażania. Procesy w węźle zarządzanym mogą obejmować elementy klastra, wykorzystywane przez menedżer wdrażania do równoważenia obciążenia w przypadku intensywnie używanych aplikacji.

Węzeł zarządzany może zawierać jeden lub więcej serwerów zarządzanych za pomocą menedżera wdrażania. Na serwerach w węźle zarządzanym można wdrażać rozwiązania, ale węzeł zarządzany nie ma własnej Konsoli administracyjnej. Węzeł zarządzany jest definiowany przez profil niestandardowy i jest dla niego dostępna konsola Pierwsze kroki.

Zagadnienia dotyczące bazy danych

W głównej bazie danych MONITOR przechowywana jest konfiguracja produktu IBM Business Monitor, metadane modelu monitorowania oraz monitorowane dane. Konfiguracja produktu IBM Cognos Business Intelligence jest przechowywana w osobnej bazie danych składnicy treści produktu IBM Cognos BI o nazwie COGNOSCS. Proces tworzenia profilu zakłada, że obie bazy danych (MONITOR i COGNOSCS) zostały utworzone w tej samej instancji bazy danych.

Dla bazy danych MONITOR i COGNOSCS można użyć wspólnej nazwy użytkownika bazy danych. Użycie oddzielnych nazw może być jednak zalecane, ponieważ produkt IBM Cognos BI tworzy własne tabele składnicy treści w schemacie udostępnionej nazwy bazy danych w momencie pierwszego uruchomienia produktu IBM Cognos BI.

Baza danych MONITOR jest używana także do przechowywania schematów na potrzeby następujących komponentów podczas tworzenia profilu autonomicznego:

- Business Space
- Składnica komunikatów mechanizmu przesyłania komunikatów infrastruktury CEI
- Składnica komunikatów mechanizmu przesyłania komunikatów produktu IBM Business Monitor

Jeśli profil autonomiczny nie jest używany, można użyć tej samej bazy danych lub różnych baz danych dla tych komponentów oraz dodatkowo dla składnicy danych infrastruktury CEI (co nie jest wymagane i dlatego nie jest domyślnie tworzone ani włączane).

W przypadku środowisk produkcyjnych można dokonać wyboru spośród następujących obsługiwanych produktów bazodanowych:

- DB2
- DB2 for z/OS
- Oracle
- Microsoft SQL Server

W bazie danych MONITOR przechowywanych jest wiele typów danych. Podczas tworzenia profilu programu IBM Business Monitor lub uruchamiania skryptów bazy danych są tworzone tabele bazy danych zawierające dane konfiguracyjne dla programu IBM Business Monitor. Następnie podczas instalowania poszczególnych modeli monitorowania są tworzone dodatkowe tabele niezbędne do przechowywania danych na potrzeby tych modeli. Podczas przetwarzania zdarzeń w tych tabelach są zapisywane dane instancji modelu monitorowania. W panelach kontrolnych znajdują się odwołania do tych tabel.

Wskazówka: W środowisku wdrożenia sieciowego bazy danych MONITOR i COGNOSCS należy utworzyć przed uruchomieniem menedżera wdrażania i utworzeniem innych profili niestandardowych.

Wskazówka: Jeśli baza danych COGNOSCS działa zdalnie względem serwera IBM Cognos BI, należy zainstalować klient bazy danych na serwerze IBM Cognos BI. Szczegółowe informacje zawierają tematy poświęcone uwagom specyficznym dla baz danych.

Tworzenie baz danych

Bazy danych MONITOR i COGNOSCS można utworzyć na kilka sposobów:

- Jeśli oprogramowanie bazy danych zostało zainstalowane na tym samym serwerze co program IBM Business Monitor, lokalne bazy danych można utworzyć przy użyciu narzędzia Profile Management Tool lub komendy manageprofiles podczas tworzenia profilu.

Uwaga:

- W przypadku bazy danych DB2 użytkownik tworzący profil musi mieć referencje do utworzenia bazy danych.
- W przypadku bazy danych Oracle lub SQL Server ID użytkownika i hasło administratora bazy danych należy wprowadzić w narzędziu Profile Management Tool albo przy użyciu komendy manageprofiles. Obiekty bazy danych można tworzyć dopiero w istniejącej instancji bazy danych.
- Skrypty bazy danych mogą zostać utworzone przez funkcję zarządzania profilem przy użyciu wartości konfiguracji wybranych podczas tworzenia profilu. Należy wybrać opcję tworzenia profilu, która opóźnia wykonanie skryptów bazy danych, i później uruchomić wygenerowane skrypty w celu utworzenia obiektów bazy danych na serwerze bazy danych.
- Istnieje możliwość ręcznego utworzenia bazy danych przy użyciu skryptów udostępnionych na nośniku instalacyjnym lub w katalogu dbscripts instalacji programu IBM Business Monitor. Zmienne w skryptach można skonfigurować ręcznie lub przy użyciu narzędzia do projektowania bazy danych (DbDesignGenerator).

Jeśli w bazie danych MONITOR zostanie zmieniona nazwa obszarów tabel danych instancji, podczas tworzenia schematu dla modeli monitorowania konieczne jest wyeksportowanie skryptów tworzenia schematów i zmiana nazw obszarów tabel w celu ich dopasowania do nazw użytych w czasie tworzenia początkowej bazy danych.

Wielkość bazy danych

Skrypty bazy danych programu IBM Business Monitor dla bazy danych MONITOR tworzą wiele obszarów tabel do przechowywania danych. Nazwy i konfiguracja obszarów tabel mogą

być zmieniane zależnie od standardów przedsiębiorstwa oraz wymagań dotyczących wydajności i wielkości. W przypadku instalacji programistycznych i testowych z minimalną ilością danych wystarczająca powinna być pamięć masowa bazy danych o wielkości 1 GB. Wielkość bazy danych dla środowisk produkcyjnych należy określić na podstawie ilości danych, które mają być monitorowane.

Zabezpieczanie baz danych

Podczas tworzenia baz danych użytkownikowi bazy danych środowiska wykonawczego domyślnie zostają nadane uprawnienia do administrowania obiektami bazy danych. Upraszcza to tworzenie baz danych i pozwala serwerowi programu IBM Business Monitor na automatyczne zarządzanie schematem bazy danych modelu monitorowania w czasie wdrażania i usuwania modeli. W razie konieczności zabezpieczenia baz danych należy zapoznać się z tematami Zabezpieczanie środowiska bazy danych MONITOR i Konfigurowanie zabezpieczeń produktu IBM Cognos BI.

Uwagi dotyczące bazy danych MONITOR dla produktu DB2

Istnieją specyficzne zalecenia dotyczące baz danych udostępnianych w produkcie DB2.

Uwagi dotyczące globalizacji

Produkt DB2 musi być zainstalowany przy użyciu uniwersalnego zestawu znaków UTF-8. Ten zestaw znaków zapewnia, że metadane modelu monitorowania i dane instancji zawierające znaki języka rodzimego mogą zostać zapisane w bazie danych. Ponadto produkt IBM Cognos Business Intelligence wymaga bazy danych UTF-8. Skrypt `createDatabase.sql` automatycznie tworzy bazę danych UTF-8.

Skrypt `createDatabase.sql` tworzy bazy danych z następującymi domyślnymi ustawieniami terytoriów:

```
TERRITORY EN_US
```

Aby zmienić język domyślny, należy zmienić wartość parametru `TERRITORY` na obsługiwaną wartość terytorium. Obsługiwane ustawienia dla produktu DB2 można znaleźć na stronie [Supported territory codes and code pages](#) (Obsługiwane kody terytorium i strony kodowe). Ustawienia terytorium muszą używać zestawu kodowego UTF-8. Na przykład aby zmienić terytorium na francuskie, należy użyć parametru:

```
TERRITORY FR_FR
```





Tabela `DIM_TIME` zawiera kolumnę na potrzeby zapełniania raportów panelu kontrolnego przetłumaczoną nazwą miesiąca. Domyślnie do zapełniania pozycji tabeli `DIM_TIME` używany jest kod ustawień narodowych dla języka angielskiego (Stany Zjednoczone) `EN_US`. Aby zmienić język domyślny, należy zastąpić wartość `EN_US` w pliku `createTables.sql` wybranymi ustawieniami narodowymi. Na przykład dla języka francuskiego należy zastąpić wartość `EN_US` wartością `FR_FR`. W pliku `createTables.sql` znajduje się również instrukcja SQL, której można użyć do nadpisania wpisów nazw miesięcy i zdefiniowania własnych nazw miesięcy.

Uwagi dotyczące produktu DB2 Express Edition

Produkt DB2 Express Edition może używać maksymalnie 4 GB pamięci instancji, nawet jeśli w systemie jest więcej niż 4 GB pamięci. Więcej informacji na temat odpowiedniej wersji produktu DB2 można znaleźć na stronach pokrewnych.

Obecnie istnieje znane ograniczenie w instalatorze bazy danych DB2 Express związane z dołączaniem łańcuchów języka narodowego (NL) we właściwościach przekazywanych z

instalatora produktu IBM Business Monitor. Następujące wartości przekazywane do instalatora produktu DB2 Express w czasie instalowania nie mogą zawierać w sobie łańcuchów NL:

-  Nazwa użytkownika i hasło instancji: bpininst i bpininst1
-  Nazwa i hasło użytkownika chronionego: bpmfenc i bpmfenc1
-  Nazwa użytkownika i hasło serwera administracyjnego (DAS): bpmadmin i bpmadmin1
-  Nazwa i hasło administratora: bpmadmin i bpmadmin1

Uwagi dotyczące zabezpieczeń bazy danych MONITOR

W przypadku tworzenia bazy danych DB2 za pomocą narzędzia Profile Management Tool lub komendy manageprofiles użytkownik administracyjny tworzący profil próbuje również utworzyć bazę danych. Użytkownik bazy danych środowiska wykonawczego produktu IBM Business Monitor (@DB_USER@) określony podczas tworzenia profilu musi już istnieć w systemie operacyjnym.

Domyślnie użytkownikowi bazy danych środowiska wykonawczego produktu IBM Business Monitor w ramach tworzenia bazy danych nadawane są uprawnienia administratora bazy danych (DBADM). Takie rozwiązanie umożliwi serwerowi produktu IBM Business Monitor automatyczne zarządzanie schematem bazy danych modelu monitorowania w czasie wdrażania i usuwania modelu. Aby zabezpieczyć bazę danych, można utworzyć ją ręcznie i nadać użytkownikowi bazy danych środowiska wykonawczego jedynie uprawnienia wymagane do wykonywania operacji środowiska wykonawczego. Więcej informacji zawierają sekcje “Ręczne instalowanie baz danych” na stronie 59 i Zabezpieczanie środowiska bazy danych monitorowania. Podsumowanie informacji o uprawnieniach dotyczących baz danych zawiera sekcja Uprawnienia do baz danych.

Uwagi dotyczące blokowania produktu DB2

Jeśli występuje duża liczba zdarzeń, baza danych MONITOR może się zakleszczać wskutek pojawienia się dwóch lub większej liczby różnych transakcji oczekujących na tę samą blokadę bazy danych. W takim przypadku jedna z transakcji kończy się niepowodzeniem i jest ponawiana.

Aby wyeliminować zakleszczenia w bazie danych DB2 LUW, zachowując możliwość przetwarzania współbieżnego w warunkach dużego obciążenia, należy wprowadzić następującą komendę w oknie komend DB2:

```
db2set DB2_SKIPINSERTED=ON  
db2set DB2_SKIPDELETED =ON
```

Wielowątkowość nie będzie powodować zakleszczeń, jeśli zmienne rejestru instancji DB2_SKIPINSERTED i DB2_SKIPDELETED mają wartość ON.




Uwagi dotyczące bazy danych COGNOSCS dla produktu DB2

Jeśli baza danych MONITOR działa zdalnie względem serwera lub klastra, na którym wdrożona jest usługa produktu IBM Cognos Business Intelligence, należy zainstalować na serwerze pełną wersję klienta bazy danych (na przykład produkt IBM Data Server Client), aby wdrożyć kostki na serwerze produktu IBM Cognos BI.

Zdalna baza danych musi zostać wpisana do katalogu przed opublikowaniem pakietów kostek produktu IBM Cognos BI podczas wdrażania modelu monitorowania. Nazwa wpisana do katalogu musi być nazwą bazy danych, która została podana dla bazy danych MONITOR. W

przeciwnym razie należy zmienić źródło danych WBMONITOR_DB w produkcie IBM Cognos BI, aby wskazywało poprawną nazwę wpisaną do katalogu.

Produkt IBM Cognos BI wymaga dostępu do komend klienta DB2 podczas publikowania pakietów kostek w czasie wdrażania modelu.

-  Klient DB2 musi znajdować się w ścieżce serwera.
-   Użytkownik uruchamiający serwer IBM Business Monitor musi używać profilu użytkownika produktu DB2.

Usługa IBM Cognos BI tworzy table w bazie danych składnicy treści produktu IBM Cognos BI przy pierwszym uruchomieniu. Ponieważ użytkownik bazy danych, który ma uzyskiwać dostęp do bazy danych składnicy treści, musi mieć uprawnienie do tworzenia tabel w bazie danych, zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

Baza danych COGNOSCS musi być używana tylko na potrzeby danych programu IBM Business Monitor. Nie wolno dodawać danych bezpośrednio do bazy danych COGNOSCS ani używać bazy danych z innymi bazami danych w celu utworzenia raportów na podstawie takich danych (połączonych lub niepołączonych z danymi utworzonymi w programie IBM Business Monitor).

Rozszerzone zabezpieczenia dla produktu IBM Cognos BI

Produkt IBM Cognos BI wymaga nadania dodatkowych praw, aby utworzyć table do użytku wewnętrznego. Po pierwszym pomyślnym uruchomieniu serwera IBM Cognos BI, użytkownikowi bazy danych można odebrać dodatkowe uprawnienia potrzebne do tworzenia tabel w bazie danych składnicy treści produktu IBM Cognos BI.

Należy użyć następującej komendy, aby odebrać dodatkowe uprawnienia (zmienną @DB_USER@ należy zastąpić nazwą użytkownika bazy danych produktu IBM Cognos BI):

```
REVOKE CREATETAB,IMPLICIT_SCHEMA ON DATABASE FROM USER @DB_USER@;
```

Więcej informacji na temat konfiguracji bazy danych dla produktu IBM Cognos BI w produkcie DB2 można znaleźć na stronie Suggested Settings for Creating the Content Store in DB2 on Linux, Windows and UNIX (Proponowane ustawienia dla tworzenia składnicy treści w produkcie DB2 w systemach Linux, Windows i UNIX).

Uwagi dotyczące bazy danych MONITOR dla produktu DB2 for z/OS

Istnieją specjalne zalecenia dotyczące baz danych udostępnianych w produkcie DB2 for z/OS. Dla programu IBM Business Monitor zaleca się stosowanie dedykowanej grupy pamięci masowej (STOGROUP). Grupę pamięci masowej należy utworzyć przed utworzeniem bazy danych MONITOR.

Produkt IBM Cognos BI nie jest obsługiwany w systemie z/OS. Produkt IBM Cognos BI nie jest obsługiwany również wtedy, gdy na potrzeby bazy danych MONITOR używany jest produkt DB2 for z/OS.

Uwagi dotyczące globalizacji

Produkt DB2 for z/OS musi być zainstalowany przy użyciu uniwersalnego zestawu znaków UTF-8. Ten zestaw znaków zapewnia, że metadane modelu monitorowania i dane instancji

zawierające znaki języka rodzimego mogą zostać zapisane w bazie danych. Skrypt `createDatabase.sql` automatycznie tworzy bazę danych UTF-8.

Tabela `DIM_TIME` zawiera kolumnę na potrzeby wypełniania raportów panelu kontrolnego przetłumaczoną nazwą miesiąca. Ustawienia położenia w systemie z/OS nie są wykorzystywane przy tworzeniu nazw miesięcy. W pliku `createTables.sql` znajduje się instrukcja SQL, której można użyć do nadpisania wpisów nazw miesięcy i zdefiniowania własnych nazw miesięcy.

Ogólne uwagi dotyczące bazy danych

W przypadku bazy danych DB2 for z/OS należy dodać dwie pule buforów. Przed uruchomieniem skryptów bazy danych administrator bazy danych musi utworzyć następujące pule buforów 32k:

- BP32K
- TMPBP32

Baza danych DB2 for z/OS wymaga bazy danych TEMP do przechowywania zadeklarowanych tabel tymczasowych.

- Należy utworzyć dedykowaną grupę `STOGROUP`, która będzie zawierać dane programu IBM Business Monitor.
- Należy utworzyć bazę danych TEMP oraz obszar tabel TEMP, które będą zawierały zadeklarowane tabele tymczasowe używane do przetwarzania kursorów przewijalnych. Przykłady zostały przedstawione poniżej.

W przypadku bazy danych DB2 for z/OS 8 należy utworzyć bazę danych TEMP i jej tymczasowy obszar tabel (jeśli nie istnieją). Poniżej przedstawiono przykład definicji bazy danych TEMP:

```
CREATE DATABASE TEMP AS TEMP STOGROUP SYSDEFLT;  
CREATE TABLESPACE TEMP IN TEMP  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

W przypadku produktu DB2 for z/OS w wersji 9 i 10 działającego w środowisku, które nie umożliwia współużytkowania danych, tymczasową bazą danych (TEMP) jest baza danych `DSNDB07`, która jest tworzona podczas instalowania bazy danych. Tymczasowe obszary tabel są dodawane do istniejącej bazy danych TEMP. Poniżej przedstawiono przykład dla tymczasowego obszaru tabel:

```
CREATE TABLESPACE WBITEMP IN DSNDB07  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

W przypadku produktu DB2 for z/OS w wersji 9 i 10 działającego w środowisku, które umożliwia współużytkowanie danych, należy utworzyć bazę danych `WORKFILE`. Na potrzeby podsystemu może zostać utworzona tylko baza danych `WORKFILE`. Poniżej przedstawiono reprezentatywny przykład tworzenia bazy danych `WORKFILE` i tymczasowego obszaru tabel:

```
CREATE DATABASE WORKTEMP AS WORKFILE STOGROUP SYSDEFLT;  
CREATE TABLESPACE WBITEMP IN WORKTEMP  
USING STOGROUP SYSDEFLT  
BUFFERPOOL BP32K  
SEGSIZE 32;
```

Szczegółowe informacje na temat konfiguracji bazy danych TEMP i obszarów tabel TEMP można znaleźć w Centrum informacyjnym produktu DB2 for z/OS. Więcej informacji można uzyskać, klikając odsyłacz do stron pokrewnych.

Uwaga: Jeśli jest używana baza danych DB2 for z/OS i jest planowane uruchamianie skryptów bazy danych za pomocą narzędzia SPUFI, do przesyłania plików na serwer bazy danych z/OS należy używać protokołu FTP. Skrypty bazy danych programu IBM Business Monitor są zakończone znakiem nowego wiersza. Serwer FTP systemu z/OS poprawnie odwzoruje znak nowego wiersza w skrypcie bazy danych.

Baza danych DB2 for z/OS 8 wymaga też bazy danych plików roboczych na potrzeby instrukcji języka SQL korzystających z roboczej pamięci masowej (na przykład instrukcji sortowania). Obsługa operacji sortowania wymaga dodatkowego obszaru tabel (oprócz bazy danych TEMP) dla wersji 8. W produkcie DB2 for z/OS w wersji 9 i 10 połączono bazę danych plików roboczych i bazę danych TEMP. Opis procedur i zalecenia dotyczące doboru wielkości podczas tworzenia baz danych plików roboczych można znaleźć w Centrum informacyjnym produktu DB2 for z/OS.

W celu uzyskania większej współbieżności dla parametru podsystemu RRULOCK należy ustawić wartość YES.

Jeśli ma być włączona usługa przenoszenia danych, należy zwiększyć liczbę blokad na użytkownika (parametr NUMLKUS) do co najmniej 100 000.

Sterownik JDBC

W produkcie IBM Business Monitor używany jest sterownik JDBC 4.0. Domyślnie narzędzie Profile Management Tool wskazuje plik db2jcc4.jar udostępniony w katalogu katalog_główny_serwera_aplikacji\jdbcdrivers\DB2. W przypadku instalacji produktu DB2 for z/OS zalecane jest użycie sterownika JDBC 3.0 db2jcc.jar, który został dostarczony z produktem DB2.

Uwagi dotyczące bazy danych MONITOR dla produktu Oracle

Istnieją specyficzne zalecenia dotyczące baz danych udostępnianych w produkcie Oracle.

Uwagi dotyczące globalizacji

Produkt Oracle musi być instalowany przy użyciu uniwersalnego zestawu znaków UTF-8 (AL32UTF8) zamiast domyślnego zestawu znaków bazy danych (WE8ISO8859P1 - ISO 8859-1 Zachodnioeuropejskie). Ten zestaw znaków zapewnia, że metadane modelu monitorowania i dane instancji zawierające znaki języka rodzimego mogą zostać zapisane w bazie danych. Ponadto produkt IBM Cognos BI wymaga bazy danych UTF-8.

Produkt Oracle zarządza ustawieniami językowymi i narodowymi za pomocą dwóch parametrów bazy danych:

NLS_LANGUAGE

NLS_TERRITORY

Aby zmienić domyślny język baz danych, należy zmienić wartość parametru NLS_LANGUAGE na język obsługiwany przez produkt Oracle. Ustawienia terytorium definiują wartości domyślne formatowania danych, waluty i tak dalej. Aby zmienić instancję produktu Oracle, należy ustawić parametr NLS_TERRITORY.

Tabela DIM_TIME zawiera kolumnę na potrzeby zapełnienia raportów panelu kontrolnego zawierających wymiary czasu przetłumaczoną nazwą miesiąca. Domyślnie do zapełniania pozycji tabeli DIM_TIME używany jest kod ustawień narodowych NLS_LANGUAGE. Aby zmienić domyślny język, należy zmienić parametr NLS_LANGUAGE instancji produktu Oracle lub bieżącej sesji przed uruchomieniem skryptu createTables.sql. W pliku createTables.sql znajduje się również instrukcja SQL, której można użyć do nadpisania

wpisów nazw miesięcy i zdefiniowania własnych nazw miesięcy.

Uwagi dotyczące zabezpieczeń programu MONITOR

W przypadku tworzenia obiektów bazy danych Oracle za pomocą narzędzia Profile Management Tool lub komendy manageprofiles użytkownik administracyjny bazy danych określony podczas tworzenia profilu tworzy obiekty bazy danych i schemat MONITOR. W bazie danych Oracle schemat zawiera zarówno kolekcję obiektów bazy danych, jak i ID użytkownika, który może logować się do bazy danych.

Domyślnie właściciel schematu MONITOR jest również użytkownikiem bazy danych środowiska wykonawczego i w ramach tworzenia bazy danych są mu nadawane uprawnienia do tworzenia innych schematów i obiektów bazy danych. Takie rozwiązanie umożliwia serwerowi produktu IBM Business Monitor automatyczne zarządzanie schematem bazy danych modelu monitorowania w czasie wdrażania i usuwania modelu. Aby zabezpieczyć bazę danych, można ją utworzyć ręcznie. Użytkownikiem bazy danych środowiska wykonawczego produktu IBM Business Monitor może być właściciel schematu MONITOR lub inny użytkownik. W środowisku zabezpieczonym można nadać użytkownikowi bazy danych środowiska wykonawczego jedynie uprawnienia wymagane do wykonywania operacji środowiska wykonawczego. W tym celu należy zapoznać się z tematami Ręczne instalowanie bazy danych i Zabezpieczanie środowiska bazy danych MONITOR znajdującymi się na stronach pokrewnych.

Sterownik JDBC

Za obsługę interfejsu JDBC odpowiadają sterowniki JDBC Oracle dla maszyny JVM 1.6. Plik sterownika JDBC ojdbc6.jar jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku ojdbc6.jar można użyć zarówno dla produktu Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

Domyślnie narzędzie Profile Management Tool wskazuje plik ojdbc6.jar udostępniony w katalogu katalog_główny_serwera_aplikacji\jdbcdrivers\Oracle. Zamiast niego można pobrać inny plik ojdbc6.jar sterownika JDBC bazy danych Oracle i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy manageprofiles.

Odtwarzanie XA

Należy nadać specjalne uprawnienia w celu umożliwienia poprawnej pracy funkcji odtwarzania biblioteki XA bazy danych Oracle. Uruchom następujące komendy jako użytkownik SYS:

```
grant select on pending_trans$ to <użytkownik>;
grant select on dba_2pc_pending to <użytkownik>;
grant select on dba_pending_transactions to <użytkownik>;
grant execute on dbms_system to <użytkownik>;
```

Gdzie <użytkownik> to nazwa użytkownika bazy danych MONITOR konfigurowana podczas tworzenia profilu.

Uwagi dotyczące bazy danych COGNOSCS dla produktu Oracle

Jeśli baza danych MONITOR działa zdalnie względem serwera lub klastra, na którym wdrożona jest usługa produktu IBM Cognos Business Intelligence, należy zainstalować na serwerze pełną wersję klienta bazy danych lub produkt Oracle Instant Client, aby wdrożyć kostki na serwerze produktu IBM Cognos BI.

Instancja bazy danych Oracle dla produktu IBM Cognos BI musi być adresowalna za pomocą pozycji TNSNAMES w kliencie produktu Oracle na serwerze. Wpis w pozycji TNSNAMES musi być taki sam jak nazwa instancji bazy danych, która została podana dla bazy danych MONITOR podczas tworzenia profilu, na przykład ORCL. W przeciwnym razie należy zmienić źródło danych WBMONITOR_DB w produkcie IBM Cognos BI, aby wskazywało poprawny wpis TNSNAMES.




Jeśli używany jest produkt Oracle Instant Client, ścieżka do klienta musi znajdować się w ścieżce systemowej. Dodatkowo do informacji dla serwera bazy danych Oracle musi zostać dołączony plik TNSNAMES.ORA, a zmienna środowiskowa TNS_ADMIN musi być ustawiona tak, aby wskazywała położenie pliku TNSNAMES.ORA.

Ważne: Razem z produktem Oracle Instant Client należy zainstalować program narzędziowy SQLPlus na potrzeby rozwiązywania problemów.

Następujący przykład przedstawia treść poprawnego pliku TNSNAMES.ORA. Napisany wielkimi literami łańcuch ORCL jest aliasem dla połączenia z bazą danych.

```
ORCL =
(DESCRIPTION =
(AADDRESS = (PROTOCOL = TCP)(HOST = 127.0.0.1)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)
```

Produkt IBM Cognos BI wymaga dostępu do komend klienta Oracle podczas publikowania pakietów kostek w czasie wdrażania modelu.

-  Klient Oracle musi znajdować się w ścieżce serwera.
-   Użytkownik uruchamiający serwer IBM Business Monitor musi używać profilu użytkownika produktu Oracle.

Usługa IBM Cognos BI tworzy tabele w bazie danych składnicy treści produktu IBM Cognos BI przy pierwszym uruchomieniu. Użytkownik bazy danych udostępniony na potrzeby uzyskiwania dostępu do bazy danych składnicy treści produktu IBM Cognos BI musi mieć pełny dostęp do bazy danych Oracle, aby tworzyć tabele, widoki, sekwencje, wyzwalacze itd. W produkcie IBM Cognos BI nie można określić oddzielnej nazwy schematu, a obiekty produktu IBM Cognos BI są tworzone w domyślnym schemacie użytkownika bazy danych. Zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

Ważne: Nie należy używać do tego celu użytkownika SYSTEM, ponieważ obiekty bazy danych produktu IBM Cognos BI nie powinny być tworzone w obszarze systemowym.

Baza danych COGNOSCS musi być używana tylko na potrzeby danych programu IBM Business Monitor. Nie wolno dodawać danych bezpośrednio do bazy danych COGNOSCS ani używać bazy danych z innymi bazami danych w celu utworzenia raportów na podstawie takich danych (połączonych lub niepołączonych z danymi utworzonymi w programie IBM Business Monitor).

Rozszerzone zabezpieczenia dla produktu IBM Cognos BI

Produkt IBM Cognos BI wymaga nadania dodatkowych praw, aby utworzyć tabele do użytku wewnętrznego. Po pierwszym pomyślnym uruchomieniu serwera IBM Cognos BI, użytkownikowi bazy danych można odebrać dodatkowe uprawnienia potrzebne do tworzenia tabel w bazie danych składnicy treści produktu IBM Cognos BI.

Należy użyć następujących komend, aby odebrać dodatkowe uprawnienia niezbędne do utworzenia schematu produktu IBM Cognos BI i pozwolić produktowi IBM Cognos BI działać w trybie środowiska wykonawczego z ograniczonymi uprawnieniami:

```
REVOKE CREATE USER FROM @SCHEMA@;  
REVOKE ALTER USER FROM @SCHEMA@;  
REVOKE DROP USER FROM @SCHEMA@;
```

```
REVOKE CREATE ANY TABLE FROM @SCHEMA@;  
REVOKE ALTER ANY TABLE FROM @SCHEMA@;  
REVOKE DROP ANY TABLE FROM @SCHEMA@;
```

```
REVOKE CREATE ANY SEQUENCE FROM @SCHEMA@;  
REVOKE ALTER ANY SEQUENCE FROM @SCHEMA@;  
REVOKE DROP ANY SEQUENCE FROM @SCHEMA@;
```

```
REVOKE CREATE ANY PROCEDURE FROM @SCHEMA@;  
REVOKE ALTER ANY PROCEDURE FROM @SCHEMA@;  
REVOKE DROP ANY PROCEDURE FROM @SCHEMA@;
```

```
REVOKE CREATE ANY VIEW FROM @SCHEMA@;  
REVOKE DROP ANY VIEW FROM @SCHEMA@;
```

```
REVOKE CREATE ANY TRIGGER FROM @SCHEMA@;  
REVOKE ALTER ANY TRIGGER FROM @SCHEMA@;  
REVOKE DROP ANY TRIGGER FROM @SCHEMA@;
```

```
REVOKE CREATE ANY INDEX FROM @SCHEMA@;  
REVOKE DROP ANY INDEX FROM @SCHEMA@;
```

```
REVOKE LOCK ANY TABLE FROM @SCHEMA@;
```

Więcej informacji na temat konfiguracji bazy danych dla produktu IBM Cognos BI w produkcie Oracle można znaleźć na stronie Suggested Settings for Creating the Content Store in Oracle (Proponowane ustawienia dla tworzenia składnicy treści w produkcie Oracle).

Uwagi dotyczące bazy danych MONITOR dla produktu Microsoft SQL Server

Istnieją specyficzne zalecenia dotyczące baz danych udostępnianych w produkcie Microsoft SQL Server.

Ważne: Podczas instalowania produktu SQL Server jako tryb uwierzytelniania należy wybrać tryb mieszany (uwierzytelnianie systemu Windows i uwierzytelnianie serwera SQL Server).

Ważne: Aby używać bazy danych SQL Server z produktem IBM Business Monitor, konieczne jest skonfigurowanie produktu SQL Server pod kątem obsługi transakcji XA. Produkt SQL Server nie jest wstępnie skonfigurowany pod kątem transakcji XA. Obsługa transakcji XA jest zapewniana w ramach dystrybucji sterownika Microsoft JDBC i zawiera bibliotekę dołączaną dynamicznie (sqljdbc_xa.dll) oraz skrypt instalacyjny (xa_install.sql). Transakcje XA nie są włączone domyślnie, więc należy zmienić konfigurację usługi MSDTC (Microsoft Windows Distributed Transaction Coordinator). Instrukcje dotyczące włączania obsługi transakcji XA w produkcie SQL Server można znaleźć w temacie Understanding XA Transactions (Informacje o transakcjach XA) w dokumentacji elektronicznej produktu Microsoft SQL Server.

W przypadku tworzenia bazy danych SQL Server za pomocą narzędzia Profile Management Tool lub komendy manageprofiles bazę danych tworzy użytkownik administracyjny bazy danych określony podczas tworzenia profilu. Użytkownik bazy danych środowiska wykonawczego produktu IBM Business Monitor (@DB_USER@) określany podczas

tworzenia profilu powinien już istnieć jako użytkownik w danych logowania i użytkownik bazy danych produktu SQL Server. W celu utworzenia danych logowania bazy danych i użytkownika bazy danych można użyć następującej komendy:

```
CREATE LOGIN @uzytkownik_bazy_danych@  
WITH PASSWORD = '@haslo_bazy_danych@',  
DEFAULT_DATABASE=@nazwa_bazy_danych@  
CREATE USER @uzytkownik_bazy_danych@ FOR LOGIN  
@uzytkownik_bazy_danych@
```

gdzie `uzytkownik_bazy_danych` to użytkownik bazy danych środowiska wykonawczego produktu IBM Business Monitor, `haslo_bazy_danych` to hasło bazy danych środowiska wykonawczego, a `nazwa_bazy_danych` to nazwa bazy danych produktu IBM Business Monitor.

Domyślnie użytkownikowi bazy danych środowiska wykonawczego produktu IBM Business Monitor w ramach tworzenia bazy danych nadawane są uprawnienia właściciela bazy danych (`db_owner`). Takie rozwiązanie umożliwia serwerowi produktu IBM Business Monitor automatyczne zarządzanie schematem bazy danych modelu monitorowania w czasie wdrażania i usuwania modelu. Aby zabezpieczyć bazę danych, można utworzyć ją ręcznie i nadać użytkownikowi bazy danych środowiska wykonawczego jedynie uprawnienia wymagane do wykonywania operacji środowiska wykonawczego. W tym celu należy zapoznać się z tematami Ręczne instalowanie bazy danych i Zabezpieczanie środowiska bazy danych MONITOR znajdującymi się na stronach pokrewnych.

Obsługę interfejsu JDBC zapewniają sterowniki SQL Server JDBC dla maszyny JVM 1.6. W produkcie IBM Business Monitor używany jest plik `sqljdbc4.jar` sterownika Microsoft JDBC 2.0. Domyślnie narzędzie Profile Management Tool wskazuje plik `sqljdbc4.jar` udostępniony w katalogu `katalog_glowny_serwera_aplikacji\jdbcdrivers\SQLServer`. Zamiast niego można pobrać inny plik `sqljdbc4.jar` sterownika JDBC Microsoft i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy `manageprofiles`. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.

Uwagi dotyczące globalizacji

Produkt SQL Server zarządza ustawieniami narodowymi za pomocą opcji `COLLATE` podczas tworzenia bazy danych. Instrukcja utworzenia bazy danych dla baz MONITOR i COGNOSCS zawiera następującą opcję:

```
COLLATE SQL_Latin1_General_CP1_CS_AS
```

Aby zmienić ustawienia narodowe, należy zmienić parametr porządkowania na obsługiwane porządkowanie dla wybranego języka. Na przykład aby zmienić porządkowanie na francuskie, należy użyć instrukcji:

```
COLLATE French_100_CS_AS
```

Produkt SQL Server zarządza językiem domyślnym na podstawie zalogowanego użytkownika. Aby zmienić domyślny język, w pliku `createDatabase.sql` należy dodać opcję `DEFAULT_LANGUAGE` do operacji tworzenia danych logowania z innym domyślnym językiem. Na przykład aby utworzyć dane logowania z językiem francuskim jako językiem domyślnym, należy użyć instrukcji:

```
IF NOT EXISTS (SELECT * FROM syslogins WHERE  
NAME = '@uzytkownik_bazy_danych@') CREATE LOGIN @uzytkownik_bazy_danych@ WITH PASSWORD =  
'@haslo_bazy_danych@', DEFAULT_DATABASE=@nazwa_bazy_danych@, DEFAULT_LANGUAGE=French;
```

Tabela `DIM_TIME` zawiera kolumnę na potrzeby zapełnienia raportów panelu kontrolnego zawierających wymiary czasu przetłumaczoną nazwą miesiąca. Domyślnie do zapełniania

pozycji tabeli DIM_TIME używany jest kod ustawień narodowych DEFAULT_LANGUAGE. Aby zmienić domyślny język, należy zmienić parametr DEFAULT_LANGUAGE dla użytkownika bazy danych przed uruchomieniem skryptu createTables.sql. W pliku createTables.sql znajduje się również instrukcja SQL, której można użyć do nadpisania wpisów nazw miesięcy i zdefiniowania własnych nazw miesięcy.

Uwagi dotyczące bazy danych COGNOSCS dla produktu Microsoft SQL Server

Jeśli baza danych MONITOR działa zdalnie względem serwera lub klastra, na którym wdrożona jest usługa produktu IBM Cognos Business Intelligence, należy zainstalować na serwerze pełną wersję klienta bazy danych Microsoft SQL Server, aby wdrożyć kostki na serwerze produktu IBM Cognos BI.

Ważne: Baza danych IBM Cognos BI wymaga porządkowania bez rozróżniania wielkości liter, natomiast baza danych IBM Business Monitor wymaga porządkowania rozróżniającego wielkość liter. Jeśli domyślne porządkowanie zostanie zmienione dla bazy danych IBM Cognos BI, porządkowanie nie może rozróżniać wielkości liter.

Firma Microsoft oferuje produkt SQL Server Native Client, który może zostać użyty zamiast pełnej instalacji klienta SQL Server. Ta minimalna instalacja zawiera wszystkie wymagane rodzime sterowniki. Wraz z rodzimym klientem należy pobrać i zainstalować narzędzia wiersza komend produktu SQL Server. Obie pozycje są dostępne na stronie Microsoft SQL Server 2008 Feature Pack, August 2008 (Pakiet składników produktu Microsoft SQL Server 2008, sierpień 2008).

Produkt IBM Cognos BI wymaga dostępu do komend klienta SQL Server podczas publikowania pakietów kostek w czasie wdrażania modelu. Klient SQL Server musi znajdować się w ścieżce serwera.

Usługa IBM Cognos BI tworzy table w bazie danych składnicy treści produktu IBM Cognos BI przy pierwszym uruchomieniu. Ponieważ użytkownik bazy danych, który ma uzyskiwać dostęp do bazy danych składnicy treści, musi mieć uprawnienie do tworzenia tabel w bazie danych, zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

Baza danych COGNOSCS musi być używana tylko na potrzeby danych programu IBM Business Monitor. Nie wolno dodawać danych bezpośrednio do bazy danych COGNOSCS ani używać bazy danych z innymi bazami danych w celu utworzenia raportów na podstawie takich danych (połączonych lub niepołączonych z danymi utworzonymi w programie IBM Business Monitor).

Rozszerzone zabezpieczenia dla produktu IBM Cognos BI

Produkt IBM Cognos BI wymaga nadania dodatkowych praw, aby utworzyć table do użytku wewnętrznego. Po pierwszym pomyślnym uruchomieniu serwera IBM Cognos BI, użytkownikowi bazy danych można odebrać dodatkowe uprawnienia potrzebne do tworzenia tabel w bazie danych składnicy treści produktu IBM Cognos BI.

Należy użyć następujących komend, aby odebrać dodatkowe uprawnienia niezbędne do utworzenia schematu produktu IBM Cognos BI i pozwolić produktowi IBM Cognos BI działać w trybie środowiska wykonawczego z ograniczonymi uprawnieniami:

```
EXEC sp_droprolemember 'db_datawriter', @COG_DB_USER@
GO
EXEC sp_droprolemember 'db_ddladmin', @COG_DB_USER@
GO
```

Więcej informacji na temat konfiguracji bazy danych dla produktu IBM Cognos BI w produkcie SQL Server można znaleźć na stronie Suggested Settings for Creating the Content Store in Microsoft SQL Server (Proponowane ustawienia dla tworzenia składnicy treści w produkcie Microsoft SQL Server).

Uprawnienia do bazy danych

W tym temacie opisano uprawnienia do baz danych niezbędne do tworzenia tabel składnicy danych lub uzyskiwania do nich dostępu w przypadku każdego systemu zarządzania bazami danych obsługiwanego przez produkt IBM Business Monitor.

Podczas tworzenia schematów przy użyciu instalatora, narzędzia Profile Management Tool lub skryptów użytkownik musi posługiwać się identyfikatorem, który ma uprawnienia umożliwiające tworzenie tabel. Po utworzeniu tabel aplikacje muszą mieć uprawnienia wystarczające do wybierania, wstawiania, aktualizowania i usuwania informacji zawartych w tabelach.

Tabela 1 opisuje uprawnienia do bazy danych, które są niezbędne do uzyskiwania dostępu do składnicy danych.

Tabela 1. Uprawnienia do bazy danych

| System zarządzania bazami danych | Minimalne uprawnienia niezbędne do używania tabel składnicy danych | Dodatkowe uprawnienie wymagane do utworzenia tabel składnicy danych |
|----------------------------------|---|---|
| DB2 | Identyfikator użytkownika musi mieć uprawnienia SELECT, INSERT, UPDATE i DELETE dla tabel. | Identyfikator użytkownika musi mieć uprawnienie CREATETAB dla bazy danych, uprawnienie USE dla obszaru tabel oraz uprawnienie CREATEIN dla schematu. |
| Oracle | Identyfikator użytkownika musi mieć uprawnienie SESSION, aby było możliwe nawiązanie połączenia z bazą danych. Jeśli ten sam identyfikator użytkownika jest właścicielem zarówno schematu składnicy danych, jak i komponentu, który łączy się z bazą danych, to ten identyfikator ma wystarczające uprawnienia do wykonywania operacji na tabelach. W przeciwnym razie identyfikator użytkownika musi mieć uprawnienia SELECT, INSERT, UPDATE i DELETE względem obiektów w tabelach, z których składa się składnica danych, oraz uprawnienie systemowe DROP ANY TABLE umożliwiające użycie instrukcji TRUNCATE TABLE. Baza danych Oracle musi zostać utworzona przy użyciu zestawu znaków UTF-8, który obsługuje inne zestawy znaków klienta obsługiwane przez produkt IBM Business Monitor. | Identyfikator użytkownika musi mieć uprawnienia wystarczające do tworzenia tabel i indeksów relacyjnych w schemacie składnicy danych. Baza danych wymaga również limitu obszaru w domyślnym obszarze tabel właściciela tego schematu. Tabela 2 na stronie 25 opisuje dodatkowe uprawnienia dla bazy danych Oracle na potrzeby komponentów produktów IBM Business Monitor i WebSphere Enterprise Service Bus. |

Tabela 1. Uprawnienia do bazy danych (kontynuacja)

| System zarządzania bazami danych | Minimalne uprawnienia niezbędne do używania tabel składnicy danych | Dodatkowe uprawnienie wymagane do utworzenia tabel składnicy danych |
|----------------------------------|---|---|
| SQL Server | Bazę danych SQL Server należy skonfigurować na potrzeby uwierzytelniania bazy danych SQL Server i systemu Windows. Dzięki temu możliwe będzie uwierzytelnianie oparte na identyfikatorze logowania i hasle bazy danych SQL Server. Użytkownik o podanym identyfikatorze może być właścicielem tabel lub członkiem grupy, która ma uprawnienia wystarczające do wykonywania instrukcji TRUNCATE TABLE. | Identyfikator użytkownika musi mieć uprawnienie do wykonywania instrukcji CREATE TABLE. |

Tabela 2 opisuje dodatkowe uprawnienia dla bazy danych Oracle na potrzeby komponentów produktu IBM Business Monitor.

Uwaga: Jeśli wszystkie poniższe komponenty są konfigurowane dla pojedynczej bazy danych Oracle, można utworzyć nadzbiór wszystkich uprawnień określonych dla poszczególnych komponentów. Jeśli te cztery komponenty są konfigurowane dla wielu baz danych, można ustawić różne uprawnienia dla każdej z tych baz danych.

Tabela 2. Dodatkowe uprawnienia bazy danych Oracle

| Komponent | Uprawnienia konfigurowania | Uprawnienia czasu wykonywania |
|------------------------------------|--|---|
| Wspólna baza danych | CREATE TABLE, CREATE INDEXTYPE, ALTER TABLE, INSERT, CREATE SEQUENCE, CREATE USER, ALTER USER, CREATE TABLESPACE | SELECT, UPDATE, DELETE, INSERT, CREATE VIEW, CREATE PROCEDURE |
| Mechanizmy przesyłania komunikatów | CREATE TABLE, CREATE INDEXTYPE | SELECT, UPDATE, DELETE, INSERT, DROP ANY TABLE |

Zagadnienia dotyczące rejestru użytkowników

W rejestrze użytkowników są przechowywane informacje, które służą do uwierzytelniania użytkowników przy użyciu uwierzytelniania podstawowego. Wybór rejestru użytkowników stanowi ważne zagadnienie podczas planowania środowiska użytkownika. Konieczne jest skonfigurowanie produktu WebSphere Application Server pod kątem korzystania z rejestru użytkowników w danym środowisku.

W rejestrze użytkowników są przechowywane informacje, które służą do uwierzytelniania użytkowników żądających dostępu do produktu IBM Business Monitor. W obrębie repozytoriów stowarzyszonych można skonfigurować wiele typów rejestrów użytkowników. W przypadku większości wdrożeń w środowiskach produkcyjnych używany jest serwer LDAP (Lightweight Directory Access Protocol). W przypadku niewielkich wdrożeń zawartych na pojedynczym serwerze można użyć rejestru użytkowników opartego na plikach.

Dla repozytorium kont użytkowników można wybrać dowolny z następujących typów:

- Repozytoria stowarzyszone
- Lokalny system operacyjny
- Autonomiczny rejestr LDAP (Standalone Lightweight Directory Access Protocol)
- Autonomiczny rejestr niestandardowy




Uwaga: W przypadku zabezpieczeń szczegółowych obsługiwanyimi rejestrami użytkowników są repozytoria stowarzyszone (plikowe), repozytoria stowarzyszone (LDAP) i autonomiczny rejestr LDAP.

Uwagi dotyczące użytkownika bez uprawnień administratora

Jeśli produkt IBM Business Monitor instalowany jest przez użytkownika niebędącego administratorem i podczas instalacji ma zostać utworzony profil testowy, przed rozpoczęciem instalacji musi zostać zainstalowany serwer DB2. Należy zapamiętać szczegóły dotyczące bazy danych, aby podać je podczas instalacji produktu.

Uwagi opisane w tym temacie dotyczą wszystkich scenariuszy instalacji, w których wybrano instalowanie przy użyciu opcji instalacji **Typowa**. Profile tworzone są automatycznie, jeśli wybrano instalowanie z opcją **Typowa**.

Dostępne są następujące opcje, aby zainstalować produkt jako użytkownik bez uprawnień administratora:

- Przed zainstalowaniem produktu należy oddzielnie zainstalować serwer DB2. Informacje na temat instalowania produktu DB2 przez użytkownika niebędącego administratorem zawiera sekcja
 -   Przegląd instalacji użytkownika innego niż root (Linux i UNIX)
 -  Konta użytkowników wymagane do instalacji serwerów DB2 (Windows)
- Zalogowanie się jako administrator i użycie instalatora produktu tylko do zainstalowania serwera DB2. Nadanie specjalnych uprawnień użytkownikowi niebędącemu administratorem. Następnie zalogowanie się jako użytkownik niebędący administratorem i zainstalowanie produktu przy użyciu zainstalowanego serwera DB2.

Zamiast tworzyć profil testowy można utworzyć profil po instalacji. Wykonaj następujące kroki:

1. Zainstaluj produkt bez tworzenia profilu. Jeśli instalacja przeprowadzana jest przez użytkownika bez uprawnień administratora, na stronie Instalacja pakietów należy usunąć zaznaczenia pola wyboru dla opcji DB2 Express. Jeśli w systemie Windows wyświetlana jest opcja zainstalowania produktu IBM Cognos Business Intelligence, należy usunąć zaznaczenia także tego pola wyboru.
2. Na stronie Składniki rozwiń serwery i upewnij się, że żaden z profili testowych nie został wybrany.
3. Użyj narzędzia Profile Management Tool, aby utworzyć profil autonomiczny lub menedżer wdrażania i profile niestandardowe. Jeśli baza danych nie jest zainstalowana, użyj dla wszystkich ścieżki **Zaawansowana**. Nie używaj ścieżki **Typowa**. Wybierz opcje opóźnienia wykonania skryptów bazy danych podczas tworzenia profilu.
4. Jeśli bazy danych nie zostały utworzone wcześniej, administrator bazy danych musi utworzyć bazy danych i tabele po utworzeniu lub rozszerzeniu profilu.
5. W przypadku środowiska wdrożenia sieciowego:
 - a. Stowarzysz profile niestandardowe z menedżerem wdrażania.
 - b. Korzystając z Konsoli administracyjnej, utwórz wymagane środowisko wdrażania.

Uwaga: Jeśli wybrano bazę danych DB2 Express dołączoną do produktu (i opcjonalnie z nim zainstalowaną), muszą zostać spełnione następujące warunki:

- Zdeinstalowanie wszystkich innych wersji produktu DB2 z systemu.
- Zainstalowanie produktu IBM Business Process Manager jako użytkownik bez uprawnień administratora.

Przykładowe ścieżki instalacji

W produkcie IBM Business Monitor można dokonać wyboru spośród kilku różnych ścieżek instalacji w celu utworzenia środowiska wdrażania.

Środowisko międzykomórkowe to takie, w którym produkt IBM Business Monitor odbiera zdarzenia z serwera znajdującego się w innej komórce niż serwer produktu IBM Business Monitor. Środowisko międzykomórkowe może mieć topologię wdrożenia sieciowego lub pojedynczego serwera. W obu przypadkach należy wykonać kilka kroków w celu włączenia komunikacji między serwerem CEI a serwerem IBM Business Monitor. Więcej informacji na temat włączania komunikacji między wieloma komórkami zawiera sekcja Konfigurowanie sposobu odbierania zdarzeń. Przykład topologii międzykomórkowej zawiera scenariusz Monitorowanie zdarzeń z systemu informacyjnego przedsiębiorstwa SAP bez mediacji.

Ścieżka instalacyjna dla topologii pojedynczego serwera

W przypadku korzystania z topologii pojedynczego serwera produkt IBM Business Monitor i wszystkie wymagane komponenty są instalowane na tym samym serwerze fizycznym.

Aby zainstalować serwer produktu IBM Business Monitor i wszystkie wymagane komponenty na tym samym serwerze, wykonaj następujące kroki ogólne:

1. Wykonaj kroki przedinstalacyjne opisane w sekcji Rozdział 3, “Przygotowywanie instalacji produktu”, na stronie 33.
2. Zainstaluj produkt IBM Business Monitor, postępując zgodnie z krokami opisanymi w sekcji “Instalowanie oprogramowania IBM Business Monitor” na stronie 39. Podczas instalowania produktu dostępne są opcje tworzenia profilu wdrożenia, które udostępniają środowisko testowe produktu, ale opcji tych nie można użyć w środowisku produkcyjnym.
3. Jeśli profil wdrożenia nie został utworzony, utwórz profil autonomiczny przy użyciu narzędzia do tworzenia profili lub komendy manageprofiles, wykonując kroki opisane w sekcji Rozdział 6, “Tworzenie i rozszerzanie profili”, na stronie 63.

Zostaną zainstalowane i skonfigurowane wszystkie wymagane komponenty produktu IBM Business Monitor.

Opcjonalnie można sprawdzić status komponentów i wykonać aktualizacje przy użyciu kreatora konfiguracji w Konsoli administracyjnej.

Ścieżka instalacji dla topologii wdrożenia sieciowego korzystającej ze wzorców środowiska wdrażania

Wdrożenie sieciowe w produkcie IBM Business Monitor wykorzystuje funkcje wdrożenia sieciowego zaimplementowane w produkcie WebSphere Application Server Network Deployment. Jeśli wybrano jeden z dostępnych wzorców środowiska wdrażania, kreator środowiska wdrażania pomoże w skonfigurowaniu wymaganych klastrów, serwerów i komponentów.

Pojęcia są takie same jak w przypadku wdrożenia sieciowego w produkcie WebSphere Application Server Network Deployment. W przypadku produktu IBM Business Monitor

dostępne są dwa wzorce: wzorzec pojedynczego klastra i wzorzec zdalnego przesyłania komunikatów, zdalnej obsługi i sieci WWW (czteroklastrowy).

Aby zainstalować serwer produktu IBM Business Monitor i wszystkie wymagane komponenty, korzystając ze środowiska wdrażania jedno- lub czteroklastrowego, wykonaj następujące kroki ogólne:

1. Wykonaj kroki przedinstalacyjne opisane w sekcji Rozdział 3, “Przygotowywanie instalacji produktu”, na stronie 33.
2. Zainstaluj produkt IBM Business Monitor, postępując zgodnie z krokami opisanymi w sekcji “Instalowanie oprogramowania IBM Business Monitor” na stronie 39. Nie twórz profilu wdrożenia.
3. Utwórz profil menedżera wdrażania przy użyciu narzędzia Profile Management Tool lub komendy manageprofiles, postępując zgodnie z krokami opisanymi w sekcji Rozdział 6, “Tworzenie i rozszerzanie profili”, na stronie 63.
4. Jeśli podczas tworzenia profilu nie utworzono bazy danych MONITOR, uruchom skrypty w celu utworzenia bazy danych, postępując zgodnie z instrukcjami zawartymi w sekcji Rozdział 5, “Tworzenie baz danych”, na stronie 53.
5. Uruchom menedżer wdrażania.
6. Utwórz węzły niestandardowe stowarzyszone w komórce menedżera wdrażania, postępując zgodnie z krokami opisanymi w sekcji Rozdział 6, “Tworzenie i rozszerzanie profili”, na stronie 63.
7. Utwórz środowisko wdrażania, wybierając wzorzec pojedynczego klastra lub wzorzec zdalnego przesyłania komunikatów, zdalnej obsługi i sieci WWW (czteroklastrowy). Wykonaj kroki opisane w sekcji “Tworzenie środowiska wdrażania za pomocą wzorca” na stronie 93.
8. Skonfiguruj dodatkowe komponenty, takie jak produkty Business Space i IBM Cognos BI, postępując zgodnie z instrukcjami zawartymi w sekcji Rozdział 10, “Konfigurowanie komponentów programu IBM Business Monitor”, na stronie 131.

Zostaną utworzone klastry oraz zostaną zainstalowane i skonfigurowane wszystkie wymagane komponenty produktu IBM Business Monitor.

Opcjonalnie można sprawdzić status komponentów i wykonać aktualizacje przy użyciu kreatora konfiguracji w Konsoli administracyjnej.

Ścieżka instalacji na potrzeby topologii niestandardowego wdrożenia sieciowego

Zamiast używać kreatora środowiska wdrożenia do tworzenia topologii jednoklastrowej lub czteroklastrowej na potrzeby wdrożenia sieciowego (ND), można utworzyć dowolnie wybraną topologię przy użyciu kreatora konfiguracji lub zadania wsadmin.

Aby zainstalować serwer produktu IBM Business Monitor i wszystkie wybrane komponenty w topologii niestandardowego wdrożenia sieciowego, wykonaj następujące kroki ogólne:

1. Wykonaj kroki przedinstalacyjne opisane w sekcji Rozdział 3, “Przygotowywanie instalacji produktu”, na stronie 33.
2. Zainstaluj produkt IBM Business Monitor, postępując zgodnie z krokami opisanymi w sekcji “Instalowanie oprogramowania IBM Business Monitor” na stronie 39. Nie twórz profilu wdrożenia.
3. Utwórz profil menedżera wdrażania przy użyciu narzędzia Profile Management Tool lub komendy manageprofiles, postępując zgodnie z krokami opisanymi w sekcji Rozdział 6, “Tworzenie i rozszerzanie profili”, na stronie 63.

4. Jeśli podczas tworzenia profilu nie utworzono bazy danych MONITOR, uruchom skrypty w celu utworzenia bazy danych, postępując zgodnie z instrukcjami zawartymi w sekcji Rozdział 5, “Tworzenie baz danych”, na stronie 53.
5. Uruchom menedżer wdrażania.
6. Utwórz węzły niestandardowe stowarzyszone w komórce menedżera wdrażania, postępując zgodnie z krokami opisanymi w sekcji Rozdział 6, “Tworzenie i rozszerzanie profili”, na stronie 63.
7. Za pomocą Konsoli administracyjnej utwórz klastry, postępując zgodnie z instrukcjami zawartymi w sekcji “Tworzenie klastrów programu IBM Business Monitor” na stronie 106.
8. Skonfiguruj wymagane usługi zdarzeń infrastruktury CEI (Common Event Infrastructure), postępując zgodnie z instrukcjami zawartymi w sekcji “Konfigurowanie usług zdarzeń infrastruktury CEI” na stronie 108.
9. Skonfiguruj środowisko za pomocą kreatora konfiguracji lub komendy wsadmin, postępując zgodnie z instrukcjami zawartymi w sekcjach “Konfigurowanie środowiska przy użyciu kreatora konfiguracji” na stronie 109 lub “Konfigurowanie środowiska przy użyciu komend narzędzia wsadmin” na stronie 116. Jednak w przypadku wymaganych komponentów współużytkowanych należy wykonać ręcznie kroki opisane w sekcji “Ręczne konfigurowanie środowiska” na stronie 118.
10. Skonfiguruj dodatkowe komponenty, takie jak produkty Business Space i IBM Cognos BI, postępując zgodnie z instrukcjami zawartymi w sekcji Rozdział 10, “Konfigurowanie komponentów programu IBM Business Monitor”, na stronie 131.

Ścieżki instalacji środowiska wdrażania zarządzanego dla programu WebSphere Business Modeler

W przypadku używania programu WebSphere Business Modeler do tworzenia i wdrażania modeli monitorowania w celach testowych należy skonfigurować środowisko wdrażania zarządzanego. Środowisko wdrażania zarządzanego można utworzyć w tym samym systemie, w którym zainstalowano program WebSphere Business Modeler, lub na innym serwerze, który jest współużytkowany przez wielu użytkowników programu WebSphere Business Modeler.

Przed utworzeniem środowiska wdrażania zarządzanego należy sprawdzić, czy w systemie, w którym tworzone jest środowisko wdrażania zarządzanego, dostępne jest co najmniej 3 GB pamięci.

Pojedynczy użytkownik programu WebSphere Business Modeler używający jednego środowiska wdrażania zarządzanego

Jeśli środowisko wdrażania zarządzanego jest tworzone w tym samym systemie, w którym zainstalowano program WebSphere Business Modeler, w konfiguracji środowiska pomocna będzie następująca ogólna ścieżka.

Przed rozpoczęciem tej ścieżki instalacji na jednej stacji roboczej powinny być już zainstalowane następujące produkty:

- WebSphere Business Modeler 7.0
- Integration Designer 7.5

Podczas instalowania produktu Integration Designer należy wybrać opcję instalacji środowiska testowego produktu Process Server.

Aby zainstalować produkt WebSphere Business Modeler dla jednego użytkownika używającego jednego środowiska wdrażania zarządzanego:

1. Zainstaluj pakiet Business Monitor Development Toolkit w istniejącym środowisku produktu Integration Designer.
2. Utwórz plik XML konfiguracji zawierający informacje o połączeniu na potrzeby serwera programu IBM Business Monitor oraz produktu Business Space. Jeśli istnieje już plik XML konfiguracji pochodzący z instalacji produktu Integration Designer, można dodać informacje o produkcie IBM Business Monitor jako dodatkowy komponent serwera. Więcej informacji zawiera temat Konfigurowanie pliku konfiguracyjnego serwera wymieniony w sekcji zadań pokrewnych.
3. Skonfiguruj program WebSphere Business Modeler pod kątem używania nowo zainstalowanego środowiska wdrażania zarządzanego.

Wielu użytkowników programu WebSphere Business Modeler używających jednego środowiska wdrażania zarządzanego

Jeśli środowisko wdrażania zarządzanego jest tworzone w systemie innym niż ten, w którym zainstalowano program WebSphere Business Modeler, lub dla wielu użytkowników programu WebSphere Business Modeler, w konfiguracji środowiska pomocna będzie następująca ogólna ścieżka.

Przed rozpoczęciem tej ścieżki instalacji na jednej stacji roboczej powinny być już zainstalowane następujące produkty:

- WebSphere Business Modeler 7.0
- Process Server 7.5 z profilem autonomicznym

Aby zainstalować produkt WebSphere Business Modeler dla wielu użytkowników używających jednego środowiska wdrażania zarządzanego:

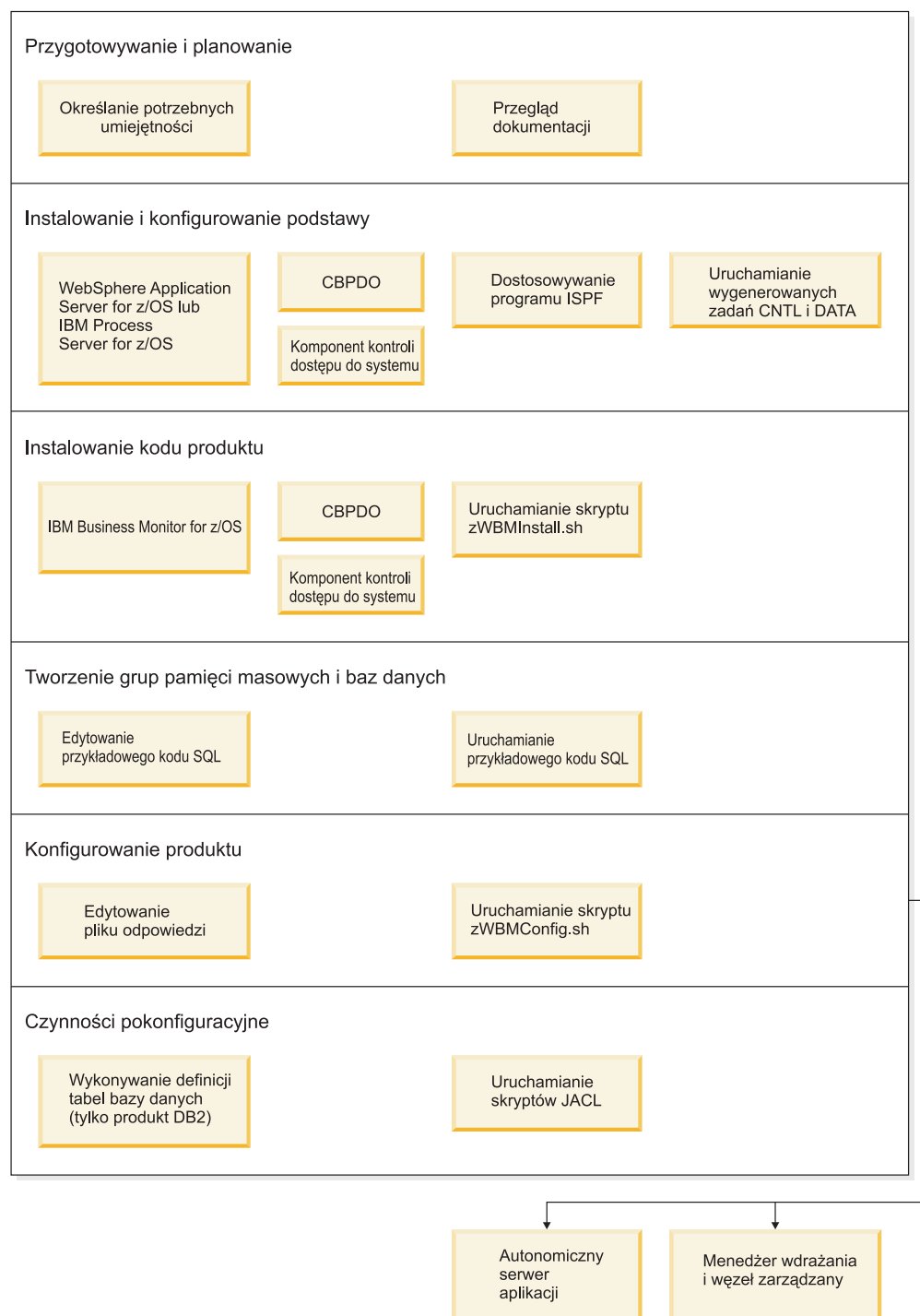
1. Korzystając ze startera produktu IBM Business Monitor, zainstaluj produkt IBM Business Monitor w istniejącym środowisku produktu Process Server. Nie twórz profilu. Istniejący autonomiczny profil produktu Process Server zostanie rozszerzony.
2. Za pomocą narzędzia Profile Management Tool rozszerz istniejący profil produktu Process Server przy użyciu szablonu programu IBM Business Monitor. Jeśli podczas tworzenia profilu początkowego produkt Business Space nie został skonfigurowany, skonfiguruj produkt Business Space podczas rozszerzania profilu.
3. Przy użyciu Konsoli administracyjnej zmodyfikuj serwer tak, aby był uruchamiany w trybie programistycznym. Przejdź na stronę **Serwery > Typy serwerów > Serwery aplikacji WebSphere** i kliknij opcję *nazwa_serwera*. Na karcie Konfiguracja zaznacz pole wyboru **Uruchom w trybie programistycznym**, kliknij przycisk **Zastosuj** i zapisz zmiany w konfiguracji.
4. Utwórz plik XML konfiguracji zawierający informacje o połączeniu na potrzeby serwera programu IBM Business Monitor oraz produktu Business Space. Jeśli istnieje już plik XML konfiguracji pochodzący z instalacji produktu Process Server, można dodać informacje o produkcie IBM Business Monitor jako dodatkowy komponent serwera.
5. Skonfiguruj program WebSphere Business Modeler pod kątem używania nowo zainstalowanego środowiska wdrażania zarządzanego.

Więcej informacji zawiera Centrum informacyjne produktu WebSphere Business Modeler dostępne po kliknięciu pokrewnego odsyłacza.

Przegląd zadania: instalacja i konfiguracja

Przed instalacją i konfiguracją produktu IBM Business Monitor for z/OS warto poznać przepływ czynności w przypadku obsługiwanych konfiguracji.

Na poniższym diagramie zilustrowano ogólny przepływ czynności niezbędnych do wykonania przed i po instalacji produktu IBM Business Monitor for z/OS, a także w celu skonfigurowania tego produktu.



Aby utworzyć kompletne, dostosowane środowisko obsługi aplikacji produktu IBM Business Monitor for z/OS, wykonaj następujące kroki:

1. Zainstaluj i skonfiguruj podstawowy serwer aplikacji (WebSphere Application Server lub Process Server).
2. Zainstaluj pliki binarne produktu.

3. Utwórz bazy danych.
4. Skonfiguruj produkt.
5. Uruchom serwer.

W zależności od konfiguracyjnych zmiennych środowiskowych oraz sposobu skonfigurowania pliku odpowiedzi zakończenie konfiguracji produktu może wymagać wykonania dodatkowych czynności konfiguracyjnych.

Rozdział 3. Przygotowywanie instalacji produktu

Przed zainstalowaniem produktu IBM Business Monitor należy sprawdzić, czy spełnione są wymagania wstępne w zakresie sprzętu i oprogramowania. Niektóre platformy operacyjne wymagają również specjalnych przygotowań przed instalacją produktu.

Wymagania dotyczące sprzętu i oprogramowania

Program IBM Business Monitor działa w systemach operacyjnych AIX, HP-UX, Windows, Linux, Linux na platformie zSeries oraz w systemach operacyjnych Solaris i z/OS.

Najbardziej aktualne wymagania programowe i sprzętowe można znaleźć w sekcji Wymagania systemowe dla produktu IBM Business Monitor.

Poniższe odsyłacze wskazują obsługiwane serwery LDAP. Program IBM Business Monitor obsługuje także autonomiczne rejestry LDAP. Wszystkie poniższe definicje bieżących dziedzin są dostępne dla repozytoriów bieżącego konta użytkownika:

- Repozytoria stowarzyszone
- Lokalny system operacyjny
- Autonomiczny rejestr LDAP
- Autonomiczny rejestr niestandardowy

Przygotowywanie systemów operacyjnych do instalacji produktu

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny. Konfiguracja zależy od typu używanego systemu operacyjnego.

Przed przygotowaniem środowiska instalacji wykonaj następujące czynności:

- Jeśli w systemie, w którym ma zostać zainstalowany produkt IBM Business Monitor, uruchomiony jest firewall, wyłącz go.
- Upewnij się, że informacje logowania użytkownika umożliwiają dostęp do komend bazy danych DB2 lub Oracle.
- Wykonaj dodatkowe czynności specyficzne dla danego systemu operacyjnego.

Przygotowywanie systemów AIX do instalacji

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny AIX.

Ponieważ produkt WebSphere Application Server jest wstępnie wymagany do oprogramowania programu IBM Business Monitor, należy wykonać wymagane kroki przygotowawcze opisane w temacie Przygotowywanie systemu operacyjnego do instalacji produktu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server.

Niektóre kroki są specyficzne dla wersji systemu operacyjnego, dlatego nie wszystkie kroki mogą mieć zastosowanie w środowisku użytkownika. Jeśli dla konkretnego kroku nie został podany kwalifikator, należy wykonać ten krok dla wszystkich wersji systemu operacyjnego.

W następującej nocie technicznej zamieszczono dodatkowe informacje przygotowawcze związane z konfigurowaniem programu Installation Manager w celu uruchomienia go w 64-bitowych systemach AIX: <http://www-01.ibm.com/support/docview.wss?uid=swg24027719>.

Przed zainstalowaniem programu IBM Business Monitor wykonaj następujące kroki w systemie AIX:

1. Jeśli planowane jest zainstalowanie portletowych paneli kontrolnych, przed instalacją produktu WebSphere Portal lub portletowych paneli kontrolnych ustaw maksymalną liczbę otwartych plików przy użyciu poniższej komendy:

```
ulimit -n 8800
```

Innym rozwiązaniem jest wykonanie następujących czynności w celu edycji pliku ograniczeń zasobów:

 - a. Otwórz plik `/etc/security/limits`.
 - b. Edytuj lub dodaj sekcję **default** i wprowadź następujący wiersz:

```
nofiles = 8800
```
 - c. Zapisz i zamknij plik.
 - d. Wyloguj się z systemu operacyjnego, a następnie zaloguj się ponownie.
2. Ustaw wartość parametru **umask** na 022 za pomocą następującej komendy:

```
umask 022
```
3. Upewnij się, że zainstalowano przeglądarkę Mozilla Firefox w wersji 3.5.x.x lub nowszej.
4. Przed uruchomieniem usługi przenoszenia danych zwiększ liczbę procesów skonfigurowanych w systemie operacyjnym AIX, aby uniknąć błędu resetowania połączenia. Liczbę procesów można zwiększyć za pomocą komendy lub interfejsu systemu AIX.
 - Uruchom następującą komendę:

```
chgdev -l sys0 -a maxuproc='256'
```
 - W interfejsie systemu AIX wprowadź komendę **smitty**, a następnie wybierz opcję **System Environments (Środowiska systemowe) > Change / Show Characteristics of Operating System (Zmień / pokaż charakterystykę systemu operacyjnego) > Number of processes allowed per user(Num.) (Liczba procesów dozwolonych dla użytkownika)**.
5. Wykonaj kroki opisane w temacie Tune AIX systems (Strojenie systemów AIX).

Przygotowywanie systemów HP-UX do instalacji

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny HP-UX.

Ponieważ produkt WebSphere Application Server jest wstępnie wymaganym oprogramowaniem programu IBM Business Monitor, należy wykonać wymagane kroki przygotowawcze opisane w temacie Przygotowywanie systemu operacyjnego do instalacji produktu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server.

Niektóre kroki są specyficzne dla wersji systemu operacyjnego, dlatego nie wszystkie kroki mogą mieć zastosowanie w środowisku użytkownika. Jeśli dla konkretnego kroku nie został podany kwalifikator, należy wykonać ten krok dla wszystkich wersji systemu operacyjnego.

Przed zainstalowaniem programu IBM Business Monitor wykonaj następujące kroki w systemie HP-UX:

1. Jeśli planowane jest zainstalowanie portletowych paneli kontrolnych, przed instalacją produktu WebSphere Portal lub portletowych paneli kontrolnych ustaw maksymalną liczbę otwartych plików przy użyciu poniższej komendy:

```
ulimit -n 8800
```

Innym rozwiązaniem jest wykonanie następujących czynności w celu edycji pliku ograniczeń zasobów:

- a. Otwórz plik `/etc/security/limits`.
 - b. Edytuj lub dodaj sekcję **default** i wprowadź następujący wiersz:

```
nofiles = 8800
```
 - c. Zapisz i zamknij plik.
 - d. Wyloguj się z systemu operacyjnego, a następnie zaloguj się ponownie.
2. Ustaw wartość parametru **umask** na 022 za pomocą następującej komendy:

```
umask 022
```
 3. Wykonaj kroki opisane w temacie Tune HP-UX systems (Strojenie systemów HP-UX).

Przygotowywanie systemów Linux do instalacji

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny Linux.

Ponieważ produkt WebSphere Application Server jest wstępnie wymagany dla produktu IBM Business Monitor, należy wykonać wszystkie wymagane kroki przygotowawcze opisane w temacie Przygotowywanie systemu operacyjnego do instalacji produktu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server.

Należy upewnić się, że zainstalowano przeglądarkę Mozilla Firefox w wersji 3.5.x.x lub nowszej.

Niektóre kroki są specyficzne dla wersji systemu operacyjnego, dlatego nie wszystkie kroki mogą mieć zastosowanie w środowisku użytkownika. Jeśli dla konkretnego kroku nie został podany kwalifikator, należy wykonać ten krok dla wszystkich wersji systemu operacyjnego. W celu zainstalowania programu Installation Manager w systemie Red Hat Enterprise Linux 6.0 (64-bitowy) należy wyświetlić sekcję Nie można zainstalować programu Installation Manager w systemie RHEL 6.0 (64-bitowy).

Jeśli jest planowane użycie produktu DB2 Express wraz z systemem Red Hat Enterprise Linux 6:

- Przed rozpoczęciem instalowania produktu DB2 Express należy uruchomić następującą komendę jako administrator:


```
sysctl -w kernel.shmmax=268435456
```

Ta komenda będzie obowiązywać tylko do momentu zrestartowania systemu. Aby trwale usunąć problem, należy uruchomić następującą komendę:

```
/etc/sysctl.conf:  
kernel.shmmax = 268435456
```

- Należy zainstalować powłokę Korn (*ksh-wersja.rpm*).

Przed zainstalowaniem produktu IBM Business Monitor wykonaj następujące kroki w systemie Linux:

1. Zwiększ maksymalną liczbę otwartych plików do co najmniej 8800. Ustawienia domyślne są zwykle niewystarczające. Aby sprawdzić bieżącą maksymalną liczbę otwartych plików, użyj komendy `ulimit -n`. W poniższym przykładzie zaprezentowano, jak zwiększyć maksymalną liczbę otwartych plików do 8800. 

- a. Otwórz plik `/etc/security/limits.conf`.
- b. Znajdź parametr `nofile` i zwiększ jego wartość. Jeśli wiersz zawierający parametr `nofile` nie istnieje, dodaj następujące wiersze do pliku:
 - * hard nofile 8800
 - * soft nofile 8800
- c. Zapisz i zamknij plik.
- d. Wyloguj się i zaloguj ponownie.

Więcej informacji o tym ustawieniu można uzyskać, uruchamiając komendę `man limits.conf` lub przeglądając temat Przygotowywanie systemu operacyjnego do instalacji produktu w Centrum informacyjnym serwera WebSphere Application Server.

2. Zainstaluj następujące pakiety dla używanego systemu operacyjnego:

| Opcja | Opis |
|----------------------------------|--|
| Red Hat Enterprise Linux 4 | compat-libstdc++-33-3.2.3-47.3 compat-db-4.1.25-9 xorg-x11-deprecated-libs-6.8.1 or xorg-x11-deprecated-libs-6.8.2 rpm-build-4.3.3-7.nonptl compat-libstdc++-296-2.96-132.7.2 |
| Red Hat Enterprise Linux 5 | compat-libstdc++-33-3.2.3-61 compat-db-4.2.52-5.1 libXp-1.0.0-8 rpm-build-4.4.2-37.el5 tylko jądro 64-bitowe: compat-libstdc++-296-2.96-138 |
| Red Hat Enterprise Linux 6 | Powłoka Korn (ksh-wersja.rpm) Szczegółowe instrukcje i listę pakietów zawarto w sekcji Nie można zainstalować programu Installation Manager w systemie RHEL 6.0 (64-bitowy). |
| SUSE Linux Enterprise Server 9.0 | XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9 |

Można również zainstalować nowszą wersję dowolnego z tych pakietów, jeśli udostępniono nowe pakiety w ramach erraty. Jeśli dostępne są dodatkowe pakiety specyficzne dla konkretnego sprzętu, należy je zainstalować.

Zależności (wszystkie wymagane pakiety) można zainstalować przy użyciu komend wpisanych w jednym wierszu. W poniższych przykładach pokazano zastosowanie domyślnych menedżerów pakietów w obsługiwanych dystrybucjach systemu Linux.

- **Red Hat Enterprise Linux 5 (32-bitowy):**
`yum install compat-libstdc++-33 compat-db libXp rpm-build RHEL 5.x`
- **Red Hat Enterprise Linux 5 (64-bitowy):**
`yum install compat-libstdc++-33 compat-db libXp rpm-build compat-libstdc++-296`
- **SUSE Linux:**
`zypper install XFree86-libs-32bit-9 glibc-32bit-9 glib-32bit-9 gtk-32bit-9`

3. Ustaw wartość parametru `umask` na 022 za pomocą następującej komendy:

umask 022

4. W systemach Red Hat Enterprise Linux 5 wyłącz technologię SELinux lub ustaw ją na tryb pozwalający.
5. Zrestartuj komputer.
6. Wykonaj kroki opisane w temacie Tune Linux systems (Strojenie systemów Linux).

Przygotowywanie systemów Solaris do instalacji

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny Solaris.

Ponieważ produkt WebSphere Application Server jest wstępnie wymaganym oprogramowaniem programu IBM Business Monitor, należy wykonać wymagane kroki przygotowawcze opisane w temacie Przygotowywanie systemu operacyjnego do instalacji produktu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server.

Maszyna HotSpot JVM została utworzona przez firmę Sun Microsystems dla systemu operacyjnego Solaris i przeniesiona do systemu operacyjnego HP-UX. Struktura sterty Java i zarządzanie nią w przypadku maszyny HotSpot JVM różnią się od analogicznych rozwiązań w innych maszynach JVM. W używanym środowisku może zaistnieć konieczność dostosowania funkcji zarządzania stertą maszyny JVM w celu uniknięcia błędów `java.lang.OutOfMemoryError: PermGen` podczas tworzenia profilu lub działania serwera. Może być konieczne zaktualizowanie wartości parametru **MaxPermSize** maszyny JVM.

Niektóre kroki są specyficzne dla wersji systemu operacyjnego, dlatego nie wszystkie kroki mogą mieć zastosowanie w środowisku użytkownika. Jeśli dla konkretnego kroku nie został podany kwalifikator, należy wykonać ten krok dla wszystkich wersji systemu operacyjnego.

W następującej nocie technicznej zamieszczono dodatkowe informacje przygotowawcze związane z konfigurowaniem programu Installation Manager w celu uruchomienia go w 64-bitowych systemach AIX: <http://www-01.ibm.com/support/docview.wss?uid=swg24027719>.

W systemach Solaris przed instalacją programu IBM Business Monitor wykonaj następujące kroki:

1. Jeśli planowane jest zainstalowanie portletowych paneli kontrolnych, przed instalacją produktu WebSphere Portal lub portletowych paneli kontrolnych ustaw maksymalną liczbę otwartych plików przy użyciu poniższej komendy:

```
ulimit -Hn 8800
```

Innym rozwiązaniem jest wykonanie następujących czynności w celu edycji pliku ograniczeń zasobów:

 - a. Otwórz plik `/etc/system`
 - b. Dodaj następujący wiersz na końcu pliku:

```
set rlim_fd_max=8800
```
 - c. Zapisz i zamknij plik.
 - d. Wyloguj się z systemu operacyjnego, a następnie zaloguj się ponownie.
2. Ustaw wartość parametru `umask` na `022` przy użyciu następującej komendy:

```
umask 022
```
3. Wykonaj kroki opisane w temacie Tune Solaris systems (Strojenie systemów Solaris).

Przed utworzeniem lub rozszerzeniem profili produktu IBM Business Monitor w systemie Solaris należy zmienić parametr **MaxPermSize** maszyny JVM, postępując zgodnie z

procedurą opisaną w sekcji Eliminowanie błędów braku pamięci (OutOfMemoryError) występujących podczas tworzenia profilu w systemach Solaris i HP-UX.

Przygotowywanie systemów Windows do instalacji

Zanim będzie możliwe zainstalowanie produktu IBM Business Monitor, należy przygotować system operacyjny Windows.

Ponieważ produkt WebSphere Application Server stanowi wymaganie wstępne dla produktu IBM Business Monitor, należy wykonać wszystkie czynności przygotowawcze dotyczące produktu WebSphere Application Server przed zainstalowaniem produktu IBM Business Monitor.

Przed zainstalowaniem produktu IBM Business Monitor wykonaj następujące kroki w systemie Windows:

1. Wykonaj kroki opisane w temacie Przygotowywanie systemów Windows do instalacji w Centrum informacyjnym produktu WebSphere Application Server.
2. Wykonaj kroki opisane w temacie Strojenie systemów Windows.

Rozdział 4. Instalowanie produktu IBM Business Monitor

Program IBM Business Monitor można zainstalować w wielu topologiach. Istnieje możliwość zainstalowania wszystkich komponentów na pojedynczym serwerze lub rozmieszczenia ich w wielu systemach. Aby uzyskać środowisko wysokiej dostępności z obsługą przełączania awaryjnego, produkt IBM Business Monitor można zainstalować w środowisku klastrowym, w którym używana jest technologia klastrowa produktu WebSphere Application Server lub Process Server.

Ważne: Produkt IBM Business Monitor działa na wielu platformach. Szczegółowe informacje o obsługiwanych systemach operacyjnych oraz sprzęcie, a także wymagania dotyczące pamięci i wolnego miejsca na dysku można znaleźć w serwisie WWW IBM Business Monitor System requirements (Wymagania systemowe produktu IBM Business Monitor).

Instalowanie oprogramowania IBM Business Monitor

Produkt IBM Business Monitor można zainstalować w trybie interaktywnym lub cichym. Istnieje możliwość używania produktu IBM Business Monitor w środowisku monitorowania wraz z innym oprogramowaniem, w tym z produktami WebSphere Portal i Process Server.

Podczas interaktywnego instalowania produktu IBM Business Monitor wymagane jest użycie programu Installation Manager niezależnie od tego, czy wszystkie komponenty produktu IBM Business Monitor są instalowane na pojedynczym serwerze, czy też w klastrach w środowisku wdrożenia sieciowego.

Inna możliwość to wcześniejsze skonfigurowanie pliku odpowiedzi i zainstalowanie produktu IBM Business Monitor w trybie cichym przy użyciu wiersza komend, bez korzystania z programu instalacyjnego produktu IBM Business Monitor.

Instalowanie z poziomu startera produktu

Starter produktu IBM Business Monitor jest programem, w którym można wyświetlić informacje o wersji produktu IBM Business Monitor oraz z którego w razie potrzeby można zainstalować produkt WebSphere Application Server i uruchomić proces instalacji.

Należy wykonać czynności początkowe opisane w sekcji Rozdział 3, “Przygotowywanie instalacji produktu”, na stronie 33, jeśli nie zostały one jeszcze wykonane.

Informacje na temat domyślnego miejsca instalacji udostępniają strony pokrewne.



Windows Aby zainstalować lub uruchomić produkt IBM Business Monitor w systemie Windows 7, Windows Vista lub Windows Server 2008, należy zwiększyć uprawnienia konta użytkownika systemu Microsoft Windows. Zarówno w przypadku użytkownika będącego administratorem, jak i użytkownika niebędącego administratorem należy kliknąć prawym przyciskiem myszy program launchpad.exe i wybrać opcję **Uruchom jako administrator**.

Starter produktu powinien być używany do uruchamiania instalacji programu IBM Business Monitor w następujących przypadkach:

- Instalowanie z dysków DVD produktu
- Instalowanie z elektronicznego obrazu instalacji w lokalnym systemie plików
- Instalowanie z elektronicznego obrazu instalacji na dysku współużytkowanym

Aby uruchomić starter i zainstalować produkt WebSphere Application Server, jeśli nie został zainstalowany wcześniej, wykonaj następujące kroki:

1. Włóż pierwszy instalacyjny dysk DVD produktu IBM Business Monitor do napędu DVD.

  Sprawdź, czy napęd DVD został podłączony.

2. Jeśli w systemie włączono funkcję automatycznego uruchamiania, starter programu IBM Business Monitor zostanie otwarty automatycznie. Jeśli funkcja automatycznego uruchamiania nie jest włączona w systemie:
 - Uruchom plik `launchpad.sh` znajdujący się w katalogu głównym dysku DVD.
 - Uruchom plik `launchpad.exe` lub `launchpad64.exe` (w przypadku systemu 64-bitowego) znajdujący się w katalogu głównym dysku DVD.
3. Opcjonalne: Kliknij opcję **Instalacja systemu pomocy**, aby zainstalować system pomocy i dokumentację produktu na komputerze. System pomocy to środowisko Eclipse do wyświetlania dokumentacji.
4. Jeśli należysz do grupy administratorów w systemie Windows bądź jesteś administratorem w systemie Linux lub UNIX, upewnij się, że zostało zaznaczone pole wyboru **Instaluj jako administrator**. Należy anulować zaznaczenie tego pola wyboru tylko wtedy, gdy użytkownik nie jest administratorem lub zamierza przeprowadzić instalację przy użyciu własnej nazwy użytkownika bez nadawania uprawnień innym użytkownikom.
5. **Jeśli nie zainstalowano jeszcze serwera WebSphere Application Server**, kliknij przycisk **Instaluj**, aby rozpocząć instalację programu IBM Business Monitor. Program Installation Manager zostanie uruchomiony i skonfigurowany automatycznie. Pozostałe instrukcje dotyczące instalacji można znaleźć w sekcji “Interaktywne instalowanie programu IBM Business Monitor” na stronie 41.
6. **Aby zainstalować program IBM Business Monitor w istniejącej instalacji serwera WebSphere Application Server**, kliknij opcję **Instalacja na istniejącym serwerze WebSphere Application Server**.
 - a. Jeśli należysz do grupy administratorów w systemie Windows bądź jesteś administratorem w systemie Linux lub UNIX, upewnij się, że zostało zaznaczone pole wyboru **Instaluj jako administrator**. Należy anulować zaznaczenie tego pola wyboru tylko wtedy, gdy użytkownik nie jest administratorem lub zamierza przeprowadzić instalację przy użyciu własnej nazwy użytkownika bez nadawania uprawnień innym użytkownikom.
 - b. Kliknij opcję **Importuj lub aktualizuj**.
 - Jeśli zostanie wyświetlone okno Otwieranie pliku, kliknij opcję **Uruchom**. Zostanie otwarty program Installation Manager.
 - Kliknij przycisk **Importuj**, aby zaimportować produkt WebSphere Application Server do programu Installation Manager. Zaimportowanie produktu WebSphere Application Server jest konieczne, jeśli nigdy wcześniej nie wykonano tej operacji lub jeśli po ostatnim importowaniu tego produktu zaktualizowano go za pomocą instalatora aktualizacji.
 - Kliknij przycisk **Przełóżaj** i wybierz katalog, w którym zainstalowano produkt WebSphere Application Server, na przykład `katalog_główny_serwera_aplikacji`.
 - Kliknij przycisk **Dalej**, a następnie opcję **Importuj**.
 - Kliknij przycisk **Zakończ**.
 - W oknie programu Installation Manager kliknij opcję **Aktualizuj**.
 - Wybierz grupę pakietów **IBM WebSphere Application Server - ND**.

Wskazówka: Na stronie Aktualizacja pakietów należy wybrać opcję **Pokaż wszystkie**, aby wyświetlić dostępne aktualizacje.

- Kliknij przycisk **Dalej** i wykonuj instrukcje na poszczególnych stronach, akceptując wartości domyślne. Pakiet Feature Pack for XML zostanie zaktualizowany do wymaganego poziomu.
 - Zamknij program Installation Manager i wróć do aplikacji startera.
- c. Kliknij przycisk **Instaluj**, aby rozpocząć instalację programu IBM Business Monitor. Jeśli zostanie wyświetlone okno Otwieranie pliku, kliknij opcję **Uruchom**.
- d. Kliknij przycisk **Instaluj IBM Business Monitor**. Program Installation Manager zostanie uruchomiony i skonfigurowany automatycznie. Pozostałe instrukcje dotyczące instalacji można znaleźć w sekcji “Interaktywne instalowanie programu IBM Business Monitor”.

Jeśli system operacyjny obsługuje tę możliwość, można kliknąć opcję **Instalacja systemu pomocy** w starterze w celu zainstalowania Centrum informacyjnego.

Interaktywne instalowanie programu IBM Business Monitor

Użytkownik może interaktywnie zainstalować produkt IBM Business Monitor 7.5 za pomocą programu Installation Manager niezależnie od tego, czy wszystkie komponenty są instalowane na pojedynczym serwerze, czy w klastrach środowiska wdrożenia sieciowego.

Uruchom program Installation Manager z poziomu startera produktu. Więcej informacji na ten temat można znaleźć w sekcji “Instalowanie z poziomu startera produktu” na stronie 39.

Informacje na temat domyślnego miejsca instalacji są dostępne po użyciu odsyłacza do strony pokrewnej.

Aby zainstalować program IBM Business Monitor, wykonaj następujące kroki:

1. Na stronie początkowej programu Installation Manager kliknij opcję **Zainstaluj pakiety** i kliknij przycisk **Dalej**, aby kontynuować. Zostaną wybrane następujące pakiety:
 - IBM Cognos Business Intelligence (usuń zaznaczenie pola wyboru, jeśli używasz systemu Windows jako użytkownik inny niż administrator)
 - WebSphere Application Server - ND (usuń zaznaczenie pola wyboru, jeśli pakiet jest już zainstalowany)
 - WebSphere Application Server Feature Pack for XML (usuń zaznaczenie pola wyboru, jeśli pakiet jest już zainstalowany)
 - DB2 Express (usuń zaznaczenie pola wyboru, jeśli istnieje już baza danych, która ma zostać użyta, lub nie masz uprawnień administratora)
 - IBM Business Monitor

Jeśli podczas sprawdzania wymagań wstępnych zostanie wyświetlony poniższy komunikat ostrzegawczy, należy wykonać następujące specyficzne dla platformy kroki w celu zwiększenia wartości ulimit.

Bieżący system wykrył niższą wartość ulimit niż zalecana wartość 8799. Zwiększ wartość ulimit do minimalnej wartości 8799 i zrestartuj instalację.

Zamknij

instalator. Jeśli jesteś administratorem, otwórz wiersz komend i uruchom komendę ulimit -n 8799, a następnie zrestartuj instalator. Jeśli nie jesteś administratorem, skontaktuj się z administratorem systemu w sprawie zwiększenia wartości ulimit za pomocą opcji -n 8799, a następnie zrestartuj instalator.

- a. Ustaw maksymalną liczbę otwartych plików przy użyciu następującej komendy:

Linux



- 1) Otwórz plik /etc/security/limits.conf.
- 2) Znajdź parametr nofile i zwiększ jego wartość. Jeśli wiersz zawierający parametr nofile nie istnieje, dodaj następujące wiersze do pliku:

* hard nofile 8800

* soft nofile 8800

- 3) Zapisz i zamknij plik.
 - 4) Wyloguj się i zaloguj ponownie.
 - b. Zrestartuj komputer.
 - c. Zrestartuj instalator.
2. Na stronie Licencje przeczytaj umowę licencyjną dla wybranego pakietu.
- Jeśli wybrano instalację kilku pakietów, dla każdego z nich może istnieć osobna umowa licencyjna. Aby wyświetlić umowę licencyjną dla danej wersji pakietu, należy ją kliknąć w lewej części strony **Licencja**. Wersje pakietu wybrane do zainstalowania (na przykład pakiet podstawowy i aktualizacja) są wyświetlane pod nazwą pakietu.
- a. Jeśli akceptujesz warunki wszystkich umów licencyjnych, kliknij opcję **Akceptuję warunki umów licencyjnych**.
 - b. Kliknij przycisk **Dalej**, aby kontynuować.
3. Jeśli produkt IBM Business Monitor 7.5 jest pierwszym pakietem instalowanym przy użyciu programu Installation Manager, w polu **Katalog zasobów współużytkowanych** wpisz ścieżkę do *katalogu zasobów współużytkowanych* lub zaakceptuj ścieżkę domyślną. Katalog zasobów współużytkowanych zawiera zasoby, które mogą być współużytkowane przez jedną lub kilka grup pakietów.

Ważne:

- a. Katalog zasobów współużytkowanych można określić tylko podczas pierwszej instalacji pakietu. Określając ten katalog, należy użyć największego dysku w celu zapewnienia odpowiedniej ilości miejsca dla zasobów współużytkowanych przyszłych pakietów. Położenia katalogu nie można zmienić, chyba że zostaną zdeinstalowane wszystkie pakiety.
 - b. Należy upewnić się, że ścieżka instalacji nie zawiera nawiasów.
 - c.   Należy upewnić się, że ścieżka instalacji nie zawiera spacji. Kliknij przycisk **Dalej**, aby kontynuować.
4. Na następnej stronie Położenie można utworzyć *grupę pakietów*, w której ma zostać zainstalowany pakiet produktu IBM Business Monitor. Aby utworzyć nową grupę pakietów:
- a. Wybierz opcję **Utwórz nową grupę pakietów**.
 - b. Wpisz ścieżkę do katalogu instalacyjnego grupy pakietów. Upewnij się, że ścieżka instalacji nie zawiera nawiasów. W przypadku systemów Linux lub UNIX upewnij się, że ścieżka do katalogu nie zawiera żadnych spacji. Nazwa grupy pakietów zostanie utworzona automatycznie.
 - c. Kliknij przycisk **Dalej**, aby kontynuować.
- Kreator instalacji pakietów wyświetli komunikat, jeśli wykryje jakiegokolwiek działające procesy (na przykład serwer WebSphere Application Server). Jeśli komunikat zostanie wyświetlony, należy kliknąć przycisk **Anuluj**, zamknąć działające procesy i ponownie rozpocząć instalację.
5. Na stronie Składniki wybierz składniki pakietu, które mają zostać zainstalowane.
- a. Opcjonalne: Aby wyświetlić relacje zależności między składnikami, zaznacz pole wyboru **Pokaż zależności**.
 - b. Opcjonalne: Kliknij składnik, aby wyświetlić jego krótki opis w obszarze **Szczegóły**.
 - c. Zaznacz lub usuń zaznaczenie składników w pakiecie. Program Installation Manager automatycznie wymusi wszystkie zależności między wybranymi i pozostałymi składnikami, a następnie wyświetli zaktualizowane wartości określające wielkość pobieranych danych oraz wymaganą ilość miejsca na dysku.

- Jeśli nie wybrano żadnych składników, zainstalowane zostaną pliki licencji produktu Business Space i IBM Business Monitor.
- Jeśli rozwinięto opcję **Serwer programu Business Monitor** i wybrano jeden lub większą liczbę autonomicznych profili programistycznych, profile są tworzone w trakcie instalacji. Aby utworzyć profile programistyczne produktu Process Server lub WebSphere Enterprise Service Bus, te pakiety muszą już być zainstalowane.

Autonomiczny profil programistyczny to domyślny profil programistyczny udostępniający środowisko testowe programu IBM Business Monitor. Profil programistyczny produktu Process Server jest dostarczany wraz z włączonym menedżerem reguł biznesowych. Aby utworzyć autonomiczny profil programistyczny, należy podać referencje zabezpieczeń administratora (nazwa użytkownika i hasło) dla serwera, który jest tworzony.

Autonomiczny profil programistyczny nie może być używany w środowisku produkcyjnym. Jeśli domyślny autonomiczny profil programistyczny nie zostanie zainstalowany, można zainstalować go później, uruchamiając program Installation Manager i klikając opcję **Modyfikuj** na pierwszej stronie.

- d. Po wybraniu składników kliknij przycisk **Dalej**, aby kontynuować.
6. Jeśli wybrano autonomiczny profil programistyczny, na stronie Profile wprowadź referencje dla danego profilu. Domyślna nazwa użytkownika to **admin**, a domyślne hasło to **admin**.
7. Jeśli istnieje już baza danych, na stronie Konfiguracje wspólne wprowadź referencje dla tej bazy. Jeśli wybrano bazę danych DB2 Express, wpisz nazwę i hasło użytkownika produktu DB2. Domyślna nazwa użytkownika to **bpmadmin**, a domyślne hasło to **bpmadmin1**.

Ważne: Jeśli domyślne hasło nie jest zgodne ze strategią haseł używanego systemu operacyjnego (np. Windows 2008), konieczna jest zmiana tego hasła.

Ograniczenie: Nazwy użytkowników nie mogą zawierać znaków języka narodowego. Kliknij przycisk **Dalej**, aby kontynuować.

8. Przed zainstalowaniem pakietu programu IBM Business Monitor przejrzyj wybrane ustawienia na stronie Podsumowanie. Aby zmienić ustawienia wybrane na poprzednich stronach, kliknij przycisk **Wstecz** i wprowadź zmiany. Jeśli ustawienia wybrane dla instalacji są poprawne, kliknij przycisk **Instaluj**, aby zainstalować pakiet. Informacja o procencie wykonania instalacji jest przekazywana za pośrednictwem wskaźnika postępu.
9. Po zakończeniu instalacji zostanie wyświetlony komunikat potwierdzający jej pomyślny przebieg.
 - a. Opcjonalne: Kliknij opcję **Wyświetl plik dziennika**, aby otworzyć plik dziennika instalacji dla bieżącej sesji w nowym oknie. Aby kontynuować, zamknij okno Dziennik instalacji.
 - b. W obszarze **Który program ma zostać uruchomiony?** wybierz, czy po zamknięciu ma zostać uruchomione narzędzie Profile Management Tool. Jeśli utworzono już autonomiczny profil programistyczny, można wybrać opcję **Brak**. Do zastosowań produkcyjnych za pomocą narzędzia Profile Management Tool lub komendy manageprofiles należy zdefiniować profil serwera autonomicznego lub menedżer wdrażania. Więcej informacji można znaleźć w sekcji Tworzenie i rozszerzanie profili.
- c. Kliknij przycisk **Zakończ**, aby zamknąć program Installation Manager.

W przypadku środowiska produkcyjnego konieczne jest utworzenie profilu serwera autonomicznego lub menedżera wdrażania za pomocą narzędzia Profile Management Tool lub komendy manageprofiles.

Ograniczenie: Jeśli w trakcie instalacji utworzono autonomiczny profil programistyczny, należy pamiętać, że ten profil nie działa w środowisku produkcyjnym. Celem profilu jest zaznajomienie użytkownika z programem IBM Business Monitor bez konieczności tworzenia działającego profilu produkcyjnego. Profil można uruchomić przy użyciu konsoli Pierwsze kroki.

- Otwórz okno komend. Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.sh.
- Wybierz opcję **Start > Wszystkie programy > IBM > Business Monitor 7.5 > Profile > nazwa_profilu > Pierwsze kroki**.
- Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.bat.

Ważne: Aby zainstalować lub uruchomić konsolę Pierwsze kroki w systemach Windows 7, Windows Vista lub Windows Server 2008, konieczne jest zwiększenie uprawnień konta użytkownika systemu Microsoft Windows przez kliknięcie prawym przyciskiem myszy pliku firststeps.bat i wybranie opcji **Uruchom jako administrator**. Jest to wymagane zarówno w przypadku administratorów, jak i użytkowników innych niż administratorzy.

Jeśli system operacyjny obsługuje tę możliwość, można kliknąć opcję **Instalacja systemu pomocy** w starterze w celu zainstalowania Centrum informacyjnego.

Instalacja cicha produktu IBM Business Monitor

Pakiet produktu IBM Business Monitor można zainstalować w trybie *instalacji cichej*. Podczas instalowania w trybie cichym interfejs użytkownika nie jest dostępny. W tym przypadku jest uruchamiana komenda w celu użycia pliku odpowiedzi, który instaluje produkt.

Dla tej procedury instalacji cichej nie ma znaczenia, czy wymagane wstępnie produkty podstawowe produktu IBM Business Monitor są zainstalowane. Produkty te obejmują serwer WebSphere Application Server Network Deployment, program Installation Manager i pakiet składników Feature Pack for XML.

Przed zainstalowaniem produktu IBM Business Monitor należy przejrzeć wymagania systemowe dla tego produktu.

Szczególnie istotne znaczenie mają wersje systemu operacyjnego i wstępnie wymaganego oprogramowania. Mimo że proces instalacyjny automatycznie dokonuje przeglądu wstępnie wymaganych poprawek dla systemu operacyjnego, należy przejrzeć te wymagania, jeśli nie zostało to jeszcze wykonane. W tym temacie znajduje się lista wszystkich obsługiwanych systemów operacyjnych oraz poprawek systemu operacyjnego, które muszą być zainstalowane w celu zapewnienia zgodnego systemu operacyjnego. Udostępniono również listę wymaganych wersji wstępnie wymaganego oprogramowania.

Windows **Ważne:** aby zainstalować lub uruchomić produkt IBM Business Monitor w systemie Windows 7, Windows Vista lub Windows Server 2008, należy zwiększyć uprawnienia konta użytkownika systemu Microsoft Windows, klikając prawym przyciskiem myszy wiersz komend, w którym zostanie uruchomiona komenda instalacji cichej, i wybierając opcję **Uruchom jako administrator**. Jest to wymagane zarówno w przypadku administratorów, jak i użytkowników innych niż administratorzy.

Instalacja cicha wykonuje wszystkie lub niektóre spośród następujących zadań:

- Instalacja programu Installation Manager, jeśli nie jest jeszcze zainstalowany, lub aktualizacja do odpowiedniej wersji, jeśli program jest zainstalowany.

- Instalacja wymaganych produktów podstawowych i programu IBM Business Monitor przy użyciu pliku odpowiedzi utworzonego przez użytkownika.

Aby zainstalować program IBM Business Monitor w trybie cichym, wykonaj następujące kroki:

1. Przed instalacją przeczytaj i zaakceptuj warunki licencji. Dodanie opcji `-acceptLicense` w pliku odpowiedzi oznacza akceptację wszystkich licencji.
2. Utwórz plik odpowiedzi, który zainstaluje wymagane produkty podstawowe i program IBM Business Monitor. Aby utworzyć własny plik odpowiedzi, skopiuj przykładowy plik odpowiedzi do następującego katalogu:

katalog_główny_dysku_DVD/responsefiles/BPM/template_response.xml

3. Aby utworzyć własny plik odpowiedzi, zmodyfikuj parametry w sposób opisany w tekście szablonu pliku odpowiedzi. Plik odpowiedzi można również utworzyć, rejestrując czynności w programie Installation Manager. Podczas rejestrowania pliku odpowiedzi wybory dokonane w programie Installation Manager są zapisywane w pliku XML. Kiedy program Installation Manager jest uruchomiony w trybie instalacji cichej, używa danych z pliku odpowiedzi XML do przeprowadzenia instalacji.

Ważne: Sprawdź, czy położenie repozytorium określone u góry przykładowego pliku odpowiedzi jest poprawnym położeniem w danym środowisku.

4. Uruchom następującą komendę:

Administrator: 

```
katalog_główny_dysku_DVD\IM\installc.exe
-acceptLicense input
katalog_główny_dysku_DVD/responsefiles\identyfikator_produkту\template_response.xml
-log preferowane_położenie_dziennika\silent_install.log
```

```
katalog_główny_dysku_DVD/IM/installc -acceptLicense input
katalog_główny_dysku_DVD/responsefiles/identyfikator_produkту/template_response.xml
-log preferowane_położenie_dziennika/silent_install.log
```

Użytkownik niebędący administratorem: 

```
katalog_główny_dysku_DVD\IM\userinstc.exe
-acceptLicense input
katalog_główny_dysku_DVD/responsefiles\identyfikator_produkту\template_response.xml
-log preferowane_położenie_dziennika\silent_install.log
```

```
katalog_główny_dysku_DVD/IM/userinstc
-acceptLicense input
katalog_główny_dysku_DVD/responsefiles/identyfikator_produkту/template_response.xml
-log preferowane_położenie_dziennika/silent_install.log
```

Program Installation Manager instaluje wszelkie wymagane wstępnie oprogramowanie oraz produkt IBM Business Monitor, a następnie zapisuje plik dziennika do podanego katalogu.

Za pomocą narzędzia Profile Management Tool lub komendy `manageprofiles` należy zdefiniować profil serwera autonomicznego lub menedżer wdrażania. W środowisku produkcyjnym mogą być używane jedynie profile utworzone za pomocą narzędzia Profile Management Tool lub komendy `manageprofiles`.

Praca z programem IBM Installation Manager

W tej sekcji opisano niektóre typowe czynności powiązane z programem IBM Installation Manager. Więcej informacji na ten temat zawiera Centrum informacyjne programu Installation Manager.

Instalowanie programu Installation Manager w systemie Windows

Jeśli instalacja produktu jest uruchamiana za pomocą startera, to instalacja programu IBMInstallation Manager jest przeprowadzana automatycznie, o ile ten program nie jest jeszcze zainstalowany na stacji roboczej użytkownika. W innych przypadkach należy uruchomić proces instalacji programu Installation Manager ręcznie.

Aby zainstalować ręcznie program Installation Manager:

1. Uruchom program `install.exe` z folderu IM w obrazie instalacji.
2. Kliknij przycisk **Dalej** znajdujący się na stronie Instalacja pakietów.
3. Przeczytaj umowę licencyjną wyświetloną na stronie Umowa licencyjna. Aby zaakceptować warunki tej umowy, wybierz opcję **Akceptuję warunki umowy licencyjnej**. Kliknij przycisk **Dalej**.
4. W razie potrzeby kliknij przycisk **Przeglądaj** znajdujący się na stronie Folder docelowy, aby zmienić miejsce instalacji. Kliknij przycisk **Dalej**.
5. Kliknij przycisk **Instaluj** znajdujący się na stronie Podsumowanie. Po zakończeniu instalacji zostanie wyświetlony komunikat potwierdzający jej pomyślny przebieg.
6. Kliknij przycisk **Zakończ**. Program IBM Installation Manager zostanie otwarty.

Instalowanie programu Installation Manager w systemach Linux i UNIX

Jeśli instalacja produktu jest uruchamiana za pomocą startera, to instalacja programu IBMInstallation Manager jest przeprowadzana automatycznie, o ile ten program nie jest jeszcze zainstalowany na stacji roboczej użytkownika. .

Aby zainstalować ręcznie program Installation Manager:

1. Otwórz okno terminalu z uprawnieniami administratora.
2. Uruchom program `install` z poziomu folderu `IM_linux` w obrazie instalacji.
3. Kliknij przycisk **Dalej** znajdujący się na ekranie Instalacja pakietów.
4. Przeczytaj umowę licencyjną wyświetloną na stronie Umowa licencyjna. Aby zaakceptować warunki tej umowy, wybierz opcję **Akceptuję warunki umowy licencyjnej**. Kliknij przycisk **Dalej**.
5. W razie potrzeby zmodyfikuj położenie katalogu instalacyjnego. Kliknij przycisk **Dalej**.
6. Kliknij przycisk **Instaluj** znajdujący się na stronie podsumowania. Po zakończeniu instalacji zostanie wyświetlony komunikat potwierdzający jej pomyślny przebieg.
7. Kliknij przycisk **Zakończ**. Jeśli instalacja produktu jest uruchamiana za pomocą startera, to instalacja programu IBMInstallation Manager jest przeprowadzana automatycznie, o ile ten program nie jest jeszcze zainstalowany na stacji roboczej użytkownika.

Uruchamianie programu Installation Manager w systemie Windows

Jeśli instalacja produktu jest uruchamiana za pomocą startera, to instalacja programu IBMInstallation Manager jest przeprowadzana automatycznie, o ile ten program nie jest jeszcze zainstalowany na stacji roboczej użytkownika. W przypadku instalacji automatycznej program Installation Manager jest uruchamiany ze skonfigurowaną preferencją repozytorium

oraz z wybranymi pakietami produktu IBM Business Monitor. Jeśli program Installation Manager został uruchomiony bezpośrednio, należy ustawić preferencję repozytorium oraz wybrać ręcznie pakiety produktu.

Aby uruchomić program Installation Manager ręcznie:

1. Otwórz menu **Start**, klikając przycisk na **pasku zadań**.
2. Wybierz opcję **Wszystkie programy > IBM Installation Manager > IBM Installation Manager**.

Uruchamianie programu Installation Manager w systemach Linux i UNIX

Jeśli instalacja produktu jest uruchamiana za pomocą startera, to instalacja programu IBM Installation Manager jest przeprowadzana automatycznie, o ile ten program nie jest jeszcze zainstalowany na stacji roboczej użytkownika. W przypadku instalacji automatycznej program Installation Manager jest uruchamiany ze skonfigurowaną preferencją repozytorium oraz z wybranymi pakietami produktu IBM Business Monitor. Jeśli program Installation Manager został uruchomiony bezpośrednio, należy ustawić preferencję repozytorium oraz wybrać ręcznie pakiety produktu.

Aby uruchomić program Installation Manager ręcznie:

1. Otwórz okno terminalu z uprawnieniami administratora.
2. Zmień katalog na katalog instalacyjny programu Installation Manager (domyślnie `/opt/IBM/InstallationManager/eclipse` w przypadku instalacji przeprowadzanej przez administratora, *katalog_główny_użytkownika/IBM/InstallationManager/eclipse* w przypadku instalacji przeprowadzanej przez użytkownika niebędącego administratorem) i uruchom komendę IBMIM.

Deinstalowanie programu Installation Manager w systemie Windows

Aby ręcznie zdeinstalować program Installation Manager:

1. W tym celu należy kliknąć opcję **Start > Ustawienia > Panel sterowania**, a następnie kliknąć dwukrotnie ikonę **Dodaj lub usuń programy**.
2. Wybierz pozycję programu IBM Installation Manager i kliknij przycisk **Usuń**.

Deinstalowanie programu Installation Manager w systemach Linux i UNIX

Deinstalowanie programu IBM Installation Manager musi zostać przeprowadzone przy użyciu narzędzia do zarządzania pakietami dołączonego do wersji systemu Linux lub UNIX używanej przez użytkownika.

Aby ręcznie zdeinstalować program Installation Manager:

1. Otwórz okno terminalu z uprawnieniami administratora.
2. Zmień katalog na katalog deinstalacyjny programu Installation Manager. Domyślnie jest to katalog `/var/ibm/InstallationManager/uninstall`.
3. Uruchom program `./uninstall`.

Aktualizowanie programu Installation Manager przy użyciu serwera proxy

Serwery proxy umożliwiają nawiązywanie połączeń ze zdalnymi serwerami znajdującymi się za firewallem. Preferencje dla serwerów proxy można ustawić w programie Installation Manager lub w pliku odpowiedzi. Po włączeniu serwera proxy jest on używany dla

wszystkich połączeń serwera. Szczegółowe informacje na temat konfigurowania serwera proxy dla programu Installation Manager znajdują się w sekcji Preferencje dotyczące Internetu Centrum informacyjnego programu Installation Manager.

Instalowanie i deinstalowanie programu Installation Manager w trybie cichym

Program IBM Installation Manager można zainstalować i zdeinstalować w trybie cichym.

Instalowanie programu Installation Manager w trybie cichym:

Aby zainstalować program Installation Manager w trybie cichym, należy wyodrębnić instalator i przejść do podkatalogu IM, a następnie użyć poniższych komend:

- `install --launcher.ini -acceptLicense silent-install.ini -log <ścieżka do pliku dziennika i jego nazwa>`. Przykład: `install --launcher.ini -acceptLicense silent-install.ini -log /root/moje_dzienniki/mój_plik_dziennika.xml`
- `installc --launcher.ini -acceptLicense silent-install.ini -log <ścieżka do pliku dziennika i jego nazwa>`. Przykład: `installc --launcher.ini -acceptLicense silent-install.ini -log c:\mój_plik_dziennika.xml`

Po zakończeniu instalacji można użyć programu Installation Manager lub instalatora programu Installation Manager w celu zainstalowania pakietów instalacyjnych w trybie cichym.

Deinstalowanie programu Installation Manager w systemie Windows w trybie cichym:

Aby zdeinstalować program Installation Manager w systemie Windows w trybie cichym:

1. W wierszu komend przejdź do katalogu deinstalacyjnego programu Installation Manager. Domyślnie jest to katalog `C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\uninstall`.
2. Wprowadź następującą komendę: `uninstallc.exe --launcher.ini silent-uninstall.ini`

Deinstalowanie programu Installation Manager w systemie Linux w trybie cichym:

Aby zdeinstalować program Installation Manager w trybie cichym na innych platformach:

1. W oknie terminalu przejdź do katalogu deinstalacyjnego programu Installation Manager. Domyślnie jest to katalog `/var/ibm/InstallationManager/uninstall`.
2. Uruchom następującą komendę: `uninstall --launcher.ini silent-uninstall.ini`

Grupy pakietów oraz katalog zasobów współużytkowanych

Podczas instalacji pakietu produktu IBM Business Monitor for z/OS przy użyciu programu IBM Installation Manager pakiet ten należy zainstalować w istniejącej grupie pakietów zawierającej serwer WebSphere Application Server.

Grupy pakietów

Grupa pakietów reprezentuje katalog, w którym pakiety współużytkują wspólny interfejs użytkownika lub środowisko robocze z innymi pakietami z tej samej grupy.

Należy pamiętać, że w przypadku jednoczesnej instalacji wielu pakietów wszystkie te pakiety są instalowane w tej samej grupie pakietów.

Nazwa grupy pakietów jest przypisywana automatycznie, natomiast katalog instalacyjny grupy pakietów jest wybierany przez użytkownika.

Katalog instalacyjny zawiera pliki i zasoby specyficzne dla pakietów zainstalowanych w tej grupie pakietów. Wtyczki Eclipse z pakietu produktu, które mogą być używane przez inne grupy pakietów, są umieszczane w katalogu zasobów współużytkowanych.

Katalog zasobów współużytkowanych

Katalog zasobów współużytkowanych to katalog, w którym znajdują się wtyczki Eclipse. Dzięki temu, że umieszczono je w tym katalogu, mogą być one używane przez jedną lub kilka grup pakietów produktów.

Ważne: Katalog zasobów współużytkowanych można określić tylko raz - przy pierwszej instalacji pakietu. Rozwiązaniem optymalnym jest określenie katalogu zasobów współużytkowanych znajdującego się na największym dysku. Położenia katalogu nie można zmienić, chyba że zostaną zdeinstalowane wszystkie pakiety.

Ustawianie preferencji repozytorium w programie Installation Manager

Jeśli program Installation Manager jest uruchamiany bezpośrednio (na przykład z repozytorium znajdującego się na serwerze WWW), to zainstalowanie pakietu produktu wymaga określenia w programie Installation Manager adresu URL katalogu zawierającego pakiet produktu.

Uwaga: Jeśli instalacja nie jest przeprowadzana z dysku DVD lub lokalnego obrazu instalacyjnego, przed rozpoczęciem procesu instalacji należy uzyskać od administratora adres URL repozytorium pakietu instalacyjnego.

Aby dodać, zmodyfikować lub usunąć położenie repozytorium w programie Installation Manager:

1. Uruchom program Installation Manager.
2. Na stronie Początek produktu Installation Manager kliknij opcję **Plik > Preferencje**, a następnie kliknij opcję **Repozytoria**. Zostanie otwarta strona Repozytoria, na której będą wyświetlane wszystkie dostępne repozytoria, a także informacje o ich położeniu oraz o tym, czy dostęp do nich jest możliwy.
3. Na stronie Repozytoria kliknij opcję **Dodaj repozytorium**.
4. W oknie Dodawanie repozytorium wpisz adres URL określający położenie repozytorium lub przejdź do tego położenia i ustaw ścieżkę do pliku. Położenie repozytorium jest zazwyczaj następujące: *katalog_obrazu/repository.config*, gdzie *katalog_obrazu* zawiera wyodrębniony obraz instalacji produktu, który ma zostać zainstalowany.
5. Kliknij przycisk **OK**. Zostanie wyświetlone nowe lub zmienione położenie repozytorium. Jeśli repozytorium nie będzie dostępne, w kolumnie **Dostępne** zostanie wyświetlony czerwony znak x.
6. Kliknij przycisk **OK**, aby wyjść z programu.

Uwaga: Aby program Installation Manager mógł przeprowadzić wyszukiwanie zainstalowanych pakietów w domyślnych położeniach repozytoriów, należy sprawdzić, czy jest wybrana preferencja **Przeszukuj repozytoria usług podczas instalowania i aktualizowania** na stronie preferencji Repozytoria.

Instalowanie Centrum informacyjnego

Centrum informacyjne produktu IBM Business Monitor jest dostępne w Internecie. Centrum można również zainstalować za pomocą startera produktu, jeśli jest on obsługiwany w używanym systemie operacyjnym.

- Zainstaluj i uruchom Centrum informacyjne z poziomu startera produktu.
 1. W starterze kliknij opcję **Instalacja systemu pomocy**.

2. Określ położenie dla lokalnego Centrum informacyjnego.
 3. Kliknij opcję **Zainstaluj i uruchom system pomocy**. Jeśli zostanie wyświetlone okno Otwieranie pliku, kliknij opcję **Uruchom**.
- Wyświetl Centrum informacyjne w Internecie. Więcej informacji zawarto w Centrum informacyjnym produktu IBM Business Process Management.

Uruchamianie i zatrzymywanie lokalnego Centrum informacyjnego

Po zainstalowaniu Centrum informacyjnego programu IBM Business Monitor można wyświetlać informacje w systemie lokalnym lub udostępniać je innym użytkownikom w sieci.

W tej procedurze zmienna katalog_główny_dokumentów reprezentuje katalog, w którym zainstalowano Centrum informacyjne.

- Aby wyświetlić Centrum informacyjne lokalnie, wykonaj następujące kroki:
 1. Przejdź do katalogu, w którym zainstalowano Centrum informacyjne.
 2. Aby uruchomić Centrum informacyjne, uruchom skrypt, który jest odpowiedni dla używanego systemu operacyjnego:
 - help_start.sh
 - help_start.bat


Zostanie otwarta domyślna przeglądarka wyświetlająca Centrum informacyjne, które zostało zainstalowane razem z produktem.
 3. Aby zatrzymać Centrum informacyjne, zamknij przeglądarkę i uruchom skrypt odpowiedni dla danego systemu operacyjnego:
 - help_end.sh
 - help_end.bat
- Aby udostępnić Centrum informacyjne w sieci i umożliwić wyświetlanie go w innych systemach, wykonaj następujące kroki:
 1. Przejdź do katalogu, w którym zainstalowany jest program IBM Business Monitor.
 2. Aby uruchomić Centrum informacyjne, uruchom skrypt, który jest odpowiedni dla używanego systemu operacyjnego:
 - IC_start.sh
 - IC_start.bat

Aby uzyskać dostęp do Centrum informacyjnego z poziomu innego systemu, użytkownicy mogą otworzyć przeglądarkę i przejść do następującego adresu URL:
http://nazwa_hosta:8888/help/index.jsp
 3. Aby zatrzymać Centrum informacyjne, zamknij przeglądarkę i uruchom skrypt odpowiedni dla danego systemu operacyjnego:
 - IC_end.sh
 - IC_end.bat

Aktualizowanie lokalnego Centrum informacyjnego

Jeśli użytkownik ma połączenie z Internetem, lokalnie zainstalowaną wersję dokumentacji można aktualizować po udostępnieniu nowej dokumentacji. Do lokalnego Centrum informacyjnego można również dołączyć zaktualizowaną dokumentację dla pozostałych produktów.

Aby zaktualizować dokumentację, wykonaj następujące kroki:

1. Kliknij ikonę **Aktualizuj** () , która znajduje się na pasku narzędzi systemu pomocy. Zostanie wyświetlona lista zainstalowanych zbiorów dokumentacji.

2. Kliknij przycisk **Dalej** znajdujący się u dołu listy zainstalowanej dokumentacji. Zostanie wyświetlona lista zbiorów dokumentacji do zainstalowania. Te zbiory obejmują dokumentację produktu w różnych językach i mogą również obejmować zbiory dokumentacji dla różnych produktów.
3. Wybierz dokumentację, która ma zostać zainstalowana.

Wskazówka: Istnieje możliwość wybrania więcej niż jednego zbioru dokumentacji.

Dokumentacja dla wybranych produktów zostanie zainstalowana w systemie pomocy na komputerze użytkownika.

Rozdział 5. Tworzenie baz danych

Program IBM Business Monitor wymaga używania dwóch baz danych - jednej na potrzeby konfiguracji programu IBM Business Monitor i jednej jako składnicy treści produktu IBM Cognos Business Intelligence.

Bazy danych MONITOR i COGNOSCS

Domyślnie baza danych produktu IBM Business Monitor nosi nazwę MONITOR, a baza danych składnicy treści produktu IBM Cognos BI ma nazwę COGNOSCS.

Bazy danych MONITOR i COGNOSCS można utworzyć w ramach tworzenia profilu autonomicznego lub profilu menedżera wdrażania. W tym celu można też użyć narzędzia do projektowania baz danych (dbDesignGenerator) lub utworzyć te bazy ręcznie, uruchamiając pliki skryptowe bazy danych przed utworzeniem profilu lub po jego utworzeniu. W środowisku wdrożenia sieciowego najlepiej utworzyć bazy danych przed uruchomieniem menedżera wdrażania i utworzeniem profili niestandardowych.

Jeśli istnieje już serwer IBM Cognos BI, nie jest konieczne tworzenie bazy danych COGNOSCS, ponieważ składnica treści jest już zdefiniowana.

Wskazówka: Jeśli baza danych COGNOSCS działa zdalnie względem serwera IBM Cognos BI, należy zainstalować klient bazy danych na serwerze IBM Cognos BI. Szczegółowe informacje zawierają tematy poświęcone uwagom specyficznym dla baz danych.

Bazy danych MONITOR i COGNOSCS mogą znajdować się na tym samym serwerze używanym jako serwer produktu IBM Business Monitor lub na innym serwerze. Aby bazy danych zostały utworzone automatycznie podczas tworzenia profilu, serwer bazy danych musi być lokalny względem komputera, na którym uruchomiono narzędzie Profile Management Tool lub komendę manageprofiles. W przeciwnym razie do utworzenia baz danych należy użyć plików skryptów bazy danych. Plików skryptów bazy danych należy użyć do utworzenia baz danych również wtedy, gdy jest używany system z/OS bądź serwer bazy danych zawiera wiele wersji bazy danych lub wiele jej instancji.

Skrypty bazy danych

Podczas tworzenia profilu autonomicznego lub profilu menedżera wdrażania są generowane skrypty bazy danych zgodne z wartościami wprowadzonymi w trakcie tworzenia profilu, co zapewnia spójność nazw między serwerem programu IBM Business Monitor i bazą danych programu IBM Business Monitor.

Skrypty bazy danych można również utworzyć samodzielnie, używając jednej z następujących metod:

- Skonfigurowanie wartości za pomocą narzędzia do projektowania baz danych (DbDesignGenerator), które jest instalowane z serwerem programu IBM Business Monitor. Jedną z zalet użycia narzędzia do projektowania baz danych jest możliwość jednoczesnego zaprojektowania bazy danych MONITOR, bazy danych produktu IBM Cognos BI, bazy danych produktu Business Space oraz baz danych mechanizmów przesyłania komunikatów programu IBM Business Monitor i infrastruktury CEI (Common Event Infrastructure). Instrukcje można znaleźć w sekcji “Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych” na stronie 54.
- Ręczne skonfigurowanie wartości. Instrukcje można znaleźć w sekcji “Ręczne konfigurowanie skryptów bazy danych” na stronie 56.

Po wygenerowaniu lub dostosowaniu skryptów bazy danych należy je uruchomić zgodnie z procedurami opisanymi w sekcji “Ręczne instalowanie baz danych” na stronie 59.

Tabele mechanizmów przesyłania komunikatów

Mechanizmy przesyłania komunikatów magistrali integracji usług programu IBM Business Monitor i magistrali infrastruktury CEI (Common Event Infrastructure) wymagają tabel bazy danych. Tabele te mogą zostać utworzone automatycznie przez serwer WebSphere Application Server, jeśli użytkownik bazy danych programu IBM Business Monitor ma wystarczające uprawnienia i ustawiono opcję składnicy komunikatów magistrali integracji usług powodującą automatyczne tworzenie tabel. Domyślnie dla tej opcji jest ustawiona wartość true (prawda), chyba że jest używana baza danych DB2 w systemie z/OS. Skrypty bazy danych dla tabel mechanizmu przesyłania komunikatów można również wygenerować, używając jednej z następujących opcji:

- Utworzenie skryptu za pomocą narzędzia do projektowania baz danych (DbDesignGenerator). Instrukcje można znaleźć w sekcji “Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych”.
- Ręczne utworzenie tabel. Instrukcje można znaleźć w sekcji “Ręczne tworzenie tabel mechanizmu przesyłania komunikatów” na stronie 60.

Tabele produktu Business Space

W przypadku używania produktu Business Space należy również skonfigurować tabele produktu Business Space przy użyciu skryptów wygenerowanych podczas tworzenia profilu autonomicznego lub za pomocą narzędzia do projektowania baz danych. Więcej informacji na ten temat zawiera sekcja Konfigurowanie tabel bazy danych produktu Business Space w Centrum informacyjnym produktu Business Space.

Zabezpieczenia bazy danych

Podczas tworzenia baz danych użytkownikowi bazy danych środowiska wykonawczego domyślnie zostają nadane uprawnienia do administrowania obiektami bazy danych. Upraszcza to tworzenie baz danych i pozwala serwerowi programu IBM Business Monitor na automatyczne zarządzanie schematem bazy danych modelu monitorowania w czasie wdrażania i usuwania modeli. W razie konieczności zabezpieczenia baz danych należy zapoznać się z tematami Zabezpieczanie środowiska bazy danych MONITOR i Konfigurowanie zabezpieczeń produktu IBM Cognos BI.

Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych

Do generowania skryptów bazy danych, które mogą być wykonywane przed utworzeniem profilu programu IBM Business Monitor lub po jego utworzeniu, można użyć narzędzia do projektowania baz danych (DbDesignGenerator) zainstalowanego z serwerem programu IBM Business Monitor.

Jedną z zalet użycia narzędzia do projektowania baz danych jest możliwość jednoczesnego zaprojektowania baz danych dla programu IBM Business Monitor, produktu IBM Cognos BI, produktu Business Space i mechanizmu przesyłania komunikatów. Skrypty bazy danych są generowane dla każdego komponentu. Generowany jest również plik dbdesign, który można później przekazać do kreatora środowiska wdrażania w celu automatycznego skonfigurowania źródeł danych podczas tworzenia złożonej topologii programu IBM Business Monitor.

W przypadku wybrania ścieżki **Advanced** (Zaawansowane) w narzędziu Profile Management Tool, można wybrać opcję **Configure the database using a design file** (Skonfiguruj bazę danych przy użyciu pliku projektu) i wybrać utworzony wcześniej plik projektu.

Więcej informacji na temat narzędzia do projektowania baz danych można uzyskać na stronach pokrewnych.

Aby edytować pliki skryptu bazy danych za pomocą narzędzia do projektowania baz danych, wykonaj następujące kroki:

1. Przejdź do katalogu `catalog_główny_serwera_aplikacji/util/dbUtils`.
2. Wykonaj następującą komendę, aby uruchomić program narzędziowy.
 - `DbDesignGenerator.bat`
 - `DbDesignGenerator.sh`
3. Z menu głównego wybierz opcję **(1) Create a database design for Standalone profile or Deployment Environment** (1. Utwórz projekt bazy danych dla profilu autonomicznego lub środowiska wdrażania).
4. W odpowiedzi na zachętę **Please pick one of the following db designs that are supported** (Wybierz jeden z następujących obsługiwanych projektów bazy danych) wybierz opcję **(1)monitor.nd.topology** lub **(2)monitor.standalone**. Opcja `monitor.nd.topology` zapewnia elastyczniejszą dystrybucję komponentów bazy danych w wielu bazach danych.
5. W odpowiedzi na zachętę **Please pick one of the following [database component(s)]** (Wybierz jeden z następujących komponentów bazy danych) wybierz opcję **(1)[Monitor] MONITOR : [master] [status = not complete]** (1 [Monitor] MONITOR : [główny] [status = niezakończone]).
6. W odpowiedzi na zachętę **Edit this db component?** (Czy edytować ten komponent bazy danych?) wpisz `y`.
7. W odpowiedzi na zachętę **Please pick one of the following DB types that are supported** (Wybierz jeden z następujących obsługiwanych typów bazy danych) wybierz liczbę oznaczającą daną platformę bazy danych.
8. Odpowiedz na serię pytań lub naciśnij klawisz Enter, aby zaakceptować wartości domyślne tam, gdzie będzie to możliwe. Użytkownik zostanie poproszony o wpisanie nazwy bazy danych, nazwy schematu, nazwy użytkownika, hasła i przedrostka katalogu położenia obszaru tabel.
9. Aby kontynuować wprowadzanie informacji, w odpowiedzi na zachętę **To skip data source properties, enter 's'; or enter anything else to continue** (Aby pominąć właściwości źródła danych, naciśnij klawisz `s`. Aby kontynuować, naciśnij dowolny inny klawisz), wpisz `c` (lub dowolny inny znak oprócz `S`).
10. Odpowiedz na serię pytań lub naciśnij klawisz Enter, aby zaakceptować wartości domyślne tam, gdzie będzie to możliwe. Użytkownik zostanie poproszony o wprowadzenie właściwości źródła danych.
11. Przed skonfigurowaniem innych komponentów sprawdź, czy zakończono konfigurowanie komponentu bazy danych produktu IBM Business Monitor. Baza danych produktu IBM Cognos BI jest wyświetlana ze statusem niezakończony oraz wymaga podania nazwy i hasła użytkownika bazy danych. Dla innych ustawień można zaakceptować wartości domyślne.
12. Gdy ponownie zostanie wyświetlona zachęta **Please pick one of the following [database component(s)]** (Wybierz jeden z następujących komponentów bazy danych), wprowadzanie właściwości zostało zakończone, jeśli we wszystkich wierszach jest wyświetlana wartość **[status = complete]** ([status = zakończone]), na przykład **(1)[Monitor] MONITOR : [master] [status = complete]** (1. [Monitor] MONITOR :

[główny] [status = zakończone]). Wprowadź wartość **5 [save and exit]** (5 [zapisz i wyjdź]) i naciśnij klawisz Enter, aby zapisać projekt bazy danych.

Komponent bazy danych [**Cognos**] **COGNOSCS** wymaga dodatkowej konfiguracji po zakończeniu konfigurowania bazy danych MONITOR. Status [**status = not complete**] ([status = niezakończony]) bazy danych COGNOSCS nie zmieni się do momentu całkowitego skonfigurowania tego komponentu.

13. W odpowiedzi na zachętę **Please enter the output directory** (Wprowadź katalog wyjściowy) naciśnij klawisz Enter, aby zaakceptować wartość domyślną (`katalog_główny_serwera_aplikacji/util/dbUtils`) lub wprowadź położenie, w którym pliki projektu bazy danych mają zostać zapisane.
14. W odpowiedzi na zachętę **Please enter the output filename** (Wprowadź nazwę pliku wyjściowego) naciśnij klawisz Enter, aby zaakceptować wartość domyślną (`monitor.standalone.dbdesign`) lub wpisz nazwę pliku.
15. W odpowiedzi na zachętę **Generate db script?** (Czy wygenerować skrypt bazy danych?) wpisz **y** i naciskaj klawisz Enter, aby zaakceptować położenia domyślne. Zostaną utworzone podkatalogi dla skryptów baz danych MONITOR i COGNOSCS, skryptu składnicy danych mechanizmu przesyłania komunikatów i skryptów bazy danych produktu Business Space.

Ręczne konfigurowanie skryptów bazy danych

Skrypty bazy danych wymagane do utworzenia baz danych MONITOR i COGNOSCS są dostarczane na nośniku instalacyjnym i kopiowane na serwer aplikacji podczas instalowania serwera programu IBM Business Monitor. Te skrypty bazy danych można dostosować ręcznie w taki sposób, aby można było utworzyć bazy danych przed zainstalowaniem serwera lub utworzeniem profilu.

Aby ręcznie edytować skrypty bazy danych, wykonaj następujące kroki:

1. Za pomocą edytora tekstu otwórz plik skryptu bazy danych dla oprogramowania bazy danych. Skrypt `createDatabase.sql` tworzy bazę danych i wszystkie wymagane tabele dla produktu IBM Business Monitor. Dostępne są następujące pliki:

Tworzenie bazy danych: `createDatabase.sql`

Tworzenie tabel (dotyczy tylko bazy danych MONITOR): `createTables.sql`

Domyślnie pliki znajdują się w następujących katalogach:

(tylko rozproszone) `katalog_główny_dysku_DVD/scripts/database/Monitor/platforma`

`katalog_główny_dysku_DVD/scripts/database/Cognos/platforma`

`katalog_główny_serwera_aplikacji/dbscripts/Monitor`

`katalog_główny_serwera_aplikacji/dbscripts/Cognos`

`katalog_główny_serwera_aplikacji/profiles/nazwa_profilu/dbscripts/Monitor`
(autonomiczny)

`katalog_główny_serwera_aplikacji/profiles/nazwa_profilu/dbscripts.wbm` (menedżer wdrażania)

`katalog_główny_serwera_aplikacji/profiles/nazwa_profilu/dbscripts/Cognos`

Gdzie:

`katalog_główny_dysku_DVD` to katalog, do którego rozpakowano zawartość dysku DVD lub pobrany obraz

`platforma` to system operacyjny bazy danych (na przykład DB2, Oracle lub SQL Server)

`katalog_główny_serwera_aplikacji` to katalog, w którym zainstalowano produkt IBM Business Monitor

2. Zmodyfikuj następujące zmienne w plikach skryptów bazy danych dla używanego oprogramowania bazy danych:

- W przypadku bazy danych DB2 dokonaj edycji następujących zmiennych:

@DB_NAME@

Reprezentuje nazwę bazy danych programu IBM Business Monitor (na przykład MONITOR lub Cognos).

@SCHEMA@

Reprezentuje nazwę schematu programu IBM Business Monitor (na przykład MONITOR lub Cognos).

@TSDIR@

Reprezentuje katalog obszaru tabel.

Jeśli zmienna @TSDIR@ zostanie pominięta w specyfikacji pliku danych obszaru tabel, plik danych jest tworzony w katalogu menedżera bazy danych.

@DB_USER@

Reprezentuje użytkownika bazy danych środowiska wykonawczego programu IBM Business Monitor.

- W przypadku bazy danych DB2 for z/OS zmodyfikuj następujące zmienne:

@STOGRP@

Reprezentuje nazwę grupy pamięci masowej bazy danych DB2, na przykład: SYSDEFLT.

@DB_NAME@

Reprezentuje nazwę bazy danych produktu IBM Business Monitor.

@SCHEMA@

Reprezentuje nazwę kwalifikatora schematu programu IBM Business Monitor.

@DB_USER@

Reprezentuje użytkownika bazy danych środowiska wykonawczego programu IBM Business Monitor.

- W przypadku bazy danych SQL Server dokonaj edycji następujących zmiennych:

@DB_NAME@

Reprezentuje nazwę bazy danych produktu IBM Business Monitor, na przykład: MONITOR.

@SCHEMA@

Reprezentuje nazwę schematu produktu IBM Business Monitor, na przykład: MONITOR.

@DB_USER@

Reprezentuje użytkownika bazy danych środowiska wykonawczego programu IBM Business Monitor.

@DB_PASSWORD@

Reprezentuje hasło użytkownika bazy danych środowiska wykonawczego programu IBM Business Monitor. Użytkownika bazy danych i hasło można utworzyć przed uruchomieniem skryptu lub tak zaprojektować skrypt, aby tworzył użytkownika bazy danych i hasło. Jeśli użytkownik bazy danych i hasło mają być tworzone przy użyciu skryptu, należy w nim określić zmienną @DB_PASSWORD@.

- W przypadku bazy danych Oracle dokonaj edycji następujących zmiennych:

@SCHEMA@

Reprezentuje nazwę użytkownika bazy danych, który jest właścicielem tabel bazy danych produktu IBM Business Monitor.

@DB_PASSWORD@

Reprezentuje hasło dla użytkownika bazy danych zidentyfikowanego przez zmienną \$\$SCHEMA\$.

@TSDIR@

Reprezentuje katalog obszaru tabel.

Jeśli zmienna @TSDIR@ zostanie pominięta w specyfikacji pliku danych obszaru tabel, plik danych jest tworzony w katalogu menedżera bazy danych. Jeśli dla zmiennej @TSDIR@ określono pełną ścieżkę, katalog musi istnieć przed wywołaniem skryptu.

@DB_USER@

Reprezentuje użytkownika bazy danych środowiska wykonawczego programu IBM Business Monitor.

Obszary tabel są tworzone w pliku createDatabase.sql. Jeśli domyślne nazwy obszarów tabel będą zastępowane własnymi, podczas wdrażania modeli należy wyeksportować skrypty schematów modeli i zmodyfikować je tak, aby odwoływały się do wybranych nazw obszarów tabel.

Uwaga: Dotyczy wyłącznie bazy danych MONITOR: jeśli w ramach jednej instalacji bazy danych Oracle jest konfigurowana dodatkowa instancja monitorowania, konieczne jest również zastąpienie łańcucha DEFAULTTS w skrypcie createDatabase.sql unikalnym identyfikatorem tej dodatkowej instancji monitorowania w następujących czterech wierszach:

```
CREATE TABLESPACE MONDSTS
  DATAFILE 'DEFAULTTS_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONDMSTS
  DATAFILE 'DEFAULTTS_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONIDXTS
  DATAFILE 'DEFAULTTS_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONLOBTS
  DATAFILE 'DEFAULTTS_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON
NEXT 40M MAXSIZE UNLIMITED LOGGING; ;
```

Jeśli na przykład unikalnym identyfikatorem dodatkowej instancji monitorowania jest MONDEV1_MONDSTS, zmienione wiersze będą wyglądać następująco:

```
CREATE TABLESPACE MONDSTS
  DATAFILE 'MONDEV1_MONDSTS.dbf' SIZE 500M AUTOEXTEND ON
NEXT 100M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONDMSTS
  DATAFILE 'MONDEV1_MONDMSTS.dbf' SIZE 100M AUTOEXTEND ON
NEXT 20M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONIDXTS
  DATAFILE 'MONDEV1_MONIDXTS.dbf' SIZE 250M AUTOEXTEND ON
NEXT 50M MAXSIZE UNLIMITED LOGGING;
```

```
CREATE TABLESPACE MONLOBTS
  DATAFILE 'MONDEV1_MONLOBTS.dbf' SIZE 200M AUTOEXTEND ON NEXT 40M MAXSIZE UNLIMITED LOGGING;
```

Tę procedurę należy powtórzyć dla wszystkich dodatkowych instancji monitorowania.

Uwaga: W programie IBM Business Monitor 6.2. są używane obszary tabel inne niż w poprzednich wersjach. W związku z tym, jeśli jest używana baza danych Oracle i jest planowane wdrożenie modelu w wersji 6.1 w produkcie IBM Business Monitor 7.5, należy wybrać jedną z poniższych opcji:

- Uruchomienie instrukcji obszaru tabel o wersji 6.1 podczas instalacji bazy danych w wersji 7.5.
- Wyeksportowanie skryptu bazy danych modelu i ręczna zmiana odwołań do obszaru tabel tak, aby wskazywały nazwy obszaru tabel w wersji 7.0, przeprowadzone podczas wdrażania modelu monitorowania. Jeśli zostanie wybrana druga opcja, należy ją stosować zawsze wtedy, gdy model w wersji 6.1 jest wdrażany na serwerze w wersji 7.0.

Prostą metodą uniknięcia tego problemu jest przeprowadzenie migracji z wersji 6.1 do wersji 7.5 z wdrożonymi istniejącymi modelami i wygenerowanie nowych modeli za pomocą pakietu IBM Business Monitor Development Toolkit w wersji 6.2 lub 7.5. Odzworowanie nazw obszarów tabel przedstawiono w poniższej tabeli.

Tabela 3. Odzworowanie nazw obszarów tabel z poprzednich wersji produktu IBM Business Monitor

| Bieżący obszar tabel | Obszar tabel 6.1.x |
|----------------------|--------------------|
| MONDSTS | INSTANCE |
| MONDMSTS | DMSTS |
| MONIDXTS | INDEXTS |
| MONLOBTS | LOBTS |

3. Zapisz i zamknij plik.

Ręczne instalowanie baz danych

Korzystając ze skryptów bazy danych, użytkownik może ręcznie zainstalować bazy danych składnicy treści produktu IBM Cognos Business Intelligence i programu IBM Business Monitor na tym samym serwerze co serwer programu IBM Business Monitor lub jako zdalne bazy danych na innym serwerze. Przed uruchomieniem skryptów bazy danych należy się upewnić, że skonfigurowano w nich zmienne specyficzne dla środowiska - ręcznie lub przy użyciu narzędzia do projektowania bazy danych.

Przed wykonaniem tej czynności należy zapoznać się z sekcją Zagadnienia dotyczące baz danych oraz ze wszystkimi wymaganiami wstępnymi konkretnej bazy danych. Jeśli na przykład jest używana baza danych DB2 for z/OS, dla programu IBM Business Monitor jest zalecana dedykowana grupa pamięci masowej (STOGROUP). Konieczne jest utworzenie grupy pamięci masowej przed utworzeniem bazy danych.

Wykonaj następujące kroki na serwerze, na którym zainstalowano oprogramowanie bazy danych:

1. Zaloguj się na serwerze bazy danych jako użytkownik mający uprawnienia do tworzenia obszarów tabel i obiektów bazy danych.
2. Znajdź skrypty DDL.
 - Jeśli mają być używane skrypty dostarczone podczas instalacji programu IBM Business Monitor, znajdują się one w katalogach katalog_główny_serwera_aplikacji/dbscripts/Monitor i katalog_główny_serwera_aplikacji/dbscripts/Cognos.
 - Jeśli do wygenerowania skryptów z podstawionymi wartościami zmiennych użytkownika użyto programu DbDesignGenerator, skrypty znajdują się w katalogu

- wyjściowym wybranym podczas uruchamiania tego programu narzędziowego (domyślnie katalog_główny_serwera_aplikacji/util/dbUtils).
- Jeśli skrypty z podstawionymi wartościami zmiennych użytkownika zostały wygenerowane przez utworzenie profilu, znajdują się one w katalogu wyjściowym wybranym podczas tworzenia profilu (domyślnie katalog_główny_serwera_aplikacji/profiles/<profil>/dbscripts/Monitor).
3. Z poziomu interfejsu wiersza komend uruchom dwukrotnie skrypt createDatabase, po jednym razie dla bazy danych MONITOR i bazy danych COGNOSCS, używając w tym celu następującej komendy w zależności od używanego oprogramowania bazy danych. Skrypt createDatabase tworzy bazę danych i wszystkie wymagane tabele dla produktu IBM Business Monitor.
 - **DB2:** db2 -tf createDatabase.sql
 - **DB2 for z/OS:** db2 -tf createDatabase.sql. Skrypt bazy danych można uruchomić przy użyciu programu narzędziowego SPUFI lub DSNTPE2.
 - **Microsoft SQL Server:** sqlcmd -U administrator_bazy_danych -P hasło -e -i createDatabase.sql, gdzie
administrator_bazy_danych to użytkownik bazy danych SQL Server z uprawnieniami administracyjnymi
 4. Dla bazy danych MONITOR uruchom skrypt createTables za pomocą jednej z następujących komend: Nie jest konieczne tworzenie tabel dla bazy danych produktu IBM Cognos BI:
 - **DB2:**

```
db2 connect to MONITOR
db2 -tf createTables.sql
db2 connect reset
```

Uwaga: Podczas uruchamiania pliku DDL może zostać wyświetlony następujący komunikat ostrzegawczy: SQL0347W Rekurencyjne wyrażenie tabelowe MON023.WBITIME może zawierać nieskończoną pętlę. SQLSTATE=01605. Ten komunikat można bezpiecznie zignorować.

 - **Oracle:** sqlplus *użytkownik/hasło@nazwa_bazy_danych @createTables.sql*
 - **Microsoft SQL Server:** sqlcmd -U *użytkownik* -P *hasło* -e -i createTables.sql
 5. Uruchom serwer WebSphere Application Server.

Ręczne tworzenie tabel mechanizmu przesyłania komunikatów

Tabele magistrali integracji usług należy utworzyć ręcznie, jeśli nie zostały utworzone automatycznie dla mechanizmu przesyłania komunikatów produktu IBM Business Monitor podczas tworzenia profilu autonomicznego bądź podczas korzystania z kreatora konfiguracji środowiska wdrażania lub kreatora konfiguracji. Tabele należy również utworzyć ręcznie, jeśli na potrzeby składnicy danych mechanizmu przesyłania komunikatów jest używana baza danych DB2 for z/OS.

Użytkownik może również utworzyć tabelę mechanizmu przesyłania komunikatów infrastruktury CEI. Podczas tworzenia środowiska wdrażania programu są generowane skrypty bazy danych dla infrastruktury CEI. Jeśli ma zostać włączona składnica zdarzeń infrastruktury CEI, skrypty należy uruchomić ręcznie w celu zakończenia konfigurowania (nie jest to zalecane w środowiskach produkcyjnych).

Do generowania skryptów dla tabel magistrali integracji usług w wersji 7.5 należy użyć narzędzia do projektowania baz danych (DbDesignGenerator).

Alternatywnie można również użyć programu narzędziowego sibDDLGenerator. Na przykład komenda generująca skrypty DDL SIB dla bazy danych DB2 for z/OS to sibDDLGenerator -system db2 -version 8.1 -platform zos.

W dokumentacji komendy sibDDLGenerator znajdują się informacje o obsługiwanych wersjach bazy danych DB2. Nie jest to lista wszystkich wersji bazy danych DB2 obsługiwanych przez produkt IBM Business Monitor. Jednak można określić wersję 8.1, tak jak w powyższym przykładzie, i wynikowy skrypt DDL powinien być zgodny ze wszystkimi obsługiwanyymi wersjami.

Ponieważ program IBM Business Monitor może zawierać zarówno mechanizm przesyłania komunikatów infrastruktury CEI, jak i mechanizm przesyłania komunikatów programu IBM Business Monitor (każdy tworzony z tym samym obszarem tabel i nazwami tabel), należy się upewnić, że są używane dwie różne bazy danych lub dwie różne nazwy schematów.

Rozdział 6. Tworzenie i rozszerzanie profili

Po zainstalowaniu produktu IBM Business Monitor należy utworzyć co najmniej jeden profil w celu przygotowania środowiska wykonawczego. Profile można tworzyć i rozszerzać za pomocą narzędzia Profile Management Tool lub przy użyciu komendy `manageprofiles`.

Jeśli jest używana 64-bitowa wersja produktu IBM Business Monitor, należy użyć komendy `manageprofiles`. Jeśli jest używany system z/OS, nie można skorzystać z komendy lub narzędzia Profile Management Tool. Należy wyświetlić temat Tworzenie wspólnych konfiguracji dla programu IBM Business Monitor for z/OS.

Dostępne są trzy typy profili: profil serwera autonomicznego, profil menedżera wdrażania (profil zarządzania z serwerem menedżera wdrażania) oraz profil niestandardowy (węzeł zarządzany). Każdy profil definiuje oddzielne środowisko wykonawcze zawierające osobne pliki (komendy, pliki konfiguracyjne i pliki dziennika).

Tworzenie i rozszerzanie profili przy użyciu narzędzia Profile Management Tool

Narzędzie Profile Management Tool umożliwia tworzenie i rozszerzanie profili służących do zarządzania środowiskiem wykonawczym.

Ograniczenie: Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, należy użyć komendy `manageprofiles`. Interfejs użytkownika narzędzia Profile Management Tool jest niedostępny dla wersji 64-bitowych. Jeśli jest używany system z/OS, należy wyświetlić temat Tworzenie wspólnych konfiguracji dla programu IBM Business Monitor for z/OS.

W przypadku środowiska jednoserwerowego należy utworzyć profil autonomiczny.

W przypadku środowiska wdrażania sieciowego wykonaj następujące kroki:

1. Przed utworzeniem innych profili należy utworzyć profil menedżera wdrażania. Jeśli profil menedżera wdrażania utworzono przed zainstalowaniem produktu IBM Business Monitor (na przykład dla produktu WebSphere Application Server lub Process Server) i jeśli planowane jest używanie tego samego profilu menedżera wdrażania do zarządzania węzłami produktu IBM Business Monitor, należy rozszerzyć profil przy użyciu szablonu udostępnionego w produkcie IBM Business Monitor.
2. Profil niestandardowy należy utworzyć dla każdego węzła, który ma zostać dodany do klastra serwerów. Można również rozszerzyć istniejący profil niestandardowy dla każdego węzła, który ma zostać dodany.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

W przypadku korzystania z bazy danych Oracle obsługa interfejsu JDBC jest zapewniana przez sterowniki JDBC Oracle dla maszyny JVM 1.6. Plik sterownika JDBC `ojdbc6.jar` jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku `ojdbc6.jar` można użyć zarówno dla produktu

Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

Domyślnie narzędzie Profile Management Tool wskazuje plik `ojdbc6.jar` udostępniony w katalogu `katalog_główny_serwera_aplikacji\jdbcdrivers\Oracle`. Zamiast niego można pobrać inny plik `ojdbc6.jar` sterownika JDBC bazy danych Oracle i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy `manageprofiles`.

W przypadku korzystania z bazy danych SQL Server obsługa interfejsu JDBC jest zapewniana przez sterowniki JDBC SQL Server dla maszyny JVM 1.6. W produkcie IBM Business Monitor używany jest plik `sqljdbc4.jar` sterownika Microsoft JDBC 2.0. Domyślnie narzędzie Profile Management Tool wskazuje plik `sqljdbc4.jar` udostępniony w katalogu `katalog_główny_serwera_aplikacji\jdbcdrivers\SQLServer`. Zamiast niego można pobrać inny plik `sqljdbc4.jar` sterownika JDBC Microsoft i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy `manageprofiles`. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.





Tworzenie profili autonomicznych

Jeśli podczas instalowania pojedynczego serwera nie utworzono profilu programu IBM Business Monitor, konieczne jest jego utworzenie. Ten profil zostanie utworzony w katalogu profili serwera WebSphere Application Server.

Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.

Aby utworzyć profil autonomicznego serwera aplikacji, wykonaj następujące kroki przy użyciu narzędzia Profile Management Tool:


1. Przy użyciu jednej z następujących metod otwórz narzędzie Profile Management Tool:
 - W konsoli Pierwsze kroki programu IBM Business Monitor kliknij opcję **Narzędzie Profile Management Tool**.
 -  Kliknij opcję **Start > Programy > IBM > Business Monitor7.5 > Profile Management Tool**.
 -  Uruchom plik `pmt.bat`, który znajduje się w następującym katalogu: `katalog_główny_serwera_aplikacji\bin\ProfileManagement`.
 -   Przejdź do katalogu `katalog_główny_serwera_aplikacji/bin/ProfileManagement` i wpisz komendę `./pmt.sh` w oknie terminalu.
2. Na panelu Witamy w narzędziu Profile Management Tool przejrzyj podane informacje i kliknij przycisk **Uruchom narzędzie Profile Management Tool**.
3. Na panelu Profile kliknij przycisk **Utwórz**, aby utworzyć nowy profil.
4. Na panelu Wybór środowiska rozwiń listę IBM Business Monitor i kliknij opcję **Autonomiczny serwer programu Monitor**, a następnie kliknij przycisk **Dalej**.

Ograniczenie: Jeśli opcja programu IBM Business Monitor nie jest wyświetlana, może to oznaczać, że używana jest wersja 64-bitowa. Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, nie można korzystać z narzędzia Profile Management Tool i należy użyć komendy `manageprofiles`.

5. Na panelu Opcje tworzenia profilu wybierz żądany typ instalacji i kliknij przycisk **Dalej**.
 - **Typowe tworzenie profilu** (wartość domyślna): Powoduje utworzenie profilu programu IBM Business Monitor korzystającego z domyślnych ustawień konfiguracyjnych. Narzędzie Profile Management Tool przypisuje unikalne nazwy do profilu, węzła i komórki. Narzędzie to instaluje również Konsolę administracyjną i domyślne aplikacje oraz przypisuje unikalne wartości portów. Podczas konfigurowania istnieje możliwość włączenia zabezpieczeń administracyjnych. W zależności od systemu operacyjnego i uprawnień użytkownika narzędzie może utworzyć usługę systemową uruchamiającą program IBM Business Monitor.
 - **Zaawansowane tworzenie profilu**: Powoduje utworzenie profilu programu IBM Business Monitor przy użyciu domyślnych ustawień konfiguracyjnych lub umożliwia użytkownikowi określenie komponentów programu IBM Business Monitor. Użytkownik może przypisać własne wartości portów. Istnieje możliwość wdrożenia Konsoli administracyjnej i aplikacji przykładowych oraz utworzenia definicji serwera WWW. W zależności od systemu operacyjnego i uprawnień użytkownika można wybrać opcję uruchamiania programu IBM Business Monitor jako usługi systemowej. Możliwe jest określenie konfiguracji modelu programu IBM Business Monitor. Istnieje możliwość określenia pliku projektu bazy danych lub przypisania własnych wartości konfiguracyjnych bazy danych programu IBM Business Monitor. . Możliwe jest wybranie konfiguracji produktu IBM Cognos BI na potrzeby analizy danych wielowymiarowych.
6. W przypadku wybrania opcji **Typowe tworzenie profilu** przejdź do kroku Krok 11: Panel Zabezpieczenia administracyjne.
7. Zaawansowane: na panelu Wdrażanie opcjonalnych aplikacji wybierz opcję **Przeprowadź wdrożenie Konsoli administracyjnej i Przeprowadź wdrożenie domyślnej aplikacji**. Aplikacją domyślną jest aplikacja serwera WebSphere Application Server. Kliknij przycisk **Dalej**.
8. Zaawansowane: na panelu Nazwa i położenie profilu zaakceptuj domyślną nazwę i położenie lub określ nazwę profilu oraz ścieżkę do katalogu, który będzie zawierał pliki środowiska wykonawczego (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Domyślna nazwa profilu to WBMon01. W systemie Windows katalog typowego profilu to C:\IBM\WebSphere\AppServer\profiles\WBMon01.
9. Zaawansowane: ustaw poziom dostrajania wydajności odpowiedni dla tworzonego profilu. Ten parametr jest parametrem serwera WebSphere Application Server. Więcej informacji na ten temat zawiera sekcja Strojenie serwera aplikacji w Centrum informacyjnym serwera WebSphere Application Server.
10. Zaawansowane: Na panelu Nazwy węzła i hosta wpisz nowe wartości lub zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**.
 - Nazwa węzła jest używana na potrzeby administrowania. Jeśli węzeł jest stowarzyszony, jego nazwa musi być unikalna w obrębie komórki.
 - Nazwa serwera jest nazwą logiczną dla serwera programu IBM Business Monitor.
 - Nazwa hosta jest nazwą DNS (krótką lub długą) albo adresem IP tego komputera.
 - Nazwa komórki jest nazwą logiczną dla grupy węzłów administrowanych przez ten menedżer wdrażania.
11. Na panelu Zabezpieczenia administracyjne wybierz jedną z następujących opcji, a następnie kliknij przycisk **Dalej**.
 - Aby włączyć zabezpieczenia, zaznacz pole wyboru **Włącz zabezpieczenia administracyjne** oraz wpisz nazwę użytkownika i hasło.
 - Aby wyłączyć zabezpieczenia, usuń zaznaczenie pola wyboru **Włącz zabezpieczenia administracyjne**.

Informacje umożliwiające określenie, czy należy włączyć zabezpieczenia znajdują się w sekcji Administrative security (Zabezpieczenia administracyjne) Centrum informacyjnego serwera WebSphere Application Server.

W przypadku wybrania opcji **Typowe tworzenie profilu** przejdź do kroku Krok 21: Panel Konfiguracja bazy danych.

12. Zaawansowane: Na panelu Certyfikat bezpieczeństwa (część 1) wybierz, czy ma zostać utworzony domyślny certyfikat osobisty oraz główny certyfikat podpisywania, czy też ma zostać przeprowadzone importowanie z magazynu kluczy. W celu tworzenia nowych certyfikatów kliknij przycisk **Dalej**, aby przejść do strony weryfikacji. W celu zaimportowania istniejących certyfikatów z magazynów kluczy wskaż certyfikaty i kliknij przycisk **Dalej**, aby przejść do strony weryfikacji.
13. Zaawansowane: Na panelu Certyfikat bezpieczeństwa (część 2) zmodyfikuj informacje dotyczące certyfikatu, aby utworzyć nowe certyfikaty podczas tworzenia profilu. Jeśli są importowane istniejące certyfikaty z magazynów kluczy, użyj tych informacji, aby sprawdzić, czy wybrane certyfikaty zawierają odpowiednie informacje. Jeśli wybrane certyfikaty ich nie zawierają, kliknij przycisk **Wstecz**, aby zaimportować inne certyfikaty. W celu zabezpieczenia plików kluczy oraz certyfikatów SSL należy zmienić domyślne hasło magazynu kluczy. Więcej informacji na temat zabezpieczania komunikacji między serwerem i klientem można znaleźć w temacie Securing communications (Zabezpieczanie komunikacji) w Centrum informacyjnym serwera WebSphere Application Server.
14. Zaawansowane: Na panelu Przypisywanie wartości portów przejrzyj wartości portów, które zostaną przypisane podczas tworzenia profilu. Numery portów można zanotować. Zaakceptuj podane wartości lub określ inne numery portów i kliknij przycisk **Dalej**.
15.  Zaawansowane: w systemach Windows jest wyświetlany panel Definicja usługi systemu Windows. Opcja **Uruchom proces serwera aplikacji jako usługę systemu Windows** jest domyślnie włączona i skonfigurowana w taki sposób, aby do logowania używała informacji z lokalnego konta systemowego. Zaakceptuj ustawienia domyślne usługi systemu Windows lub wyłącz tę opcję, a następnie kliknij przycisk **Dalej**. Aby zmienić informacje logowania usługi systemu Windows, należy wybrać opcję **Zaloguj jako określone konto użytkownika** i wprowadzić nazwę użytkownika oraz hasło alternatywnego konta.

Dla usługi systemu Windows opcja **Typ uruchamiania** jest domyślnie ustawiana na wartość **Automatyczne**. Korzystając z listy, można zmienić wartość opcji **Typ uruchamiania** na wartość **Ręczne** lub **Wyłączone**.

Ponieważ w systemach operacyjnych Windows usługi są ustawiane globalnie, każdy profil może uruchomić usługę. To utrudnia śledzenie, który profil wydał na przykład komendę "startServer". Aby uniknąć potencjalnych konfliktów żądania usług występujących między różnymi profilami, należy wyłączyć opcję **Uruchom proces serwera aplikacji jako usługę systemu Windows**.

16. Zaawansowane: Na panelu Definicja serwera WWW wybierz jedną z następujących opcji:
 - Aby utworzyć definicję serwera WWW, zaznacz opcję **Utwórz definicję serwera WWW**. Zaakceptuj udostępnione informacje o serwerze WWW lub wprowadź konieczne modyfikacje.

Typ serwera WWW

Dostępne są następujące opcje: IBM HTTP Server, Microsoft Internet Information Services, Sun Java System, Lotus Domino Web Server oraz Apache Web Server.

System operacyjny serwera WWW

Dostępne są następujące opcje: Windows, AIX, HP, Solaris oraz z/OS.

Nazwa serwera WWW

Należy wprowadzić nazwę serwera WWW. Nazwą domyślną jest "webserv1".

Nazwa hosta lub adres IP serwera WWW

Należy wprowadzić nazwę hosta lub adres IP serwera WWW. Domyślnie wyświetlana jest nazwa hosta lokalnego.

Port serwera WWW (domyślnie 80)

Należy wprowadzić numer portu serwera WWW lub zaakceptować wartość domyślną (80).

- Aby nie tworzyć definicji serwera WWW, usuń zaznaczenie pola wyboru **Utwórz definicję serwera WWW**.

Definicje serwera WWW określają serwer WWW zewnętrzny względem serwera WebSphere Application Server, co umożliwia zarządzanie plikami konfiguracyjnymi wtyczek serwera WWW, a w niektórych przypadkach także zarządzanie serwerem WWW. Jeśli serwer WWW nie został zainstalowany lub odłożono to na później, można to łatwo zrobić przy użyciu Konsoli administracyjnej.

17. Zaawansowane: Na panelu Definicja serwera WWW (część 2) wpisz ścieżkę do katalogu instalacyjnego serwera WWW i ścieżkę do katalogu instalacyjnego wtyczek serwera WWW.
18. Zaawansowane: na panelu Modele monitorowania produktu IBM Business Process Manager wybierz opcję **Wdróż model monitorowania procesu globalnego produktu IBM Business Monitor**, aby zainstalować i skonfigurować aplikację modelu monitorowania procesu globalnego. Ten model umożliwia monitorowanie procesów BPEL lub BPMN uruchomionych w produkcie IBM Business Process Manager bez generowania i wdrażania modeli monitorowania.

Aby zainstalować i skonfigurować aplikację czynności personelu, należy kliknąć opcję **Wdróż model monitorowania czynności personelu (wymaga produktu IBM Business Process Manager Advanced)**. Aplikacja czynności personelu jest wymagana do wyświetlenia czynności personelu na panelu kontrolnym przy użyciu widgetu Czynności personelu. Aby zainstalować te aplikacje, konieczne jest podanie nazwy hosta i numeru portu RMI istniejącego produktu IBM Business Process Manager. Domyślny numer portu to 2809. Przed kontynuowaniem tworzenia lub rozszerzania profilu musi istnieć baza danych albo należy umożliwić utworzenie bazy danych MONITOR przez narzędzie Profile Management Tool.

Jeśli te aplikacje nie zostaną zainstalowane podczas instalacji, można je zainstalować później, postępując zgodnie z instrukcjami zamieszczonymi w sekcjach Konfigurowanie monitorowania czynności personelu i Konfigurowanie modelu monitorowania procesu globalnego.

19. Zaawansowane: Na panelu Konfiguracja produktu Business Space wybierz opcję **Konfiguruj produkt Business Space** w celu wdrożenia struktury produktu Business Space i zarejestrowania w ramach niej widgetów programu IBM Business Monitor.
20. Opcjonalne: Zaawansowane: skonfiguruj bazy danych przy użyciu pliku projektu.
 - a. Wybierz opcję **Użyj pliku projektu bazy danych w celu skonfigurowania bazy danych**, jeśli ma zostać użyty plik projektu zamiast określania parametrów bazy danych na poniższych panelach.
 - b. Kliknij przycisk **Przeglądaj**.
 - c. Podaj pełną ścieżkę do pliku projektu.
 - d. Kliknij przycisk **Dalej**.
 - e. Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli podczas tworzenia profilu lokalne bazy danych nie mają zostać utworzone i

skonfigurowane automatycznie lub tabele nie mają zostać utworzone w istniejących bazach danych. Jeśli nie zaznaczono tego pola wyboru, lokalne bazy danych zostaną utworzone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch @DB_PASSWORD@ hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

Jeśli zostanie wskazany plik projektu, panele konfiguracji bazy danych narzędzia Profile Management Tool zostaną pominięte. Położenie pliku projektu zostanie wówczas przekazane do wiersza komend, aby zakończyć procedurę konfigurowania bazy danych. Więcej informacji na temat konfigurowania bazy danych za pomocą pliku projektu zawiera temat Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych.

21. Na panelu Konfiguracja bazy danych sprawdź informacje dotyczące konfiguracji bazy danych MONITOR:
 - a. Wybierz bazę danych z listy **Produkt bazy danych**.
 - b. Aby określić katalog docelowy dla wygenerowanych skryptów, włącz opcję **Zastąp katalog docelowy dla wygenerowanych skryptów** i wprowadź ścieżkę w polu **Katalog danych wyjściowych skryptu bazy danych**. Domyślny katalog to katalog_główny_programu_Monitor\profiles\WBMon01\dbscripts\Monitor\platforma\.
 - c. Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli podczas tworzenia profilu lokalne bazy danych nie mają zostać utworzone i skonfigurowane automatycznie lub tabele nie mają zostać utworzone w istniejących bazach danych. Jeśli nie zaznaczono tego pola wyboru, lokalne bazy danych zostaną utworzone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch @DB_PASSWORD@ hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.
 - d. W polu **Nazwa bazy danych** wprowadź nazwę bazy danych lub zaakceptuj nazwę domyślną (MONITOR).
 - e. W polu **Nazwa schematu** wpisz nazwę schematu lub zaakceptuj nazwę domyślną (MONITOR). Jeśli używana jest baza danych DB2 w systemie z/OS, nazwa schematu bazy danych produktu IBM Business Monitor musi być inna niż nazwa schematu wspólnej bazy danych produktu Process Server, aby zapobiec kolizjom obiektów baz danych.

- f. Kliknij przycisk **Dalej**.
22. Wykonaj następujące kroki na panelu Konfiguracja bazy danych (część 2):
- a. W polu **Nazwa użytkownika** wpisz wartość *nazwa_uzytkownika* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje istniejący ID użytkownika z uprawnieniami odczytu i zapisu do tabel bazy danych MONITOR.

Uwaga: Jeśli używana jest baza danych Oracle, tego pola nie można edytować.

- b. W polu **Hasło** wpisz wartość *haslo* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje hasło określonego ID użytkownika bazy danych.
- c. W polu **Potwierdzenie hasła** wpisz wartość *haslo*. Ta wartość musi być zgodna z wartością podaną w polu **Hasło**.
- d. Wskaż lub wprowadź ścieżkę do plików ścieżki klasy sterownika JDBC. Sterowniki JDBC baz danych DB2, Oracle i SQL Server znajdują się w katalogu `katalog_główny_programu_Monitor/jdbcdrivers`. Domyślna ścieżka klasy sterownika JDBC jest ustawiana w celu użycia plików specyficznych dla produktu umieszczonych w tym katalogu na podstawie typu bazy danych wybranego na panelu Konfiguracja bazy danych. Alternatywnie należy kliknąć przycisk **Przełączaj**, aby wprowadzić ścieżkę do plików ścieżki klasy sterownika JDBC.

- Baza danych DB2: domyślnie jest tworzony następujący katalog:
`katalog_główny_programu_Monitor/jdbcdrivers/DB2`
- Baza danych Oracle: Domyślnie jest tworzony następujący katalog:
`katalog_główny_programu_Monitor/jdbcdrivers/Oracle`

Plik sterownika JDBC `ojdbc6.jar` jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku `ojdbc6.jar` można użyć zarówno dla produktu Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

- Baza danych SQL Server: Domyślnie jest tworzony następujący katalog:
`katalog_główny_programu_Monitor/jdbcdrivers/SQLServer`

Plik sterownika JDBC `sqljdbc4.jar` jest sterownikiem JDBC obsługiwany przez produkt Microsoft SQL Server 2.0. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.

- e. Wybierz jedną z następujących opcji dla typu sterownika JDBC:
- W przypadku baz danych Oracle:
 - **OCI:** Sterownik OCI wymaga lokalnej instalacji klienta bazy danych Oracle.
 - **Cienki:** sterownik cienki do komunikacji z bazą danych używa języka Java i nie wymaga obecności klienta w systemie lokalnym.
 - W przypadku baz danych DB2 profile programu IBM Business Monitor w systemach operacyjnych innych niż system z/OS są tworzone ze sterownikami typu 4, a profile w systemie z/OS są tworzone ze sterownikami typu 2. Typ można zmienić po utworzeniu profilu, edytując właściwości źródła danych w Konsoli administracyjnej. Sterownik typu 2 jest sterownikiem o rodzimym interfejsie API i wymaga zainstalowania oprogramowania bazy danych lub klienta bazy danych w systemie lokalnym. Sterownik typu 4 jest implementacją czystego języka Java i zazwyczaj zapewnia najwyższą wydajność. W przypadku bazy danych MONITOR nie jest wymagane instalowanie oprogramowania bazy danych ani klientów bazy danych w systemie lokalnym.
- f. Wpisz *nazwę_hosta* w polu **Nazwa hosta lub adres IP serwera bazy danych**. Wartość domyślna to `localhost` lub pełna nazwa hosta lokalnego (jeśli ją

zdefiniowano). Wartości tej należy używać w przypadku instalacji z pojedynczym serwerem. Jeśli baza danych znajduje się na serwerze zdalnym, należy wpisać pełną nazwę hosta lub adres IP.



Uwaga: Ponieważ elementy klastra zależą od rzeczywistej nazwy hosta lub adresu IP, *nie* należy używać wartości localhost w przypadkach innych niż instalacja z pojedynczym serwerem.

- g. Wpisz *numer_portu* w polu **Port usługi TCP/IP lub programu nasłuchującego bazy danych**. Ta wartość reprezentuje port przypisany usłudze TCP/IP lub port, na którym nasłuchuje baza danych.
 - h. Opcjonalne: Jeśli używana jest baza danych DB2 w systemie z/OS, wpisz wartość *nazwa_podsystemu* w polu **Nazwa podsystemu**. Ta wartość określa położenie bazy danych DB2 for z/OS. W nazwie nie można stosować spacji.
 - i. W przypadku używania bazy danych Oracle lub SQL Server i wybrania opcji automatycznego utworzenia bazy danych wprowadź następujące informacje:
 - W polu **Nazwa administratora bazy danych** wpisz wartość *nazwa_uzytkownika_systemu*. Ta wartość jest nazwą administratora bazy danych Oracle lub SQL Server. Ten użytkownik musi mieć uprawnienia dostępu umożliwiające tworzenie i usuwanie baz danych oraz użytkowników.
 - Wpisz wartość *haslo* w polu **Hasło**. Ta wartość jest hasłem administratora systemu określonego w poprzednim polu.
 - W polu **Potwierdzenie hasła** wpisz wartość *haslo*.
 - j. Kliknij przycisk **Dalej**. Jeśli baza danych MONITOR nie została jeszcze utworzona, zostanie wyświetlony komunikat z ostrzeżeniem. Kliknij przycisk **Tak**, aby kontynuować. Bazę danych można utworzyć później.
23. Na panelu Konfiguracja produktu IBM Cognos BI skonfiguruj produkt IBM Cognos BI na potrzeby wielowymiarowej analizy danych z poziomu używanych paneli kontrolnych.
- Aby wdrożyć produkt IBM Cognos BI, kliknij opcję **Utwórz nową konfigurację serwera Cognos** i podaj nazwę bazy danych, która zostanie użyta przez składnicę treści produktu IBM Cognos BI. Nazwa domyślna to COGNOSCS. W przypadku produktu Oracle nazwa bazy danych musi być globalną nazwą bazy danych Oracle (można ją znaleźć za pomocą następującego zapytania: SELECT * FROM GLOBAL_NAME). W przypadku produktu Microsoft SQL Server nazwa bazy danych musi być inna niż nazwa bazy danych MONITOR.

Należy podać hasło i nazwę użytkownika bazy danych. Jeśli na potrzeby składnicy treści używana jest taka sama nazwa użytkownika jak w przypadku bazy danych MONITOR, należy użyć tego samego hasła. Ponieważ użytkownik bazy danych, który ma uzyskiwać dostęp do bazy danych składnicy treści, musi mieć uprawnienie do tworzenia tabel w bazie danych, zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

Dodatkowo konieczne jest podanie nazwy i hasła administratora produktu IBM Cognos BI.

Uwaga: Nazwa i hasło użytkownika bazy danych składnicy treści produktu IBM Cognos BI są przechowywane w elemencie Cognos_JDBC_Alias, dzięki czemu wszystkie referencje bazy danych mogą być obsługiwane w jednym miejscu. Przy każdym uruchomieniu serwera IBM Cognos BI produktu IBM Business Monitor bieżące wartości są przekazywane do konfiguracji produktu IBM Cognos BI, co pozwala na uzyskanie przez produkt IBM Cognos BI dostępu do składnicy treści. Ze względu na tę integrację nie jest możliwe zmodyfikowanie nazwy i hasła użytkownika składnicy treści z poziomu aplikacji konfiguracyjnej produktu IBM Cognos BI.

- Jeśli ma być używana istniejąca wersja produktu IBM Cognos BI, kliknij opcję **Użyj istniejącej konfiguracji serwera Cognos** i podaj identyfikator URI zewnętrznego programu rozsyłającego serwera IBM Cognos BI. Ten identyfikator URI można znaleźć w kliencie konfiguracji produktu IBM Cognos BI po wybraniu opcji **Konfiguracja lokalna > Środowisko > Ustawienia programu rozsyłającego** (na przykład `http://host:port/p2pd/servlet/dispatch/ext`). Jeśli zabezpieczenia administracyjne serwera IBM Cognos BI są włączone, należy także podać nazwę użytkownika i hasło administratora serwera IBM Cognos BI.
Serwer produktu IBM Cognos BI nie musi być dostępny, aby można było ustawić tę wartość. Serwer jest wymagany podczas instalowania modeli monitorowania, jeśli dla tych modeli ma zostać przeprowadzona analiza danych wielowymiarowych.
24. Na panelu Podsumowanie operacji tworzenia profilu przejrzyj wyświetlone informacje. Jeśli konieczne jest wprowadzenie modyfikacji, należy kliknąć przycisk **Wstecz** i dokonać odpowiednich zmian.
 25. Kliknij przycisk **Utwórz**, aby utworzyć profil.
 26. Na panelu Zakończono tworzenie profilu przejrzyj informacje o zakończonym procesie tworzenia profilu.
 27. Opcjonalne: Uruchom konsolę Pierwsze kroki.
 -  Wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 -   Przejdź do katalogu `katalog_główny_profilu/firststeps.wbm` i uruchom komendę `firststeps.sh`.
 28. Kliknij przycisk **Zakończ**, aby zakończyć pracę narzędzia Profile Management Tool.

Podczas tworzenia profilu należy ustawić numery wszystkich wymaganych portów. Zmiana numerów portów po instalacji spowoduje, że konieczne będzie ponowne skonfigurowanie wszystkich numerów portów, aby program IBM Business Monitor działał poprawnie.


Tworzenie profili menedżera wdrażania




Użytkownik musi mieć profil menedżera wdrażania, aby zarządzać wszystkimi serwerami stowarzyszonymi w klastrze. Jeśli skonfigurowane jest środowisko wdrożenia sieciowego, należy najpierw utworzyć ten profil.

Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.
- Zainstalowanie bazy danych.

Aby utworzyć profil menedżera wdrażania, wykonaj następujące kroki przy użyciu narzędzia Profile Management Tool:

1. Przy użyciu jednej z następujących metod otwórz narzędzie Profile Management Tool:
 - W konsoli Pierwsze kroki programu IBM Business Monitor kliknij opcję **Narzędzie Profile Management Tool**.
 -  Kliknij opcję **Start > Programy > IBM > Business Monitor7.5 > Profile Management Tool**.

-  Uruchom plik pmt.bat, który znajduje się w następującym katalogu: katalog_główny_serwera_aplikacji\bin\ProfileManagement.
 -   Przejdź do katalogu katalog_główny_serwera_aplikacji/bin/ProfileManagement i wpisz komendę ./pmt.sh w oknie terminalu.
2. Na panelu Witamy w narzędziu Profile Management Tool przejrzyj podane informacje i kliknij przycisk **Uruchom narzędzie Profile Management Tool**.
 3. Na panelu Profile kliknij przycisk **Utwórz**, aby utworzyć nowy profil.
 4. Na panelu Wybór środowiska rozwiń listę IBM Business Monitor i kliknij opcję **Menedżer wdrażania serwera programu Monitor**, a następnie kliknij przycisk **Dalej**.

Ograniczenie: Jeśli opcja programu IBM Business Monitor nie jest wyświetlana, może to oznaczać, że używana jest wersja 64-bitowa. Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, nie można korzystać z narzędzia Profile Management Tool i należy użyć komendy manageprofiles.

5. Na panelu Opcje tworzenia profilu wybierz żądany typ instalacji i kliknij przycisk **Dalej**.
 - **Typowe tworzenie profilu** (wartość domyślna): Powoduje utworzenie profilu menedżera wdrażania korzystającego z domyślnych ustawień konfiguracyjnych. Narzędzie Profile Management Tool przypisuje unikalne nazwy do profilu, węzła, hosta i komórki. Narzędzie to instaluje również Konsolę administracyjną oraz przypisuje unikalne wartości portów. Podczas konfigurowania istnieje możliwość włączenia zabezpieczeń administracyjnych. W zależności od systemu operacyjnego i uprawnień użytkownika narzędzie to może utworzyć usługę systemową uruchamiającą menedżer wdrażania. Użytkownik może określić własne wartości konfiguracyjne bazy danych programu IBM Business Monitor.
 - **Zaawansowane tworzenie profilu:** Powoduje utworzenie profilu menedżera wdrażania przy użyciu domyślnych ustawień konfiguracyjnych. Można określić wartości dla hosta i komórki, przypisać własne wartości portów oraz wybrać, czy ma zostać wdrożona Konsola administracyjna. W zależności od systemu operacyjnego i uprawnień użytkownika można skorzystać z opcji uruchamiania menedżera wdrażania jako usługi systemowej. Istnieje możliwość określenia pliku projektu bazy danych lub przypisania własnych wartości konfiguracyjnych bazy danych programu IBM Business Monitor.
6. Jeśli wybrano opcję **Typowe tworzenie profilu**, należy przejść do kroku Krok 10: Panel Zabezpieczenia administracyjne.
7. Zaawansowane: na panelu Wdrażanie opcjonalnych aplikacji wybierz opcję **Przeprowadź wdrożenie Konsoli administracyjnej**, a następnie kliknij przycisk **Dalej**.
8. Zaawansowane: na panelu Nazwa i położenie profilu zaakceptuj domyślną nazwę i położenie lub określ nazwę profilu oraz ścieżkę do katalogu, który będzie zawierał pliki środowiska wykonawczego (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Domyślna nazwa profilu to Dmgr01. W systemie Windows katalog typowego profilu to C:\IBM\WebSphere\AppServer\profiles\Dmgr01.
9. Zaawansowane: Na panelu Nazwy węzła, hosta i komórki wpisz nowe wartości lub zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**.
 - Nazwa węzła jest używana na potrzeby administrowania. Jeśli węzeł jest stowarzyszony, jego nazwa musi być unikalna w obrębie komórki.
 - Nazwa hosta jest nazwą DNS (krótką lub długą) albo adresem IP tego komputera.
 - Nazwa komórki jest nazwą logiczną dla grupy węzłów administrowanych przez ten menedżer wdrażania.
10. Na panelu Zabezpieczenia administracyjne wybierz jedną z następujących opcji, a następnie kliknij przycisk **Dalej**.

- Aby włączyć zabezpieczenia, zaznacz pole wyboru **Włącz zabezpieczenia administracyjne** oraz wpisz nazwę użytkownika i hasło.
- Aby wyłączyć zabezpieczenia, usuń zaznaczenie pola wyboru **Włącz zabezpieczenia administracyjne**.

Informacje umożliwiające określenie, czy należy włączyć zabezpieczenia znajdują się w sekcji Administrative security (Zabezpieczenia administracyjne) Centrum informacyjnego serwera WebSphere Application Server.

W przypadku wybrania opcji **Typowe tworzenie profilu** należy przejść do kroku Krok 16: Panel Konfiguracja bazy danych.

11. Zaawansowane: Na panelu Certyfikat bezpieczeństwa (część 1) wybierz, czy ma zostać utworzony domyślny certyfikat osobisty oraz główny certyfikat podpisywania, czy też ma zostać przeprowadzone importowanie z magazynu kluczy. W celu tworzenia nowych certyfikatów kliknij przycisk **Dalej**, aby przejść do strony weryfikacji. W celu zaimportowania istniejących certyfikatów z magazynów kluczy wskaż certyfikaty i kliknij przycisk **Dalej**, aby przejść do strony weryfikacji.
12. Zaawansowane: Na panelu Certyfikat bezpieczeństwa (część 2) zmodyfikuj informacje dotyczące certyfikatu, aby utworzyć nowe certyfikaty podczas tworzenia profilu. Jeśli są importowane istniejące certyfikaty z magazynów kluczy, użyj tych informacji, aby sprawdzić, czy wybrane certyfikaty zawierają odpowiednie informacje. Jeśli wybrane certyfikaty ich nie zawierają, kliknij przycisk **Wstecz**, aby zaimportować inne certyfikaty. W celu zabezpieczenia plików kluczy oraz certyfikatów SSL należy zmienić domyślne hasło magazynu kluczy. Więcej informacji na temat zabezpieczania komunikacji między serwerem i klientem można znaleźć w temacie Securing communications (Zabezpieczanie komunikacji) w Centrum informacyjnym serwera WebSphere Application Server.
13. Zaawansowane: Na panelu Przypisywanie wartości portów przejrzyj wartości portów, które zostaną przypisane podczas tworzenia profilu. Numery portów można zanotować. Zaakceptuj podane wartości lub określ inne numery portów i kliknij przycisk **Dalej**.
14.  Zaawansowane: w systemach Windows jest wyświetlany panel Definicja usługi systemu Windows. Opcja **Uruchom proces serwera aplikacji jako usługę systemu Windows** jest domyślnie włączona i skonfigurowana w taki sposób, aby do logowania używała informacji z lokalnego konta systemowego. Zaakceptuj ustawienia domyślne usługi systemu Windows lub wyłącz tę opcję, a następnie kliknij przycisk **Dalej**. Aby zmienić informacje logowania usługi systemu Windows, należy wybrać opcję **Zaloguj jako określone konto użytkownika** i wprowadzić nazwę użytkownika oraz hasło alternatywnego konta.
Dla usługi systemu Windows opcja **Typ uruchamiania** jest domyślnie ustawiana na wartość **Automatyczne**. Korzystając z listy, można zmienić wartość opcji **Typ uruchamiania** na wartość **Ręczne** lub **Wyłączone**.
Ponieważ w systemach operacyjnych Windows usługi są ustawiane globalnie, każdy profil może uruchomić usługę. To utrudnia śledzenie, który profil wydał na przykład komendę "startServer". Aby uniknąć potencjalnych konfliktów żądania usług występujących między różnymi profilami, należy wyłączyć opcję **Uruchom proces serwera aplikacji jako usługę systemu Windows**.
15. Opcjonalne: Zaawansowane: skonfiguruj bazy danych przy użyciu pliku projektu.
 - a. Wybierz opcję **Użyj pliku projektu bazy danych w celu skonfigurowania bazy danych**, jeśli ma zostać użyty plik projektu zamiast określania parametrów bazy danych na poniższych panelach.
 - b. Kliknij przycisk **Przeglądaj**.
 - c. Podaj pełną ścieżkę do pliku projektu.
 - d. Kliknij przycisk **Dalej**.

- e. Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli podczas tworzenia profilu lokalne bazy danych nie mają zostać utworzone i skonfigurowane automatycznie lub tabele nie mają zostać utworzone w istniejących bazach danych. Jeśli nie zaznaczono tego pola wyboru, lokalne bazy danych zostaną utworzone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch `@DB_PASSWORD@` hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

Jeśli zostanie wskazany plik projektu, panele konfiguracji bazy danych narzędzia Profile Management Tool zostaną pominięte. Położenie pliku projektu zostanie wówczas przekazane do wiersza komend, aby zakończyć procedurę konfigurowania bazy danych. Więcej informacji na temat konfigurowania bazy danych za pomocą pliku projektu zawiera temat Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych.

16. Na panelu Konfiguracja bazy danych sprawdź informacje dotyczące konfiguracji bazy danych MONITOR:
- Wybierz bazę danych z listy.
 - Aby określić katalog docelowy dla wygenerowanych skryptów, włącz opcję **Zastąp katalog docelowy dla wygenerowanych skryptów** i wprowadź ścieżkę w polu **Katalog danych wyjściowych skryptu bazy danych**. Domyślny katalog to `katalog_główny_programu_Monitor\profiles\WBMon01\dbscripts\Monitor\platforma\`.
 - Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli lokalna baza danych nie ma być tworzona i konfigurowana automatycznie lub jeśli tabele w istniejącej bazie danych nie mają być tworzone podczas tworzenia lub rozszerzania profilu. Lokalna baza danych zostanie utworzona, jeśli to pole wyboru nie zostanie zaznaczone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch `@DB_PASSWORD@` hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.
 - W polu **Nazwa bazy danych** wprowadź nazwę bazy danych lub zaakceptuj nazwę domyślną (MONITOR).
 - W polu **Nazwa schematu** wpisz nazwę schematu lub zaakceptuj nazwę domyślną (MONITOR). Jeśli używana jest baza danych DB2 w systemie z/OS, nazwa

schematu bazy danych produktu IBM Business Monitor musi być inna niż nazwa schematu wspólnej bazy danych produktu Process Server, aby zapobiec kolizjom obiektów baz danych.

f. Kliknij przycisk **Dalej**.

17. Dla bazy danych MONITOR wykonaj następujące kroki na panelu Konfiguracja bazy danych (część 2):

a. W polu **Nazwa użytkownika** wpisz wartość *nazwa_użytkownika* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje istniejący ID użytkownika z uprawnieniami odczytu i zapisu do tabel bazy danych MONITOR.

Uwaga: Jeśli używana jest baza danych Oracle, tego pola nie można edytować.

b. W polu **Hasło** wpisz wartość *hasło* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje hasło określonego ID użytkownika bazy danych.

c. W polu **Potwierdzenie hasła** wpisz wartość *hasło*. Ta wartość musi być zgodna z wartością podaną w polu **Hasło**.

d. Wskaż lub wprowadź ścieżkę do plików ścieżki klasy sterownika JDBC. Sterowniki JDBC baz danych DB2, Oracle i SQL Server znajdują się w katalogu `katalog_główny_programu_Monitor/jdbcdrivers`. Domyślna ścieżka klasy sterownika JDBC jest ustawiana w celu użycia plików specyficznych dla produktu umieszczonych w tym katalogu na podstawie typu bazy danych wybranego na panelu Konfiguracja bazy danych. Alternatywnie należy kliknąć przycisk **Przeglądaj**, aby wprowadzić ścieżkę do plików ścieżki klasy sterownika JDBC.

- Baza danych DB2: domyślnie jest tworzony następujący katalog:

`katalog_główny_programu_Monitor/jdbcdrivers/DB2`

- Baza danych Oracle: Domyślnie jest tworzony następujący katalog:

`katalog_główny_programu_Monitor/jdbcdrivers/Oracle`

Plik sterownika JDBC `ojdbc6.jar` jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku `ojdbc6.jar` można użyć zarówno dla produktu Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

- Baza danych SQL Server: Domyślnie jest tworzony następujący katalog:

`katalog_główny_programu_Monitor/jdbcdrivers/SQLServer`

Plik sterownika JDBC `sqljdbc4.jar` jest sterownikiem JDBC obsługiwany przez produkt Microsoft SQL Server 2.0. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.

e. Wybierz jedną z następujących opcji dla typu sterownika JDBC:

- W przypadku baz danych Oracle:

- **OCI:** Sterownik OCI wymaga lokalnej instalacji klienta bazy danych Oracle.

- **Cienki:** sterownik cienki do komunikacji z bazą danych używa języka Java i nie wymaga obecności klienta w systemie lokalnym.

- W przypadku baz danych DB2 profile programu IBM Business Monitor w systemach operacyjnych innych niż system z/OS są tworzone ze sterownikami typu 4, a profile w systemie z/OS są tworzone ze sterownikami typu 2. Typ można zmienić po utworzeniu profilu, edytując właściwości źródła danych w Konsoli administracyjnej. Sterownik typu 2 jest sterownikiem o rodzimym interfejsie API i wymaga zainstalowania oprogramowania bazy danych lub klienta bazy danych w systemie lokalnym. Sterownik typu 4 jest implementacją czystego języka Java i zazwyczaj zapewnia najwyższą wydajność. W przypadku

bazy danych MONITOR nie jest wymagane instalowanie oprogramowania bazy danych ani klientów bazy danych w systemie lokalnym.




- f. Wpisz *nazwę_hosta* w polu **Nazwa hosta lub adres IP serwera bazy danych**. Wartość domyślna to `localhost` lub pełna nazwa hosta lokalnego (jeśli ją zdefiniowano). Wartości tej należy używać w przypadku instalacji z pojedynczym serwerem. Jeśli baza danych znajduje się na serwerze zdalnym, należy wpisać pełną nazwę hosta lub adres IP.

Uwaga: Ponieważ elementy klastra zależą od rzeczywistej nazwy hosta lub adresu IP, *nie* należy używać wartości `localhost` w przypadkach innych niż instalacja z pojedynczym serwerem.

- g. Wpisz *numer_portu* w polu **Port usługi TCP/IP lub programu nasłuchującego bazy danych**. Ta wartość reprezentuje port przypisany usłudze TCP/IP lub port, na którym nasłuchuje baza danych.
- h. Opcjonalne: Jeśli używana jest baza danych DB2 w systemie z/OS, wpisz wartość *nazwa_podsystemu* w polu **Nazwa podsystemu**. Ta wartość określa położenie bazy danych DB2 for z/OS. W nazwie nie można stosować spacji.
- i. W przypadku używania bazy danych Oracle lub SQL Server i wybrania opcji automatycznego utworzenia bazy danych wprowadź następujące informacje:
- W polu **Nazwa administratora bazy danych** wpisz wartość *nazwa_użytkownika_systemu*. Ta wartość jest nazwą administratora bazy danych Oracle lub SQL Server. Ten użytkownik musi mieć uprawnienia dostępu umożliwiające tworzenie i usuwanie baz danych oraz użytkowników.
 - Wpisz wartość *hasło* w polu **Hasło**. Ta wartość jest hasłem administratora systemu określonego w poprzednim polu.
 - W polu **Potwierdzenie hasła** wpisz wartość *hasło*.
- j. Kliknij przycisk **Dalej**. Jeśli baza danych MONITOR nie została jeszcze utworzona, zostanie wyświetlony komunikat z ostrzeżeniem. Kliknij przycisk **Tak**, aby kontynuować. Bazę danych można utworzyć później.
18. Jeśli nie istnieje jeszcze instalacja produktu IBM Cognos Business Intelligence, która ma zostać użyta, na panelu Baza danych składnicy treści produktu Cognos wprowadź informacje umożliwiające utworzenie bazy danych składnicy treści produktu IBM Cognos BI na potrzeby przeprowadzenia wielowymiarowej analizy danych za pomocą paneli kontrolnych.
- a. Kliknij opcję **Utwórz nową bazę danych składnicy treści produktu Cognos**.
- b. Podaj nazwę bazy danych, która zostanie użyta na potrzeby składnicy treści produktu IBM Cognos BI. Nazwa domyślna to `COGNOSCS`. W przypadku produktu Oracle nazwa bazy danych musi być globalną nazwą bazy danych Oracle (można ją znaleźć za pomocą następującego zapytania: `SELECT * FROM GLOBAL_NAME`). W przypadku produktu Microsoft SQL Server nazwa bazy danych musi być inna niż nazwa bazy danych MONITOR.
- c. Podaj nazwę użytkownika oraz hasło dla bazy danych i potwierdź hasło. Jeśli na potrzeby składnicy treści używana jest taka sama nazwa użytkownika jak w przypadku bazy danych MONITOR, należy użyć tego samego hasła. Ponieważ ten użytkownik wymaga praw pełnego dostępu, warto utworzyć nowego użytkownika bazy danych tylko na potrzeby bazy danych składnicy treści.

Uwaga: Nazwa i hasło użytkownika bazy danych składnicy treści produktu IBM Cognos BI są przechowywane w elemencie `Cognos_JDBC_Alias`, dzięki czemu wszystkie referencje bazy danych mogą być obsługiwane w jednym miejscu. Przy każdym uruchomieniu serwera IBM Cognos BI produktu IBM Business Monitor bieżące wartości są przekazywane do konfiguracji produktu IBM Cognos BI, co pozwala na uzyskanie przez produkt IBM Cognos BI dostępu do składnicy treści. Ze

względu na tę integrację nie jest możliwe zmodyfikowanie nazwy i hasła użytkownika składnicy treści z poziomu aplikacji konfiguracyjnej produktu IBM Cognos BI.

19. Na panelu Podsumowanie operacji tworzenia profilu przejrzyj wyświetlone informacje. Jeśli konieczne jest wprowadzenie modyfikacji, należy kliknąć przycisk **Wstecz** i dokonać odpowiednich zmian.
20. Kliknij przycisk **Utwórz**, aby utworzyć profil.
21. Na panelu Zakończono tworzenie profilu przejrzyj informacje o zakończonym procesie tworzenia profilu.
22. Opcjonalne: Uruchom konsolę Pierwsze kroki.
 -  Wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 -   Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.sh.
23. Kliknij przycisk **Zakończ**, aby zakończyć pracę narzędzia Profile Management Tool.

Podczas tworzenia profilu należy ustawić numery wszystkich wymaganych portów. Zmiana numerów portów po instalacji spowoduje, że konieczne będzie ponowne skonfigurowanie wszystkich numerów portów, aby program IBM Business Monitor działał poprawnie.

Rozszerzanie profili menedżera wdrażania



W środowisku wdrożenia sieciowego niezbędny jest profil menedżera wdrażania. Zamiast tworzyć nowy profil menedżera wdrażania można tak rozszerzyć już istniejący profil, aby uzyskał status profilu menedżera wdrażania dla programu IBM Business Monitor.



Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.
- Zainstalowanie bazy danych.

Istniejący profil produktu WebSphere Application Server, Process Server lub WebSphere Enterprise Service Bus można rozszerzyć przy użyciu szablonu programu IBM Business Monitor. Podobnie jeśli zainstalowano produkt WebSphere Application Server i rozszerzono profil dla programu IBM Business Monitor, profil można rozszerzyć przy użyciu produktu Process Server lub WebSphere Enterprise Service Bus.

Aby rozszerzyć istniejący profil menedżera wdrażania, wykonaj następujące kroki przy użyciu narzędzia Profile Management Tool:

1. Przy użyciu jednej z następujących metod otwórz narzędzie Profile Management Tool:
 - W konsoli Pierwsze kroki programu IBM Business Monitor kliknij opcję **Narzędzie Profile Management Tool**.
 -  Kliknij opcję **Start > Programy > IBM > Business Monitor7.5 > Profile Management Tool**.
 -  Uruchom plik pmt.bat, który znajduje się w następującym katalogu: katalog_główny_serwera_aplikacji\bin\ProfileManagement.

-   Przejdź do katalogu katalog_główny_serwera_aplikacji/bin/ProfileManagement i wpisz komendę `./pmt.sh` w oknie terminalu.
2. Na panelu Witamy w narzędziu Profile Management Tool przejrzyj podane informacje i kliknij przycisk **Uruchom narzędzie Profile Management Tool**.
 3. Na panelu Profile wybierz profil z listy i kliknij opcję **Rozszerz**, aby rozszerzyć istniejący profil. Profil można rozwinąć w celu wyświetlenia już wykonanych rozszerzeń. Aby uzyskać profil menedżera wdrażania programu IBM Business Monitor, do rozszerzenia należy wybrać istniejący profil menedżera wdrażania.

Ograniczenie: Jeśli opcja programu IBM Business Monitor nie jest wyświetlana, może to oznaczać, że używana jest wersja 64-bitowa. Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, nie można korzystać z narzędzia Profile Management Tool i należy użyć komendy `manageprofiles`.

4. Na liście panelu Wybór rozszerzenia kliknij opcję **Menedżer wdrażania serwera programu Monitor** i kliknij przycisk **Dalej**.
5. Na panelu Opcje rozszerzania profilu kliknij opcję **Zaawansowane rozszerzanie profilu** i kliknij przycisk **Dalej**. W przypadku kliknięcia opcji **Typowa** niektóre panele nie są wyświetlane.
6. Opcjonalne: Jeśli rozszerzany profil ma włączone zabezpieczenia, wykonaj następujące kroki na panelu zabezpieczeń administracyjnych:
 - a. W polu **Nazwa użytkownika** wpisz wartość *nazwa_użytkownika*.
 - b. W polu **Hasło** wpisz wartość *hasło*.
 - c. W polu **Potwierdzenie hasła** wpisz wartość *hasło*.
 - d. Kliknij przycisk **Dalej**.
7. Opcjonalne: Zaawansowane: skonfiguruj bazy danych przy użyciu pliku projektu.
 - a. Wybierz opcję **Użyj pliku projektu bazy danych w celu skonfigurowania bazy danych**, jeśli ma zostać użyty plik projektu zamiast określania parametrów bazy danych na poniższych panelach.
 - b. Kliknij przycisk **Przeglądaj**.
 - c. Podaj pełną ścieżkę do pliku projektu.
 - d. Kliknij przycisk **Dalej**.
 - e. Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli podczas tworzenia profilu lokalne bazy danych nie mają zostać utworzone i skonfigurowane automatycznie lub tabele nie mają zostać utworzone w istniejących bazach danych. Jeśli nie zaznaczono tego pola wyboru, lokalne bazy danych zostaną utworzone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch `@DB_PASSWORD@` hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

Jeśli zostanie wskazany plik projektu, panele konfiguracji bazy danych narzędzia Profile Management Tool zostaną pominięte. Położenie pliku projektu zostanie wówczas

przekazane do wiersza komend, aby zakończyć procedurę konfigurowania bazy danych. Więcej informacji na temat konfigurowania bazy danych za pomocą pliku projektu zawiera temat Tworzenie lub konfigurowanie skryptów bazy danych za pomocą narzędzia do projektowania baz danych.

8. Na panelu Konfiguracja bazy danych sprawdź informacje dotyczące konfiguracji bazy danych MONITOR:
 - a. Wybierz bazę danych z listy.
 - b. Aby określić katalog docelowy dla wygenerowanych skryptów, włącz opcję **Zastąp katalog docelowy dla wygenerowanych skryptów** i wprowadź ścieżkę w polu **Katalog danych wyjściowych skryptu bazy danych**. Domyślny katalog to katalog_główny_programu_Monitor\profiles\WBMon01\dbscripts\Monitor\platforma\.
 - c. Wybierz opcję **Opóźnij wykonywanie skryptów bazy danych (ta właściwość musi być wybrana w przypadku korzystania ze zdalnej bazy danych)**, jeśli lokalna baza danych nie ma być tworzona i konfigurowana automatycznie lub jeśli tabele w istniejącej bazie danych nie mają być tworzone podczas tworzenia lub rozszerzania profilu. Lokalna baza danych zostanie utworzona, jeśli to pole wyboru nie zostanie zaznaczone. W przypadku zaznaczenia tego pola wyboru użytkownik lub administrator bazy danych będzie musiał ręcznie uruchomić skrypty umieszczone w katalogu określonym za pomocą umieszczonego na tej stronie pola Katalog wyjściowy skryptów bazy danych. W przypadku tworzenia skryptów dla bazy danych Oracle przed ich wykonaniem należy zastąpić łańcuch @DB_PASSWORD@ hasłem dla nazwy schematu.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

- d. W polu **Nazwa bazy danych** wprowadź nazwę bazy danych lub zaakceptuj nazwę domyślną (MONITOR).
 - e. W polu **Nazwa schematu** wpisz nazwę schematu lub zaakceptuj nazwę domyślną (MONITOR). Jeśli używana jest baza danych DB2 w systemie z/OS, nazwa schematu bazy danych produktu IBM Business Monitor musi być inna niż nazwa schematu wspólnej bazy danych produktu Process Server, aby zapobiec kolizjom obiektów baz danych.
 - f. Kliknij przycisk **Dalej**.
9. Dla bazy danych MONITOR wykonaj następujące kroki na panelu Konfiguracja bazy danych (część 2):
 - a. W polu **Nazwa użytkownika** wpisz wartość *nazwa_użytkownika* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje istniejący ID użytkownika z uprawnieniami odczytu i zapisu do tabel bazy danych MONITOR.

Uwaga: Jeśli używana jest baza danych Oracle, tego pola nie można edytować.

- b. W polu **Hasło** wpisz wartość *hasło* na potrzeby uwierzytelniania w bazie danych. Ta wartość reprezentuje hasło określonego ID użytkownika bazy danych.
 - c. W polu **Potwierdzenie hasła** wpisz wartość *hasło*. Ta wartość musi być zgodna z wartością podaną w polu **Hasło**.
 - d. Wskaż lub wprowadź ścieżkę do plików ścieżki klasy sterownika JDBC. Sterowniki JDBC baz danych DB2, Oracle i SQL Server znajdują się w katalogu katalog_główny_programu_Monitor/jdbcdrivers. Domyślna ścieżka klasy sterownika JDBC jest ustawiana w celu użycia plików specyficznych dla produktu

umieszczonych w tym katalogu na podstawie typu bazy danych wybranego na panelu Konfiguracja bazy danych. Alternatywnie należy kliknąć przycisk **Przeglądaj**, aby wprowadzić ścieżkę do plików ścieżki klasy sterownika JDBC.

- Baza danych DB2: domyślnie jest tworzony następujący katalog:
katalog_główny_programu_Monitor/jdbcdrivers/DB2
- Baza danych Oracle: Domyślnie jest tworzony następujący katalog:
katalog_główny_programu_Monitor/jdbcdrivers/Oracle

Plik sterownika JDBC `ojdbc6.jar` jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku `ojdbc6.jar` można użyć zarówno dla produktu Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

- Baza danych SQL Server: Domyślnie jest tworzony następujący katalog:
katalog_główny_programu_Monitor/jdbcdrivers/SQLServer

Plik sterownika JDBC `sqljdbc4.jar` jest sterownikiem JDBC obsługiwany przez produkt Microsoft SQL Server 2.0. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.




- e. Wybierz jedną z następujących opcji dla typu sterownika JDBC:
- W przypadku baz danych Oracle:
 - **OCI**: Sterownik OCI wymaga lokalnej instalacji klienta bazy danych Oracle.
 - **Cienki**: sterownik cienki do komunikacji z bazą danych używa języka Java i nie wymaga obecności klienta w systemie lokalnym.
 - W przypadku baz danych DB2 profile programu IBM Business Monitor w systemach operacyjnych innych niż system z/OS są tworzone ze sterownikami typu 4, a profile w systemie z/OS są tworzone ze sterownikami typu 2. Typ można zmienić po utworzeniu profilu, edytując właściwości źródła danych w Konsoli administracyjnej. Sterownik typu 2 jest sterownikiem o rodzimym interfejsie API i wymaga zainstalowania oprogramowania bazy danych lub klienta bazy danych w systemie lokalnym. Sterownik typu 4 jest implementacją czystego języka Java i zazwyczaj zapewnia najwyższą wydajność. W przypadku bazy danych MONITOR nie jest wymagane instalowanie oprogramowania bazy danych ani klientów bazy danych w systemie lokalnym.
- f. Wpisz *nazwę hosta* w polu **Nazwa hosta lub adres IP serwera bazy danych**. Wartość domyślna to `localhost` lub pełna nazwa hosta lokalnego (jeśli ją zdefiniowano). Wartości tej należy używać w przypadku instalacji z pojedynczym serwerem. Jeśli baza danych znajduje się na serwerze zdalnym, należy wpisać pełną nazwę hosta lub adres IP.

Uwaga: Ponieważ elementy klastra zależą od rzeczywistej nazwy hosta lub adresu IP, *nie* należy używać wartości `localhost` w przypadkach innych niż instalacja z pojedynczym serwerem.

- g. Wpisz *numer portu* w polu **Port usługi TCP/IP lub programu nasłuchującego bazy danych**. Ta wartość reprezentuje port przypisany usłudze TCP/IP lub port, na którym nasłuchuje baza danych.
- h. Opcjonalne: Jeśli używana jest baza danych DB2 w systemie z/OS, wpisz wartość *nazwa podsystemu* w polu **Nazwa podsystemu**. Ta wartość określa położenie bazy danych DB2 for z/OS. W nazwie nie można stosować spacji.
- i. W przypadku używania bazy danych Oracle lub SQL Server i wybrania opcji automatycznego utworzenia bazy danych wprowadź następujące informacje:

- W polu **Nazwa administratora bazy danych** wpisz wartość *nazwa_uzytkownika_systemu*. Ta wartość jest nazwą administratora bazy danych Oracle lub SQL Server. Ten użytkownik musi mieć uprawnienia dostępu umożliwiające tworzenie i usuwanie baz danych oraz użytkowników.
 - Wpisz wartość *haslo* w polu **Hasło**. Ta wartość jest hasłem administratora systemu określonego w poprzednim polu.
 - W polu **Potwierdzenie hasła** wpisz wartość *haslo*.
- j. Kliknij przycisk **Dalej**. Jeśli baza danych MONITOR nie została jeszcze utworzona, zostanie wyświetlony komunikat z ostrzeżeniem. Kliknij przycisk **Tak**, aby kontynuować. Bazę danych można utworzyć później.
10. Jeśli nie istnieje jeszcze instalacja produktu IBM Cognos Business Intelligence, która ma zostać użyta, na panelu Baza danych składnicy treści produktu Cognos wprowadź informacje umożliwiające utworzenie bazy danych składnicy treści produktu IBM Cognos BI na potrzeby przeprowadzenia wielowymiarowej analizy danych za pomocą paneli kontrolnych.
- a. Kliknij opcję **Utwórz nową bazę danych składnicy treści produktu Cognos**.
 - b. Podaj nazwę bazy danych, która zostanie użyta na potrzeby składnicy treści produktu IBM Cognos BI. Nazwa domyślna to COGNOSCS. W przypadku produktu Oracle nazwa bazy danych musi być globalną nazwą bazy danych Oracle (można ją znaleźć za pomocą następującego zapytania: SELECT * FROM GLOBAL_NAME). W przypadku produktu Microsoft SQL Server nazwa bazy danych musi być inna niż nazwa bazy danych MONITOR.
 - c. Podaj nazwę użytkownika oraz hasło dla bazy danych i potwierdź hasło. Jeśli na potrzeby składnicy treści używana jest taka sama nazwa użytkownika jak w przypadku bazy danych MONITOR, należy użyć tego samego hasła. Ponieważ ten użytkownik wymaga praw pełnego dostępu, warto utworzyć nowego użytkownika bazy danych tylko na potrzeby bazy danych składnicy treści.

Uwaga: Nazwa i hasło użytkownika bazy danych składnicy treści produktu IBM Cognos BI są przechowywane w elemencie Cognos_JDBC_Alias, dzięki czemu wszystkie referencje bazy danych mogą być obsługiwane w jednym miejscu. Przy każdym uruchomieniu serwera IBM Cognos BI produktu IBM Business Monitor bieżące wartości są przekazywane do konfiguracji produktu IBM Cognos BI, co pozwala na uzyskanie przez produkt IBM Cognos BI dostępu do składnicy treści. Ze względu na tę integrację nie jest możliwe zmodyfikowanie nazwy i hasła użytkownika składnicy treści z poziomu aplikacji konfiguracyjnej produktu IBM Cognos BI.

11. Na panelu Podsumowanie operacji rozszerzania profilu przejrzyj wyświetlone informacje. Jeśli konieczne jest wprowadzenie modyfikacji, należy kliknąć przycisk **Wstecz** i dokonać odpowiednich zmian.
12. Kliknij opcję **Rozszerz**, aby rozszerzyć profil.
13. Na panelu Zakończono rozszerzanie profilu przejrzyj informacje o ukończonej operacji rozszerzania profilu.
14. Opcjonalne: Uruchom konsolę Pierwsze kroki.
-  Wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 -   Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.sh.
15. Kliknij przycisk **Zakończ**, aby zakończyć pracę narzędzia Profile Management Tool.

Podczas tworzenia profilu należy ustawić numery wszystkich wymaganych portów. Zmiana numerów portów po instalacji spowoduje, że konieczne będzie ponowne skonfigurowanie wszystkich numerów portów, aby program IBM Business Monitor działał poprawnie.

Tworzenie profili niestandardowych dla węzłów





W przypadku wdrożenia sieciowego profilu niestandardowy należy utworzyć w przypadku każdego węzła, który ma zostać dodany do klastra serwerów programu IBM Business Monitor. Ten profil zostanie utworzony w katalogu profili serwera WebSphere Application Server.

Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.
- Upewnienie się, że działa menedżer wdrażania.

Wskazówka: Jeśli jest planowane włączenie zabezpieczeń w tych węzłach, należy skonfigurować zabezpieczenia przed kontynuowaniem tworzenia węzła niestandardowego. Poniżej znajduje się odsyłacz do szczegółowych informacji na temat konfigurowania zabezpieczeń.

Aby utworzyć profil niestandardowy dla każdego elementu klastra, wykonaj następujące kroki przy użyciu narzędzia Profile Management Tool:

1. Przy użyciu jednej z następujących metod otwórz narzędzie Profile Management Tool:
 - W konsoli Pierwsze kroki programu IBM Business Monitor kliknij opcję **Narzędzie Profile Management Tool**.
 -  Kliknij opcję **Start > Programy > IBM > Business Monitor7.5 > Profile Management Tool**.
 -  Uruchom plik pmt.bat, który znajduje się w następującym katalogu: katalog_główny_serwera_aplikacji\bin\ProfileManagement.
 -   Przejdź do katalogu katalog_główny_serwera_aplikacji/bin/ProfileManagement i wpisz komendę ./pmt.sh w oknie terminalu.
2. Na panelu Witamy w narzędziu Profile Management Tool przejrzyj podane informacje i kliknij przycisk **Uruchom narzędzie Profile Management Tool**.
3. Na panelu Profile kliknij przycisk **Utwórz**, aby utworzyć nowy profil.
4. Na panelu Wybór środowiska rozwiń listę IBM Business Monitor i kliknij opcję **Profil niestandardowy serwera programu Monitor**, a następnie kliknij przycisk **Dalej**.
Utworzenie profilu niestandardowego zapewni elastyczność podczas tworzenia serwerów i klastrów w miarę kontynuowania konfigurowania środowiska.

Ograniczenie: Jeśli opcja programu IBM Business Monitor nie jest wyświetlana, może to oznaczać, że używana jest wersja 64-bitowa. Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, nie można korzystać z narzędzia Profile Management Tool i należy użyć komendy manageprofiles.




5. Na panelu Opcje tworzenia profilu wybierz żądany typ instalacji i kliknij przycisk **Dalej**.
 - **Typowe tworzenie profilu** (wartość domyślna): Powoduje utworzenie profilu niestandardowego korzystającego z domyślnych ustawień konfiguracyjnych.

Narzędzie Profile Management Tool przypisuje unikalne nazwy do profilu, węzła i hosta. Węzeł zostanie stowarzyszony z istniejącym menedżerem wdrażania.

- **Zaawansowane tworzenie profilu:** Powoduje utworzenie profilu niestandardowego przy użyciu domyślnych wartości konfiguracyjnych. Można określić wartości dla położenia profilu oraz nazw profilu, węzła i hosta. Węzeł zostanie stowarzyszony z istniejącym menedżerem wdrażania.
6. W przypadku wybrania opcji **Typowe tworzenie profilu** przejdź do kroku Krok 10: Panel Stowarzyszanie.
 7. Zaawansowane: na panelu Nazwa i położenie profilu zaakceptuj domyślną nazwę i położenie lub określ nazwę profilu oraz ścieżkę do katalogu, który będzie zawierał pliki środowiska wykonawczego (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Domyślna nazwa profilu to Custom01. W systemie Windows katalog typowego profilu to C:\IBM\WebSphere\AppServer\profiles\Custom01.
 8. Opcjonalne: Zaawansowane: Jeśli tworzony profil ma być używany jako profil domyślny, wybierz opcję **Ustaw ten profil jako domyślny**. Kliknij przycisk **Dalej**.
 9. Zaawansowane: Na panelu Nazwy węzła i hosta wpisz nowe wartości lub zaakceptuj wartości domyślne, a następnie kliknij przycisk **Dalej**.
 - Nazwa węzła jest używana na potrzeby administrowania. Jeśli węzeł jest stowarzyszony, jego nazwa musi być unikalna w obrębie komórki.
 - Nazwa hosta jest nazwą DNS (krótką lub długą) albo adresem IP tego komputera.
 10. Aby zidentyfikować przeznaczony do użycia profil menedżera wdrażania, na panelu Stowarzyszanie wykonaj następujące kroki:

Uwaga: W celu stowarzyszenia węzła w późniejszym terminie (przy użyciu komendy `add_node`) można wybrać opcję **Stowarzysz ten węzeł później**. W przypadku wybrania tej opcji wszystkie pola zostaną wyłączone. Zaletą późniejszego stowarzyszenia jest to, że użytkownik może uniknąć dwukrotnego tworzenia profilu. Jeśli węzeł został stowarzyszony podczas tworzenia profilu i z jakiegokolwiek powodu tworzenie profilu nie powiodło się (na przykład zegar komputera węzła nie był zsynchronizowany z zegarem menedżera wdrażania), konieczne jest ponowne utworzenie profilu, aby zagwarantować jego poprawność. Dlatego też stowarzyszenie węzła w późniejszym czasie zapewnia lepszą kontrolę nad procedurą stowarzyszenia.

- a. Wpisz *nazwę_hosta* w polu **Nazwa hosta lub adres IP menedżera wdrażania**. Należy podać pełną nazwę hosta lub adres IP serwera, na którym utworzono profil menedżera wdrażania.
 - b. Wpisz *numer_portu* w polu **Numer portu SOAP menedżera wdrażania**. Wartość domyślna to 8879.
 - c. Opcjonalne: Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, wpisz *nazwę_użytkownika* w polu **Nazwa użytkownika**. Nazwa użytkownika musi być nazwą istniejącego na serwerze WebSphere Application Server użytkownika mającego dostęp do menedżera wdrażania. Ta wartość jest wymagana do uwierzytelniania w menedżerze wdrażania.
 - d. Opcjonalne: Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, wpisz *hasło* w polu **Hasło**. Musi to być hasło dla podanej *nazwy_użytkownika*.
 - e. Kliknij przycisk **Dalej**.
11. W przypadku wybrania opcji **Typowe tworzenie profilu** przejdź do kroku Krok 15: Panel Podsumowanie operacji tworzenia profilu.
 12. Zaawansowane: Na panelu Konfiguracja bazy danych wykonaj następujące kroki:
 - a. Wybierz bazę danych z listy rozwijanej.
 - b. W polu **Położenie (katalog) plików ścieżki klasy sterownika JDBC** wpisz lub wskaż katalog, w którym znajdują się pliki ścieżki klasy sterownika JDBC.

- c. Kliknij przycisk **Dalej**.
13. Na panelu Podsumowanie operacji tworzenia profilu przejrzyj wyświetlone informacje. Jeśli konieczne jest wprowadzenie modyfikacji, należy kliknąć przycisk **Wstecz** i dokonać odpowiednich zmian.
 14. Kliknij przycisk **Utwórz**, aby utworzyć profil.
 15. Na panelu Zakończono tworzenie profilu przejrzyj informacje o zakończonym procesie tworzenia profilu.
 16. Opcjonalne: Uruchom konsolę Pierwsze kroki.
 -  Wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 -   Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.sh.
 17. Kliknij przycisk **Zakończ**, aby zakończyć pracę narzędzia Profile Management Tool.

Podczas tworzenia profilu należy ustawić numery wszystkich wymaganych portów. Zmiana numerów portów po instalacji spowoduje, że konieczne będzie ponowne skonfigurowanie wszystkich numerów portów, aby program IBM Business Monitor działał poprawnie.





Rozszerzanie profili niestandardowych dla węzłów

W przypadku wdrożenia sieciowego profilu niestandardowego należy utworzyć dla każdego węzła, który ma zostać dodany do klastra serwerów programu IBM Business Monitor. Zamiast utworzyć nowy profil, można rozszerzyć istniejący profil niestandardowy w każdym węźle.

Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.
- Upewnienie się, że działa menedżer wdrażania.

Aby rozszerzyć profil dla każdego elementu klastra, wykonaj następujące kroki przy użyciu narzędzia Profile Management Tool:




1. Przy użyciu jednej z następujących metod otwórz narzędzie Profile Management Tool:
 - W konsoli Pierwsze kroki programu IBM Business Monitor kliknij opcję **Narzędzie Profile Management Tool**.
 -  Kliknij opcję **Start > Programy > IBM > Business Monitor7.5 > Profile Management Tool**.
 -  Uruchom plik pmt.bat, który znajduje się w następującym katalogu: katalog_główny_serwera_aplikacji\bin\ProfileManagement.
 -   Przejdź do katalogu katalog_główny_serwera_aplikacji/bin/ProfileManagement i wpisz komendę ./pmt.sh w oknie terminalu.
2. Na panelu Witamy w narzędziu Profile Management Tool przejrzyj podane informacje i kliknij przycisk **Uruchom narzędzie Profile Management Tool**.
3. Na panelu Profile wybierz profil z listy i kliknij opcję **Rozszerz**, aby rozszerzyć istniejący profil. Profil można rozwinąć w celu wyświetlenia już wykonanych rozszerzeń. Aby uzyskać profil niestandardowy programu IBM Business Monitor, do

rozszerzenia konieczne jest wybranie istniejącego profilu niestandardowego. Profil niestandardowy zapewni elastyczność podczas tworzenia serwerów i klastrów w miarę kontynuowania konfigurowania środowiska.

Ograniczenie: Jeśli opcja programu IBM Business Monitor nie jest wyświetlana, może to oznaczać, że używana jest wersja 64-bitowa. Jeśli używana jest 64-bitowa wersja produktu IBM Business Monitor, nie można korzystać z narzędzia Profile Management Tool i należy użyć komendy `manageprofiles`.

4. Na liście panelu Wybór rozszerzenia kliknij opcję **Profil niestandardowy serwera programu Monitor** i kliknij przycisk **Dalej**.
5. Na panelu Opcje rozszerzania profilu kliknij opcję **Zaawansowane rozszerzanie profilu** i kliknij przycisk **Dalej**. W przypadku kliknięcia opcji **Typowa** niektóre panele nie są wyświetlane.
6. Jeśli został wyświetlony panel Stowarzyszenie, wykonaj następujące kroki, aby zidentyfikować profil menedżera wdrażania przeznaczony do użycia:

Uwaga: Jeśli profil nie został wcześniej stowarzyszony, ten panel nie zostanie wyświetlony.

- a. Wpisz *nazwę_hosta* w polu **Nazwa hosta lub adres IP menedżera wdrażania**. Należy podać pełną nazwę hosta lub adres IP serwera, na którym utworzono profil menedżera wdrażania.
 - b. Wpisz *numer_portu* w polu **Numer portu SOAP menedżera wdrażania**. Wartość domyślna to 8879.
 - c. Opcjonalne: Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, wpisz *nazwę_użytkownika* w polu **Nazwa użytkownika**. Nazwa użytkownika musi być nazwą istniejącego na serwerze WebSphere Application Server użytkownika mającego dostęp do menedżera wdrażania. Ta wartość jest wymagana do uwierzytelniania w menedżerze wdrażania.
 - d. Opcjonalne: Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, wpisz *hasło* w polu **Hasło**. Musi to być hasło dla podanej *nazwy_użytkownika*.
 - e. Kliknij przycisk **Dalej**.
7. Na panelu Konfiguracja bazy danych wykonaj następujące kroki:
 - a. Wybierz bazę danych z listy.
 - b. W polu **Położenie (katalog) plików ścieżki klasy sterownika JDBC** wpisz lub wskaż katalog, w którym znajdują się pliki ścieżki klasy sterownika JDBC.
 - c. Kliknij przycisk **Dalej**.
 8. Kliknij opcję **Rozszerz**, aby rozszerzyć profil.
 9. Na panelu Zakończono rozszerzanie profilu przejrzyj informacje o ukończonej operacji rozszerzania profilu.
 10. Opcjonalne: Uruchom konsolę Pierwsze kroki.
 -  Wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 -   Przejdź do katalogu `katalog_główny_profilu/firststeps.wbm` i uruchom komendę `firststeps.sh`.
 11. Kliknij przycisk **Zakończ**, aby zakończyć pracę narzędzia Profile Management Tool.

Podczas tworzenia profilu należy ustawić numery wszystkich wymaganych portów. Zmiana numerów portów po instalacji spowoduje, że konieczne będzie ponowne skonfigurowanie wszystkich numerów portów, aby program IBM Business Monitor działał poprawnie.

Tworzenie i rozszerzanie profili za pomocą komendy manageprofiles

Zamiast używać narzędzia Profile Management Tool, można użyć komendy manageprofiles, aby utworzyć profile z poziomu wiersza komend. Jeśli jest używana 64-bitowa wersja programu IBM Business Monitor, konieczne jest użycie komendy manageprofiles, ponieważ narzędzie Profile Management Tool nie jest obsługiwane. Jeśli jest używany system z/OS, należy wyświetlić temat Tworzenie wspólnych konfiguracji dla programu IBM Business Monitor for z/OS.

Przed utworzeniem lub rozszerzeniem profilu należy szczegółowo rozważyć dostępne parametry. Po utworzeniu lub rozszerzeniu profilu nie można go w łatwy sposób zmodyfikować.

Przed wykonaniem tego zadania konieczne jest wykonanie następujących zadań:

- Sprawdzenie, czy zostały spełnione wszystkie wymagania wstępne dotyczące sprzętu i oprogramowania.
- Zainstalowanie programu IBM Business Monitor.
- Zalogowanie się do systemu jako użytkownik posiadający odpowiednie uprawnienia (do odczytu, zapisywania i uruchamiania) w katalogu profili produktu WebSphere Application Server.

W przypadku korzystania z bazy danych Oracle obsługa interfejsu JDBC jest zapewniana przez sterowniki JDBC Oracle dla maszyny JVM 1.6. Plik sterownika JDBC ojdbc6.jar jest obsługiwany przez produkt Oracle sterownikiem JDBC przeznaczonym do użytku z wersją 7 serwera WebSphere Application Server. Pliku ojdbc6.jar można użyć zarówno dla produktu Oracle 10g, jak i dla produktu Oracle 11g. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych Oracle są dostępne na stronie pokrewnej.

Domyślnie narzędzie Profile Management Tool wskazuje plik ojdbc6.jar udostępniony w katalogu katalog_główny_serwera_aplikacji\jdbcdrivers\Oracle. Zamiast niego można pobrać inny plik ojdbc6.jar sterownika JDBC bazy danych Oracle i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy manageprofiles.

W przypadku korzystania z bazy danych SQL Server obsługa interfejsu JDBC jest zapewniana przez sterowniki JDBC SQL Server dla maszyny JVM 1.6. W produkcie IBM Business Monitor używany jest plik sqljdbc4.jar sterownika Microsoft JDBC 2.0. Domyślnie narzędzie Profile Management Tool wskazuje plik sqljdbc4.jar udostępniony w katalogu katalog_główny_serwera_aplikacji\jdbcdrivers\SQLServer. Zamiast niego można pobrać inny plik sqljdbc4.jar sterownika JDBC Microsoft i wskazać go podczas uruchamiania narzędzia Profile Management Tool lub komendy manageprofiles. Informacje dotyczące minimalnych wymaganych ustawień dla bazy danych SQL Server są dostępne na stronie pokrewnej.

W przypadku środowiska jednoserwerowego należy utworzyć profil autonomiczny.

W przypadku środowiska wdrażania sieciowego wykonaj następujące kroki:

1. Przed utworzeniem innych profili należy utworzyć profil menedżera wdrażania. Jeśli profil menedżera wdrażania utworzono przed zainstalowaniem produktu IBM Business Monitor (na przykład dla produktu WebSphere Application Server lub Process Server) i jeśli planowane jest używanie tego samego profilu menedżera wdrażania do zarządzania węzłami produktu IBM Business Monitor, należy rozszerzyć profil przy użyciu szablonu udostępnionego w produkcie IBM Business Monitor.
2. Profil niestandardowy należy utworzyć dla każdego węzła, który ma zostać dodany do klastra serwerów. Można również rozszerzyć istniejący profil niestandardowy dla każdego węzła, który ma zostać dodany.

Uwaga: Jeśli serwer bazy danych zawiera wiele zainstalowanych wersji bazy danych DB2 lub wiele instancji bazy danych DB2, podczas tworzenia profilu zostanie użyta domyślna wersja lub instancja bazy danych DB2. Aby określić używaną wersję lub instancję bazy danych DB2, należy skorzystać z procedury ręcznego instalowania bazy danych. Dzięki temu administrator bazy danych może zapewnić, że używana jest odpowiednia wersja lub instancja.

Aby utworzyć profil ręcznie, wykonaj następujące kroki:

1. Otwórz wiersz komend i przejdź do następującego katalogu:
katalog_główny_serwera_aplikacji/bin
2. Uruchom plik `manageprofiles.bat` lub `manageprofiles.sh`, używając wymaganych parametrów. Informacje dotyczące parametrów dla każdego typu profilu znajdują się na stronach informacji dodatkowych.

Rozdział 7. Weryfikowanie instalacji

Po zainstalowaniu produktu IBM Business Monitor i utworzeniu profilu można opcjonalnie użyć konsoli Pierwsze kroki do sprawdzenia, czy produkt został zainstalowany poprawnie.

1. Uruchom konsolę Pierwsze kroki.
 - Otwórz okno komend. Przejdź do katalogu `katalog_główny_profilu/firststeps.wbm` i uruchom komendę `firststeps.sh`.
 - Na panelu Zakończono tworzenie profilu wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 - Wybierz opcję **Start > Wszystkie programy > IBM > Business Monitor 7.5 > Profile > nazwa_profilu > Pierwsze kroki**.
 - Przejdź do katalogu `katalog_główny_profilu/firststeps.wbm` i uruchom komendę `firststeps.bat`.

Ważne: Aby zainstalować lub uruchomić konsolę Pierwsze kroki w systemach Windows 7, Windows Vista lub Windows Server 2008, konieczne jest zwiększenie uprawnień konta użytkownika systemu Microsoft Windows przez kliknięcie prawym przyciskiem myszy pliku `firststeps.bat` i wybranie opcji **Uruchom jako administrator**. Jest to wymagane zarówno w przypadku administratorów, jak i użytkowników innych niż administratorzy.

2. W konsoli Pierwsze kroki wybierz opcję wykonania testu sprawdzającego instalację.
3. Przejrzyj wyniki.

Jeśli dla programu IBM Business Monitor włączono zabezpieczenia, po zakończeniu instalacji należy skonfigurować użytkowników, podając ID użytkownika i hasło dla aliasu uwierzytelniania `MonitorBusAuth`. Więcej szczegółów zawiera sekcja Określanie referencji w zabezpieczonym środowisku programu IBM Business Monitor.

Oprócz testu sprawdzania poprawności instalacji konsola Pierwsze kroki udostępnia opcje pozwalające na uruchomienie narzędzia Profile Management Tool, otwieranie Konsoli administracyjnej serwera WebSphere Application Server i otwieranie produktu Business Space.

W systemie Linux lub UNIX może być konieczna zmiana prawa własności z użytkownika `root` na innego użytkownika. Zadanie to jest wykonywane w programie IBM Business Monitor dokładnie tak samo, jak w przypadku serwera WebSphere Application Server lub Process Server. Więcej informacji na ten temat jest dostępnych w poniższych odsyłaczach do stron pokrewnych.

Jeśli w wyniku tworzenia nowego profilu produktu IBM Business Monitor lub rozszerzania istniejącego profilu za pomocą produktu IBM Business Monitor został zwrócony kod wyniku `INSTCONFPARTIALSUCCESS` lub `INSTCONFFAILED`, należy sprawdzić informacje w tabeli, do której odwołuje się odsyłacz do strony pokrewnej.

Rozdział 8. Określanie numerów portów

Aby określić numer portu do użycia przez interfejsy WWW, takie jak produkt Business Space i portletowe panele kontrolne, należy przejrzeć konfigurację w Konsoli administracyjnej serwera WebSphere Application Server.

Ze względów bezpieczeństwa i w celu równoważenia obciążenia w środowisku wdrożenia sieciowego zwykle jest używany serwer proxy lub serwer HTTP. Przychodzące żądania HTTP, zamiast przechodzić bezpośrednio do określonego elementu klastra, są kierowane na serwer proxy, który może rozdzielać żądania między wiele działających elementów klastra. W takim przypadku jest potrzebna nazwa hosta i numer portu serwera proxy lub serwera WWW, który z kolei przekazuje żądanie do elementu klastra.

- Aby określić numery portów serwera aplikacji, wykonaj następujące kroki:
 1. W Konsoli administracyjnej serwera WebSphere Application Server wybierz opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere**.
 2. Wybierz nazwę serwera lub elementu klastra (na przykład **serwer1**).
 3. W sekcji Komunikacja kliknij opcję **Porty**.

Numer portu dla interfejsów WWW, takich jak produkt Business Space i portletowe panele kontrolne, jest określony jako wartość opcji **WC_defaulthost_secure** w zabezpieczonym środowisku i jako wartość opcji **WC_defaulthost** w środowisku bez zabezpieczeń. Na tej stronie są też dostępne inne porty, w tym numer portu programu startowego i portu konektora, których wprowadzenie może być wymagane podczas pracy z programem IBM Business Monitor.

- Aby określić numery portów serwera proxy, wykonaj następujące kroki:
 1. W Konsoli administracyjnej produktu WebSphere Application Server wybierz opcję **Serwery > Typy serwerów > Serwery proxy WebSphere**.
 2. Wybierz nazwę serwera (na przykład **proxy**).
 3. W sekcji Komunikacja kliknij opcję **Porty**.

Numer portu dla interfejsów WWW, takich jak produkt Business Space i portletowe panele kontrolne jest określony jako wartość opcji **PROXY_HTTPS_ADDRESS** w środowisku z zabezpieczeniami i jako wartość opcji **PROXY_HTTP_ADDRESS** w środowisku bez zabezpieczeń. Na tej stronie są też dostępne inne porty, w tym numer portu programu startowego i portu konektora, których wprowadzenie może być wymagane podczas pracy z programem IBM Business Monitor.

Moduły WWW są wdrażane na hoście wirtualnym (o domyślnej nazwie **defaulthost**). Hosty wirtualne są konfigurowane w Konsoli administracyjnej po kliknięciu opcji **Środowisko > Hosty wirtualne**. Hosty wirtualne wybrane dla poszczególnych modułów WWW muszą mieć określony port HTTP lub HTTPS używany przez serwer (lub element klastra), na którym wdrożono moduły WWW. Dodatkowo każdy z modułów WWW produktu IBM Business Monitor powinien używać tego samego hosta wirtualnego. Moduły WWW znajdują się w większości aplikacji produktów IBM Business Monitor i Business Space oraz usługi REST (w plikach EAR).

Rozdział 9. Konfigurowanie środowiska

Po zainstalowaniu produktu IBM Business Monitor w topologii wdrożenia sieciowego (ND) należy wykonać dodatkowe zadania konfiguracyjne w celu zainstalowania wymaganych zasobów i pełnego przygotowania środowiska do monitorowania.

W przypadku utworzenia profilu autonomicznego dla produktu IBM Business Monitor wymagane zasoby są tworzone automatycznie jako część procesu tworzenia profilu. Konsola administracyjna umożliwia sprawdzenie statusu lub ponowne wdrożenie ręcznie usuniętego komponentu, jednak zazwyczaj zadania konfiguracyjne przedstawione w tej sekcji są wymagane tylko przy wdrożeniach sieciowych.

Tworzenie środowiska wdrażania za pomocą wzorca

Za pomocą kreatora konfiguracji środowiska wdrażania można utworzyć jeden lub większą liczbę klastrów i skonfigurować wszystkie wymagane komponenty dla topologii wdrożenia sieciowego programu IBM Business Monitor.

Przed utworzeniem klastrów i skonfigurowaniem komponentów programu IBM Business Monitor należy upewnić się, że zostały wykonane następujące czynności:

- Zainstalowano produkt IBM Business Monitor.
- Utworzono profil menedżera wdrażania programu IBM Business Monitor lub rozszerzono istniejący profil menedżera wdrażania za pomocą programu IBM Business Monitor.
- Utworzono bazę danych MONITOR.
- Uruchomiono menedżer wdrażania.
- Utworzono i stowarzyszono co najmniej jeden profil niestandardowy produktu IBM Business Monitor lub rozszerzono istniejący profil niestandardowy za pomocą produktu IBM Business Monitor.
- Uruchomiono profil lub profile niestandardowe.

Przed rozpoczęciem procesu konfiguracji należy upewnić się, że zmiany węzła są synchronizowane automatycznie. W tym celu w Konsoli administracyjnej należy kliknąć opcję **Administrowanie systemem > Preferencje konsoli** i wybrać opcję **Synchronizuj zmiany z węzłami**. W przeciwnym razie zmiany należy aktualizować ręcznie po każdym głównym kroku.

Dla produktu IBM Business Monitor dostępne są dwa wzorce: wzorzec pojedynczego klastra oraz wzorzec zdalnego przesyłania komunikatów, zdalnej obsługi i sieci WWW (czteroklastrowy).

Jeden z opcjonalnych kroków kreatora konfiguracji środowiska wdrażania obejmuje import dokumentu projektu bazy danych. Dokument projektu bazy danych definiuje konfigurację bazy danych dla wybranych składników środowiska wdrażania, a informacje z tego dokumentu są prezentowane w kreatorze na stronie Baza danych. Produkt IBM Business Monitor zawiera sterowane odpowiedziami narzędzie do projektowania baz danych (DbDesignGenerator) zadające użytkownikowi pytania dotyczące baz danych, które będą używane przez produkt IBM Business Monitor (dotyczy to informacji takich, jak platforma bazy danych oraz nazwy bazy danych, schematu i użytkownika). Wynikiem działania narzędzia do projektowania baz danych jest dokument projektu bazy danych używany przez to narzędzie do tworzenia skryptów bazy danych.

Aby skonfigurować środowisko wdrażania, wykonaj następujące kroki:

1. W Konsoli administracyjnej kliknij opcję **Serwery > Środowiska wdrażania**.
2. Aby uruchomić kreator konfiguracji środowiska wdrażania, kliknij opcję **Nowy** na stronie Środowiska wdrażania.
 - a. Opcja **Utwórz środowisko wdrażania w oparciu o wzorzec** jest wybrana.
 - b. W polu **Nazwa środowiska wdrażania** wprowadź unikalną nazwę środowiska wdrażania.
 - c. Aby wyświetlić wszystkie kroki konfiguracji w kreatorze, wybierz opcję **Szczegółowy: Pokaż wszystkie kroki**. Jeśli zostanie wybrana opcja **Krótką ścieżką: Pokaż tylko wymagane kroki**, kreator wyświetli wyłącznie strony, które nie mają przypisanej wartości domyślnej. Opcję **Krótką ścieżką: Pokaż tylko wymagane kroki** należy wybrać wyłącznie wtedy, gdy użytkownik akceptuje wartości domyślne udostępnione przez system dla konfiguracji środowiska wdrażania. W tym temacie założono, że wybrana została opcja **Szczegółowy: Pokaż wszystkie kroki**.
 - d. Kliknij przycisk **Dalej**, aby wyświetlić stronę Składniki środowiska wdrażania.
3. Na stronie Składniki środowiska wdrażania wybierz składnik środowiska wdrażania i kliknij przycisk **Dalej**, aby wyświetlić listę zgodnych składników albo listę wzorców środowiska wdrażania. Składniki reprezentują możliwości przetwarzania środowiska wykonawczego dla danego środowiska wdrażania. Lista dostępnych składników wyświetlana na stronie Składniki środowiska wdrażania jest oparta na profilu menedżera wdrażania. Jeśli profil menedżera wdrażania został rozszerzony i poza produktem IBM Business Monitor obejmuje również inne produkty (na przykład produkt IBM Business Process Manager), strona Składniki środowiska wdrażania będzie również zawierać te składniki. Wartość domyślna składnika środowiska wdrażania odpowiada możliwościom środowiska wykonawczego danego menedżera wdrażania.
4. Na stronie Wybór zgodnych składników środowiska wdrażania wybierz dodatkowe wymagane składniki i kliknij przycisk **Dalej**, aby wyświetlić listę wzorców powiązanych z wybranymi składnikami. Wraz ze składnikiem WBM może istnieć tylko jedna konfiguracja środowiska wdrażania. Jeśli konfiguracja środowiska wdrażania ze składnikiem WBM już istnieje, nie będzie możliwości kontynuowania, nawet jeśli ta konfiguracja środowiska wdrażania nie została wygenerowana.
5. Na stronie Wybór wzorca środowiska wdrażania wybierz wzorzec i kliknij przycisk **Dalej**, aby wyświetlić stronę Wybór węzłów.

Lista wzorców wyświetlana na stronie Wzorce środowiska wdrażania jest dynamiczna. Lista jest aktywowana przez następujące warunki środowiska i decyzje konfiguracyjne oraz zależna od nich:

 - Platforma, na której zainstalowano oprogramowanie.
 - Wybory dokonane na stronach Wybór składników środowiska wdrażania i Wybór zgodnych składników środowiska wdrażania.

Zazwyczaj istnieje możliwość wyboru między wzorcem pojedynczego klastra a wzorcem zdalnego przesyłania komunikatów, zdalnej obsługi i sieci WWW (czteroklastrowym). Opis tych wzorców znajduje się na stronie Topologia wysokiej dostępności (wdrożenie sieciowe) w sekcji planowania.
6. Na stronie Wybór węzłów wybierz węzły, które mają zostać włączone do danego środowiska wdrażania, a następnie kliknij przycisk **Dalej**, aby wyświetlić stronę Elementy klastra.

Należy wybrać jeden lub wiele węzłów produktu IBM Business Monitor dla środowiska wdrażania. Węzły programu IBM Business Monitor można zidentyfikować według wpisu dla produktu WBM w kolumnie wersji listy. Jeśli węzeł nie ma swojego wpisu dla produktu WBM w kolumnie wersji, a użytkownik chce go włączyć na potrzeby

programu IBM Business Monitor, należy rozszerzyć profil tego węzła za pomocą programu IBM Business Monitor i zrestartować kreator konfiguracji środowiska wdrażania.

Wszystkie wybrane węzły muszą mieć postać węzłów programu IBM Business Monitor. Jeśli w trzecim kroku zostaną wybrane dodatkowe funkcje, należy wybrać węzły obsługujące te funkcje.

W przypadku środowisk wysokiej dostępności i środowisk z funkcją przełączania awaryjnego należy wybrać przynajmniej dwa węzły na co najmniej dwóch odrębnych hostach. Aby uzyskać dodatkową skalowalność, należy wybrać więcej niż dwa węzły.

Aby włączyć węzeł, należy zaznaczyć pole wyboru obok nazwy węzła.

7. Na stronie Klastry przypisz przynajmniej jeden element klastra w przynajmniej jednym węźle dla każdej funkcji środowiska wdrażania.

Domyślnie w każdym węźle do każdej funkcji przypisany jest jeden element klastra. Aby zmienić tę liczbę, należy zastąpić liczby w poszczególnych kolumnach. W przypadku wdrożenia sieciowego klastry mogą współpracować w celu udostępnienia konkretnej funkcji w środowisku. W zależności od wymagań do każdego klastra w środowisku wdrażania należy przypisać konkretne funkcje, aby zapewnić wydajność, przełączanie awaryjne i moc obliczeniową.

Wartość 0 (zero) dla węzła oznacza, że dany węzeł nie bierze udziału w wybranej funkcji w oparciu o wybrane składniki.

Każdej funkcji należy przypisać przynajmniej jeden element klastra. W przypadku środowisk wysokiej dostępności i środowisk z funkcją przełączania awaryjnego należy wskazać przynajmniej dwa elementy klastra na funkcję. Aby uzyskać większą skalowalność, należy wskazać dodatkowe elementy klastra dla każdej funkcji.

Po przypisaniu elementu klastra można kliknąć przycisk **Dalej**, aby wyświetlić strony nazewnictwa klastrów dla poszczególnych typów klastrów środowiska wdrażania. Wyświetlane kroki podrzędne dotyczące nazewnictwa klastrów będą zależeć od wybranego wzorca środowiska wdrażania. Jeśli nazwy klastrów ani nazwy elementów klastrów nie mają być dostosowywane, należy użyć panelu nawigacyjnego kreatora, aby przejść od razu na stronę usług REST i przystąpić do realizacji następnego kroku.

- a. Opcjonalne: Dostosuj nazwy klastrów i elementów klastrów. Użyj strony nazewnictwa klastrów do skonfigurowania nazw klastrów i nazw elementów klastrów dla danego typu klastra. Zmodyfikować można również nazwy skrócone klastrów i elementów klastrów. Dla każdego typu klastra w ramach wybranego wzorca istnieje jedna strona kroku podrzędnego. Każda strona kroku podrzędnego zawiera następujące informacje:

| Pole | Opis | Wartość |
|---------|---|--|
| Klaster | Pole tylko do odczytu określające funkcjonalną rolę danego klastra. | <p>Pole może mieć następującą wartość (zależnie od typu klastra):</p> <ul style="list-style-type: none"> • Miejsce docelowe wdrażania aplikacji • Infrastruktura obsługi • Infrastruktura przesyłania komunikatów • Infrastruktura aplikacji WWW <p>Więcej informacji na temat ról funkcjonalnych udostępnianych przez poszczególne typy klastrów zawiera sekcja Topologie i wzorce środowisk wdrażania.</p> |

| Pole | Opis | Wartość |
|------------------------|--|--|
| Nazwa klastra | Wygenerowana przez system wartość domyślna dla nazwy klastra. | Wartości domyślne generuje się zgodnie z konwencją nazewnictwa <i>nazwa środowiska wdrażania.nazwa typu klastra</i> , gdzie <i>nazwa typu klastra</i> to jedna z następujących wartości: <ul style="list-style-type: none"> • CelAplikacji - dla klastrów pełniących rolę miejsca docelowego wdrażania aplikacji • PrzesyłanieKomunikatów - dla klastrów pełniących rolę infrastruktury przesyłania komunikatów • Obsługa - dla klastrów pełniących rolę infrastruktury obsługi • WWW - dla klastrów występujących w roli pomocniczych aplikacji WWW |
| Nazwa elementu klastra | Wygenerowana przez system wartość domyślna nazwy elementu klastra. Serwery wchodzące w skład klastra określa się mianem elementów klastra. | Należy zaakceptować wygenerowaną przez system wartość domyślną lub określić dowolną nazwę. Wartość domyślna nazwy elementu klastra jest generowana zgodnie z następującą konwencją nazewnictwa: <i>nazwa klastra.nazwa węzła.numer kolejny węzła</i> . Liczba nazw elementów klastra wyświetlanych w tabeli odpowiada liczbie elementów klastra wpisanych dla typu klastra w danej kolumnie i wierszu węzła na stronie Klastry. |

8. Na stronie Punkty końcowe systemowej usługi REST skonfiguruj punkty końcowe usługi dla aplikacyjnych interfejsów programistycznych (API) usług REST (Representational State Transfer).

Jeśli widżety mają być dostępne w produkcie Business Space, konieczne jest skonfigurowanie dla tych widżetów punktów końcowych usługi REST. Aby żądania usługi REST były przekazywane bezpośrednio do serwera aplikacji, jako nazwę hosta i port należy wprowadzić nazwę hosta i port serwera aplikacji. Aby żądania usługi REST były przekazywane przez serwer proxy lub serwer HTTP, który znajduje się przed jednym lub wieloma serwerami aplikacji, należy wprowadzić nazwę hosta i port serwera proxy lub serwera HTTP. W drugim przypadku serwer proxy lub serwer HTTP musi być już skonfigurowany. W przeciwnym razie należy pominąć tę stronę i skonfigurować punkty końcowe w późniejszym czasie.

- Skonfiguruj pełną ścieżkę adresu URL do wszystkich usług REST, wybierając z listy **Protokół** wartość **https://** lub **http://**.
- Wprowadź nazwę serwera proxy lub serwera HTTP w polu **Nazwa hosta lub host wirtualny w środowisku z równoważeniem obciążenia**.

Należy wpisać nazwę hosta lub hosta wirtualnego i numer portu, które są potrzebne klientowi do komunikowania się z serwerem lub klastrem. W środowisku klastrowym zwykle wpisuje się nazwę hosta i numer portu systemu równoważenia obciążenia. Jeśli pola hosta i portu pozostaną puste, jako wartości domyślne zostaną przyjęte host elementu klastra oraz jego port HTTP. W przypadku środowiska z równoważeniem obciążenia należy później zmienić wartości domyślne na nazwę hosta wirtualnego i port systemu równoważenia obciążenia. Koniecznie należy wpisać pełną nazwę hosta.

- c. W polu **Port** wprowadź numer portu wymaganego przez klient w celu komunikacji z serwerem lub klastrem.
 - d. Jeśli zachodzi potrzeba zmodyfikowania opisu punktu końcowego usługi REST, w tabeli usług REST zastąp wpis w polu Opis. Pozostałe pola są tylko do odczytu.
 - e. Kliknij przycisk **Dalej**, aby przejść do strony Import konfiguracji bazy danych.
9. Opcjonalne: Na stronie Import konfiguracji bazy danych kliknij przycisk **Przełóżaj**, aby przejść do dokumentu projektu bazy danych, lub wpisz ścieżkę do dokumentu projektu bazy danych. Następnie kliknij przycisk **Dalej**, aby przejść do strony Źródła danych. Po zaimportowaniu dokumentu projektu informacje z tego dokumentu są odzwierciedlane w kreatorze na stronie Baza danych. Dokument projektu może być oparty na projekcie bazy danych utworzonym przy użyciu narzędzia do projektowania bazy danych lub może to być dostarczony dokument projektu oparty na wybranym wzorcu i składniku.
10. Na stronie Baza danych skonfiguruj parametry bazy danych dla źródeł danych środowiska wdrażania, a następnie kliknij przycisk **Dalej**, aby przejść do strony Zabezpieczenia.

Na tej stronie należy zdefiniować informacje bazy danych dla komponentów włączonych do danego środowiska wdrażania. Jeśli jest to możliwe, kreator podaje domyślne informacje dla parametrów, ale te wartości należy zmienić tak, aby odpowiadały wartościom zdefiniowanym podczas planowania środowiska. W przypadku zmiany dostawców można kliknąć przycisk **Edytuj dostawcę**, aby edytować wybranego dostawcę.

Uwaga: Jeśli dokument projektu bazy danych zaimportowano, informacje na stronie Baza danych odzwierciedlają konfigurację źródła danych istniejącą w zaimportowanym dokumencie projektu bazy danych. W przypadku wprowadzenia zmian w konfiguracji źródła danych już po zaimportowaniu dokumentu projektu bazy danych zastosowane modyfikacje mogą okazać się niezgodne ze skryptem DDL wygenerowanym przez narzędzie do projektowania bazy danych oraz z oryginalnymi wartościami.

Ten krok jest wyświetlany warunkowo w konfiguracji środowiska wdrażania w trybie krótkiej ścieżki. Krok jest wyświetlany w konfiguracji środowiska wdrażania w trybie krótkiej ścieżki, jeśli zdefiniowano więcej niż jedną bazę danych.

Krok jest zawsze wyświetlany, jeśli jako dostawca bazy danych używana jest baza danych DB2 for z/OS lub Oracle .

Składnik IBM Business Monitor udostępnia następujące wpisy:

| Komponent | Źródło danych |
|--|---|
| Źródło danych dla mechanizmu przesyłania komunikatów produktu Business Monitor | Źródło danych dla mechanizmu przesyłania komunikatów produktu IBM Business Monitor. |
| Składnica treści produktu Cognos | Źródło danych dla składnicy treści produktu IBM Cognos Business Intelligence. Źródło jest wyświetlane tylko wtedy, gdy zainstalowano produkt IBM Cognos BI, lecz jeszcze go nie skonfigurowano. |

| Komponent | Źródło danych |
|----------------|---|
| Business Space | Źródło danych dla komponentu Business Space. Opcja Utwórz tabelę nie jest dostępna dla tego komponentu. Jeśli środowisko wdrażania zawiera komponent Business Space, należy ręcznie utworzyć tabelę bazy danych dla tego komponentu. |

Jeśli wybrano inne składniki produktu dla tej topologii, mogą zostać wyświetlone także inne wpisy (właściwe tym składnikom).

Domyślne nazwy schematów wyświetlane na tej stronie mogą być sprzeczne z konwencją nazewnictwa serwisu lub powodować konflikty z istniejącymi schematami. W większości przypadków nazwę schematu należy zmienić.

Uwaga: W przypadku baz danych DB2 for z/OS nazwa schematu skonfigurowana na tym panelu zostanie użyta w roli wartości identyfikatora DB2 z/OS SQLID. Jeśli w bieżącym środowisku wartość identyfikatora DB2 z/OS SQLID musi być inna, po zakończeniu pracy z kreatorem środowiska wdrażania można ręcznie zaktualizować utworzone źródła danych i ustawić poprawną wartość we właściwości niestandardowej currentSQLID.

Istnieje możliwość edytowania wszystkich kluczowych parametrów, takich jak nazwa bazy danych, opcja określająca tworzenie tabel, nazwa użytkownika środowiska wykonawczego źródła danych oraz nazwa użytkownika i hasło dla źródła danych umożliwiające nawiązanie połączenia z bazą danych.

Uwaga: W przypadku baz danych DB2 for z/OS nazwa bazy danych jest jednocześnie nazwą podsystemu bazy danych. W przypadku pozostałych wersji bazy danych DB2 nazwa bazy danych odpowiada nazwie bazy danych MONITOR. W przypadku baz danych Oracle nazwa bazy danych odpowiada identyfikatorowi Oracle System ID.

Dla danego komponentu można wybrać, która baza danych ma być używana.

Opcja **Utwórz tabelę** nie jest dostępna, jeśli w roli dostawcy bazy danych jest używana baza danych DB2 for z/OS lub Oracle.

W przypadku bazy danych Oracle pole **Schemat** jest wyłączone i puste, a pole **Nazwa użytkownika** nie jest wstępnie wypełnione nazwą użytkownika wspólnej bazy danych. Należy wprowadzić nazwę użytkownika i hasło dla każdego źródła danych.

Uwaga: Program nie wykonuje sprawdzenia, czy wprowadzone nazwy użytkownika są unikalne, dlatego należy zadbać, aby nie zostały wprowadzone duplikaty nazwy użytkownika, co będzie skutkowało konfliktami tabel.

- Na stronie Zabezpieczenia wpisz ID użytkowników i hasła niezbędne do skonfigurowania komponentów programu IBM Business Monitor. Składnik IBM Business Monitor udostępnia następujące wpisy:

| Komponent | ID użytkownika i hasło |
|--|---|
| Alias uwierzytelniania na potrzeby zasobów JMS usługi zdarzeń infrastruktury CEI | Określa identyfikator użytkownika i hasło, które zostaną użyte do zabezpieczenia domyślnej magistrali integracji usług infrastruktury CEI (Common Event Infrastructure). |
| Uwierzytelnianie dostępu administracyjnego produktu Cognos | Określa identyfikator i hasło użytkownika z prawami administracyjnymi do usługi produktu IBM Cognos BI. Źródło jest wyświetlane tylko wtedy, gdy zainstalowano produkt IBM Cognos BI, lecz jeszcze go nie skonfigurowano. |

Jeśli wybrano inne składniki produktu dla tej topologii, mogą zostać wyświetlone także inne wpisy (właściwe tym składnikom).

- Opcjonalne: Jeśli została wyświetlona strona produktu Business Process Choreographer, ustaw parametry konfiguracji produktu Business Process Choreographer, a następnie

kliknij przycisk **Dalej**, aby wyświetlić stronę Systemowe aplikacje WWW. Na tej stronie należy określić wartości dla następujących opcji:

- Role zabezpieczeń
 - Aliasy uwierzytelniania
13. Opcjonalne: Jeśli została wyświetlona strona Systemowe aplikacje WWW, określ kontekstowy katalog główny dla aplikacji WWW opartych na komponentach w danym środowisku wdrażania lub zaakceptuj udostępnione przez system wartości domyślne dla kontekstowych katalogów głównych. Następnie kliknij przycisk **Dalej**, aby wyświetlić stronę Podsumowanie.

Tabela zawiera następujące informacje sterujące.

Aplikacja WWW

Nazwa aplikacji WWW.

Niektóre z komponentów, które są częścią tworzonego środowiska wdrażania, zawierają aplikacje WWW. W kolumnie **Aplikacja WWW** mogą znajdować się następujące komponenty:

- Eksplorator produktu Business Process Choreographer
- Business Space
- Menedżer reguł biznesowych

Kontekstowy katalog główny

Bieżąca wartość kontekstowego katalogu głównego dla komponentu.

Domyślnie stosowany jest domyślny kontekstowy katalog główny dla aplikacji WWW. Kontekstowe katalogi główne można zmieniać, wpisując nową wartość w polu **Kontekstowy katalog główny**.

Uwaga: Kontekstowy katalog główny produktu Business Space jest tylko do odczytu i nie może być edytowany.

14. Sprawdź, czy informacje podane na stronie Podsumowanie są poprawne i kliknij opcję **Zakończ i wygeneruj środowisko**, aby zapisać i zakończyć konfigurację środowiska wdrażania. Aby wyjść bez zakończenia konfiguracji, kliknij przycisk **Zakończ**.

Kliknięcie przycisku **Zakończ** powoduje zapisanie konfiguracji środowiska wdrażania, ale nie zostanie ona wygenerowana.

Kliknięcie przycisku **Anuluj** powoduje anulowanie konfiguracji wdrożenia. Konfiguracja nie zostanie zapisana.

15. Jeśli środowisko wdrażania wygenerowano, klikając przycisk **Zakończ i generuj środowisko**, zatrzymaj i zrestartuj wszystkie klastry, węzły i menedżer wdrażania.

Jeśli pracy z kreatorem konfiguracji środowiska wdrażania nie zakończono wygenerowaniem tego środowiska (jeśli kliknięto przycisk **Zakończ** zamiast przycisku **Zakończ i generuj środowisko**), można teraz wyświetlić konfigurację środowiska wdrażania, wybierając opcję **Serwer > Środowiska wdrażania > nazwa środowiska wdrażania**. Aby po wybraniu tej opcji wygenerować środowisko wdrażania, należy kliknąć przycisk **Generuj**. Po zakończeniu konfiguracji można sprawdzić pliki konfiguracyjne w celu przejrzania zmian.

Zmiany należy zapisać w konfiguracji głównej lub je odrzucić. W przypadku kliknięcia środowiska wdrażania na liście, jeśli niektóre kroki konfiguracji nie zostały jeszcze wykonane, zostanie wyświetlona lista odroczonej konfiguracji. Po wygenerowaniu środowiska wdrażania należy zatrzymać i zrestartować wszystkie klastry, węzły i menedżer wdrażania.

Importowanie definicji środowisk wdrażania opartych na dokumentach projektu

Istnieje możliwość zaimportowania istniejącej definicji środowiska wdrażania opartej na dokumencie projektu z innego menedżera wdrażania, aby posłużyła jako podstawa do konfiguracji nowego środowiska wdrażania.

- Dostępna musi być kopia dokumentu projektu środowiska wdrażania wyeksportowanego z innego menedżera wdrażania.
- Użytkownik musi posiadać dostęp do dokumentu projektu środowiska wdrażania (plik XML) z menedżera wdrażania, do którego projekt środowiska wdrażania będzie importowany.
- Menedżer wdrażania, do którego będzie importowana definicja środowiska wdrażania musi obsługiwać co najmniej wszystkie funkcje, jakie są zdefiniowane w dokumencie projektu środowiska wdrażania. Na przykład projekt środowiska wdrażania utworzony w menedżerze wdrażania produktu WebSphere Enterprise Service Bus można zaimportować do menedżera wdrażania produktu Process Server, ale w odwrotną stronę taki import jest niemożliwy.

Uwaga: Jeśli włączono zabezpieczenia i autoryzację opartą na rolach, aby móc wykonać tę czynność, należy zalogować się do Konsoli administracyjnej jako administrator.

Ważne: Nie można jednocześnie importować wielu dokumentów projektu środowiska wdrażania z pliku skompresowanego. Należy wyodrębnić dokumenty projektów z pliku skompresowanego, a następnie pojedynczo importować pliki XML.

Przed rozpoczęciem procesu konfiguracji należy upewnić się, że zmiany węzła są zsynchronizowane automatycznie. W tym celu w Konsoli administracyjnej należy kliknąć opcję **Administrowanie systemem > Preferencje konsoli** i wybrać opcję **Synchronizuj zmiany z węzłami**. W przeciwnym razie zmiany należy aktualizować ręcznie po każdym głównym kroku.

Importowanie istniejącego projektu środowiska wdrażania w celu utworzenia nowego środowiska pozwala ograniczyć czas poświęcony na konfigurowanie środowiska wdrażania. Jeśli istniejące środowisko jest podobne do tworzonego środowiska, należy wyeksportować jego projekt, a następnie zaimportować go do konfigurowanego menedżera wdrażania.

1. W Konsoli administracyjnej kliknij opcję **Serwery > Środowiska wdrażania**.

2. Na stronie Środowiska wdrażania kliknij opcję **Importuj**, aby uruchomić kreator Konfiguracja środowiska wdrażania.

Kreator jest uruchamiany z wybraną opcją **Utwórz środowisko wdrażania w oparciu o zaimportowany projekt**.

3. Kliknij przycisk **Przeglądaj** i wybierz dokument projektu środowiska wdrażania (plik XML) do zaimportowania lub wpisz pełną ścieżkę do tego dokumentu.

4. Kliknij przycisk **Dalej**, aby załadować konfigurację i uruchomić kreator Import środowiska wdrażania.

Kreator wyświetla stronę Wybór węzłów, chyba że wszystkie nazwy węzłów odpowiadają aktualnie stowarzyszonym węzłom. Jeśli wszystkie węzły są zgodne, kreator wyświetla stronę Baza danych.

Ważne: Kliknięcie opcji Konfiguruj na dowolnym panelu kreatora spowoduje skonfigurowanie środowiska wdrażania przy użyciu bieżących wartości.

5. Opcjonalne: Z listy możliwych węzłów na stronie Wybór węzłów wybierz węzły, które mają być włączone do środowiska wdrażania i kliknij przycisk **Dalej**.

Aby włączyć węzeł, należy zaznaczyć pole wyboru obok nazwy węzła.

Ważne: Przycisk **Dalej** jest niedostępny, jeśli wybrane węzły nie spełniają ograniczeń narzuconych przez zaimportowany projekt środowiska wdrażania. Na przykład, jeśli środowisko wdrażania musi zawierać węzeł o nazwie “Węzeł_obowiązkowy” i 3 inne węzły o dowolnej nazwie, nie będzie można kontynuować, dopóki nie zostanie wybrany węzeł “Węzeł_obowiązkowy” i 3 inne węzły.

6. Na stronie Klastry przypisz przynajmniej jeden element klastra w przynajmniej jednym węźle dla każdej funkcji środowiska wdrażania.

Domyślnie w każdym węźle do każdej funkcji przypisany jest jeden element klastra. Aby zmienić tę liczbę, należy zastąpić liczby w poszczególnych kolumnach. W przypadku wdrożenia sieciowego klastry mogą współpracować w celu udostępnienia konkretnej funkcji w środowisku. W zależności od wymagań do każdego klastra w środowisku wdrażania należy przypisać konkretne funkcje, aby zapewnić wydajność, przełączanie awaryjne i moc obliczeniową.

Wartość 0 (zero) dla węzła oznacza, że dany węzeł nie bierze udziału w wybranej funkcji w oparciu o wybrane składniki.

Każdej funkcji należy przypisać przynajmniej jeden element klastra. W przypadku środowisk wysokiej dostępności i środowisk z funkcją przełączania awaryjnego należy wskazać przynajmniej dwa elementy klastra na funkcję. Aby uzyskać większą skalowalność, należy wskazać dodatkowe elementy klastra dla każdej funkcji.

Po przypisaniu elementu klastra można kliknąć przycisk **Dalej**, aby wyświetlić strony nazewnictwa klastrów dla poszczególnych typów klastrów środowiska wdrażania. Wyświetlane kroki podrzędne dotyczące nazewnictwa klastrów będą zależeć od wybranego wzorca środowiska wdrażania. Jeśli nazwy klastrów ani nazwy elementów klastrów nie mają być dostosowywane, należy użyć panelu nawigacyjnego kreatora, aby przejść od razu na stronę usług REST i przystąpić do realizacji następnego kroku.

- a. Opcjonalne: Dostosuj nazwy klastrów i elementów klastrów. Użyj strony nazewnictwa klastrów do skonfigurowania nazw klastrów i nazw elementów klastrów dla danego typu klastra. Zmodyfikować można również nazwy skrócone klastrów i elementów klastrów. Dla każdego typu klastra w ramach wybranego wzorca istnieje jedna strona kroku podrzędnego. Każda strona kroku podrzędnego zawiera następujące informacje:

| Pole | Opis | Wartość |
|---------|---|--|
| Klaster | Pole tylko do odczytu określające funkcjonalną rolę danego klastra. | <p>Pole może mieć następującą wartość (zależnie od typu klastra):</p> <ul style="list-style-type: none"> Miejsce docelowe wdrażania aplikacji Infrastruktura obsługi Infrastruktura przesyłania komunikatów Infrastruktura aplikacji WWW <p>Więcej informacji na temat ról funkcjonalnych udostępnianych przez poszczególne typy klastrów zawiera sekcja Topologie i wzorce środowisk wdrażania.</p> |

| Pole | Opis | Wartość |
|------------------------|--|--|
| Nazwa klastra | Wygenerowana przez system wartość domyślna dla nazwy klastra. | Wartości domyślne generuje się zgodnie z konwencją nazewnictwa <i>nazwa środowiska wdrażania.nazwa typu klastra</i> , gdzie <i>nazwa typu klastra</i> to jedna z następujących wartości: <ul style="list-style-type: none"> • CelAplikacji - dla klastrów pełniących rolę miejsca docelowego wdrażania aplikacji • PrzesyłanieKomunikatów - dla klastrów pełniących rolę infrastruktury przesyłania komunikatów • Obsługa - dla klastrów pełniących rolę infrastruktury obsługi • WWW - dla klastrów występujących w roli pomocniczych aplikacji WWW |
| Nazwa elementu klastra | Wygenerowana przez system wartość domyślna nazwy elementu klastra. Serwery wchodzące w skład klastra określa się mianem elementów klastra. | Należy zaakceptować wygenerowaną przez system wartość domyślną lub określić dowolną nazwę. Wartość domyślna nazwy elementu klastra jest generowana zgodnie z następującą konwencją nazewnictwa: <i>nazwa klastra.nazwa węzła.numer kolejny węzła</i> . Liczba nazw elementów klastra wyświetlanych w tabeli odpowiada liczbie elementów klastra wpisanych dla typu klastra w danej kolumnie i wierszu węzła na stronie Klastry. |

7. Na stronie Punkty końcowe systemowej usługi REST skonfiguruj punkty końcowe usługi dla aplikacyjnych interfejsów programistycznych (API) usług REST (Representational State Transfer).

Jeśli widżety mają być dostępne w produkcie Business Space, konieczne jest skonfigurowanie dla tych widżetów punktów końcowych usługi REST. Aby żądania usługi REST były przekazywane bezpośrednio do serwera aplikacji, jako nazwę hosta i port należy wprowadzić nazwę hosta i port serwera aplikacji. Aby żądania usługi REST były przekazywane przez serwer proxy lub serwer HTTP, który znajduje się przed jednym lub wieloma serwerami aplikacji, należy wprowadzić nazwę hosta i port serwera proxy lub serwera HTTP. W drugim przypadku serwer proxy lub serwer HTTP musi być już skonfigurowany. W przeciwnym razie należy pominąć tę stronę i skonfigurować punkty końcowe w późniejszym czasie.

- Skonfiguruj pełną ścieżkę adresu URL do wszystkich usług REST, wybierając z listy **Protokół** wartość **https://** lub **http://**.
- Wprowadź nazwę serwera proxy lub serwera HTTP w polu **Nazwa hosta lub host wirtualny w środowisku z równoważeniem obciążenia**.

Należy wpisać nazwę hosta lub hosta wirtualnego i numer portu, które są potrzebne klientowi do komunikowania się z serwerem lub klastrem. W środowisku klastrowym zwykle wpisuje się nazwę hosta i numer portu systemu równoważenia obciążenia. Jeśli pola hosta i portu pozostaną puste, jako wartości domyślne zostaną przyjęte host elementu klastra oraz jego port HTTP. W przypadku środowiska z równoważeniem obciążenia należy później zmienić wartości domyślne na nazwę hosta wirtualnego i port systemu równoważenia obciążenia. Koniecznie należy wpisać pełną nazwę hosta.

- c. W polu **Port** wprowadź numer portu wymaganego przez klient w celu komunikacji z serwerem lub klastrem.
 - d. Jeśli zachodzi potrzeba zmodyfikowania opisu punktu końcowego usługi REST, w tabeli usług REST zastąp wpis w polu Opis. Pozostałe pola są tylko do odczytu.
 - e. Kliknij przycisk **Dalej**, aby przejść do strony Import konfiguracji bazy danych.
8. Opcjonalne: Na stronie Import konfiguracji bazy danych kliknij przycisk **Przeglądaj**, aby przejść do dokumentu projektu bazy danych, lub wpisz ścieżkę do dokumentu projektu bazy danych. Następnie kliknij przycisk **Dalej**, aby przejść do strony Źródła danych. Po zaimportowaniu dokumentu projektu informacje z tego dokumentu są odzwierciedlane w kreatorze na stronie Baza danych. Dokument projektu może być oparty na projekcie bazy danych utworzonym przy użyciu narzędzia do projektowania bazy danych lub może to być dostarczony dokument projektu oparty na wybranym wzorcu i składniku.
9. Na stronie Baza danych skonfiguruj parametry bazy danych dla źródeł danych środowiska wdrażania, a następnie kliknij przycisk **Dalej**, aby przejść do strony Zabezpieczenia.

Na tej stronie należy zdefiniować informacje bazy danych dla komponentów włączonych do danego środowiska wdrażania. Jeśli jest to możliwe, kreator podaje domyślne informacje dla parametrów, ale te wartości należy zmienić tak, aby odpowiadały wartościom zdefiniowanym podczas planowania środowiska. W przypadku zmiany dostawców można kliknąć przycisk **Edytuj dostawcę**, aby edytować wybranego dostawcę.

Uwaga: Jeśli dokument projektu bazy danych zaimportowano, informacje na stronie Baza danych odzwierciedlają konfigurację źródła danych istniejącą w zaimportowanym dokumencie projektu bazy danych. W przypadku wprowadzenia zmian w konfiguracji źródła danych już po zaimportowaniu dokumentu projektu bazy danych zastosowane modyfikacje mogą okazać się niezgodne ze skryptem DDL wygenerowanym przez narzędzie do projektowania bazy danych oraz z oryginalnymi wartościami.

Ten krok jest wyświetlany warunkowo w konfiguracji środowiska wdrażania w trybie krótkiej ścieżki. Krok jest wyświetlany w konfiguracji środowiska wdrażania w trybie krótkiej ścieżki, jeśli zdefiniowano więcej niż jedną bazę danych.

Krok jest zawsze wyświetlany, jeśli jako dostawca bazy danych używana jest baza danych DB2 for z/OS lub Oracle .

Składnik IBM Business Monitor udostępnia następujące wpisy:

| Komponent | Źródło danych |
|--|---|
| Źródło danych dla mechanizmu przesyłania komunikatów produktu Business Monitor | Źródło danych dla mechanizmu przesyłania komunikatów produktu IBM Business Monitor. |
| Składnica treści produktu Cognos | Źródło danych dla składnicy treści produktu IBM Cognos Business Intelligence. Źródło jest wyświetlane tylko wtedy, gdy zainstalowano produkt IBM Cognos BI, lecz jeszcze go nie skonfigurowano. |

| Komponent | Źródło danych |
|----------------|---|
| Business Space | Źródło danych dla komponentu Business Space. Opcja Utwórz tabelę nie jest dostępna dla tego komponentu. Jeśli środowisko wdrażania zawiera komponent Business Space, należy ręcznie utworzyć tabelę bazy danych dla tego komponentu. |

Jeśli wybrano inne składniki produktu dla tej topologii, mogą zostać wyświetlone także inne wpisy (właściwe tym składnikom).

Domyślne nazwy schematów wyświetlane na tej stronie mogą być sprzeczne z konwencją nazewnictwa serwisu lub powodować konflikty z istniejącymi schematami. W większości przypadków nazwę schematu należy zmienić.

Uwaga: W przypadku baz danych DB2 for z/OS nazwa schematu skonfigurowana na tym panelu zostanie użyta w roli wartości identyfikatora DB2 z/OS SQLID. Jeśli w bieżącym środowisku wartość identyfikatora DB2 z/OS SQLID musi być inna, po zakończeniu pracy z kreatorem środowiska wdrażania można ręcznie zaktualizować utworzone źródła danych i ustawić poprawną wartość we właściwości niestandardowej currentSQLID.

Istnieje możliwość edytowania wszystkich kluczowych parametrów, takich jak nazwa bazy danych, opcja określająca tworzenie tabel, nazwa użytkownika środowiska wykonawczego źródła danych oraz nazwa użytkownika i hasło dla źródła danych umożliwiające nawiązanie połączenia z bazą danych.

Uwaga: W przypadku baz danych DB2 for z/OS nazwa bazy danych jest jednocześnie nazwą podsystemu bazy danych. W przypadku pozostałych wersji bazy danych DB2 nazwa bazy danych odpowiada nazwie bazy danych MONITOR. W przypadku baz danych Oracle nazwa bazy danych odpowiada identyfikatorowi Oracle System ID.

Dla danego komponentu można wybrać, która baza danych ma być używana.

Opcja **Utwórz tabelę** nie jest dostępna, jeśli w roli dostawcy bazy danych jest używana baza danych DB2 for z/OS lub Oracle.

W przypadku bazy danych Oracle pole **Schemat** jest wyłączone i puste, a pole **Nazwa użytkownika** nie jest wstępnie wypełnione nazwą użytkownika wspólnej bazy danych. Należy wprowadzić nazwę użytkownika i hasło dla każdego źródła danych.

Uwaga: Program nie wykonuje sprawdzenia, czy wprowadzone nazwy użytkownika są unikalne, dlatego należy zadbać, aby nie zostały wprowadzone duplikaty nazwy użytkownika, co będzie skutkowało konfliktami tabel.

- Na stronie Zabezpieczenia wpisz ID użytkowników i hasła niezbędne do skonfigurowania komponentów programu IBM Business Monitor. Składnik IBM Business Monitor udostępnia następujące wpisy:

| Komponent | ID użytkownika i hasło |
|--|---|
| Alias uwierzytelniania na potrzeby zasobów JMS usługi zdarzeń infrastruktury CEI | Określa identyfikator użytkownika i hasło, które zostaną użyte do zabezpieczenia domyślnej magistrali integracji usług infrastruktury CEI (Common Event Infrastructure). |
| Uwierzytelnianie dostępu administracyjnego produktu Cognos | Określa identyfikator i hasło użytkownika z prawami administracyjnymi do usługi produktu IBM Cognos BI. Źródło jest wyświetlane tylko wtedy, gdy zainstalowano produkt IBM Cognos BI, lecz jeszcze go nie skonfigurowano. |

Jeśli wybrano inne składniki produktu dla tej topologii, mogą zostać wyświetlone także inne wpisy (właściwe tym składnikom).

- Opcjonalne: Jeśli została wyświetlona strona produktu Business Process Choreographer, ustaw parametry konfiguracji produktu Business Process Choreographer, a następnie

kliknij przycisk **Dalej**, aby wyświetlić stronę Systemowe aplikacje WWW. Na tej stronie należy określić wartości dla następujących opcji:

- Role zabezpieczeń
 - Aliasy uwierzytelniania
12. Opcjonalne: Jeśli została wyświetlona strona Systemowe aplikacje WWW, określ kontekstowy katalog główny dla aplikacji WWW opartych na komponentach w danym środowisku wdrażania lub zaakceptuj udostępnione przez system wartości domyślne dla kontekstowych katalogów głównych. Następnie kliknij przycisk **Dalej**, aby wyświetlić stronę Podsumowanie.

Tabela zawiera następujące informacje sterujące.

Aplikacja WWW

Nazwa aplikacji WWW.

Niektóre z komponentów, które są częścią tworzonego środowiska wdrażania, zawierają aplikacje WWW. W kolumnie **Aplikacja WWW** mogą znajdować się następujące komponenty:

- Eksplorator produktu Business Process Choreographer
- Business Space
- Menedżer reguł biznesowych

Kontekstowy katalog główny

Bieżąca wartość kontekstowego katalogu głównego dla komponentu.

Domyślnie stosowany jest domyślny kontekstowy katalog główny dla aplikacji WWW. Kontekstowe katalogi główne można zmieniać, wpisując nową wartość w polu **Kontekstowy katalog główny**.

Uwaga: Kontekstowy katalog główny produktu Business Space jest tylko do odczytu i nie może być edytowany.

13. Sprawdź, czy informacje podane na stronie Podsumowanie są poprawne i kliknij opcję **Zakończ i wygeneruj środowisko**, aby zapisać i zakończyć konfigurację środowiska wdrażania. Aby wyjść bez zakończenia konfiguracji, kliknij przycisk **Zakończ**.

Kliknięcie przycisku **Zakończ** powoduje zapisanie konfiguracji środowiska wdrażania, ale nie zostanie ona wygenerowana.

Kliknięcie przycisku **Anuluj** powoduje anulowanie konfiguracji wdrożenia. Konfiguracja nie zostanie zapisana.

14. Jeśli środowisko wdrażania wygenerowano, klikając przycisk **Zakończ i generuj środowisko**, zatrzymaj i zrestartuj wszystkie klastry, węzły i menedżer wdrażania.

Jeśli pracy z kreatorem konfiguracji środowiska wdrażania nie zakończono wygenerowaniem tego środowiska (jeśli kliknięto przycisk **Zakończ** zamiast przycisku **Zakończ i generuj środowisko**), można teraz wyświetlić konfigurację środowiska wdrażania, wybierając opcję **Serwer > Środowiska wdrażania > nazwa środowiska wdrażania**. Aby po wybraniu tej opcji wygenerować środowisko wdrażania, należy kliknąć przycisk **Generuj**. Po zakończeniu konfiguracji można sprawdzić pliki konfiguracyjne w celu przejrzania zmian.

Zmiany należy zapisać w konfiguracji głównej lub je odrzucić. W przypadku kliknięcia środowiska wdrażania na liście, jeśli niektóre kroki konfiguracji nie zostały jeszcze wykonane, zostanie wyświetlona lista odroczonej konfiguracji. Po wygenerowaniu środowiska wdrażania należy zatrzymać i zrestartować wszystkie klastry, węzły i menedżer wdrażania.

Tworzenie środowiska wdrażania przy użyciu topologii niestandardowej

Zamiast używać jednego z udostępnionych wzorców środowiska wdrażania można skonfigurować własne klastry i komponenty produktu IBM Business Monitor w topologii wdrożenia sieciowego.

Przed utworzeniem klastrów i skonfigurowaniem komponentów programu IBM Business Monitor należy upewnić się, że zostały wykonane następujące czynności:

- Zainstalowano produkt IBM Business Monitor.
- Utworzono profil menedżera wdrażania programu IBM Business Monitor lub rozszerzono istniejący profil menedżera wdrażania za pomocą programu IBM Business Monitor.
- Utworzono bazę danych MONITOR.
- Uruchomiono menedżer wdrażania.
- Utworzono i stowarzyszono co najmniej jeden profil niestandardowy produktu IBM Business Monitor lub rozszerzono istniejący profil niestandardowy za pomocą produktu IBM Business Monitor.
- Uruchomiono profil lub profile niestandardowe.

W następujących instrukcjach opisano tworzenie klastrów, konfigurowanie usługi zdarzeń infrastruktury CEI oraz instalowanie i konfigurowanie wymaganych komponentów za pomocą kreatora konfiguracji lub komend wsadmin.

Tworzenie klastrów programu IBM Business Monitor

W środowisku wdrożenia sieciowego komponenty programu IBM Business Monitor muszą być wdrożone w klastrach.

Przed utworzeniem klastrów i skonfigurowaniem komponentów programu IBM Business Monitor należy upewnić się, że zostały wykonane następujące czynności:

- Zainstalowano produkt IBM Business Monitor.
- Utworzono profil menedżera wdrażania programu IBM Business Monitor lub rozszerzono istniejący profil menedżera wdrażania za pomocą programu IBM Business Monitor.
- Utworzono bazę danych MONITOR.
- Uruchomiono menedżer wdrażania.
- Utworzono i stowarzyszono co najmniej jeden profil niestandardowy produktu IBM Business Monitor lub rozszerzono istniejący profil niestandardowy za pomocą produktu IBM Business Monitor.
- Uruchomiono profil lub profile niestandardowe.

W celu utworzenia pierwszego elementu klastra należy użyć istniejącego profilu niestandardowego. W każdym tworzonym klastrze można dodać dowolną liczbę elementów (informacje na ten temat zawiera sekcja Dodawanie elementów klastra). Aby utworzyć klaster programu IBM Business Monitor, wykonaj następujące kroki w Konsoli administracyjnej:

1. Na panelu nawigacyjnym kliknij opcję **Serwery > Klastry > Klastry serwerów aplikacji WebSphere**.
2. Kliknij opcję **Nowy**, aby uruchomić kreator tworzenia nowego klastra.
3. Podaj nazwę klastra.
4. Wybierz opcję **Preferuj lokalne**, aby włączyć optymalizację routingu w zasięgu hosta. To ustawienie zwiększa wydajność dzięki wyszukiwaniu komponentów EJB w elemencie klastra w tym samym węźle, jeśli jest to możliwe.
5. Kliknij przycisk **Dalej**, aby przejść do kroku tworzenia pierwszego elementu klastra.
6. Określ nazwę pierwszego elementu klastra.

7. Określ węzeł dla pierwszego elementu klastra. Ten węzeł musi być węzłem programu IBM Business Monitor.
8. Wybierz opcję **Utwórz element, używając szablonu serwera aplikacji**.
9. Wybierz szablon serwera aplikacji, w którego nazwie zawarty jest tekst *defaultWBM*, i kliknij przycisk **Dalej**.

Ważne: Jeśli nie istnieje żaden szablon, którego nazwa zawiera tekst defaultWBM, należy się upewnić, że wybrano węzeł rozszerzony przy użyciu programu IBM Business Monitor.

Jeśli pierwszy element klastra nie został utworzony za pomocą szablonu serwera aplikacji z tekstem defaultWBM w nazwie, środowisko programu IBM Business Monitor nie będzie działać poprawnie. W takiej sytuacji niezbędne będzie usunięcie wszystkich istniejących elementów klastra i ponowne utworzenie pierwszego elementu klastra.

10. Kliknij przycisk **Dalej**, aby przejść do kroku tworzenia dodatkowych elementów klastra.
11. Opcjonalne: Aby dodać kolejne elementy klastra, wykonaj następujące kroki dla każdego z nich:
 - a. Określ unikalną nazwę dodatkowego elementu. Ta nazwa musi być unikalna w obrębie węzła.
 - b. Określ węzeł dla dodatkowego elementu klastra. Ten węzeł musi być węzłem programu IBM Business Monitor.
 - c. Kliknij opcję **Dodaj element**.
12. Kliknij przycisk **Dalej**, aby przejść do panelu podsumowania.
13. Przeczytaj wyświetlone informacje i kliknij przycisk **Zakończ**.
14. Kliknij przycisk **Zapisz**, aby zapisać zmiany w konfiguracji głównej.

Po wstępnym utworzeniu klastra w dowolnym momencie można dodać kolejne elementy klastra.

W celu pierwszego uruchomienia klastra po zainstalowaniu usługi IBM Cognos Business Intelligence każdy serwer należy uruchomić osobno. Nie należy używać opcji Uruchom kaskadowo, ponieważ nie zapewnia ona produktowi IBM Cognos BI czasu wystarczającego do zainicjowania.

Konsola administracyjna może zgłosić problemy podczas pierwszego uruchomienia serwera IBM Cognos Business Intelligence. Inicjowanie każdej instancji serwera w bazie danych składnicy treści i obszarze dysków produktu IBM Cognos Business Intelligence podczas pierwszego uruchamiania trwa znacznie dłużej niż w przypadku normalnego uruchamiania produktu IBM Cognos Business Intelligence.

Dodawanie elementów klastra

Do istniejącego klastra można dodać dowolną liczbę elementów.

Ważne: Jeśli pierwszy element klastra nie został utworzony za pomocą szablonu serwera aplikacji z tekstem defaultWBM w nazwie, środowisko programu IBM Business Monitor nie będzie działać poprawnie. W takiej sytuacji niezbędne będzie usunięcie wszystkich istniejących elementów klastra i ponowne utworzenie pierwszego elementu klastra.

Aby utworzyć dodatkowe elementy klastra, wykonaj następujące kroki:

1. Na panelu nawigacyjnym kliknij opcję **Serwery > Klastry > Klastry serwerów aplikacji WebSphere > nazwa_klastra > Elementy klastra**.
2. Kliknij opcję **Nowy**, aby uruchomić kreator tworzenia nowych elementów klastra.

3. Dla każdego nowego elementu klastra, wykonaj następujące kroki:
 - a. Określ unikalną nazwę dodatkowego elementu. Ta nazwa musi być unikalna w obrębie węzła.
 - b. Określ węzeł dla dodatkowego elementu klastra. Ten węzeł musi być węzłem programu IBM Business Monitor.
 - c. Kliknij opcję **Dodaj element**.
4. Kliknij przycisk **Dalej**, aby przejść do panelu podsumowania.
5. Przeczytaj wyświetlone informacje i kliknij przycisk **Zakończ**.
6. Kliknij przycisk **Zapisz**, aby zapisać zmiany w konfiguracji głównej.

Uwaga: Podczas instalowania programu IBM Business Monitor w węzle instalowana jest również usługa Cognos, która zostanie skonfigurowana na nowym serwerze po dodaniu elementu do klastra.

Stwarzanie dodatkowych węzłów

Po utworzeniu środowiska wysokiej dostępności w komórce wdrożenia sieciowego można później w razie potrzeby stwarzyszyc z komórką dodatkowe węzły.

Ważne: Produkt IBM Business Monitor nie umożliwia umieszczania portletowych paneli kontrolnych w tej samej komórce, w której znajduje się serwer IBM Business Monitor 7.5.

Aby stwarzyszyc istniejące węzły w menedżerze wdrażania, wykonaj następujące kroki dla każdego węzła:

1. Uruchom menedżer wdrażania.
2. W katalogu profilu odpowiadającemu węzłowi, który ma zostać stwarzyszony, uruchom komendę `addNode`, podając nazwę hosta menedżera wdrażania i opcjonalnie numer portu SOAP menedżera wdrażania.

```
katalog_główny_profilu\bin\addNode.bat nazwa_hosta_menedżera_wdrażania
[numer_portu_SOAP_menedżera_wdrażania]
```

```
katalog_główny_profilu\bin\addNode.sh nazwa_hosta_menedżera_wdrażania
[numer_portu_SOAP_menedżera_wdrażania]
```

Aby uruchomić komendę z włączonym śledzeniem, należy użyć opcji `-trace`, na przykład: `addNode nazwa_hosta -trace`.

Dodatkowe szczegóły na temat uruchamiania komendy `addNode` zawierają informacje pokrewne w Centrum informacyjnym produktu WebSphere Application Server.

Konfigurowanie usług zdarzeń infrastruktury CEI

Przed rozpoczęciem konfigurowania komponentów programu IBM Business Monitor przy użyciu Konsoli administracyjnej w komórce wdrożenia sieciowego musi istnieć usługa zdarzeń infrastruktury CEI, która może być używana przez program IBM Business Monitor do wysyłania zdarzeń. Ta sama usługa zdarzeń infrastruktury CEI może być także używana do odbierania zdarzeń.

Jeśli utworzono profil autonomiczny programu IBM Business Monitor lub użyto kreatora konfiguracji środowiska wdrażania, usługa zdarzeń infrastruktury CEI została już utworzona. Jeśli program IBM Business Monitor jest dodawany w topologii produktu Process Server, można skorzystać z usługi zdarzeń infrastruktury CEI wdrożonej przez produkt Process Server dla programu IBM Business Monitor. W przeciwnym razie należy utworzyć nową usługę zdarzeń infrastruktury CEI zgodnie z instrukcjami przedstawionymi na tej stronie.

W celu zainstalowania usługi zdarzeń infrastruktury CEI na serwerze lub w klastrze i utworzenia zasobów wymaganych przez tę usługę (magistrali integracji usług i mechanizmu

przesyłania komunikatów) należy użyć komendy `wbmDeployCEIEventService`. W razie potrzeby można także skonfigurować zabezpieczenia i włączyć domyślną składnicę danych usługi zdarzeń infrastruktury CEI. (Tworzenie składnicy danych usługi zdarzeń jest niezalecane w przypadku środowisk produkcyjnych). W topologii podstawowej w celu zapewnienia wysokiej dostępności usługa zdarzeń infrastruktury CEI jest instalowana w klastrze obsługi.

Aby zainstalować i skonfigurować nową usługę zdarzeń infrastruktury CEI, wykonaj następujące kroki:

1. Otwórz wiersz komend i przejdź do katalogu `bin` profilu menedżera wdrażania (domyślnie `DMGR01`), w którym zainstalowano produkt WebSphere Application Server, lub do katalogu `bin` profilu autonomicznego w środowisku jednoserwerowym.
2. Uruchom narzędzie `wsadmin` za pomocą następującej komendy:
 - `wsadmin.sh`
 - `wsadmin.bat`
3. Uruchom komendę `wbmDeployCEIEventService` interaktywnie, wprowadzając następującą komendę w wierszu komend:

```
(jcl) $AdminTask.wbmDeployCEIEventService {-interactive}
(jython) AdminTask.wbmDeployCEIEventService('-interactive')
```

Ewentualnie można uruchomić komendę, podając wszystkie parametry. Na przykład patrz temat Konfigurowanie komponentów produktu IBM Business Monitor przy użyciu komend `wsadmin` znajdujący się w sekcji odsyłaczy do stron pokrewnych.

4. Zapisz wyniki przy użyciu następującej komendy:

```
(jcl) $AdminConfig.save
(jython) AdminConfig.save()
```
5. Aby zsynchronizować węzły, w Konsoli administracyjnej kliknij opcję **Administrowanie systemem > Węzły**, wybierz wszystkie węzły, a następnie kliknij opcję **Pełna resynchronizacja**.
6. Zrestartuj menedżer wdrażania, aby wyświetlić odsyłacze infrastruktury CEI w Konsoli administracyjnej.

Usługa zdarzeń infrastruktury CEI zostanie aktywowana.

Pełną listę parametrów oraz przykład można znaleźć w sekcji IBM Business MonitorUsługa zdarzeń infrastruktury CEI.

Jeśli podczas działania komendy `wbmDeployCEIEventService` zostanie pominięty krok dotyczący składnicy danych, składnicę danych dla usługi zdarzeń infrastruktury CEI można opcjonalnie utworzyć później. Instrukcje można znaleźć w sekcji Konfigurowanie bazy danych infrastruktury CEI.

Konfigurowanie środowiska przy użyciu kreatora konfiguracji

Wymagane środowisko programu IBM Business Monitor można skonfigurować przy użyciu kreatora konfiguracji w Konsoli administracyjnej.

Muszą zostać wykonane następujące czynności:

- Utworzenie i stowarzyszenie co najmniej jednego profilu niestandardowego programu IBM Business Monitor lub rozszerzenie istniejącego profilu niestandardowego za pomocą programu IBM Business Monitor (więcej informacji na ten temat zawiera sekcja Tworzenie i rozszerzanie profili).

- Utworzenie co najmniej jednego klastra za pomocą szablonu serwera aplikacji defaultWBM (więcej informacji na ten temat zawiera sekcja Tworzenie klastrów programu IBM Business Monitor).
- Skonfigurowanie lokalnej usługi zdarzeń infrastruktury CEI (Common Event Infrastructure), przy użyciu której program IBM Business Monitor będzie wysyłać i odbierać zdarzenia (więcej informacji na ten temat zawiera sekcja Konfigurowanie usług zdarzeń infrastruktury CEI).

Przed rozpoczęciem procesu konfiguracji należy upewnić się, że zmiany węzła są zsynchronizowane automatycznie. W tym celu w Konsoli administracyjnej należy kliknąć opcję **Administrowanie systemem > Preferencje konsoli** i wybrać opcję **Synchronizuj zmiany z węzłami**. W przeciwnym razie zmiany należy aktualizować ręcznie po każdym głównym kroku.

Wymagane i opcjonalne komponenty można skonfigurować przy użyciu sekcji konfiguracji Konsoli administracyjnej programu IBM Business Monitor. Aby zapoznać się z instrukcjami dotyczącymi ręcznego konfigurowania wszystkich komponentów programu IBM Business Monitor, należy użyć odsyłaczy do informacji pokrewnych służących do uzyskiwania dostępu do informacji o czynności.

1. Na panelu nawigacyjnym kliknij opcję **Serwery > Konfiguracja produktu IBM Business Monitor**. Zostanie wyświetlona lista wymaganych i opcjonalnych komponentów. Należy przejrzeć status każdego komponentu. W przypadku środowiska wdrożenia sieciowego i braku konfiguracji środowiska wdrożenia żaden komponent nie zostanie zainstalowany ani skonfigurowany i należy wykonać pozostałe kroki w celu zainstalowania i skonfigurowania komponentów.
2. Skonfiguruj usługę zdarzeń wychodzących infrastruktury CEI, wykonując następujące kroki. Usługa zdarzeń wychodzących infrastruktury CEI służy do wysyłania zdarzeń (w tym alertów) z programu IBM Business Monitor. Należy skonfigurować fabrykę emiterów zdarzeń tak, aby wskazywała usługę zdarzeń wychodzących infrastruktury CEI.

Ważne: Przed rozpoczęciem konfigurowania fabryki emiterów zdarzeń musi istnieć lokalna usługa infrastruktury CEI, która może być używana przez program IBM Business Monitor do wysyłania zdarzeń. Jeśli konieczne jest utworzenie lokalnej usługi infrastruktury CEI, odpowiednie instrukcje można znaleźć w sekcji “Konfigurowanie usług zdarzeń infrastruktury CEI” na stronie 108.

- a. Na liście komponentów kliknij pozycję **Usługa zdarzeń wychodzących CEI**. Zostanie wyświetlony status usługi zdarzeń wychodzących infrastruktury CEI oraz fabryki emiterów zdarzeń. W przypadku istniejącej fabryki MonitorEmitterFactory w polu statusu zostanie wyświetlona nazwa usługi zdarzeń infrastruktury CEI używanej przez fabrykę emiterów. Jeśli nie skonfigurowano jeszcze fabryki emiterów, zostanie wyświetlony komunikat „Istnieje lokalna usługa zdarzeń CEI, ale nie istnieje fabryka emiterów zdarzeń”. W takim przypadku należy utworzyć i skonfigurować fabrykę emiterów.
- b. W obszarze **Konfiguruj fabrykę emiterów zdarzeń** wybierz serwer lub klastr dla fabryki emiterów zdarzeń. Lista zawiera wszystkie dostępne serwery i klastry. Można wybrać tylko serwery, na których skonfigurowano usługę zdarzeń infrastruktury CEI. Dostępne serwery i klastry są oznaczone gwiazdką (*). Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węzle.
- c. Aby uruchomić kreator konfiguracji, kliknij opcję **Konfiguruj fabrykę emiterów zdarzeń**. Dla komórki zostanie utworzona fabryka emiterów zdarzeń wychodzących o nazwie MonitorEmitterFactory. Pole statusu usługi zdarzeń wychodzących

infrastruktury CEI zostanie zaktualizowane tak, aby wskazywało usługę zdarzeń infrastruktury CEI używaną przez fabrykę MonitorEmitterFactory.

- d. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
3. Utwórz magistralę integracji usług i skonfiguruj mechanizm przesyłania komunikatów, wykonując następujące kroki. Do monitorowania zdarzeń program IBM Business Monitor wymaga własnej magistrali oraz własnego mechanizmu przesyłania komunikatów.

Jeśli użytkownik nie dysponuje istniejącą magistralą, zostanie ona utworzona podczas konfiguracji mechanizmu przesyłania komunikatów. Magistrala nosi nazwę **MONITOR.<nazwa_komórki>.Bus** i nazwy tej nie można zmieniać.

- a. Na liście komponentów kliknij pozycję **Mechanizm przesyłania komunikatów**. Zostanie wyświetlony status magistrali integracji usług i mechanizmu przesyłania komunikatów.
- b. Aby uruchomić kreator konfiguracji, kliknij opcję **Konfiguruj mechanizm przesyłania komunikatów**.
- c. Na panelu **Wybór elementu magistrali** wybierz jedną z następujących opcji w celu określenia położenia, w którym ma zostać utworzony mechanizm przesyłania komunikatów, a następnie kliknij przycisk **Dalej**:
 - **Klaster**: Tę opcję należy wybrać w celu utworzenia mechanizmu przesyłania komunikatów w istniejącym klastrze. Nazwę klastra należy wybrać z listy.
 - **Serwer**: Tę opcję należy wybrać w celu utworzenia mechanizmu przesyłania komunikatów na serwerze. Serwer należy wybrać z listy. Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.
- d. Na panelu **Wybór typu składnicy komunikatów** wybierz jedną z następujących opcji, a następnie kliknij przycisk **Dalej**:
 - **Składnica danych**: Składnica danych to składnica komunikatów zawierająca zestaw tabel, które są dostępne dla wszystkich elementów klastra udostępniającego mechanizm przesyłania komunikatów.
 - **Składnica plików**: Składnica plików to składnica komunikatów używająca plików z systemu plików przy użyciu systemu operacyjnego. Ta opcja nie jest dostępna, jeśli na panelu **Wybór elementu magistrali** wybrano opcję **Klaster**.
- e. Jeśli używana jest składnica danych, na panelu **Określanie właściwości składnicy komunikatów** wybierz jedną z następujących opcji:
 - **Utwórz domyślne źródło danych z wygenerowaną nazwą JNDI**: Domyślnie składnica danych używa bazy danych Derby. Ta opcja nie jest dostępna, jeśli na panelu **Wybór elementu magistrali** wybrano opcję **Klaster**.
 - **Użyj istniejącego źródła danych**: W przypadku wybrania tej opcji należy wypełnić następujące pola:
 - **Nazwa JNDI źródła danych**: W tym polu należy wybrać nazwę JNDI odpowiadającą bazie danych, która ma zostać użyta. Na przykład jdbc/wbm/MonitorMEDatabase.
 - **Nazwa schematu**: W tym polu należy wprowadzić nazwę schematu. Na przykład MONME00.
 - **Alias uwierzytelniania**: W tym polu należy wybrać alias uwierzytelniania, który ma zostać użyty. Aby utworzyć tabele, należy wybrać alias uwierzytelniania. Na przykład Monitor_JDBC_Alias.
 - **Utwórz tabele**: Tę opcję należy wybrać w celu utworzenia tabel w bazie danych. Jeśli ta opcja nie zostanie wybrana, administrator bazy danych musi utworzyć tabele.

- f. Na panelu **Potwierdzenie** przejrzyj informacje, a następnie kliknij przycisk **Zakończ**, aby zakończyć konfigurację. Pola statusu magistrali i mechanizmu przesyłania komunikatów zostaną zaktualizowane nowymi informacjami o konfiguracji.

Uwaga: Pomyślne uruchomienie mechanizmu przesyłania komunikatów może trochę potrwać.

- g. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
4. Sprawdź, czy magistrala i mechanizm przesyłania komunikatów mają poprawny identyfikator użytkownika dla danego środowiska:
 - a. Na panelu nawigacyjnym kliknij opcję **Zabezpieczenia > Zabezpieczenia magistrali**.
 - b. Kliknij magistralę dla serwera programu IBM Business Monitor. Zostanie wyświetlona strona właściwości konfiguracyjnych magistral.
 - c. W obszarze Właściwości dodatkowe kliknij opcję **Zabezpieczenia**. Zostanie wyświetlona kolejna strona właściwości.
 - d. W obszarze Strategia autoryzacji kliknij opcję **Użytkownicy i grupy w roli konektora magistrali**.
 - e. Sprawdź, czy dany identyfikator użytkownika istnieje. Jeśli nie istnieje, wykonaj następujące kroki, aby go dodać:
 - 1) Kliknij przycisk **Nowy**.
 - 2) Wybierz opcję **Nazwa użytkownika** i w przylegającym polu wprowadź nowy identyfikator użytkownika.
 - 3) Kliknij przycisk **OK**.
 5. Zainstaluj aplikację usług działań programu IBM Business Monitor, wykonując następujące kroki. Aplikacja usług działań wywołuje działania, takie jak wysyłanie alertów panelu kontrolnego lub powiadomień e-mail, po odebraniu zdefiniowanych zdarzeń sytuacji, które są emitowane przez produkt i inne aplikacje. Zdarzenia sytuacji wskazują zwykle sytuacje biznesowe wymagające uwagi, na przykład niedobór papieru w drukarce lub przekroczenie określonej wartości przez pomiar.
 - a. Na liście komponentów kliknij pozycję **Usługi działań**. Zostanie wyświetlony status aplikacji. Jeśli aplikacja została poprawnie zainstalowana, jej położenie będzie znajdować się na liście w polu statusu.
 - b. W obszarze **Wdróż usługi działań** wybierz z listy serwer lub klastrer dla aplikacji usług działań. Lista zawiera wszystkie dostępne serwery i klastry. Należy wybrać serwer, na którym zainstalowano program IBM Business Monitor. Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.
 - c. Aby zainstalować aplikację, kliknij opcję **Wdróż usługi działań**. Aplikacja zostanie zainstalowana i zostanie utworzony profil grupy usług działań programu Monitor. Pole statusu aplikacji zostanie zaktualizowane położeniem zainstalowanej aplikacji o nazwie IBM_WBM_ACTIONSERVICES. Jeśli ta aplikacja została zainstalowana w klastrze, będzie ona wyświetlana jako niedostępna do momentu zsynchronizowania wszystkich węzłów w klastrze.
 - d. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
 6. Zainstaluj aplikację usług planowanych programu Monitor, wykonując następujące kroki. Należy zainstalować tę aplikację, aby planować usługi powtarzalne, takie jak usługa przenoszenia danych i historia kluczowych wskaźników wydajności dla modeli monitorowania.

- a. Na liście komponentów kliknij pozycję **Usługi planowane programu Monitor**. Zostanie wyświetlony status aplikacji. Jeśli aplikacja została poprawnie zainstalowana, jej położenie będzie znajdować się na liście w polu statusu.
- b. W obszarze **Wdróż usługi planowane programu Monitor** wybierz z listy serwer lub klaster dla aplikacji usług planowanych programu Monitor. Lista zawiera wszystkie dostępne serwery i klastry. Należy wybrać serwer, na którym zainstalowano program IBM Business Monitor. Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.
- c. Aby zainstalować aplikację, kliknij opcję **Wdróż usługi planowane programu Monitor**. W polu statusu zostanie zaktualizowane położenie zainstalowanej aplikacji o nazwie IBM_WBM_DATA_SERVICES. Jeśli ta aplikacja została zainstalowana w klastrze, będzie ona wyświetlana jako niedostępna do momentu zsynchronizowania wszystkich węzłów w klastrze.
- d. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.

Istnieje możliwość wyświetlenia planowanych usług dla każdego zainstalowanego modelu monitorowania. W tym celu należy kliknąć opcję **Aplikacje > Usługi programu Monitor > Usługi planowane programu Monitor**.

7. Opcjonalne: Jeśli jest planowane użycie usługi IBM Cognos Business Intelligence do przeprowadzenia wielowymiarowej analizy na panelach kontrolnych, na liście komponentów kliknij opcję **Usługa Cognos**. Zostanie wyświetlony status usługi. Jeśli usługa została poprawnie zainstalowana, jej położenie będzie znajdować się na liście w polu statusu. Jeśli produkt IBM Cognos BI zainstalowano z produktem IBM Business Monitor i utworzono profil autonomiczny, usługa IBM Cognos BI jest już wdrożona.
 - a. Aby wdrożyć nową usługę IBM Cognos BI, wybierz z listy serwer lub klaster dla usługi IBM Cognos BI. Lista zawiera wszystkie dostępne serwery i klastry. Dostępne serwery i klastry są oznaczone gwiazdką (*). Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.

Należy podać nazwę bazy danych, która ma być używana na potrzeby składnicy treści. W przypadku produktów DB2 i Microsoft SQL Server nazwa bazy danych musi być inna niż nazwa bazy danych MONITOR. Należy podać hasło i nazwę użytkownika bazy danych. Jeśli na potrzeby składnicy treści używana jest taka sama nazwa użytkownika jak w przypadku bazy danych MONITOR, należy użyć tego samego hasła. Ponieważ użytkownik bazy danych, który ma uzyskiwać dostęp do bazy danych składnicy treści, musi mieć uprawnienie do tworzenia tabel w bazie danych, zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

Uwaga: Nazwa i hasło użytkownika bazy danych składnicy treści produktu IBM Cognos BI są przechowywane w elemencie Cognos_JDBC_Alias, dzięki czemu wszystkie referencje bazy danych mogą być obsługiwane w jednym miejscu. Przy każdym uruchomieniu serwera IBM Cognos BI produktu IBM Business Monitor bieżące wartości są przekazywane do konfiguracji produktu IBM Cognos BI, co pozwala na uzyskanie przez produkt IBM Cognos BI dostępu do składnicy treści. Ze względu na tę integrację nie jest możliwe zmodyfikowanie nazwy i hasła użytkownika składnicy treści z poziomu aplikacji konfiguracyjnej produktu IBM Cognos BI.

Jeśli zabezpieczenia administracyjne są włączone, należy także podać nazwę użytkownika i hasło administratora produktu IBM Cognos BI.

Należy kliknąć opcję **Deploy Cognos Service** (Wdróż usługę Cognos). Pole statusu zostanie zaktualizowane położeniem zainstalowanej usługi. Jeśli ta usługa została zainstalowana w klastrze, będzie ona wyświetlana jako niedostępna do momentu zsynchronizowania i zrestartowania wszystkich węzłów w klastrze. Jeśli wdrażanie

- zajmie więcej czasu niż wynosi limit czasu odpowiedzi Konsoli administracyjnej, może zostać wyświetlony następujący komunikat o przekroczeniu limitu czasu: Wait a few more minutes before attempting to restart the servers (Poczekaj kilka minut, zanim podejmiesz próbę zrestartowania serwerów).
- b. Jeśli jest już zainstalowana wersja produktu IBM Cognos BI, w obszarze Użyj istniejącej usługi Cognos podaj identyfikator URI zewnętrznego programu rozsyłającego serwera IBM Cognos BI. Ten identyfikator URI można znaleźć w kliencie konfiguracji produktu IBM Cognos BI po wybraniu opcji **Konfiguracja lokalna > Środowisko > Ustawienia programu rozsyłającego** (na przykład `http://host:port/p2pd/servlet/dispatch/ext`). Jeśli zabezpieczenia administracyjne serwera IBM Cognos BI są włączone, należy także podać nazwę użytkownika i hasło administratora serwera IBM Cognos BI.
Należy kliknąć opcję **Użyj istniejącej usługi Cognos**. Pole statusu zostanie zaktualizowane położeniem zainstalowanej usługi.
 - c. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
8. Opcjonalne: Jeśli panele kontrolne programu IBM Business Monitor mają być używane na urządzeniach przenośnych, należy zainstalować aplikację, wykonując poniższe kroki. Jeśli nie jest planowane używanie paneli kontrolnych na urządzeniach przenośnych, wykonanie tych kroków nie jest wymagane.
- a. Na liście komponentów kliknij pozycję **Panele kontrolne dla urządzeń przenośnych**. Zostanie wyświetlony status aplikacji. Jeśli aplikacja została poprawnie zainstalowana, jej położenie będzie znajdować się na liście w polu statusu.
 - b. W obszarze **Wdróż panele kontrolne dla urządzeń przenośnych** wybierz z listy serwer lub klastrę dla aplikacji paneli kontrolnych na urządzeniach przenośnych. Lista zawiera wszystkie dostępne serwery i klastry. Należy wybrać serwer, na którym zainstalowano program IBM Business Monitor. Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.
 - c. Aby zainstalować aplikację, kliknij opcję **Wdróż panele kontrolne dla urządzeń przenośnych**. Pole statusu aplikacji zostanie zaktualizowane położeniem zainstalowanej aplikacji o nazwie `IBM_WBM_MOBILE_DASHBOARD`. Jeśli ta aplikacja została zainstalowana w klastrze, będzie ona wyświetlana jako niedostępna do momentu zsynchronizowania wszystkich węzłów w klastrze.
 - d. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
9. Opcjonalne: Jeśli planowane jest korzystanie z usług emiterów zdarzeń JMS (Java Messaging Service) i REST (Representational State Transfer), należy zainstalować usługi aplikacji interfejsu API, wykonując następujące kroki. Później, zamiast kodować lub generować bezpośrednio zdarzenia w modelu Common Base Events, można używać tych usług emiterów zdarzeń. Użytkownik podaje plik XML zdarzenia, a usługi emitery zdarzeń odbierają ten plik i opakowują go w modelu Common Base Event w sposób umożliwiający jego przetworzenie przez produkt IBM Business Monitor.
- a. Na liście komponentów kliknij pozycję **Usługi emitery zdarzeń przychodzących (JMS i REST)**. Zostanie wyświetlony status aplikacji. Jeśli aplikacja została poprawnie zainstalowana, położenie zainstalowanych aplikacji będzie znajdować się na liście w polu statusu.
 - b. W obszarze **Wdróż usługi emitery zdarzeń** wybierz z listy serwer lub klastrę dla aplikacji. Lista zawiera wszystkie dostępne serwery i klastry. Należy wybrać serwer, na którym zainstalowano program IBM Business Monitor. Jeśli istnieje więcej niż jeden serwer o takiej samej nazwie, należy upewnić się, że wybrano serwer w poprawnym węźle.

- c. Aby zainstalować aplikacje, kliknij opcję **Wdróż usługi emiterów zdarzeń**. Pole statusu aplikacji zostanie zaktualizowane połoženiami zainstalowanych aplikacji. Jeśli aplikacje zostały zainstalowane w klastrze, będą one wyświetlane jako niedostępne do momentu zsynchronizowania wszystkich węzłów w klastrze.
 - d. Powróć na stronę konfiguracji, klikając opcję **Konfiguracja produktu IBM Business Monitor** w ścieżce nawigacyjnej.
10. Opcjonalne: Aby skonfigurować bramę usług REST (Representational State Transfer) dla widgetów w produkcie Business Space, wykonaj następujące kroki.

Uwaga: Ponieważ brama usług REST jest komponentem współużytkowanym, nie można jej skonfigurować przy użyciu kreatora konfiguracji. Jeśli utworzono klastry przy użyciu kreatora konfiguracji środowiska wdrażania lub utworzono profil autonomiczny, brama usług REST jest już skonfigurowana. Aby zespół mógł używać widgetów w produkcie Business Space, konieczne jest wdrożenie bramy usług REST i jej zarejestrowanie w produkcie Business Space.

- a. W Konsoli administracyjnej kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere** lub **Serwery > Klastry > Klastry serwerów aplikacji WebSphere**.
 - b. Kliknij nazwę żadanego serwera lub klastra.
 - c. Na stronie Konfiguracja, w obszarze **Integracja biznesowa** kliknij opcję **Usługi REST**.
11. Opcjonalne: Aby skonfigurować produkt Business Space, wykonaj następujące kroki.

Uwaga: Ponieważ produkt Business Space jest komponentem współużytkowanym, nie można go skonfigurować przy użyciu kreatora konfiguracji. Jeśli utworzono klastry przy użyciu kreatora konfiguracji środowiska wdrażania lub utworzono profil autonomiczny, produkt Business Space jest już skonfigurowany.

- a. W Konsoli administracyjnej kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere** lub **Serwery > Klastry > Klastry serwerów aplikacji WebSphere**.
 - b. Kliknij nazwę żadanego serwera lub klastra.
 - c. Kliknij opcję **Konfiguracja produktu Business Space** w sekcji **Integracja biznesowa** na stronie Konfiguracja.
12. Po zakończeniu konfigurowania komponentów zsynchronizuj węzły. W Konsoli administracyjnej kliknij opcję **Administrowanie systemem > Węzły**, wybierz wszystkie węzły, a następnie kliknij opcję **Pełna resynchronizacja**. Następnie zatrzymaj i uruchom ponownie wszystkie klastry i serwery.

Aby sprawdzić, czy wszystkie aplikacje zostały poprawnie zainstalowane, należy wylogować się z Konsoli administracyjnej. Następnie należy zalogować się do Konsoli administracyjnej i przejść do sekcji **Serwery > Konfiguracja produktu IBM Business Monitor**. Należy sprawdzić, czy wszystkie elementy są kompletne i zaznaczone ikoną zielonego znacznika wyboru.

W przypadku rezygnacji z utworzenia tabel mechanizmu przesyłania komunikatów lub braku uprawnień do ich utworzenia konieczne jest ręczne utworzenie tych tabel przez administratora bazy danych. Więcej informacji można znaleźć w temacie Ręczne tworzenie tabel mechanizmu przesyłania komunikatów wymienionym w sekcji Strony pokrewne.

Jeśli mają być odbierane zdarzenia ze źródła zdarzeń infrastruktury CEI działającego na serwerze zdalnym, należy również przeprowadzić konfigurację międzykomórkową. Instrukcje można znaleźć w temacie Konfigurowanie sposobu odbierania zdarzeń.

Konfigurowanie środowiska przy użyciu komend narzędzia wsadmin

Środowisko programu IBM Business Monitor można skonfigurować za pomocą narzędzia administracyjnego wiersza komend produktu WebSphere (wsadmin) bez używania kreatora konfiguracji.

Do skonfigurowania programu IBM Business Monitor są niezbędne następujące komendy narzędzia wsadmin.

Tabela 4. Wymagane komendy narzędzia wsadmin

| Komenda | Cel |
|---------------------------------|---|
| wbmDeployCEIEventService | Tworzy i konfiguruje usługę zdarzeń infrastruktury CEI wymaganą przez program IBM Business Monitor do odbierania i wysyłania zdarzeń. |
| wbmConfigureEventEmitterFactory | Konfiguruje fabrykę emiterów zdarzeń używaną przez program IBM Business Monitor do generowania i wysyłania zdarzeń. Tę komendę należy uruchamiać po uruchomieniu komendy wbmDeployCEIEventService. |
| wbmDeployMessagingEngine | Instaluje i konfiguruje mechanizm przesyłania komunikatów oraz magistralę integracji usług, które są wymagane przez program IBM Business Monitor |
| wbmDeployActionServices | Instaluje aplikację usług działań programu IBM Business Monitor. Ta aplikacja wywołuje działania, takie jak wysyłanie alertów panelu kontrolnego lub powiadomień e-mail, po odebraniu zdefiniowanych zdarzeń sytuacji. Tę komendę należy uruchomić po uruchomieniu komendy wbmConfigureEventEmitterFactory. |
| wbmDeployScheduledServices | Instaluje aplikację usług planowanych programu Monitor, która planuje usługi powtarzalne, takie jak usługa przenoszenia danych i historia kluczowych wskaźników wydajności dla modeli monitorowania. |

Następujące komendy narzędzia wsadmin są opcjonalne .

Tabela 5. Opcjonalne komendy narzędzia wsadmin

| Komenda | Cel |
|---|--|
| wbmDeployCognosService wbmSetCognosDispatcher | Instaluje nową usługę IBM Cognos Business Intelligence na potrzeby analizy wielowymiarowej lub nawiązuje połączenie z istniejącą usługą IBM Cognos BI. |
| wbmSetCognosDatabaseUser wbmSetCognosAdminUser | Umożliwia zmianę haseł bazy danych składnicy treści produktu IBM Cognos BI oraz administratora produktu IBM Cognos BI. |
| wbmRemoveCognosService | Usuwa usługę IBM Cognos BI, która została zainstalowana z programem IBM Business Monitor. |

Tabela 5. Opcjonalne komendy narzędzia wsadmin (kontynuacja)

| Komenda | Cel |
|---|--|
| wbmDeployDashboardsForMobileDevices | Instaluje i konfiguruje aplikację wymaganą do uruchamiania paneli kontrolnych na urządzeniach przenośnych. |
| wbmDeployEventEmitterServices | Instaluje aplikacje usługi emitera zdarzeń REST i usługi emitera zdarzeń JMS. Emiter zdarzeń JMS (Java Messaging Service) umożliwia asynchroniczne publikowanie zdarzeń XML do kolejki JMS bez opakowania w postaci modelu Common Base Event. Dzięki temu zdarzenia XML mogą być umieszczane w kolejce JMS nawet wtedy, gdy usługi programu IBM Business Monitor są niedostępne. Emiter zdarzeń REST umożliwia synchroniczne publikowanie zdarzeń bez opakowania w postaci modelu Common Base Event. Użytkownik określa definicję XSD opisującą strukturę informacji biznesowych, a interfejs API REST generuje i wysyła zdarzenia w prawidłowym formacie dla programu IBM Business Monitor. |
| wbmDeployBPMEmitterService | Instaluje i konfiguruje aplikację usługi emitera zdarzeń produktu IBM Business Process Manager w celu użycia przez produkt IBM BPM. |
| wbmConfigureQueueBypassDatasource | Tworzy źródło danych konieczne do włączenia komunikacji z pominięciem kolejki, gdy program IBM Business Monitor jest zainstalowany w innej komórce niż serwer infrastruktury CEI. |
| wbmDeployAlphabloxService wbmCheckAlphabloxInstall wbmRemoveAlphabloxService wbmEnableAlphabloxConfiguration | Umożliwia wdrażanie i konfigurowanie produktu Alphablox. |

Aby uruchomić narzędzie wsadmin, wykonaj następujące kroki:

- Otwórz wiersz komend i przejdź do katalogu bin profilu menedżera wdrażania (domyślnie DMGR01), w którym zainstalowano produkt WebSphere Application Server, lub do katalogu bin profilu autonomicznego w środowisku jednoserwerowym.
- Uruchom narzędzie wsadmin za pomocą jednej z następujących komend:
 - wsadmin.sh -lang jacl -user <nazwa_użytkownika> -password <hasło>
 - wsadmin.sh -lang jython -user <nazwa_użytkownika> -password <hasło>
 - wsadmin.bat -lang jacl -user <nazwa_użytkownika> -password <hasło>
 - wsadmin.bat -lang jython -user <nazwa_użytkownika> -password <hasło>
- Uruchom potrzebne komendy. W poniższym przykładzie użyto języka Jacl do uruchomienia komendy wbmConfigureEventEmitterFactory i późniejszego zapisania zmian:

```
$AdminTask
wbmConfigureEventEmitterFactory {-cluster pierwszy_klaster}
$AdminConfig save
```

W poniższym przykładzie użyto języka Jython:

```
AdminTask.wbmConfigureEventEmitterFactory('[-cluster pierwszy_klaster]')
AdminConfig.save()
```

- Po uruchomieniu komend zapisz zmiany przed wyjściem z narzędzia wsadmin. Aby zapisać zmiany, użyj następującej składni:


```
(jac1) $AdminConfig save
(jython) AdminConfig.save()
```
- Zsynchronizuj węzły w środowisku wdrożenia sieciowego. W Konsoli administracyjnej kliknij opcję **Administrowanie systemem > Węzły**, wybierz wszystkie węzły, a następnie kliknij opcję **Pełna resynchronizacja**. Następnie zatrzymaj i uruchom ponownie wszystkie klastry i serwery.

Tryb interaktywny

Jeśli komenda administracyjna jest używana w trybie interaktywnym, informacje wprowadzane przez użytkownika są gromadzone w serii kroków. Ten proces udostępnia kreator w trybie tekstowym, którego działanie przypomina pracę z kreatorem w Konsoli administracyjnej. Użycie parametru `-interactive` powoduje, że użytkownik będzie proszony o podanie kolejnych wartości.

W poniższych przykładach opisano, jak należy używać tego parametru.

```
(jac1) $AdminTask wbmConfigureEventEmitterFactory {-interactive}
(jython) AdminTask.wbmConfigureEventEmitterFactory('-interactive')
```

Komenda `help` umożliwia uzyskanie pomocy dotyczącej każdej z komend administracyjnych.

```
(jac1) $AdminTask help wbmConfigureEventEmitterFactory
(jython) print AdminTask.help ('wbmConfigureEventEmitterFactory')
```

Szczegółowe informacje o komendach oraz parametry komend można znaleźć w temacie *Komendy konfiguracyjne (wsadmin)*.

Komendy produktu Business Space zawarto w sekcji *Komendy (skrypty programu wsadmin) konfigurowania produktu Business Space*.

Ręczne konfigurowanie środowiska

Do konfigurowania środowiska produktu IBM Business Monitor należy zawsze używać kreatora konfiguracji produktu IBM Business Monitor lub kreatora konfiguracji środowiska wdrażania. Informacje znajdujące się w tym podręczniku ułatwiają wykonywanie scenariuszy zaawansowanych i dotyczących rozwiązywania problemów.

Konfigurowanie fabryki emiterów zdarzeń dla produktu IBM Business Monitor for z/OS

Do tworzenia i wysyłania zdarzeń program IBM Business Monitor używa usługi zdarzeń wychodzących infrastruktury CEI. Natomiast usługa zdarzeń wykorzystuje fabrykę emiterów zdarzeń, która wymaga konfiguracji. Preferowanym sposobem instalowania fabryki emiterów zdarzeń jest użycie kreatora konfiguracji produktu IBM Business Monitor, kreatora konfiguracji środowiska wdrażania lub zadania wsadmin. Istnieje także możliwość ręcznego skonfigurowania fabryki emiterów zdarzeń.

W Konsoli administracyjnej menedżera wdrażania wykonaj następujące kroki:

- Na panelu nawigacyjnym kliknij opcję **Integracja usług > Infrastruktura CEI > Fabryki emiterów zdarzeń > Domyślna infrastruktura CEI**.
- W sekcji **Właściwości dodatkowe** kliknij opcję **Transmisja usługi zdarzeń**.
- Wybierz usługę zdarzeń z listy **Usługa zdarzeń** i kliknij przycisk **OK**.
- Kliknij opcję **Zapisz**, aby zapisać wszystkie zmiany w konfiguracji głównej.
- Na panelu nawigacyjnym kliknij opcję **Integracja usług > Infrastruktura CEI > Fabryki emiterów zdarzeń**.

6. W polu **Zasięg** wybierz opcję **Komórka**.
7. Kliknij przycisk **Nowy**.
8. Wpisz *nazwę_fabryki* w polu **Nazwa**. Gdzie *nazwa_fabryki* to dowolna wybrana nazwa. Na przykład MonitorEmitterFactory.
9. Wpisz łańcuch `com/ibm/monitor/MonitorEmitterFactory` w polu **Nazwa JNDI**.
10. W obszarze **Transmisja zdarzeń**:
 - a. Zaznacz pole wyboru **Obsłuż transmisję usługi zdarzeń**.
 - b. Z listy w polu **Nazwa JNDI dla transmisji usługi zdarzeń** wybierz pozycję **Użyj poniższego wpisu**.
 - c. W polu wprowadzania znajdującym się pod polem **Nazwa JNDI dla transmisji usługi zdarzeń** wpisz jedną z następujących wartości:
 - Klaster: `cell/clusters/nazwa_klastra/com/ibm/events/configuration/bus-transmission/Default`
Gdzie:
Zmienna *nazwa_klastra* reprezentuje klaster, w którym jest wdrażana infrastruktura CEI.
 - Serwer: `cell/nodes/nazwa_węzła/servers/nazwa_serwera/com/ibm/events/configuration/bus-transmission/Default`
Gdzie:
Zmienna *nazwa_węzła* reprezentuje węzeł, w którym jest wdrażana infrastruktura CEI.
Zmienna *nazwa_serwera* reprezentuje serwer, na którym jest wdrażana infrastruktura CEI.
11. Usuń zaznaczenie pola wyboru **Tryb zgodności z poprzednim protokołem transmisji usługi zdarzeń**.
12. Kliknij przycisk **OK**, a następnie kliknij przycisk **Zapisz**, aby zapisać zmiany w konfiguracji głównej.

Konfigurowanie bazy danych infrastruktury CEI (Common Event Infrastructure)

Bazę danych infrastruktury CEI (Common Event Infrastructure) można skonfigurować ręcznie, a następnie korzystać z funkcjonalności infrastruktury CEI w programie IBM Business Monitor.

Procedura zawarta w tym temacie opisuje sposób konfigurowania bazy danych infrastruktury CEI w celu użycia z programem IBM Business Monitor.

Produkt IBM Business Monitor nie wymaga używania bazy danych infrastruktury CEI. Co więcej, jest to niezalecane, ponieważ takie rozwiązanie jest niewydajne w kontekście obsługi zdarzeń produktu IBM Business Monitor. Należy użyć zdarzeń rejestrowania i odtwarzania.

1. Aby utworzyć składnicę danych dla usługi zdarzeń infrastruktury CEI, uruchom odpowiednią komendę:
 - Komenda `configEventServiceDB2DB`
 - Komenda `configEventServiceDB2ZOSDB`
 - Komenda `configEventServiceOracleDB`
 - Komenda `configEventServiceSQLServerDB`

Ważne: Nie należy tworzyć składnicy danych usługi zdarzeń dla środowisk produkcyjnych, ponieważ może to mieć wpływ na wydajność utrwalania zdarzeń.

- Po wygenerowaniu skryptów bazy danych zapisz zmiany przy użyciu komendy `$AdminConfig save`. Oprócz wygenerowania skryptów bazy danych te komendy tworzą zasoby JDBC na potrzeby usługi zdarzeń infrastruktury CEI.
- Skopiuj wygenerowane skrypty na serwer bazy danych. Położenie katalogu skryptów zależy od zasięgu wdrożenia infrastruktury CEI. Domyślne położenie skryptów to jeden z poniższych katalogów, zależnie od zasięgu wdrożenia infrastruktury CEI:

```

katalog_główny_profilu/databases/event/<nazwa_klastra>/dbscripts/
<typ_bazy_danych>
katalog_główny_profilu/databases/event/<nazwa_węzła>/<nazwa_serwera>/
dbscripts/<typ_bazy_danych>

```

Gdzie:

Zmienna `katalog_główny_profilu` to katalog profilu menedżera wdrażania.

Zmienna `nazwa_klastra` to nazwa klastra, w którym wdrożono infrastrukturę CEI.

Zmienna `nazwa_węzła` to nazwa węzła, w którym wdrożono infrastrukturę CEI.

Zmienna `nazwa_serwera` to nazwa serwera, na którym wdrożono infrastrukturę CEI.

Zmienna `typ_bazy_danych` to katalog używanej bazy danych, na przykład `db2` lub `oracle`.

- Zaloguj się na serwerze bazy danych jako użytkownik mający uprawnienia do odczytu i zapisu w bazie danych. Otwórz wiersz komend i zainicjuj interfejs wiersza komend dla oprogramowania bazy danych. Aby utworzyć bazę danych zdarzeń, uruchom skrypt dla używanego typu bazy danych (na przykład `cr_event_db2 server <użytkownik_db2>`).

Należy również utworzyć tabele mechanizmu przesyłania komunikatów dla infrastruktury CEI. Więcej informacji można znaleźć w temacie Ręczne tworzenie tabel mechanizmu przesyłania komunikatów wymienionym w sekcji Strony pokrewne.

Instalowanie aplikacji usług działań programu IBM Business Monitor

Aplikacja usług działań programu IBM Business Monitor wywołuje działania, takie jak wysyłanie alertów panelu kontrolnego lub powiadomień e-mail, po odebraniu zdefiniowanych zdarzeń sytuacji, które są emitowane przez produkt IBM Business Monitor i inne aplikacje. Zdarzenia sytuacji wskazują zwykle sytuacje biznesowe wymagające uwagi, na przykład niedobór papieru w drukarce lub przekroczenie określonej wartości przez pomiar.

Przed zainstalowaniem aplikacji `monactionmgr.ear` należy włączyć infrastrukturę CEI oraz usługę komponentów bean uruchamiania na serwerze, na którym instalowana jest aplikacja usług działań.

Aby zainstalować aplikację usług działań za pomocą Konsoli administracyjnej, wykonaj następujące kroki:

- Na panelu nawigacyjnym kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.
- Kliknij przycisk **Instaluj**.
- Wybierz jedną z następujących opcji w polu **Ścieżka do nowej aplikacji**:
 - Lokalny system plików**: Wybierz tę opcję, jeśli plik znajduje się w systemie lokalnym.
 - Zdalny system plików**: Wybierz tę opcję, jeśli dostęp do Konsoli administracyjnej uzyskiwany jest przy użyciu przeglądarki WWW w innym systemie.
- Kliknij przycisk **Przeglądaj**, znajdź i wskaż plik `monactionmgr.ear`, a następnie kliknij przycisk **Dalej**. Po instalacji pliki EAR znajdują się w następującym katalogu:

```

katalog_główny_programu_Monitor/installableApps.wbm

```

Gdzie:

Zmienna katalog_główny_programu_Monitor reprezentuje katalog, w którym zainstalowano produkt IBM Business Monitor.

5. Na panelu Wybór opcji instalacji kliknij przycisk **Dalej**.
6. Na panelu Odwzorowywanie modułów na serwery kliknij pole *nazwa_serwera* lub *nazwa_klastra*, określając w ten sposób pożądane miejsce instalacji aplikacji.
7. Zaznacz pola wyboru w wierszach powiązanych z każdym modułem i kliknij przycisk **Zastosuj**.
8. Kliknij przycisk **Dalej**.
9. Przeczytaj informacje podsumowania i kliknij przycisk **Zakończ**.

Tworzenie profilu grupy usług działań programu Monitor

Po zainstalowaniu aplikacji usług działań programu Monitor należy utworzyć profil grupy zdarzeń na potrzeby odbierania zdarzeń.

Przed rozpoczęciem tej czynności należy wykonać następujące czynności:

- Zainstalowanie aplikacji usług działań programu Monitor
- Konfigurowanie usług zdarzeń wspólnej infrastruktury zdarzeń (CEI) dla programu IBM Business Monitor
- Uruchomienie menedżera wdrażania

Aby utworzyć profil grupy zdarzeń, przy użyciu Konsoli administracyjnej wykonaj następujące kroki:

1. Na panelu nawigacyjnym kliknij opcję **Integracja usług > Infrastruktura CEI > Usługa zdarzenia**.
2. W sekcji Właściwości dodatkowe kliknij opcję **Usługi zdarzeń**.
3. Kliknij opcję **Domyślny serwer zdarzeń infrastruktury CEI**.
4. W sekcji Właściwości dodatkowe kliknij opcję **Grupy zdarzeń**.
5. Kliknij przycisk **Nowy**.
6. W polu **Nazwa grupy zdarzeń** wpisz nazwę Profil grupy usług działań.
7. Wpisz wartość `CommonBaseEvent[extendedDataElements/@name = 'BusinessSituationName']` w polu **Łącuch selektora zdarzeń**.
8. Kliknij przycisk **Zastosuj**.
9. W sekcji Właściwości dodatkowe kliknij opcję **Kolejki dystrybucji**.
10. Kliknij przycisk **Nowy**.
11. Z listy rozwijanej **Nazwa JNDI kolejki** wybierz opcję `jms/ActionManager/queue`.
12. W polu **Nazwa JNDI fabryki połączeń kolejki** wybierz opcję `jms/ActionManager/QueueConnFactory`.
13. Kliknij przycisk **Zastosuj**.
14. Kliknij przycisk **Zapisz**, aby zapisać zmiany w konfiguracji głównej.

Instalowanie usług planowanych programu Monitor

Aplikacja usług planowanych programu Monitor obsługuje wiele usług. Niektóre z nich służą do optymalizowania wydajności lub przetwarzania podstawowego. Można je skonfigurować w Konsoli administracyjnej serwera WebSphere Application Server. Należy zainstalować tę aplikację, aby planować usługi powtarzalne, takie jak usługa przenoszenia danych i historia kluczowych wskaźników wydajności dla modeli monitorowania.

Aby zainstalować aplikację usług planowanych programu Monitor, wykonaj następujące kroki:

1. Na panelu nawigacyjnym kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.
 2. Kliknij przycisk **Instaluj**.
 3. Wybierz jedną z następujących opcji w polu **Ścieżka do nowej aplikacji**:
 - **Lokalny system plików**: Wybierz tę opcję, jeśli plik znajduje się w systemie lokalnym.
 - **Zdalny system plików**: Wybierz tę opcję, jeśli dostęp do Konsoli administracyjnej uzyskiwany jest przy użyciu przeglądarki WWW w innym systemie.
 4. Kliknij przycisk **Przeglądaj**, znajdź i wskaż plik MonitorDataServices.ear, a następnie kliknij przycisk **Dalej**. Po instalacji pliki EAR znajdują się w następującym katalogu:
katalog_główny_programu_Monitor/installableApps.wbm
- Gdzie:
- Zmienna katalog_główny_programu_Monitor reprezentuje katalog, w którym zainstalowano produkt IBM Business Monitor.
5. Na panelu Wybór opcji instalacji kliknij przycisk **Dalej**.
 6. Na panelu Odwzorowywanie modułów na serwery kliknij pole *nazwa_serwera* lub *nazwa_klastra*, określając w ten sposób pożądane miejsce instalacji aplikacji.
 7. Zaznacz pola wyboru w wierszach powiązanych z każdym modułem i kliknij przycisk **Zastosuj**.
 8. Kliknij przycisk **Dalej**.
 9. Przeczytaj informacje podsumowania i kliknij przycisk **Zakończ**.

W środowisku wdrożenia sieciowego po zainstalowaniu aplikacji usług planowanych programu Monitor w tym samym klastrze należy utworzyć zasób programu planującego. W tym celu należy wykonać instrukcje z sekcji Tworzenie i konfigurowanie zasobu programu planującego.

Tworzenie i konfigurowanie zasobu programu planującego:

Zasób programu planującego to komponent sterujący przetwarzaniem programu planującego, delegując pracę do lokalnego menedżera pracy, który jest tworzony w zasięgu komórki podczas instalacji. W środowisku serwera autonomicznego zasób programu planującego jest tworzony podczas instalowania produktu IBM Business Monitor. W środowisku wdrożenia sieciowego zasób programu planującego należy utworzyć na tym samym serwerze lub w tym samym klastrze, w którym znajduje się plik MonitorDataServices.ear. W tym temacie opisano kroki procedury tworzenia zasobu programu planującego przy użyciu Konsoli administracyjnej.

Należy wcześniej zainstalować usługi planowane programu Monitor, wykonując instrukcje, do których kieruje poniższy odsyłacz.

Po zainstalowaniu usług planowanych wykonaj poniższe kroki, aby utworzyć zasób programu planującego dla serwera lub klastra.

1. Na panelu nawigacyjnym Konsoli administracyjnej kliknij opcję **Zasoby > Programy planujące**.
2. W polu **Zasięg** wybierz zasięg serwera lub klastra. Musi być to ten sam serwer lub klastr, w którym znajduje się plik MonitorDataServices.ear.
3. Kliknij przycisk **Nowy**.
4. W polu **Nazwa** wprowadź nazwę, która ma być wyświetlana dla zasobu, na przykład Program planujący usług danych.
5. W polu **Nazwa JNDI** wprowadź łańcuch sched/wbm/DataServicesScheduler.

6. Wprowadź krótki opis tego zasobu programu planującego.
7. Opcjonalnie: Wprowadź kategorię, która będzie używana do klasyfikowania lub grupowania zasobów.
8. W polu **Nazwa JNDI źródła danych** wybierz opcję jdbc/wbm/MonitorDatabase.
9. Jako alias źródła danych wybierz opcję **Alias_JDBC_programu_Monitor**.
10. W polu **Przedrostek tabeli** wprowadź łańcuch przedrostka, który ma zostać przypisany do tabel programu planującego (uwzględniając schemat bazy danych). Ten przedrostek pozwoli odróżnić od siebie programy planujące, dzięki czemu będą one mogły współużytkować tę samą bazę danych. W typowym środowisku programu Monitor ten przedrostek powinien być zgodny z przedrostkiem, którego użyto w pliku DDL podczas instalowania programu Monitor
(`<NAZWA_SCHEMATU_PROGRAMU_MONITOR>.MONSCHED_`, na przykład `MONITOR.MONSCHED_</NAZWA_SCHEMATU_PROGRAMU_MONITOR>`).
11. W polu **Okres odpytywania** określ w sekundach odstęp czasu między operacjami odpytywania, które w bazie danych wykonuje program planujący w celu znalezienia nowej pracy. W przypadku produktu IBM Business Monitor zalecane jest użycie wartości od 30 do 60 sekund.
12. W polu **Nazwa JNDI menedżera pracy** wybierz menedżer pracy **wm/wbm/DataServicesWorkManager**.
13. Aby włączyć zabezpieczenia administracyjne, które zezwalają na dostęp tylko administratorom, kliknij opcję **Użyj ról administracyjnych**.
14. Kliknij przycisk **OK**, aby zapisać ten zasób programu planującego.

Instalowanie paneli kontrolnych dla urządzeń przenośnych

Panele kontrolne programu IBM Business Monitor mogą być używane na urządzeniach przenośnych. Aplikację należy zainstalować przy użyciu Konsoli administracyjnej serwera WebSphere Application Server.

Aby zainstalować aplikację paneli kontrolnych na urządzeniach przenośnych, wykonaj następujące kroki:

1. Na panelu nawigacyjnym kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.
2. Kliknij przycisk **Instaluj**.
3. Wybierz jedną z następujących opcji w polu **Ścieżka do nowej aplikacji**:
 - **Lokalny system plików**: Wybierz tę opcję, jeśli plik znajduje się w systemie lokalnym.
 - **Zdalny system plików**: Wybierz tę opcję, jeśli dostęp do Konsoli administracyjnej uzyskiwany jest przy użyciu przeglądarki WWW w innym systemie.
4. Kliknij przycisk **Przeglądaj**, znajdź i wskaż plik `MobileDashboard.ear`, a następnie kliknij przycisk **Dalej**. Po instalacji pliki EAR znajdują się w następującym katalogu:
`katalog_główny_programu_Monitor/installableApps.wbm`

Gdzie:

Zmienna `katalog_główny_programu_Monitor` reprezentuje katalog, w którym zainstalowano produkt IBM Business Monitor.

5. Na panelu Wybór opcji instalacji kliknij przycisk **Dalej**.
6. Na panelu Odwzorowywanie modułów na serwery kliknij pole *nazwa_serwera* lub *nazwa_klastra*, określając w ten sposób pożądane miejsce instalacji aplikacji.
7. Zaznacz pola wyboru w wierszach powiązanych z każdym modułem i kliknij przycisk **Zastosuj**.
8. Kliknij przycisk **Dalej**.

9. Przeczytaj informacje podsumowania i kliknij przycisk **Zakończ**.

Po zainstalowaniu aplikacji i modeli monitorowania dostęp do panelu kontrolnego dla urządzeń przenośnych będzie można uzyskać przy użyciu następującego adresu WWW:

`http://nazwa_hosta:numer_portu/mobile`

Gdzie:

nazwa_hosta reprezentuje pełną nazwę hosta albo adres IP serwera, na którym zainstalowano aplikację.

numer_portu reprezentuje domyślny port aplikacji programu IBM Business Monitor.

W celu zapewnienia poprawnego działania paneli kontrolnych na urządzeniach przenośnych konieczne jest skonfigurowanie produktu Business Space. Aby skonfigurować produkt Business Space, konieczne jest wykonanie czynności takich jak włączenie widgetów i skonfigurowanie usług REST.

Instalowanie usług emiterów zdarzeń

Istnieje możliwość ręcznego zainstalowania usług emiterów zdarzeń używanych z programem IBM Business Monitor. Przed rozpoczęciem ręcznej instalacji usług emiterów zdarzeń należy najpierw utworzyć dla nich zasoby.

Tworzenie zasobów dla ręcznie instalowanych usług emiterów zdarzeń:

Jeśli usługi emiterów zdarzeń są instalowane ręcznie, należy w pierwszej kolejności utworzyć zasoby. Jeśli użytkownik nie korzysta z kreatora konfiguracji do instalacji usług emiterów albo jeśli z przyczyn związanych z wydajnością zostanie zainstalowana więcej niż jedna instancja usług emiterów, należy ręcznie utworzyć wszystkie wymagane zasoby dla usług emiterów zdarzeń. Więcej informacji można uzyskać, klikając odsyłacze do stron pokrewnych. Do utworzenia wymaganych zasobów należy użyć Konsoli administracyjnej produktu IBM Business Monitor.

Przed rozpoczęciem tej czynności należy utworzyć magistralę integracji usług programu IBM Business Monitor. Odpowiednie instrukcje zawierają pokrewne informacje dodatkowe.

Ten temat zawiera instrukcje dotyczące tworzenia następujących wymaganych zasobów:

- Kolejka docelowa JMS
- Docelowa kolejka błędów JMS
- Fabryka połączeń kolejki błędów
- Fabryka połączeń kolejki
- Kolejka JMS
- Kolejka błędów JMS
- Specyfikacja aktywowania
- Fabryka emiterów zdarzeń dla usługi emiterów zdarzeń REST
- Fabryka emiterów zdarzeń dla usługi emiterów zdarzeń JMS

Uwaga: Jeśli zasoby dla emitera usług JMS są tworzone na serwerze po raz pierwszy (jeśli usługi zdarzeń nie były wcześniej wdrożone na serwerze za pomocą kreatora konfiguracji lub ręcznie), w celu uproszczenia instalacji usług emiterów można użyć nazw domyślnych. W poniższych krokach wskazano nazwy domyślne. Użytkownik może ponownie wykorzystać wcześniej zdefiniowane fabryki emiterów zdarzeń lub utworzyć nowe. Dla usług REST oraz JMS należy utworzyć odrębne fabryki emiterów zdarzeń.

Do utworzenia zasobów należy użyć Konsoli administracyjnej programu IBM Business Monitor. Zasoby muszą być tworzone w podanej kolejności.

1. Aby utworzyć kolejkę docelową JMS, wykonaj następujące czynności:
 - a. Wybierz opcję **Integracja usług > Magistrale** i kliknij pozycję **MONITOR.nazwa_komórki.Bus**.
 - b. Wybierz opcję **Zasoby docelowe > Miejsca docelowe** i kliknij opcję **Nowy**.
 - c. Po uruchomieniu kreatora **Tworzenie nowego miejsca docelowego kolejki** należy sprawdzić, czy wybrana jest opcja **Kolejka**, a następnie kliknąć przycisk **Dalej**.
 - d. Podaj nazwę zasobu *MonitorEventEmitterQueue2*. Nazwa domyślna to: *MonitorEventEmitterQueue*.
 - e. W polu opisu podaj ogólny opis kolejki. Na przykład: *Kolejka emiterów zdarzeń usługi JMS serwera programu Business Monitor*. Kliknij przycisk **Dalej**.
 - f. W polu **Węzeł** wybierz węzeł, w którym znajduje się element magistrali, kliknij przycisk **Dalej**, a następnie kliknij przycisk **Zakończ**.
2. Aby utworzyć docelową kolejkę błędów JMS, powtórz krok 1. Należy określić nazwę zasobu *MonitorEventEmitterErrorQueue2*. Nazwa domyślna to: *MonitorEventEmitterErrorQueue*. W polu opisu wpisz *Magistrala kolejki błędów emitera zdarzeń usługi JMS serwera programu Business Monitor*.
3. Określ kolejkę błędów jako kolejkę docelową wyjątków.
 - a. Wybierz opcję **Integracja usług > Magistrale** i kliknij pozycję **MONITOR.nazwa_komórki.Bus**.
 - b. Wybierz opcję **Zasoby docelowe > Miejsca docelowe** i wybierz kolejkę docelową utworzoną w kroku 1.
 - c. W sekcji **Miejsca docelowe wyjątków** kliknij przycisk **Określ** i określ nazwę kolejki błędów utworzonej w kroku 2.
 - d. Kliknij przycisk **OK**, a następnie przycisk **Zapisz**.
4. Aby utworzyć fabrykę połączeń kolejki błędów, wykonaj następujące kroki:
 - a. Wybierz opcję **Zasoby > JMS > Fabryki połączeń kolejki**.
 - b. Wybierz odpowiedni zasięg nowej fabryki połączeń kolejki błędów i kliknij opcję **Nowy**.
 - c. Kliknij przycisk **OK**, aby zaakceptować domyślnego dostawcę przesyłania komunikatów.
 - d. Na karcie **Konfiguracja** podaj wartości w polach **Nazwa**, **Opis** i **Nazwa JNDI** dla nowej fabryki połączeń kolejki błędów oraz wybierz nazwę w polu **Nazwa magistrali**. Kliknij przycisk **OK**, a następnie **Zapisz**. Patrz pozycje poniższej listy:
 - **Nazwa:** *MonitorEmitterErrorQConnFactory2*
 - Nazwa domyślna: *MonitorEmitterErrorQConnFactory*
 - **Opis:** *Fabryka połączeń kolejki błędów dla kolejki emiterów zdarzeń usługi JMS serwera programu Business Monitor*
 - **Nazwa JNDI:** *jms/MonitorEventEmitter/ErrorQConnFactory2*
 - Domyślna nazwa JNDI: *jms/MonitorEventEmitter/ErrorQConnFactory*
 - **Nazwa magistrali:** Wybierz docelową kolejkę błędów JMS utworzoną w kroku 2.
 - e. Określ Ustawienia zabezpieczeń w celu zabezpieczenia środowiska i kliknij przycisk **Zastosuj**. Alias uwierzytelniania dla odtwarzania XA to: *MonitorBusAuth*. Alias uwierzytelniania zarządzanego przez kontener to: *MonitorBusAuth*.
5. Aby utworzyć fabrykę połączeń kolejki, powtórz krok 4. Użyj następujących informacji:
 - **Nazwa:** *MonitorEmitterQConnFactory2*
 - Nazwa domyślna: *MonitorEmitterQueueConnFactory*

- **Opis:** Fabryka połączeń kolejki dla kolejki emiterów zdarzeń usługi JMS serwera programu Business Monitor
 - **Nazwa JNDI:** *jms/MonitorEventEmitter/QueueConnFactory2*
 - Domyślna nazwa JNDI: *jms/MonitorEventEmitter/QueueConnFactory*
 - **Nazwa magistrali:** Wybierz kolejkę docelową JMS utworzoną w kroku 1 na stronie 125.
- .
6. Aby utworzyć kolejkę JMS, wykonaj następujące kroki:
 - a. Wybierz opcję **Zasoby > JMS > Kolejki**.
 - b. Wybierz odpowiedni zasięg nowej kolejki i kliknij opcję **Nowy**.
 - c. Kliknij przycisk **OK**, aby zaakceptować domyślnego dostawcę przesyłania komunikatów.
 - d. Na karcie **Konfiguracja** podaj wartości w polach **Nazwa** i **Nazwa JNDI** dla nowej kolejki oraz wybierz nazwę magistrali i nazwę kolejki w odpowiednich polach **Nazwa magistrali** i **Nazwa kolejki**. Kliknij przycisk **Zastosuj**. Patrz pozycje poniższej listy:
 - **Nazwa:** *MonitorEventEmitterQueue2*
 - Nazwa domyślna: *MonitorEventEmitterQueue*
 - **Nazwa JNDI:** *jms/MonitorEventEmitter/Queue2*
 - Domyślna nazwa JNDI: *jms/MonitorEventEmitter/Queue*
 - **Nazwa magistrali:** *MONITOR.nazwa_komórki.Bus*
 - **Nazwa kolejki:** Wybierz kolejkę docelową JMS utworzoną w kroku 1 na stronie 125.
 7. Aby utworzyć kolejkę błędów JMS, powtórz krok 6. Użyj następujących informacji:
 - **Nazwa:** *MonitorEventEmitterErrorQueue2*
 - Nazwa domyślna: *MonitorEventEmitterErrorQueue*
 - **Nazwa JNDI:** *jms/MonitorEventEmitter/ErrorQueue2*
 - Domyślna nazwa JNDI: *jms/MonitorEventEmitter/ErrorQueue*
 - **Nazwa magistrali:** *MONITOR.nazwa_komórki.Bus*
 - **Nazwa kolejki:** Wybierz docelową kolejkę błędów JMS utworzoną w kroku 2 na stronie 125.
 8. Aby utworzyć specyfikację aktywowania, wykonaj następujące kroki:
 - a. Wybierz opcję **Zasoby > JMS > Specyfikacja aktywowania**.
 - b. Wybierz odpowiedni zasięg nowej specyfikacji aktywowania i kliknij opcję **Nowy**.
 - c. Kliknij przycisk **OK**, aby zaakceptować domyślnego dostawcę przesyłania komunikatów.
 - d. Na karcie **Konfiguracja** podaj wartości w polach **Nazwa** i **Nazwa JNDI** oraz w odpowiednich polach **Nazwa magistrali**, **Typ miejsca docelowego** i **Nazwa JNDI miejsca docelowego** wybierz nazwę magistrali, typ miejsca docelowego i nazwę JNDI miejsca docelowego dla specyfikacji aktywowania. Patrz pozycje poniższej listy:
 - **Nazwa:** *MonitorEventEmitterActivationSpec2*
 - Nazwa domyślna: *MonitorEventEmitterActivationSpec*
 - **Nazwa JNDI:** *jms/MonitorEventEmitter/ActivationSpec2*
 - Domyślna nazwa JNDI: *jms/MonitorEventEmitter/ActivationSpec*
 - **Nazwa magistrali:** *MONITOR.nazwa_komórki.Bus*
 - **Typ miejsca docelowego:** Kolejka

- **Nazwa JNDI miejsca docelowego:** Wybierz miejsce docelowe JMS utworzone w kroku 1 na stronie 125.
- e. Ustaw opcję **Alias uwierzytelniania** na wartość *MonitorBusAuth*. Kliknij przycisk **OK**, a następnie **Zapisz**.
9. Aby utworzyć fabrykę emiterów zdarzeń dla usługi emiterów zdarzeń REST, wykonaj następujące kroki:
 - a. Wybierz opcję **Integracja usług > Common Event Infrastructure > Fabryki emiterów zdarzeń**.
 - b. Wybierz odpowiedni zasięg nowej fabryki emiterów zdarzeń i kliknij opcję **Nowy**.
 - c. Na karcie **Konfiguracja** podaj wartości w polach **Nazwa** i **Nazwa JNDI** dla nowej fabryki emiterów zdarzeń. Kliknij przycisk **Zastosuj**. Patrz pozycje poniższej listy:
 - **Nazwa:** *EmitterFactoryForREST2*
 - Nazwa domyślna: *EmitterFactoryForREST*
 - **Nazwa JNDI:** *com/ibm/monitor/EmitterFactoryForREST2*
 - Domyślna nazwa JNDI: *com/ibm/monitor/EmitterFactoryForREST*
 - d. W obszarze Transmisja zdarzeń wybierz opcję **Obsłuż transmisję usługi zdarzeń**, wybierz opcję **Użyj poniższego wpisu** i wpisz wartość *com/ibm/events/configuration/bus-transmission/Default*.
 10. Aby utworzyć fabrykę emiterów zdarzeń dla usługi emiterów zdarzeń JMS, powtórz krok 9. Kliknij przycisk **OK**, a następnie **Zapisz**. Patrz pozycje poniższej listy:
 - **Nazwa:** *EmitterFactory2*
 - Nazwa JNDI: *com/ibm/monitor/EmitterFactory2*
 - **Nazwa domyślna:** *EmitterFactory*
 - Domyślna nazwa JNDI: *com/ibm/monitor/EmitterFactory*
 11. Zrestartuj serwer, aby zmiany zostały uwzględnione. Jeśli zasoby są tworzone w środowisku wdrożenia sieciowego, zrestartuj klaster, w którym utworzono zasoby.

Ręczne instalowanie usług emiterów zdarzeń:

Istnieje możliwość ręcznego zainstalowania usług emiterów zdarzeń używanych w produkcji IBM Business Monitor. Podczas ręcznego instalowania usług emiterów zdarzeń można użyć istniejących zasobów lub utworzyć zasoby dla usług emiterów zdarzeń.

Jeśli zasoby dla usług emiterów zdarzeń mają być tworzone, muszą one zostać utworzone przed rozpoczęciem ręcznej instalacji usług emiterów zdarzeń. Instrukcje dotyczące tworzenia zasobów można uzyskać, korzystając z odsyłaczy do stron pokrewnych.

Uwaga: W celu poprawienia wydajności w środowisku wdrożenia sieciowego należy wdrożyć aplikację `IBM_WBM_EMITTER_SERVICES` na serwerze, na którym zainstalowana jest usługa zdarzeń infrastruktury CEI (Common Event Infrastructure). Jeśli skonfigurowano klastry, usługi emiterów należy wdrożyć w klastrze obsługi wraz z usługą zdarzeń infrastruktury CEI.

Aby ręcznie zainstalować usługi emiterów zdarzeń, wykonaj następujące kroki:

1. W Konsoli administracyjnej produktu IBM Business Monitor wybierz opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.

Uwaga: Jeśli zasoby zostały utworzone w sposób opisany w sekcji Tworzenie zasobów dla ręcznie instalowanych usług emiterów, zrestartuj serwer przed wdrożeniem aplikacji. Jeśli zasoby zostały utworzone w środowisku wdrożenia sieciowego, zrestartuj klaster, w którym utworzono zasoby.

2. Kliknij przycisk **Instaluj**.

3. Wybierz jedną z następujących opcji w polu **Ścieżka do nowej aplikacji**:
 - **Lokalny system plików**: Wybierz tę opcję, jeśli plik znajduje się w systemie lokalnym.
 - **Zdalny system plików**: Wybierz tę opcję, jeśli dostęp do Konsoli administracyjnej uzyskiwany jest przy użyciu przeglądarki WWW w innym systemie.
4. Kliknij przycisk **Przeglądaj**, wskaż plik EmitterServices.ear i kliknij przycisk **Dalej**. Po instalacji pliki EAR znajdują się w następującym katalogu:

katalog_główny_programu_Monitor/installableApps.wbm

Gdzie:

Zmienna katalog_główny_programu_Monitor reprezentuje katalog, w którym zainstalowano produkt IBM Business Monitor.

5. Na panelu Wybór opcji instalacji wybierz opcję **Szczegółowy**, a następnie kliknij przycisk **Dalej**. Na następnym panelu kliknij opcję **Kontynuuj**.
6. Jeśli aplikacja usług emiterów została już wdrożona przez administratora lub kreator konfiguracji, utwórz unikalną nazwę dla aplikacji. Na przykład: *IBM_WBM_EMITTER_SERVICES2*.
 - a. Na panelu Odwzorowywanie modułów na serwery kliknij pozycję *nazwa_serwera* lub *nazwa_klastra*, aby wskazać serwer lub klastrę, na którym aplikacja ma zostać zainstalowana.
7. Zaznacz pola wyboru w wierszach powiązanych z każdym modułem i kliknij przycisk **Zastosuj**.
8. Kliknij przycisk **Dalej**.
9. Opcjonalne: Aby użyć utworzonych zasobów i nie akceptować wartości domyślnych, należy wprowadzić zmiany na panelu Tworzenie powiązań obiektów nasłuchiwanie dla komponentów bean sterowanych komunikatami.
 - a. W polu **Nazwa JNDI zasobu docelowego specyfikacji aktywowania** podaj nazwę JNDI utworzoną w kroku 8 sekcji Tworzenie zasobów dla ręcznie instalowanych usług emiterów. Nazwa domyślna to: *jms/MonitorEventEmitter/ActivationSpec*.
 - b. W polu **Nazwa JNDI miejsca docelowego** określ nazwę JNDI kolejki JMS (nie kolejki docelowej) utworzonej w kroku 6 sekcji Tworzenie zasobów dla ręcznie instalowanych usług emiterów. Nazwa domyślna to: *jms/MonitorEventEmitter/Queue*.
 - c. Ustaw wartość opcji **Alias uwierzytelniania specyfikacji aktywowania** na **MonitorBusAuth**.
10. Opcjonalne: Na panelu Odwzorowywanie odwołań do zasobów na zasoby można określić utworzone zasoby lub zaakceptować wartości domyślne. Następnie kliknij przycisk **Dalej**.
 - a. W polu **Nazwa JNDI zasobu docelowego dla sterowanego komunikatami komponentu bean emitera zdarzeń** określ nazwę JNDI utworzoną w kroku 9 sekcji Tworzenie zasobów dla ręcznie instalowanych usług emiterów lub użyj wartości domyślnej. Wartość domyślna to: *com/ibm/monitor/EmitterFactory*.
 - b. W polu **Nazwa JNDI zasobu docelowego dla usług REST emitera zdarzeń** określ nazwę JNDI utworzoną w kroku 9 sekcji Tworzenie zasobów dla ręcznie instalowanych usług emiterów lub użyj wartości domyślnej. Wartość domyślna to: *com/ibm/monitor/EmitterFactoryForREST*.

Uwaga: Po kliknięciu przycisku **Dalej** może zostać wyświetlona następująca informacja:

ADMA8019E: Zasoby przypisane do aplikacji są poza zasięgiem docelowym wdrożenia. Zasoby znajdują się w zasięgu docelowym wdrożenia, jeśli są one zdefiniowane na poziomie komórki, węzła, serwera lub aplikacji, gdy miejscem docelowym wdrożenia jest serwer, lub na poziomie komórki, klastra lub

aplikacji, gdy miejscem docelowym wdrożenia jest klaster. Przypisz zasoby znajdujące się w zasięgu docelowym wdrożenia aplikacji lub potwierdź, że określone przypisanie zasobów jest poprawne.

Ta informacja nie jest komunikatem o błędzie. Należy kliknąć przycisk **Kontynuuj**.

11. Opcjonalne: Jeśli aplikacja usług emiterów została już wdrożona podczas instalacji produktu lub ręcznie przez administratora, nadaj unikalną nazwę powiązanemu kontekstowemu katalogowi głównemu aplikacji.
 - a. Na panelu Odwzorowywanie kontekstowych katalogów głównych na moduły WWW określ nazwę powiązanego kontekstowego katalogu głównego */rest/bpm/events2*. Wartość domyślna to: */rest/bpm/events*.
12. Wykonując ten krok, można odwzorować użytkowników lub grupy na rolę eventemitters. Istnieje również możliwość odwzorowania wszystkich uwierzytelnionych użytkowników przez wybranie roli eventEmitters i kliknięcie opcji **Odwzoruj podmioty specjalne**, a następnie **Wszyscy uwierzytelnieni w dziedzinie aplikacji**.
 - a. Na panelu Odwzorowywanie ról zabezpieczeń na użytkowników lub grupy wybierz opcję **Rola eventEmitters**, kliknij opcję **Odwzoruj podmioty specjalne**, a następnie opcję **Wszyscy uwierzytelnieni w dziedzinie aplikacji dla zabezpieczonego środowiska**. Jeśli zabezpieczenia nie są włączone, wybierz opcję **Wszyscy**.
13. Przeczytaj informacje podsumowania i kliknij przycisk **Zakończ**.
14. Wybierz opcję **Aplikacje > Aplikacje korporacyjne > IBM_WBM_EMITTER_REST_SERVICES** i kliknij opcję **Uruchom**.

Instalowanie usług emiterów zdarzeń za pomocą kreatora konfiguracji:

Przy użyciu kreatora konfiguracji można zainstalować usługi emiterów zdarzeń dla produktu IBM Business Monitor. Więcej informacji można uzyskać, klikając odsyłacz do stron pokrewnych.

Rozdział 10. Konfigurowanie komponentów programu IBM Business Monitor

Po zainstalowaniu programu IBM Business Monitor można skonfigurować dodatkowe komponenty.

Konfigurowanie produktu IBM Cognos BI

Aby przygotować usługę IBM Cognos Business Intelligence do przeprowadzania analizy wielowymiarowej za pomocą paneli kontrolnych, można skonfigurować nową usługę IBM Cognos BI po zainstalowaniu produktu IBM Business Monitor lub istniejącą usługę IBM Cognos BI w celu użycia z produktem IBM Business Monitor.

Konfigurowanie nowej usługi IBM Cognos BI

Podczas instalowania programu IBM Business Monitor opcjonalnie można zainstalować nową usługę IBM Cognos Business Intelligence. Dostępne są następujące sposoby konfigurowania nowej usługi IBM Cognos BI: utworzenie środowiska wdrażania, uruchomienie kreatora konfiguracji w Konsoli administracyjnej, użycie komendy `wbmDeployCognosService` lub utworzenie profilu autonomicznego za pomocą narzędzia Profile Management Tool. Konieczne jest również utworzenie bazy danych produktu IBM Cognos BI i określenie nazwy użytkownika na potrzeby składnicy treści.

Wymagania dotyczące wielkości

W przypadku elementów klastra dla produktu IBM Cognos BI wymagany jest co najmniej 1 GB dodatkowego miejsca na dysku, ponieważ instancja środowiska wykonawczego musi zostać utworzona w każdym elemencie klastra.

Wymagania dotyczące bazy danych

Usługa IBM Cognos BI wymaga oddzielnej bazy danych na potrzeby własnego repozytorium składnicy treści. Bazę danych produktu IBM Cognos BI można utworzyć podczas konfigurowania profilu autonomicznego lub profilu menedżera wdrażania za pomocą narzędzia do projektowania baz danych (`dbDesignGenerator`) bądź ręcznie przy użyciu skryptów udostępnianych przez produkt IBM Business Monitor.

Usługa IBM Cognos BI tworzy table w bazie danych składnicy treści produktu IBM Cognos BI przy pierwszym uruchomieniu. Ponieważ użytkownik bazy danych, który ma uzyskiwać dostęp do bazy danych składnicy treści, musi mieć uprawnienie do tworzenia tabel w bazie danych, zalecane jest utworzenie nowego użytkownika bazy danych przeznaczonego tylko dla bazy danych składnicy treści.

W systemach, w których uruchomiono serwer produktu IBM Cognos BI, musi być zainstalowany klient bazy danych. Środowisko produktu WebSphere musi mieć dostęp do klienta, który z kolei musi zostać skonfigurowany w celu umożliwienia połączenia z bazą danych MONITOR. Należy wyświetlić stronę Zagadnienia dotyczące bazy danych i zapoznać się z informacjami dotyczącymi konkretnej bazy danych.

W przypadku pierwszego wdrożenia produktu IBM Cognos BI wstępnie skonfigurowana grupa o nazwie Wszyscy należy do kilku wbudowanych grup i ról w przestrzeni nazw produktu IBM Cognos BI, w tym do roli Administratorzy systemu. Konieczne jest usunięcie grupy Wszyscy ze wszystkich wbudowanych grup i ról, a następnie zastąpienie jej grupami,

rolami lub użytkownikami autoryzowanymi do ograniczania dostępu do oprogramowania IBM Cognos BI i administrowania nim.

Tryby bitowe

Wszystkie serwery produktu IBM Cognos BI są konfigurowane pod kątem uruchamiania w tym samym trybie bitowym co menedżer wdrażania. Jeśli na przykład menedżer wdrażania działa na platformie 32-bitowej, wszystkie serwery produktu IBM Cognos BI są konfigurowane w trybie 32-bitowym.

Aby zmienić tryb bitowy, dla każdego serwera IBM Cognos BI wykonaj następujące kroki:

1. W Konsoli administracyjnej kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere > nazwa_serwera**. Zostanie wyświetlony panel Konfiguracja.
2. W obszarze Infrastruktura serwera rozwiń pozycję **Java i zarządzanie procesami**, a następnie kliknij opcję **Definicja procesu**.
3. W obszarze Właściwości dodatkowe kliknij opcję **Wpisy środowiskowe**. Dla każdego serwera kliknij wpis **PATH** i zaktualizuj ustawienia ścieżki dla zmiennych środowiskowych tak, aby wskazywały poprawny katalog. W przypadku systemów 32-bitowych wskaż katalog `bin`. W przypadku systemów 64-bitowych wskaż katalog `bin64`.
4. Zsynchronizuj węzeł i zrestartuj serwer.

Konfigurowanie istniejącej usługi IBM Cognos BI

Jeśli produkt IBM Cognos Business Intelligence jest już zainstalowany, istniejącej usługi IBM Cognos BI można użyć razem z programem IBM Business Monitor. Dostępne są następujące sposoby połączenia z istniejącą usługą IBM Cognos BI: uruchomienie kreatora konfiguracji programu IBM Business Monitor w Konsoli administracyjnej, użycie komendy `wbmSetCognosDispatcher` lub utworzenie profilu autonomicznego za pomocą narzędzia Profile Management Tool. Następnie należy wykonać kilka kroków konfiguracyjnych.

Po połączeniu programu IBM Business Monitor z serwerem produktu IBM Cognos BI konieczne jest wykonanie dodatkowych kroków w celu skonfigurowania produktu Business Space i umożliwienia obsługi usług danych.

Ważne: Zdalny produkt IBM Cognos BI musi działać na serwerze WebSphere, a w przypadku włączenia zabezpieczeń administracyjnych repozytorium użytkowników musi znajdować się na serwerze programu IBM Business Monitor i na serwerze produktu IBM Cognos BI.

Należy upewnić się, że klient bazy danych działa i ma dostęp do bazy danych produktu IBM Business Monitor.

Jeśli środowisko wdrażania utworzono z poziomu Konsoli administracyjnej, automatycznie został zainstalowany nowy produkt IBM Cognos BI. Aby usunąć ten produkt, należy użyć komendy `wbmRemoveCognosService`.

Aby skonfigurować produkt Business Space do pracy z istniejącym produktem IBM Cognos BI, wykonaj następujące kroki:

1. Skonfiguruj funkcję pojedynczego logowania między serwerem WebSphere Application Server, na którym działa produkt Business Space, i serwerem WebSphere Application Server z uruchomioną usługą IBM Cognos BI. Więcej informacji zawiera temat Włączanie pojedynczego logowania.

2. Skonfiguruj produkt IBM Cognos BI pod kątem pojedynczego logowania. Więcej informacji zawiera temat Konfigurowanie istniejącej usługi IBM Cognos BI dla pojedynczego logowania.

3. Zaktualizuj poniższy plik punktów końcowych.

instalacyjny_katalog_główny/BusinessSpace/registryData/endpoints/cognosEndpoints.xml W każdej z trzech sekcji <tns:url> na początku wiersza należy dodać nazwę hosta i port serwera IBM Cognos BI.

Jeśli na przykład nazwa hosta to *lc2d266009.przyklad.com*, a numer portu to 9080, treść kompletnego pliku będzie następująca:

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosServiceRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosServiceRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.przyklad.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Położenie usług pomocniczych widgetów produktu Cognos</tns:description>
</tns:Endpoint>
```

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosDispatcherRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosDispatcherRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.przyklad.com:9080/p2pd/servlet/dispatch/ext/</tns:url>
<tns:description>Położenie programu rozsyłającego produktu Cognos</tns:description>
</tns:Endpoint>
```

```
<tns:Endpoint>
<tns:id>{com.ibm.cognos}cognosWebContentRootId</tns:id>
<tns:type>{com.ibm.cognos}cognosWebContentRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>http://1c2d266009.przyklad.com:9080/p2pd/servlet/</tns:url>
<tns:description>Położenie treści WWW produktu Cognos</tns:description>
</tns:Endpoint>
</tns:BusinessSpaceRegistry>
```

Więcej informacji o modyfikowaniu plików punktów końcowych zawiera temat Włączanie widgetów produktu Business Space dla środowisk międzykomórkowych.

4. Uruchom komendę `updateBusinessSpaceWidgets` dla pliku `cognosEndpoints.xml`. Wykonaj instrukcje podane w temacie Włączanie widgetów produktu Business Space dla środowisk międzykomórkowych.

Konfigurowanie produktu IBM Cognos BI przy użyciu produktu WebSphere Portal

W przypadku używania produktu IBM Cognos Business Intelligence z produktem WebSphere Portal konieczne jest zaktualizowanie sekcji `ProxyServlet_Servlet` pliku `web.xml`.

Kompletne informacje o konfigurowaniu produktu Business Space w celu współpracy z produktem WebSphere Portal zamieszczono w sekcji Konfigurowanie widgetów do pracy z produktem WebSphere Portal.

1. Wyeksportuj plik EAR archiwum korporacyjnego (`wps.ear`) produktu WebSphere Portal zgodnie z używaną konfiguracją sieciową. W przypadku środowiska klastrowego plik EAR produktu WebSphere Portal musi zostać wyeksportowany z komputera, na którym zainstalowano serwer WebSphere Application Server Network Deployment.
 - a. W wierszu komend zmień katalog na *katalog_główny_profilu_serwera_aplikacji/bin*.
 - b. Aby wyeksportować plik `wps.ear` do katalogu tymczasowego, uruchom następującą komendę (cała komenda musi być wprowadzona w jednym wierszu):

- **Windows** `wsadmin.bat -user identyfikator_administratora -password haslo_administratora -c "$AdminApp export wps katalog/wps.ear"`
 - **Linux** **UNIX** `./wsadmin.sh -user identyfikator_administratora -password haslo_administratora -c '$AdminApp export wps katalog/wps.ear'`
- , gdzie *identyfikator_administratora* to identyfikator administratora, *haslo_administratora* to hasło administratora, a *katalog* to katalog tymczasowy.
2. Utwórz podkatalog `/wps_expanded`. Aby rozwinąć zawartość wyeksportowanego pliku EAR, skorzystaj z narzędzia skryptowego EARExpander (cała komenda musi być wprowadzona w jednym wierszu).
 - **Windows** `EARExpander.bat -ear katalog/wps.ear -operationDir katalog/wps_expanded -operation expand`
 - **Linux** **UNIX** `./EARExpander.sh -ear katalog/wps.ear -operationDir katalog/wps_expanded -operation expand`
 3. Utwórz kopię zapasową pliku `katalog/wps_expanded/wps.war/WEB-INF/web.xml`.
 4. Zaktualizuj plik `katalog/wps_expanded/wps.war/WEB-INF/web.xml`.
 - a. Otwórz plik `web.xml`.
 - b. Znajdź następującą sekcję:


```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
</servlet>
```
 - c. Zastąp tę sekcję następującym tekstem:


```
<servlet id="ProxyServlet_Servlet">
  <servlet-name>ProxyServlet</servlet-name>
  <servlet-class>com.ibm.wps.proxy.servlet.ProxyServlet</servlet-class>
  <init-param>
    <param-name>useCtxPathForCookies</param-name>
    <param-value>true</param-value>
  </init-param>
</servlet>
```
 5. Usuń oryginalny plik `wps.ear` z katalogu, do którego został pierwotnie wyeksportowany.
 6. Zwiń katalog pliku EAR do pliku EAR, korzystając z komendy EARExpander.
 - **Windows** `EARExpander.bat -ear katalog/wps.ear -operationDir katalog/wps_expanded -operation collapse`
 - **Linux** **UNIX** `./EARExpander.sh -ear katalog/wps.ear -operationDir katalog/wps_expanded -operation collapse`
 7. Użyj komendy `wsadmin`, aby zaktualizować plik EAR produktu WebSphere Portal.

Uwaga: W przypadku korzystania z komórki zarządzanej (z klastrem lub bez klastra) ten krok należy wykonać na komputerze z menedżerem wdrażania.

- **Windows** `wsadmin.bat -user identyfikator_administratora -password haslo_administratora -c "$AdminApp install katalog/wps.ear {-update -appname wps -nodeployejb}"`
- **Linux** **UNIX** `./wsadmin.sh -user identyfikator_administratora -password haslo_administratora -c '$AdminApp install katalog/wps.ear {-update -appname wps -nodeployejb}'`

, gdzie *identyfikator_administratora* to identyfikator administratora, *haslo_administratora* to hasło administratora, a *katalog* to katalog tymczasowy.

8. Zrestartuj serwer produktu WebSphere Portal. W konfiguracji klastra zrestartuj klastr.

Konfigurowanie widgetów programu IBM Business Monitor dla produktu WebSphere Portal

Program IBM Business Monitor nie udostępnia już portletowych paneli kontrolnych. Widżety programu IBM Business Monitor mogą być jednak nadal wyświetlane w produkcie WebSphere Portal.

Aby wyświetlić widżety w produkcie WebSphere Portal, wykonaj następujące kroki ogólne:

1. Skonfiguruj produkt Business Space.
2. Skonfiguruj widżety w celu współpracy z produktem WebSphere Portal.
3. Skonfiguruj produkt IBM Cognos Business Intelligence w celu współpracy z produktem WebSphere Portal.

Konfigurowanie sposobu odbierania zdarzeń

Użytkownik może skonfigurować zarówno sposób przepływu zdarzeń z aplikacji do infrastruktury CEI, jak i sposób przepływu zdarzeń z infrastruktury CEI do produktu IBM Business Monitor.

Uwagi dotyczące zdarzeń asynchronicznych

Przebieg z aplikacji emitującej do infrastruktury CEI (Common Event Infrastructure) może być synchroniczny lub asynchroniczny. W przypadku transmisji zdarzeń synchronicznych aplikacja czeka do momentu pomyślnego dostarczenia zdarzenia i dopiero po nim kontynuuje transakcję. Podczas transmisji zdarzeń asynchronicznych aplikacja umieszcza zdarzenia w kolejce i kontynuuje przetwarzanie.

Transmisja zdarzeń asynchronicznych pozwala zminimalizować wpływ na aplikację emitującą, co może być istotne w przypadku monitorowania aplikacji o niewalgiacznym znaczeniu. Jednak podczas transmisji zdarzeń asynchronicznych model monitorowania może odbierać zdarzenia w innej kolejności niż wystąpiły w aplikacji emitującej.

W przypadku modeli, w których kolejność zdarzeń jest istotna, niepoprawna kolejność zdarzeń może powodować zgłaszanie wyjątków przetwarzania modelu i błędy w obliczeniach danych. Jeśli istnieje potrzeba zagwarantowania określonej kolejności zdarzeń, należy sprawdzić, czy aplikacja emitująca zdarzenia do produktu IBM Business Monitor wykonuje to działanie synchronicznie lub zdefiniować w modelu monitorowania ścieżkę sekwencji zdarzeń w celu udostępnienia informacji o kolejności przetwarzania zdarzeń.

Jednym ze sposobów na określenie, czy zdarzenia są emitowane asynchronicznie, jest sprawdzenie w Konsoli administracyjnej. W tym celu należy wybrać opcję **Integracja usług > Common Event Infrastructure > Fabryki emiterów zdarzeń**. Należy wybrać fabrykę emiterów, której nazwa może być podobna do nazwy **Domyślny emiter infrastruktury CEI**. Wyświetlony panel zawiera obszar Transmisja zdarzeń, w którym znajdują się ustawienia sterujące sposobem emitowania zdarzeń. Transmisja JMS zachodzi w sposób asynchroniczny, a transmisja usługi zdarzeń w sposób synchroniczny.

Jeśli zostanie podjęta decyzja o używaniu asynchronicznej emisji zdarzeń, a jest ważne przetwarzanie zdarzeń w kolejności ich utworzenia, należy zdefiniować ścieżkę sekwencji zdarzeń w modelu monitorowania. Więcej informacji o sposobach definiowania ścieżek sekwencji zdarzeń można znaleźć na stronach pokrewnych.

Konfigurowanie autoryzacji asynchronicznego dostarczania zdarzeń

Jeśli planowane jest odbieranie zdarzeń emitowanych z aplikacji używającej fabryki emiterów zdarzeń z dostarczaniem asynchronicznym i do skonfigurowania środowiska nie użyto kreatora konfiguracji środowiska wdrażania lub komendy `wbmDeployCEIEventService` narzędzia `AdminTask`, należy skonfigurować serwer programu IBM Business Monitor do komunikacji z serwerem infrastruktury CEI.

Jeśli środowisko skonfigurowano przy użyciu kreatora konfiguracji środowiska wdrażania lub komendy `wbmDeployCEIEventService` narzędzia `AdminTask`, poniższa konfiguracja została już przeprowadzona. Tę czynność należy wykonać w celu skonfigurowania informacji o autoryzacji dla usługi JMS tylko wtedy, gdy konfigurowany jest własny serwer CEI lub gdy zamiast domyślnego emitera infrastruktury CEI używana jest inna niż domyślna fabryka emiterów zdarzeń.

Przed rozpoczęciem tej czynności użytkownik musi zalogować się do Konsoli administracyjnej produktu WebSphere Application Server. W przypadku korzystania ze zdalnego serwera CEI oraz odbierania zdarzeń z wykorzystaniem metody opartej na kolejce, przed rozpoczęciem tej czynności należy upewnić się, że skonfigurowano łącza magistrali integracji usług. Informacje na ten temat zawiera sekcja „Konfigurowanie zarządzania zdarzeniami opartego na kolejce w środowisku o wielu komórkach”.

Do wykonania kroków opisanych w tym temacie zamiast Konsoli administracyjnej można użyć zadania `setEventServiceJmsAuthAlias` narzędzia `wsadmin`.

Korzystając z Konsoli administracyjnej produktu WebSphere Application Server, wykonaj następujące kroki:

1. Określ alias autoryzacji dla fabryki połączeń kolejki.
 - a. Na panelu nawigacyjnym kliknij opcję **Zasoby > JMS > Fabryki połączeń kolejki**.
 - b. Na liście fabryk połączeń kolejki kliknij opcję **CommonEventInfrastructure_QueueCF**.
 - c. W sekcji Ustawienia zabezpieczeń wybierz alias z listy **Alias uwierzytelniania dla odtwarzania XA**. Alias musi mieć użytkownika, któremu przypisano rolę konektora magistrali infrastruktury CEI. W sekcji **Integracja usług > Magistrale** należy kliknąć kolumnę **Zabezpieczenia** magistrali opisanej jako **Magistrala CommonEventInfrastructure**.
 - d. Wybierz alias z listy **Alias uwierzytelnienia zarządzanego przez kontener**. Zazwyczaj można wybrać ten sam alias, który wybrano w poprzednim kroku podrzędnym.
 - e. Kliknij przycisk **OK** i zapisz zmiany w konfiguracji głównej.
2. Określ alias autoryzacji specyfikacji aktywowania.
 - a. Na panelu nawigacyjnym kliknij opcję **Zasoby > JMS > Specyfikacje aktywowania**.
 - b. Na liście specyfikacji aktywowania kliknij opcję **CommonEventInfrastructure_ActivationSpec**.
 - c. W sekcji Ustawienia zabezpieczeń wybierz alias z listy **Alias uwierzytelniania**.
 - d. Kliknij przycisk **OK** i zapisz zmiany w konfiguracji głównej.
3. Określ alias autoryzacji dla fabryk połączeń tematu.
 - a. Na panelu nawigacyjnym kliknij opcję **Zasoby > JMS > Fabryki połączeń tematu**.
 - b. Na liście fabryk połączeń tematu kliknij opcję **CommonEventInfrastructure_AllEventsTopicCF**.
 - c. W sekcji Ustawienia zabezpieczeń wybierz alias z listy **Alias uwierzytelniania dla odtwarzania XA**. Alias musi mieć użytkownika, któremu przypisano rolę konektora

magistrali infrastruktury CEI. W sekcji **Integracja usług > Magistrale** należy kliknąć kolumnę **Zabezpieczenia** magistrali opisanej jako **Magistrala CommonEventInfrastructure**.

- d. Wybierz alias z listy **Alias uwierzytelnienia zarządzanego przez kontener**. Zazwyczaj można wybrać ten sam alias, który wybrano w poprzednim kroku podrzędnym.
- e. Kliknij przycisk **OK** i zapisz zmiany w konfiguracji głównej.

Odbieranie zdarzeń z infrastruktury CEI

W produkcie IBM Business Monitor zdarzenia przychodzące z serwera infrastruktury CEI (Common Event Infrastructure) mogą być odbierane przy użyciu następujących dwóch różnych typów transportu: JMS (oparty na kolejce) i oparty na tabeli (nazywany również pomijaniem kolejki).

Metoda dostarczania zdarzeń opartego na kolejce korzysta z usługi JMS (Java Messaging Service) w celu dostarczenia zdarzeń z infrastruktury CEI do modelu monitorowania. Metoda dostarczania zdarzeń opartego na tabeli (wcześniej nazywana pomijaniem kolejki) korzysta z tabeli bazy danych w celu dostarczenia zdarzeń z infrastruktury CEI do modelu monitorowania. W przypadku metody dostarczania zdarzeń opartego na tabeli pracę można rozdzielać między wiele elementów klastra. W przypadku większości środowisk ta metoda poprawia wydajność i upraszcza konfigurowanie systemu.

Odbieranie zdarzeń przy użyciu metody dostarczania zdarzeń opartego na tabeli

Istnieje możliwość skonfigurowania usługi zdarzeń infrastruktury CEI (Common Event Infrastructure) w taki sposób, aby wysyłała zdarzenia do tabeli w bazie danych zdarzeń modelu monitorowania. Nie trzeba konfigurować łącza magistrali integracji usług i jego powiązanych zasobów. Pominięcie kolejki JMS zapewnia lepszą wydajność dzięki eliminacji dodatkowego kroku utrwalania wymaganego podczas korzystania z kolejki.

W przypadku korzystania z metody dostarczania zdarzeń opartego na tabeli w produkcie IBM Business Monitor 7.5 pracę można podzielić między wiele elementów klastra. W przypadku większości środowisk ta metoda poprawia wydajność i upraszcza konfigurowanie systemu.

- **Modele wersji wcześniejszej niż 6.2:** dostarczanie zdarzeń oparte na tabeli jest nieobsługiwane. Aby użyć tej metody w przypadku modeli monitorowania z wersji wcześniejszej niż 6.2, konieczne jest uprzednie zaktualizowanie modelu monitorowania przy użyciu pakietu Business Monitor Development Toolkit. Należy zmienić numer wersji, wygenerować nowy plik EAR i wdrożyć nową wersję modelu monitorowania. Jeśli model nie zostanie zaktualizowany, konieczne jest użycie metody dostarczania zdarzeń opartego na kolejce.
- **Modele wersji 6.2 i 7:** te modele mogą używać metody opartej na tabeli (wcześniej nazywanej pomijaniem kolejki). Aby wykorzystać rozszerzenia skalowalności wersji 7.5, konieczne jest zaktualizowanie modelu monitorowania za pomocą pakietu Business Monitor Development Toolkit w wersji 7.5.
- **Modele wersji 7.5:** te modele mogą wykorzystać rozszerzenia skalowalności, jeśli używana jest metoda dostarczania zdarzeń opartego na tabeli.

Ograniczenie: Jeśli jest używana baza danych SQL Server, nie można korzystać z metody dostarczania zdarzeń opartego na tabeli, chyba że aplikacja emitująca jest uruchomiona na serwerze WebSphere Application Server 7.0 (lub Process Server 7.0) bądź nowszym. Należy użyć metody opartej na kolejce.

Metodę opartą na tabeli można włączyć w środowisku jednokomórkowym lub wielokomórkowym. W zależności od środowiska należy wybrać jedną z poniższych czynności, aby przeprowadzić konfigurację tej metody.

Konfigurowanie metody dostarczania zdarzeń opartego na tabeli w środowisku jednokomórkowym:

W przypadku korzystania ze środowiska jednoserwerowego (autonomicznego) lub w sytuacji, gdy w każdym węźle komórki zainstalowano program IBM Business Monitor w wersji 7.0 (lub wersji 7.0.0.3 w przypadku systemu z/OS) albo nowszej, do odbierania zdarzeń nie są wymagane żadne dalsze kroki. Jeśli usługa zdarzeń infrastruktury CEI została wdrożona w węźle w komórce, w którym nie zainstalowano programu IBM Business Monitor lub Process Server, należy w tym węźle infrastruktury CEI zainstalować pliki JAR programu IBM Business Monitor dla przepływu zdarzeń.

Produkt Process Server 7.0 lub nowszy na platformach rozproszonych (oraz produkt Process Server 7.0.0.3 lub nowszy na platformach z/OS) udostępnia pliki niezbędne do obsługi zdalnej emisji zdarzeń. Jeśli jest używana wcześniejsza wersja produktu Process Server, w celu skonfigurowania metody dostarczania zdarzeń opartego na tabeli w środowisku jednokomórkowym wykonaj następujące kroki:

1. W katalogu `katalog_główny_serwera_aplikacji/scripts.wbm/crossCell` lokalnej instalacji serwera IBM Business Monitor znajdź plik odpowiedni do używanego systemu operacyjnego i wersji serwera WebSphere Application Server, na którym działa usługa zdarzeń infrastruktury CEI.
 - `monitorCommunicationWithWAS70BasedCells.tar`,
`monitorCommunicationWithWAS61BasedCells.tar` lub
`monitorCommunicationWithWAS60BasedCells.tar`
 - `monitorCommunicationWithWAS70BasedCells.zip`,
`monitorCommunicationWithWAS61BasedCells.zip` lub
`monitorCommunicationWithWAS60BasedCells.zip`
2. Skopiuj odpowiedni plik do katalogu `katalog_główny_serwera_aplikacji/plugins` każdej instalacji produktu WebSphere Application Server w węźle zdalnym z udostępnianym elementem docelowym infrastruktury CEI, w którym nie zainstalowano programu IBM Business Monitor ani produktu Process Server w wersji 7.0 (lub wersji 7.0.0.3 w przypadku systemu z/OS) albo nowszej, a następnie wyodrębnij jego zawartość.
3. W każdej instalacji produktu WebSphere Application Server, w której wyodrębniono zawartość pliku:
 - a. Zamknij wszystkie wirtualne maszyny Java (JVM), które używają katalogu `katalog_główny_serwera_aplikacji/java/bin/java`, w tym także agenty węzła, serwery, menedżery wdrażania oraz wiersze komend narzędzia `wsadmin`.
 - b. Uruchom plik `katalog_główny_profilu/bin/osgiCfglnit` dla każdego profilu w instalacji produktu WebSphere Application Server.
 - c. Zrestartuj wszystkie agenty węzłów i serwery.

Konfigurowanie metody dostarczania zdarzeń opartego na tabeli w środowisku wielokomórkowym:

Jeśli program IBM Business Monitor zainstalowano w innej komórce niż usługę zdarzeń infrastruktury CEI, należy wykonać dodatkowe kroki konfiguracyjne w celu umożliwienia komunikacji między komórkami.

W środowiskach zabezpieczonych przed wykonaniem tej czynności należy się upewnić, że wykonano następujące czynności:

- Jeśli zabezpieczenia są włączone w komórce lokalnej lub zdalnej, należy je włączyć w obu komórkach.
- Jeśli włączono zabezpieczenia, konieczne jest aktywowanie zaufania (protokół SSL) między serwerem zdalnym infrastruktury CEI a serwerem lokalnym programu IBM Business Monitor (więcej informacji zawiera sekcja Konfigurowanie połączeń SSL między serwerami w środowiskach wielokomórkowych).
- Klucze LTPA muszą być współużytkowane między komórkami, a komórki muszą mieć ten sam identyfikator (więcej informacji na ten temat zawiera sekcja Współużytkowanie kluczy LTPA).
- Ustawienie **Użyj zapewniania o tożsamości** musi być włączone zarówno w komórce lokalnej, jak i w komórce zdalnej (więcej informacji na ten temat zawiera sekcja Włączanie asercji tożsamości).

Jeśli w środowisku wielokomórkowym program IBM Business Monitor nie jest zainstalowany w komórce zdalnej emitującej zdarzenia, konieczne jest skonfigurowanie menedżera wdrażania i serwerów infrastruktury CEI w komórce zdalnej w taki sposób, aby mogły emitować zdarzenia do tabel. Produkt Process Server 7.0 lub nowszy na platformach rozproszonych (oraz produkt Process Server 7.0.0.3 lub nowszy na platformach z/OS) udostępnia pliki niezbędne do obsługi zdalnej emisji zdarzeń. We wcześniejszych wersjach produktu Process Server te pliki nie są udostępniane automatycznie. W rezultacie instrukcje różnią się nieco w zależności od tego, czy komórka zdalna emitująca zdarzenia jest komórką rozproszoną z zainstalowanym produktem Process Server w wersji 7.0 (wersja 7.0.0.3 w przypadku systemu z/OS), czy nowszym.

Aby skonfigurować metodę dostarczania zdarzeń opartego na tabeli w wielu komórkach, wykonaj następujące kroki:

- Jeśli produkt Process Server w wersji 7.0 (wersja 7.0.0.3 w przypadku systemu z/OS) lub nowszej **nie** jest zainstalowany w komórce zdalnej (komórce, w której nie zainstalowano programu IBM Business Monitor):
 1. W katalogu katalog_główny_serwera_aplikacji/scripts.wbm/crossCell lokalnej instalacji serwera IBM Business Monitor znajdź plik odpowiedni do używanego systemu operacyjnego i wersji serwera WebSphere Application Server, na którym działa usługa zdarzeń infrastruktury CEI.
 - monitorCommunicationWithWAS70BasedCells.tar lub monitorCommunicationWithWAS61BasedCells.tar
 - monitorCommunicationWithWAS70BasedCells.zip lub monitorCommunicationWithWAS61BasedCells.zip
 2. Skopiuj odpowiedni plik do katalogu katalog_główny_serwera_aplikacji/plugins menedżera wdrażania zdalnego i wyodrębnij zawartość.
 3. Skopiuj ten sam plik do katalogu katalog_główny_serwera_aplikacji/plugins każdej instalacji produktu WebSphere Application Server w komórce zdalnej z udostępnianym elementem docelowym infrastruktury CEI, w której nie zainstalowano programu IBM Business Monitor ani produktu Process Server w wersji 7.0 (wersja 7.0.0.3 w przypadku systemu z/OS) lub nowszej, a następnie wyodrębnij jego zawartość.
 4. W każdej instalacji produktu WebSphere Application Server, w której wyodrębniono zawartość pliku:
 - a. Zamknij wszystkie wirtualne maszyny Java (JVM), które używają katalogu katalog_główny_serwera_aplikacji/java/bin/java, w tym także agenty węzła, serwery, menedżery wdrażania oraz wiersze komend narzędzia wsadmin.
 - b. Uruchom plik katalog_główny_profilu/bin/osgiCfgInit dla każdego profilu w instalacji produktu WebSphere Application Server.
 - c. Zrestartuj wszystkie agenty węzłów i serwery.

5. W menedżerze wdrażania zdalnego lub na serwerze autonomicznym uruchom komendę `wbmConfigureQueueBypassDataSource` narzędzia `wsadmin`. Przykład i listę parametrów tej komendy można znaleźć w sekcji Infrastruktura CEI oparta na tabeli obejmująca wiele komórek. Po uruchomieniu tej komendy i zapisaniu zmian w konfiguracji zrestartuj menedżer wdrażania zdalnego lub serwer autonomiczny.
- Jeśli produkt Process Server w wersji 7.0 (wersji 7.0.0.3 w przypadku systemu z/OS) lub nowszej **jest** zainstalowany w komórce zdalnej:
 1. W menedżerze wdrażania zdalnego lub na serwerze autonomicznym uruchom komendę `wbmConfigureQueueBypassDataSource` narzędzia `wsadmin`. Przykład i listę parametrów tej komendy można znaleźć w sekcji Infrastruktura CEI oparta na tabeli obejmująca wiele komórek.
 2. Po uruchomieniu tej komendy i zapisaniu zmian w konfiguracji zrestartuj menedżer wdrażania zdalnego lub serwer autonomiczny.

Podczas wdrażania modelu monitorowania ze zdalną infrastrukturą CEI konieczne jest wybranie opcji położenia infrastruktury CEI **Zdalna** (zgodnie z opisem zawartym w kroku Wybierz opcje infrastruktury CEI dla modelu monitorowania znajdującym się w temacie Wdrażanie modeli monitorowania).

Jeśli serwer infrastruktury CEI działa w systemie z/OS: po zakończeniu konfigurowania infrastruktury CEI opartej na tabeli, gdy jest wdrażany model monitorowania, następujący błąd jest rejestrowany w dziennikach infrastruktury CEI w systemie z/OS:

```
CEI61Configur E
com.ibm.wbimonitor.observationmgr.spi.impl.CEI61RemoteConfigurationSessionImpl
reloadCEIConfig(String[] eventServerAppNames) CWMRT7314E: Wystąpił błąd podczas
próby przeładowania konfiguracji infrastruktury CEI.
```

Aby zakończyć konfigurację infrastruktury CEI, wykonaj następujące kroki:

1. Zrestartuj serwer lub klaster infrastruktury CEI (dla emitującej infrastruktury CEI w systemie z/OS).
2. W menedżerze wdrażania programu IBM Business Monitor uruchom metodę `confirmCEIServerReboot(String modelID)` komponentu MBean usług cyklu życia, aby wskazać, że infrastruktura CEI została zrestartowana. Aby uruchomić komendę z poziomu wiersza komend narzędzia `wsadmin`, wykonaj następujące kroki:
 - a. Nawiąż połączenie z komponentem MBean usług cyklu życia:


```
wsadmin> set ls [$AdminControl completeObjectName type=LifecycleServices,*]
```
 - b. Potwierdź, że infrastruktura CEI została zrestartowana:


```
wsadmin> $AdminControl invoke $ls confirmCEIServerReboot { "<model
ID>"}
```

Odbieranie zdarzeń przy użyciu metody dostarczania zdarzeń opartej na kolejce

Odbieranie zdarzeń za pomocą kolejek JMS (Java Messaging Service) nie wymaga wykonywania dodatkowych kroków, chyba że ma zostać umożliwiona komunikacja między serwerem IBM Business Monitor i zdalnym serwerem infrastruktury CEI. Jeśli w środowisku programu IBM Business Monitor 7.5 jest używany model monitorowania utworzony przy użyciu programu IBM Business Monitor 6.1 bez aktualizacji modelu monitorowania, konieczne jest użycie metody zarządzania zdarzeniami opartej na kolejce.

Metodę zarządzania zdarzeniami opartą na kolejce można wykorzystać w środowisku jednokomórkowym lub wielokomórkowym. Jeśli serwer infrastruktury CEI znajduje się w komórce zdalnej względem komórki, w której zainstalowany jest program IBM Business Monitor, należy wykonać dodatkowe czynności konfiguracyjne, aby umożliwić komunikację między dwiema komórkami.

Konfigurowanie metody dostarczania zdarzeń opartego na kolejce w środowisku jednokomórkowym:

Jeśli program IBM Business Monitor jest zainstalowany w tej samej komórce co usługa zdarzeń infrastruktury CEI i do odbierania zdarzeń jest używana metoda oparta na kolejce, nie trzeba podejmować żadnych dalszych kroków. Wymagane pliki JAR zostały skopiowane do odpowiednich folderów, a magistrala integracji usług została utworzona podczas instalowania programu IBM Business Monitor.

Konfigurowanie metody dostarczania zdarzeń opartego na kolejce w środowisku wielokomórkowym:

Jeśli program IBM Business Monitor zainstalowano w innej komórce niż serwer infrastruktury CEI, należy wykonać dodatkowe kroki konfiguracyjne w celu umożliwienia komunikacji między komórkami. Aby możliwe było odbieranie zdarzeń z kolejki JMS w tym środowisku międzykomórkowym, należy skonfigurować serwer programu IBM Business Monitor do odbierania zdarzeń infrastruktury CEI (Common Event Infrastructure) ze zdalnego serwera CEI.

Przed wykonaniem tej czynności należy upewnić się, że zostały wykonane następujące czynności:

- Wdrożono i skonfigurowano zdalną usługę infrastruktury CEI.
- Utworzenie magistrali integracji usług dla lokalnego serwera programu IBM Business Monitor

W środowiskach zabezpieczonych należy również upewnić się, że wykonano następujące czynności:

- Jeśli zabezpieczenia są włączone w komórce lokalnej lub zdalnej, należy je włączyć w obu komórkach.
- Jeśli włączono zabezpieczenia, konieczne jest aktywowanie zaufania (protokół SSL) między serwerem zdalnym infrastruktury CEI a serwerem lokalnym programu IBM Business Monitor (więcej informacji zawiera sekcja Konfigurowanie połączeń SSL między serwerami w środowiskach wielokomórkowych).
- Klucze LTPA muszą być współużytkowane między komórkami, a komórki muszą mieć ten sam identyfikator (więcej informacji na ten temat zawiera sekcja Współużytkowanie kluczy LTPA).
- Ustawienie **Użyj zapewniania o tożsamości** musi być włączone zarówno w komórce lokalnej, jak i w komórce zdalnej (więcej informacji na ten temat zawiera sekcja Włączanie asercji tożsamości).

Aby skonfigurować metodę zarządzania zdarzeniami opartą na kolejce, należy zainstalować pliki międzykomórkowe, utworzyć zdalną magistralę integracji usług i utworzyć łącze między magistralami lokalnymi i zdalnymi. Produkt Process Server 7.0 lub nowszy na platformach rozproszonych (oraz produkt Process Server 7.0.0.3 lub nowszy na platformach z/OS) udostępnia pliki niezbędne do obsługi zdalnej emisji zdarzeń.

Aby skonfigurować funkcję zarządzania zdarzeniami opartą na kolejce w wielu komórkach, wykonaj następujące kroki:

Ważne: Jeśli w komórce zdalnej zainstalowano produkt Process Server w wersji 7.0 (lub wersji 7.0.0.3 w przypadku systemu z/OS) lub nowszej, można pominąć kroki 1-3 i przejść bezpośrednio do kroku 4.

1. W katalogu katalog_główny_serwera_aplikacji/scripts.wbm/crossCell lokalnej instalacji serwera IBM Business Monitor znajdź odpowiedni plik zależny od używanego systemu operacyjnego i wersji serwera WebSphere Application Server, na którym działa serwer CEI.
 - monitorCommunicationWithWAS70BasedCells.tar,
 - monitorCommunicationWithWAS61BasedCells.tar lub
 - monitorCommunicationWithWAS60BasedCells.tar
 - monitorCommunicationWithWAS70BasedCells.zip,
 - monitorCommunicationWithWAS61BasedCells.zip lub
 - monitorCommunicationWithWAS60BasedCells.zip
2. Skopiuj odpowiedni plik do katalogu katalog_główny_serwera_aplikacji/plugins zdalnego serwera infrastruktury CEI (serwera autonomicznego lub menedżera wdrażania zdalnego) i wyodrębnij jego zawartość.
3. Z poziomu katalogu katalog_główny_serwera_aplikacji/bin na zdalnym serwerze infrastruktury CEI uruchom odpowiednią komendę w celu skonfigurowania serwera aplikacji lub serwera procesów pod kątem rozpoznawania pliku .jar: osgiCfgInit.bat lub osgiCfgInit.sh.
4. Z poziomu katalogu katalog_główny_serwera_aplikacji/scripts.wbm/crossCell lokalnej instalacji serwera IBM Business Monitor wybierz jedną z poniższych metod w celu uruchomienia programu narzędziowego konfiguracji międzykomórkowej magistrali integracji usług. Więcej informacji na temat tego programu narzędziowego jest dostępnych na stronach pokrewnych.
 - Aby uruchomić komendę w trybie interaktywnym, wpisz:
 - configRemoteMonitorBus.sh
 - configRemoteMonitorBus.bat
 - Aby uruchomić komendę przy użyciu pliku właściwości, przejrzyj plik configRemoteMonitorBus.props i zmień wymagane właściwości. Plik configRemoteMonitorBus.props to przykład pliku właściwości, który znajduje się w katalogu katalog_główny_serwera_aplikacji/scripts.wbm/crossCell, ale można także utworzyć własny plik właściwości odpowiedni dla danej konfiguracji:
 - configRemoteMonitorBus.sh -props *nazwa_pliku_właściwości*
 - configRemoteMonitorBus.bat -props *nazwa_pliku_właściwości*

Gdzie:

Zmienna *nazwa_pliku_właściwości* jest pełną nazwą pliku właściwości, który zawiera wartości wymagane dla konfiguracji. Ścieżka do pliku właściwości musi być w pełni określona, aby skrypt mógł znaleźć plik właściwości. Narzędzie do konfigurowania obsługi wielu komórek utworzy magistralę integracji usług w komórce zdalnej. Nazwa magistrali to MONITOR.<*nazwa_komórki_zdalnej*>.bus, gdzie <*nazwa_komórki_zdalnej*> to nazwa komórki zdalnej.

5. Po zakończeniu wykonywania skryptu zrestartuj zarówno lokalny serwer programu IBM Business Monitor, jak i zdalny serwer CEI.
6. Sprawdź, czy istnieje zdalna magistrala integracji usług oraz czy łącze między lokalną i zdalną magistralą zostało utworzone pomyślnie. W tym celu wykonaj kroki opisane w temacie Weryfikowanie zdalnej magistrali programu IBM Business Monitor i połączenia integracji usług.

Podczas wdrażania modelu monitorowania ze zdalną infrastrukturą CEI konieczne jest wybranie opcji położenia infrastruktury CEI **Zdalna** (zgodnie z opisem zawartym w kroku Wybierz opcje infrastruktury CEI dla modelu monitorowania znajdującym się w temacie Wdrażanie modeli monitorowania).

Jeśli jest używane środowisko zabezpieczone: możliwe jest wdrożenie modelu monitorowania w środowisku zabezpieczonym ze zdalną infrastrukturą CEI i funkcją zarządzania zdarzeniami opartym na kolejce. Po wdrożeniu modelu monitorowania konieczne jest zakończenie instalacji przez wykonanie instrukcji zawartych w temacie Kończenie instalacji modelu monitorowania w zabezpieczonym środowisku opartym na kolejkach.

Weryfikowanie zdalnej magistrali programu IBM Business Monitor i połączenia integracji usług:

Po skonfigurowaniu serwera programu IBM Business Monitor pod kątem używania serwera infrastruktury CEI na zdalnym serwerze WebSphere Application Server lub serwerze Process Server należy sprawdzić, czy magistrala zdalna i łącze integracji usług zostały pomyślnie utworzone.

Aby sprawdzić, czy magistrala zdalna i łącze magistrali integracji usług istnieją i są aktywne, wykonaj następujące kroki:

1. W Konsoli administracyjnej zdalnego serwera WebSphere Application Server lub Process Server kliknij opcję **Integracja usług > Magistrale**.
2. Kliknij sprawdzaną magistralę MONITOR.<nazwa_komórki>.bus, gdzie <nazwa_komórki> to nazwa komórki, w której zainstalowano zdalny serwer infrastruktury CEI.
3. W sekcji Topologia kliknij opcję **Mechanizmy przesyłania komunikatów**. Zdefiniowano jeden mechanizm przesyłania komunikatów. Jeśli mechanizm przesyłania komunikatów jest aktywny, w polu **Status** wyświetlana jest zielona strzałka.
4. Kliknij mechanizm przesyłania komunikatów, a następnie kliknij opcję **Właściwości dodatkowe > Łącza magistrali integracji usług**. W przypadku łączenia zdalnej komórki z pojedynczą instalacją programu Monitor oraz instalacji programu Monitor z pojedynczą zdalną komórką zostanie zdefiniowane jedno łącze. Może jednak istnieć więcej niż jedno łącze. Jeśli połączenie jest aktywne, w polu **Status** wyświetlana jest zielona strzałka.
5. Opcjonalnie: aby do weryfikacji użyć dziennika System.out, wyszukaj w nim komunikat podobny do poniższego. Nazwa mechanizmu przesyłania komunikatów jest inna na każdym komputerze:

CWSIP0382I: Mechanizm przesyłania komunikatów FADB84EB685E209F odpowiedział na żądanie subskry

Uwaga: Tę samą procedurę można wykonać na serwerze programu IBM Business Monitor, aby sprawdzić, czy połączenie magistrali integracji usług po stronie serwera programu IBM Business Monitor jest aktywne.

Konfigurowanie produktu Business Space

Istnieje możliwość skonfigurowania produktu Business Space opartego na produkcie WebSphere, który zapewnia wspólny interfejs umożliwiający użytkownikom aplikacji tworzenie, zarządzanie i integrowanie interfejsów WWW w ramach oferty IBM Business Process Management, WebSphere Enterprise Service Bus i innych produktów firmy IBM.

Konfigurowanie produktu Business Space

Aby skonfigurować dla użytkowników aplikacji wspólny interfejs służący do tworzenia i integrowania interfejsów WWW oraz zarządzania nimi, należy zainstalować i skonfigurować produkt Business Space oparty na technologii WebSphere.

Konieczna jest instalacja oprogramowania produktu. Podczas instalacji produktu uwzględniane są pliki produktu Business Space dla skonfigurowanych profili.

Produkt Business Space jest obsługiwany z następującymi bazami danych:

- DB2 Universal
- DB2 for IBM i
- DB2 for z/OS
- Microsoft SQL Server
- Oracle 11g

Aby uzyskać informacje o tym, jakie bazy danych są obsługiwane z danym produktem IBM używanym z produktem Business Space, należy znaleźć ten produkt na liście obsługiwanych baz danych.

Jeśli jest instalowany produkt IBM Business Process Manager, WebSphere Enterprise Service Bus lub IBM Business Monitor, a ponadto jest tworzony profil serwera autonomicznego z użyciem opcji typowej, produkt Business Space jest instalowany i konfigurowany automatycznie z bazą danych DB2 Express. Jeśli jest używany profil serwera autonomicznego, za pomocą narzędzia Profile Management Tool (z opcją zaawansowaną) można skonfigurować produkt Business Space w taki sposób, aby współpracował z używanym środowiskiem wykonawczym. Więcej informacji na ten temat zawiera sekcja Konfigurowanie produktu Business Space za pomocą narzędzia Profile Management Tool.

Jeśli w przypadku dowolnego produktu są konfigurowane profil menedżera wdrażania i profil niestandardowy, najprostszym sposobem konfiguracji produktu Business Space jest skorzystanie z kreatora konfiguracji środowiska wdrażania. Więcej informacji na ten temat zawiera sekcja Konfigurowanie produktu Business Space za pomocą kreatora konfiguracji środowiska wdrażania.

Jeśli użytkownik korzysta ze środowiska serwera autonomicznego lub konfiguruje środowisko wykonawcze za pomocą kreatora środowiska wdrażania, punkty końcowe usługi REST (Representational State Transfer) są konfigurowane i włączane automatycznie. W przypadku innych środowisk należy w tym celu użyć Konsoli administracyjnej usługi REST. Jeśli widżety mają być dostępne w produkcie Business Space, dla tych widżetów należy skonfigurować punkty końcowe usługi REST. Aby produkt Business Space powiązał widżety z punktami końcowymi, a same widżety zostały udostępnione do użycia na palecie, konieczne jest zarejestrowanie punktów końcowych usługi REST.

Jeśli jest używany menedżer wdrażania i profile niestandardowe, za pomocą Konsoli administracyjnej można skonfigurować produkt Business Space.

Po przeprowadzeniu początkowej konfiguracji za pomocą narzędzia Profile Management Tool lub Konsoli administracyjnej konieczne jest również skonfigurowanie tabel bazy danych dla produktu Business Space. Więcej informacji na ten temat zawiera sekcja Konfigurowanie tabel bazy danych produktu Business Space.

Niezależnie od tego, jakiego narzędzia użyto do skonfigurowania produktu Business Space, niezbędne jest zapewnienie, że produkt Business Space korzysta z zabezpieczeń środowiska. Więcej informacji na ten temat zawiera sekcja Konfigurowanie zabezpieczeń dla produktu Business Space.

Produkt Business Space jest oparty na technologii Lotus Mashups. Często zadawane pytania i ogólne informacje o rozwiązywaniu problemów dotyczących technologii Lotus Mashups są dostępne na stronie: <http://www.lotus.com/ldd/mashupswiki.nsf/xpViewCategories.xsp?lookupName=Troubleshooting&SessionID=CDFG4HK6EQ>.

Po zainstalowaniu i skonfigurowaniu produktu Business Space użytkownicy środowiska wykonawczego mogą go utworzyć, używając następującego adresu URL:
`http://host:port/BusinessSpace`, gdzie *host* jest nazwą hosta z działającym serwerem, a *port* numerem portu serwera.

Konfigurowanie produktu Business Space w profilu produktu przy użyciu narzędzia Profile Management Tool

Przy użyciu narzędzia Profile Management Tool można skonfigurować produkt Business Space oparty na technologii WebSphere jako część profilu produktu.

Narzędzie Profile Management Tool można uruchomić po zainstalowaniu produktu. Możliwości narzędzia Profile Management Tool można także użyć po zainstalowaniu produktu z poziomu wiersza komend, korzystając z parametru **-configureBSpace** programu narzędziowego wiersza komend `manageprofiles`. W obu sytuacjach produkt Business Space jest instalowany z tym samym produktem bazy danych, który został wskazany dla wspólnej bazy danych. Jeśli wybrano bazę danych, która nie jest obsługiwana z produktem Business Space, narzędzie Profile Management Tool skonfiguruje produkt Business Space z bazą danych IBM DB2 Express.

W przypadku używania programu narzędziowego wiersza komend `manageprofiles` należy postępować zgodnie z dokumentacją programu narzędziowego wiersza komend `manageprofiles` dla produktu do zarządzania procesami biznesowymi. Należy zapoznać się z następującymi informacjami dotyczącymi używania programu narzędziowego wiersza komend `manageprofiles`:

- W przypadku używania produktu Oracle lub SQL Server na serwerze autonomicznym bazy danych należy utworzyć ręcznie, a nie za pomocą parametru **-dbCreateNew**.
- W przypadku zdalnej bazy danych w środowisku klastrowym należy ręcznie utworzyć bazę danych, skopiować wygenerowane skrypty na komputer zdalny zawierający bazę danych, a następnie uruchomić skrypty z tego miejsca.

W przypadku menedżera wdrażania i profili niestandardowych można użyć Konsoli administracyjnej lub kreatora konfiguracji środowiska wdrażania. Patrz temat Konfigurowanie produktu Business Space przy użyciu Konsoli administracyjnej lub Konfigurowanie produktu Business Space przy użyciu kreatora konfiguracji środowiska wdrażania. Jeśli menedżer wdrażania oraz profile niestandardowe (węzły zarządzane) zostaną utworzone przy użyciu narzędzia Profile Management Tool z opcją tworzenia profilu **Środowisko wdrażania**, produkt Business Space zostanie automatycznie skonfigurowany ze środowiskiem wdrażania użytkownika, ale należy ręcznie uruchomić skrypty w celu skonfigurowania tabel bazy danych.

W przypadku bardziej zaawansowanych opcji konfiguracji w profilu serwera autonomicznego należy użyć stron Konsoli administracyjnej do skonfigurowania produktu Business Space. Jeśli na przykład ma zostać wyznaczone źródło danych, które jest inne niż baza danych wybrana dla profilu (baza danych produktu IBM Business Monitor lub wspólna baza danych produktu IBM Business Process Manager), należy użyć Konsoli administracyjnej do skonfigurowania produktu Business Space.

Jeśli zdecydowano się na użycie bardziej zaawansowanych opcji konfiguracji, które wymagają użycia Konsoli administracyjnej, wykonaj następujące kroki:

- Podczas tworzenia profilu serwera autonomicznego przy użyciu narzędzia Profile Management Tool użyj opcji tworzenia profilu **Zaawansowane** i usuń zaznaczenie pola wyboru **Konfiguruj produkt Business Space**, aby produkt Business Space mógł zostać skonfigurowany później przy użyciu Konsoli administracyjnej.
- Zapoznaj się z tematem Konfigurowanie produktu Business Space przy użyciu Konsoli administracyjnej.

Opcjonalnie, jeśli produkt Business Space nie ma być konfigurowany w profilu produktu, można utworzyć oddzielne profile produktu Business Space. Na przykład w celu separacji obciążenia konieczne może być oddzielenie interfejsu użytkownika na jednym komputerze od zaplecza na drugim komputerze. W celu rozdzielania obciążenia konieczne także może być umieszczenie serwera Business Process Manager na jednym komputerze do obsługi dużego obciążenia, a produktu Business Space na innym komputerze zdalnym. Komputer zaplecza może zostać dostrojony do przetwarzania danych zaplecza, a komputer z produktem Business Space do obsługi transmisji danych z użyciem protokołu HTTP. Więcej informacji można znaleźć w sekcji “Tworzenie profili produktu Business Space” na stronie 147.

- W przypadku serwera autonomicznego uruchom narzędzie Profile Management Tool, wybierz opcję **Profil serwera autonomicznego** i wykonaj następujące kroki:
 1. Na stronie Opcje tworzenia profilu wykonaj jeden z następujących kroków:
 - Wybierz opcję tworzenia profilu **Typowe**, aby zaakceptować domyślną instalację i konfigurację produktu Business Space z użyciem bazy danych DB2 Express. Pomiń kroki od b do e.
 - Wybierz opcję **Zaawansowane**, aby skonfigurować zaawansowane opcje tworzonego profilu. Następnie na stronie Konfiguracja produktu Business Space upewnij się, że zaznaczono pole wyboru **Konfiguruj produkt Business Space**.

Produkt Business Space został skonfigurowany ze źródłem danych produktu.
 2. Podczas określania nazwy hosta dla profilu użyj pełnej nazwy hosta.
 3. Na stronie Projekt bazy danych jest dostępna opcja użycia pliku projektu bazy danych utworzonego przy użyciu narzędzia do projektowania baz danych, które zawiera wszystkie konfiguracje bazy danych dla produktu, w tym informacje dotyczące konfiguracji bazy danych dla produktu Business Space. Więcej informacji na temat plików projektu bazy danych zawiera sekcja “Tworzenie pliku właściwości projektu bazy danych produktu Business Space” na stronie 204.
 4. Zakończ tworzenie profilu przy użyciu narzędzia Profile Management Tool. Zainstalowano produkt Business Space. Został on skonfigurowany dla tego samego produktu bazy danych co produkt bazy danych wyznaczony dla wspólnej bazy danych (lub dla bazy danych DB2 Express, jeśli produkt bazy danych nie jest obsługiwany).
 5. Jeśli jest używana zdalna baza danych, skonfiguruj tabele bazy danych po uruchomieniu narzędzia Profile Management Tool. Patrz temat Konfigurowanie tabel bazy danych produktu Business Space.
- W przypadku środowiska wdrażania uruchom narzędzie Profile Management Tool, wybierz opcję **Profil menedżera wdrażania** lub **Profil niestandardowy**, a następnie wykonaj następujące kroki.
 1. Na stronie Opcje tworzenia profilu wybierz opcję **Środowisko wdrażania** w celu skonfigurowania poszczególnych profili za pomocą dostosowanych wartości konfiguracji, a następnie użycia ich w środowisku wdrażania opartym na dostarczonym wzorcu.
 2. Postępuj zgodnie z krokami narzędzia Profile Management Tool w celu utworzenia profilu menedżera wdrażania oraz profili niestandardowych (węzłów zarządzanych).
 3. Po stowarzyszeniu wszystkich węzłów niestandardowych uruchom skrypty w celu ręcznego skonfigurowania tabel bazy danych.

Ważne: Jeśli baza danych produktu to baza danych Oracle, produkt Business Space jest konfigurowany przy użyciu narzędzia Profile Management Tool lub programu narzędziowego wiersza komend manageprofiles pod kątem używania tej samej bazy danych z domyślnym schematem IBMBUSSP oraz domyślnym hasłem wprowadzonym podczas tworzenia profilu. Aby użyć innego hasła dla nazwy użytkownika IBMBUSSP, należy użyć Konsoli administracyjnej w celu zaktualizowania zasobów JDBC (należy znaleźć źródło danych

jdbc/mashupsDS). Wartość aliasu uwierzytelniania należy zmodyfikować tak, aby był zgodny z hasłem nazwy schematu produktu Business Space. Następnie należy zapisać zmiany i zrestartować serwer.

Przed rozpoczęciem używania produktu Business Space należy skonfigurować zabezpieczenia wymagane do użycia z produktem Business Space oraz widżety używane przez zespół użytkownika. Więcej informacji zawiera temat Konfigurowanie zabezpieczeń dla produktu Business Space.

Wskazówka: Produkt Business Space używa komponentu proxy w celu nawiązywania połączeń z usługami REST. W niektórych przypadkach, jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia między produktem Business Space a usługami REST w zależności od wydajności serwerów usługi REST. Więcej informacji zawiera temat Zmianie ustawień limitu czasu dla proxy Ajax produktu Business Space.

Tworzenie profili produktu Business Space:

Aby utworzyć lub rozszerzyć profile produktu Business Space, możliwe jest użycie narzędzia Profile Management Tool lub programu narzędziowego wiersza komend manageprofiles. Profile to zestawy plików definiujące środowisko wykonawcze dla menedżera wdrażania, węzła zarządzanego lub serwera autonomicznego.

Jeśli produkt Business Space jest skonfigurowany jako część profilu produktu, te zadania są opcjonalne.

Tworzenie profili produktu Business Space dla konfiguracji autonomicznej:

Aby utworzyć profile produktu Business Space dla środowiska autonomicznego, możliwe jest użycie narzędzia Profile Management Tool lub programu narzędziowego wiersza komend manageprofiles.

Jeśli produkt Business Space jest skonfigurowany jako część profilu produktu, te zadania są opcjonalne.

Tworzenie profili produktu Business Space dla konfiguracji autonomicznej za pomocą narzędzia Profile Management Tool:

Za pomocą narzędzia Profile Management Tool można tworzyć profile autonomiczne produktu Business Space.




- Należy przejrzeć kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- W przypadku korzystania z narzędzia Profile Management Tool z graficznym interfejsem użytkownika Motif w systemie operacyjnym Solaris domyślna wielkość okna narzędzia Profile Management Tool może być zbyt mała do wyświetlenia wszystkich komunikatów i przycisków.
- Jeśli planowane jest użycie pliku projektu bazy danych na potrzeby informacji dotyczących bazy danych produktu Business Space, należy wykonać kroki znajdujące się w sekcji “Tworzenie pliku właściwości projektu bazy danych produktu Business Space” na stronie 204.

Tej procedury należy użyć, jeśli jest tworzony profil produktu Business Space dla konfiguracji autonomicznej. W poniższych krokach opisano zarówno opcję Zaawansowane tworzenie profilu, jak i Typowe tworzenie profilu.

Jeśli produkt Business Space został skonfigurowany jako część profilu produktu, to zadanie jest opcjonalne.

1. Uruchom narzędzie Profile Management Tool.

Należy użyć jednej z następujących komend:

-   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
-  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`

Zostanie otwarta strona Powitanie.

2. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.

Zostanie otwarta karta Profile.

Karta Profile zawiera listę profili utworzonych na danym komputerze. Do tworzenia nowych profili lub rozszerzania profili już istniejących można użyć narzędzia Profile Management Tool.

3. Na karcie Profile kliknij opcję **Utwórz**.

W oddzielnym oknie zostanie otwarta strona Wybór środowiska.

4. Na stronie Wybór środowiska wybierz opcję **Profil autonomiczny**, a następnie kliknij przycisk **Dalej**.

5. Na stronie Opcje tworzenia profilu zdecyduj, czy utworzyć profil autonomiczny za pomocą opcji **Typowe tworzenie profilu**, czy opcji **Zaawansowane tworzenie profilu**.

6. Jeśli wybrano opcję **Typowe tworzenie profilu**, wykonaj następujące kroki:

- a. Na panelu Zabezpieczenia administracyjne wprowadź nazwę i hasło użytkownika, potwierdź hasło, a następnie kliknij przycisk **Dalej**.

Cała konfiguracja profilu, w tym opcje profilu i baza danych, są domyślnie skonfigurowane i wyświetlane na stronie Podsumowanie profilu.

- b. Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.

Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.

Ostrzeżenie: Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:

- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
- **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.

Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.

7. Jeśli wybrano opcję **Zaawansowane tworzenie profilu**, wykonaj następujące kroki:




- a. Na stronie Wdrażanie opcjonalnych aplikacji zaznacz odpowiednie pola wyboru, jeśli ma zostać wdrożona Konsola administracyjna i aplikacja domyślna.

- b. Na stronie Nazwa i położenie profilu wykonaj następujące kroki:

- 1) W polu Nazwa profilu wpisz unikalną nazwę lub zaakceptuj wartość domyślną. Każdy tworzony profil musi mieć nazwę. W przypadku, gdy istnieje więcej niż jeden profil, można je odróżnić na najwyższym poziomie za pomocą tej nazwy.

Jeśli wybrano opcję nieużywania nazwy domyślnej, w systemie Windows należy użyć krótkiej nazwy, ponieważ nazwy ścieżek mają ograniczoną długość.

- 2) W polu Katalog profilu wpisz nazwę katalogu profilu lub użyj przycisku Przeglądaj, aby przejść do katalogu profilu. Określony katalog będzie zawierać pliki definiujące środowisko wykonawcze (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Katalog domyślny jest zależny od platformy:

-   *instalacyjny_katalog_główny/profiles/nazwa_profilu*
-  *instalacyjny_katalog_główny\profiles\nazwa_profilu*
gdzie *nazwa_profilu* to podana nazwa.

Pole katalogu profilu musi spełniać następujące wymagania:

- Nazwa profilu (*nazwa_profilu*) musi być unikalna.
 - Podany katalog musi być pusty.
 - Identyfikator użytkownika musi mieć uprawnienia do katalogu.
 - Musi istnieć wystarczająca ilość miejsca do utworzenia profilu.
- 3) Opcjonalnie: jeśli tworzony profil ma być używany jako profil domyślny, należy zaznaczyć pole wyboru **Ustaw ten profil jako domyślny**. To pole wyboru zostanie wyświetlone tylko wtedy, gdy w systemie istnieje profil.
- Komendy będą działać automatycznie z profilem domyślnym. Pierwszy profil tworzony na stacji roboczej jest profilem domyślnym. Profil domyślny jest domyślnym miejscem docelowym dla komend wykonywanych z poziomu katalogu bin w instalacyjnym katalogu głównym produktu. Gdy na stacji roboczej istnieje tylko jeden profil, każda komenda jest wykonywana względem tego profilu. Jeśli istnieje więcej niż jeden profil, niektóre komendy wymagają określenia profilu będącego ich celem.

- 4) Kliknij przycisk **Dalej**.

- c. Na stronie Nazwy węzłów i hostów wykonaj następujące czynności na potrzeby tworzonego profilu:

- W polu Nazwa węzła wpisz nazwę węzła lub zaakceptuj wartość domyślną. Nazwy węzłów powinny być jak najkrótsze, ale jednocześnie każda z nich musi być unikalna w środowisku wdrażania.
- W polu Nazwa hosta wpisz nazwę hosta lub zaakceptuj wartość domyślną.
- W polu Nazwa komórki wpisz nazwę komórki lub zaakceptuj wartość domyślną.

Kliknij przycisk **Dalej**, aby wyświetlić stronę Zabezpieczenia administracyjne.

- d. Na stronie Zabezpieczenia administracyjne wprowadź nazwę i hasło użytkownika oraz potwierdź hasło. Kliknij przycisk **Dalej**.

- e. Na stronie Certyfikat bezpieczeństwa (część 1) określ, czy mają być tworzone nowe certyfikaty, czy mają zostać zaimportowane istniejące certyfikaty. Wykonaj następujące czynności:

- Aby utworzyć nowy domyślny certyfikat osobisty i nowy główny certyfikat podpisywania, wybierz opcję **Utwórz nowy domyślny certyfikat osobisty i Utwórz nowy główny certyfikat podpisywania**, a następnie kliknij przycisk **Dalej**.
- Aby zaimportować istniejące certyfikaty, wybierz opcję **Importuj istniejący domyślny certyfikat osobisty i Importuj istniejący główny osobisty certyfikat podpisywania**, a następnie podaj następujące informacje:
 - W polu Ścieżka wprowadź ścieżkę do katalogu dla istniejącego certyfikatu.
 - W polu Hasło wpisz hasło dla certyfikatu.

- W polu Typ magazynu kluczy wybierz typ magazynu kluczy dla importowanego certyfikatu.
- W polu Alias magazynu kluczy wybierz alias magazynu kluczy dla importowanego certyfikatu.
- Kliknij przycisk **Dalej**.

W przypadku importowania certyfikatu osobistego jako domyślnego certyfikatu osobistego należy zaimportować główny certyfikat, za pomocą którego podpisano certyfikat osobisty. W przeciwnym razie narzędzie Profile Management Tool dodaje osobę podpisującą dla certyfikatu osobistego do pliku trust.p12. W przypadku importowania domyślnego certyfikatu osobistego lub głównego certyfikatu podpisywania należy określić ścieżkę i hasło, a następnie wybrać typ oraz alias magazynu kluczy dla każdego importowanego certyfikatu.

- f. Na stronie Certyfikat bezpieczeństwa (część 2) sprawdź, czy informacje o certyfikacie są poprawne, i kliknij przycisk **Dalej**, aby wyświetlić stronę Przypisywanie wartości portów.

Tworząc certyfikaty, można użyć wartości domyślnych lub zmodyfikować je na potrzeby tworzenia nowych certyfikatów. Domyślny certyfikat osobisty jest domyślnie ważny przez rok i jest podpisany przez główny certyfikat podpisywania. Główny certyfikat podpisywania jest certyfikatem samopodpisanym, który domyślnie jest ważny przez 15 lat. Domyślne hasło magazynu kluczy dla głównego certyfikatu podpisywania to WebAS. To hasło należy zmienić. Hasło nie może zawierać żadnych znaków z zestawu znaków dwubajtowych (DBCS), ponieważ tych znaków nie obsługują niektóre typy magazynów kluczy, takie jak PKCS12. Obsługiwane typy magazynów kluczy są zależne od dostawców zawartych w pliku java.security.

W przypadku tworzenia lub importowania jednego bądź obu certyfikatów są tworzone następujące pliki kluczy:

- key.p12: zawiera domyślny certyfikat osobisty.
- trust.p12: zawiera certyfikat osoby podpisującej z domyślnego certyfikatu głównego.
- root-key.p12: zawiera główny certyfikat podpisywania.
- default-signers.p12: zawiera certyfikaty osób podpisujących dodawane do każdego nowego pliku kluczy tworzonego po zainstalowaniu i uruchomieniu serwera. Domyślnie w tym pliku kluczy znajdują się informacje o osobie podpisującej domyślny certyfikat główny i certyfikat osoby podpisującej serwera DataPower®.
- deleted.p12: zawiera certyfikaty usunięte za pomocą zadania deleteKeyStore, aby można je było odzyskać w razie potrzeby.
- ltpa.jceks: zawiera domyślne klucze LTPA (Lightweight Third-Party Authentication) serwera używane przez serwery w danym środowisku do wzajemnej komunikacji.

W przypadku tworzenia lub importowania certyfikatów wszystkie te pliki mają takie same hasło. Może to być hasło domyślne lub określone przez użytkownika. Importowany certyfikat jest dodawany do pliku key.p12 lub pliku root-key.p12. Jeśli zostaną zaimportowane certyfikaty, które nie zawierają żądanych informacji, należy kliknąć przycisk **Wstecz**, aby zaimportować inny certyfikat.

- g. Na stronie Przypisywanie wartości portów sprawdź, czy porty określone dla profilu są unikalne, a następnie kliknij przycisk **Dalej**.

Narzędzie Profile Management Tool wykrywa porty aktualnie używane przez inne produkty IBM WebSphere i wyświetla zalecane wartości portów, które nie powodują konfliktu z już istniejącymi. Jeśli są używane inne aplikacje, które korzystają z określonych portów, należy sprawdzić, czy porty nie powodują konfliktów. Jeśli na stronie Wdrażanie aplikacji opcjonalnych nie wybrano opcji wdrażania Konsoli

administracyjnej, jej porty nie będą dostępne na stronie Przepisywanie wartości portów. Porty są rozpoznawane jako używane, jeśli zostały przypisane do profilu utworzonego podczas instalacji przeprowadzanej przez bieżącego użytkownika lub jeśli są one aktualnie używane.

Mimo że narzędzie sprawdza poprawność portów w momencie uzyskiwania dostępu do strony Przepisywanie wartości portów, mogą występować konflikty portów, które wynikają z ustawień wybranych na kolejnych stronach narzędzia Profile Management Tool. Porty nie zostaną przypisane do momentu zakończenia procesu tworzenia profilu. Jeśli zachodzi podejrzenie wystąpienia konfliktu portów, po utworzeniu profilu można to sprawdzić.

Sprawdzając plik katalog_główny_profilu/properties/portdef.props, należy określić porty używane podczas tworzenia profilu. W tym pliku znajdują się klucze i wartości użyte podczas ustawiania portów. W przypadku wykrycia konfliktów portów można je ponownie przypisać ręcznie. Aby ponownie przypisać porty, należy zapoznać się z tematem Aktualizowanie portów istniejącego profilu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server Network Deployment. Przy użyciu opisanego w tym temacie skryptu ws_ant należy uruchomić plik updatePorts.ant.


- h. W przypadku przeprowadzania instalacji na platformie Linux lub Windows użytkownikowi będącemu administratorem lub z uprawnieniami grupy administratorów zostanie wyświetlona strona definicji usługi systemu Linux lub Windows. Na stronie Definicja usługi należy wskazać, czy serwer procesów będzie działać w usłudze systemu Windows lub Linux, a następnie należy kliknąć opcję **Dalej**, aby wyświetlić stronę Definicja serwera WWW.

Windows Strona Definicja usługi systemu Windows jest otwierana dla platformy Windows tylko wtedy, gdy ID użytkownika instalującego usługę systemu Windows ma uprawnienia grupy administratorów. Jeśli profil został skonfigurowany jako usługa systemu Windows, produkt uruchamia usługę systemu Windows dla procesów uruchomionych za pomocą komendy startServer lub startManager. Jeśli na przykład serwer lub menedżer wdrażania został skonfigurowany jako usługa systemu Windows i zostanie wydana komenda startServer lub startManager, komenda wasservice uruchomi zdefiniowane usługi.

Ważne: W przypadku logowania jako określone konto użytkownika należy podać ID i hasło użytkownika uruchamiającego usługę oraz typ uruchamiania (typ domyślny to Ręcznie). Identyfikator użytkownika nie może zawierać spacji, musi należeć do grupy Administratorzy oraz mieć uprawnienia użytkownika zaawansowanego pozwalające na logowanie w trybie usługi. Jeśli ID użytkownika należy do grupy Administratorzy, narzędzie Profile Management Tool nadaje mu uprawnienia użytkownika zaawansowanego, jeśli jeszcze ich nie ma. W ramach procesu usuwania profilu można usunąć usługę systemu Windows dodaną podczas tworzenia profilu.

Windows **Uwagi dotyczące protokołu IPv6 w przypadku uruchamiania profili jako usługi systemu Windows:** profile utworzone w celu działania jako usługa systemu Windows nie mogą zostać uruchomione w przypadku użycia protokołu IPv6, jeśli usługa została skonfigurowana do działania jako system lokalny. Aby włączyć protokół IPv6, należy utworzyć zmienną środowiskową specyficzną dla użytkownika. Ponieważ ta zmienna środowiskowa jest zmienną użytkownika, a nie zmienną systemu lokalnego, tylko usługa systemu Windows działająca jako ten konkretny użytkownik może uzyskać dostęp do tej zmiennej środowiskowej. Gdy nowy profil jest tworzony i konfigurowany w celu działania jako usługa systemu Windows, ta usługa jest domyślnie ustawiana do działania jako system lokalny. Jeśli jest podejmowana próba uruchomienia usługi systemu Windows, ta usługa nie może uzyskać dostępu do zmiennej środowiskowej użytkownika określającej protokół IPv6, w związku z czym podejmowana jest następnie próba użycia protokołu IPv4. W takim

przypadku serwer nie zostanie poprawnie uruchomiony. Aby rozwiązać ten problem, podczas tworzenia profilu należy określić, że usługa systemu Windows jest uruchamiana nie jako system lokalny, tylko jako ten sam identyfikator użytkownika, w ramach którego zdefiniowano zmienną środowiskową określającą protokół IPv6.

 Strona Definicja usługi systemu Linux jest wyświetlana tylko wtedy, gdy bieżący system operacyjny jest obsługiwana wersją systemu Linux, a bieżący użytkownik ma odpowiednie uprawnienia. Produkt podejmuje próbę uruchomienia usług systemu Linux dla procesów uruchamianych przez komendę startServer lub startManager. Jeśli na przykład serwer lub menedżer wdrażania został skonfigurowany jako usługa systemu Linux i zostanie wydana komenda startServer lub startManager, komenda wasservice uruchomi zdefiniowane usługi. Domyślnie produkt nie jest wybrany do działania jako usługa systemu Linux. Aby utworzyć usługę, użytkownik uruchamiający narzędzie Profile Management Tool musi być administratorem. Jeśli narzędzie Profile Management Tool zostanie uruchomione po zalogowaniu z użyciem identyfikatora użytkownika innego niż administrator, strona Definicja usługi systemu Linux nie zostanie wyświetlona, więc nie będzie można utworzyć usługi. Należy określić nazwę użytkownika, który uruchamia usługę. Aby usunąć usługę systemu Linux, użytkownik musi być administratorem lub mieć uprawnienia pozwalające na usunięcie usługi. W przeciwnym razie jest tworzony skrypt usuwania, za pomocą którego administrator może usunąć usługę w imieniu użytkownika.

- i. Jeśli instalacja jest przeprowadzana na jakiejś innej platformie lub jeśli instalacja jest przeprowadzana przez użytkownika niebędącego administratorem na platformie Linux lub Windows, zostanie wyświetlona strona Definicja serwera WWW. Aby do profilu dołączyć definicję serwera WWW, wykonaj następujące kroki:
 - 1) Należy zaznaczyć pole wyboru **Utwórz definicję serwera WWW**.
 - 2) Na stronie należy określić parametry serwera WWW i kliknąć przycisk **Dalej**.
 - 3) Należy określić parametry serwera WWW na drugiej części strony.

Jeśli serwer WWW służy do kierowania żądań do serwera, należy dołączyć definicję serwera WWW. Definicję można dołączyć teraz lub można później zdefiniować serwer WWW dla produktu Business Space. Jeśli definicja serwera WWW zostanie dołączona podczas tworzenia profilu, po zakończeniu tworzenia będzie można zainstalować serwer WWW i jego wtyczkę. Oba te produkty należy zainstalować w ścieżce określonej na stronach Definicja serwera WWW. Jeśli serwer WWW dla produktu Business Space zostanie zdefiniowany po utworzeniu tego profilu, należy zdefiniować serwer WWW w oddzielnym profilu.
 - 4) Kliknij przycisk **Dalej**.
- j. Jeśli ma zostać użyty plik projektu bazy danych, który został wcześniej utworzony w celu skonfigurowania baz danych, należy wykonać poniższe kroki zamiast używać stron Konfiguracja bazy danych.
 - 1) Wybierz opcję **Użyj pliku projektu bazy danych** w celu skonfigurowania bazy danych.
 - 2) Kliknij przycisk **Przeglądaj**.
 - 3) Podaj pełną ścieżkę do pliku projektu.
 - 4) Kliknij przycisk **Dalej**.
- k. Jeśli nie użyto pliku projektu bazy danych, na stronie Konfiguracja bazy danych wykonaj następujące czynności:
 - 1) Z listy Wybierz bazę danych wybierz bazę danych, która zostanie użyta przez profil.
 - 2) Zaznacz pole wyboru **Nadpisz domyślny katalog danych wyjściowych dla skryptów bazy danych**, jeśli ma zostać ustawiony katalog, do którego są

zapisywane skrypty SQL używane do tworzenia tabel baz danych. Jeśli to pole wyboru nie zostanie zaznaczone, skrypty zostaną zapisane w katalogu domyślnym.

- 3) Kliknij przycisk **Dalej**, aby wyświetlić stronę Konfiguracja bazy danych (część 2).

Informacje znajdujące się na stronie Konfiguracja bazy danych (część 2) różnią się w zależności od wartości wybranych z listy Wybór produktu bazy danych na stronie Konfiguracja bazy danych.

- l. Na stronie Konfiguracja bazy danych (część 2) dokończ konfigurację bazy danych. W zależności od bazy danych należy określić nazwę użytkownika i hasło na potrzeby uwierzytelniania w bazie danych, informacje dotyczące sterownika JDBC, a także host, port oraz schemat.
- m. Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.

Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.

Ostrzeżenie: Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:

- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
- **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.

Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.

Tworzenie profili produktu Business Space dla konfiguracji autonomicznej za pomocą programu narzędziowego wiersza komend manageprofiles:

Za pomocą programu narzędziowego wiersza komend manageprofiles możliwe jest tworzenie profili produktu Business Space dla konfiguracji serwera autonomicznego produktu Business Space.

Przed uruchomieniem programu narzędziowego wiersza komend manageprofiles należy upewnić się, że wykonano następujące czynności:

- Przejrzano kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- Przejrzano przykładowe komendy służące do tworzenia profilu.
- Sprawdzone, czy program narzędziowy wiersza komend manageprofiles nie został już uruchomiony dla tego samego profilu. W przypadku wyświetlenia komunikatu o błędzie należy ustalić, czy trwa tworzenie lub rozszerzanie innego profilu. Jeśli tak, należy poczekać do chwili zakończenia tego działania.

W tym zadaniu opisano sposób użycia programu narzędziowego wiersza komend manageprofiles do utworzenia profili produktu Business Space dla konfiguracji autonomicznej produktu Business Space. Aby utworzyć profil przy użyciu programu narzędziowego wiersza komend manageprofiles, wykonaj następujące kroki.

1. Znajdź szablon profilu default.bspace dla profili autonomicznych produktu Business Space, który definiuje serwery autonomiczne.
Szablony dla poszczególnych profili znajdują się w katalogu *instalacyjny_katalog_główny/profileTemplates/BusinessSpace*.
2. Określ, jakie parametry są wymagane do utworzenia profilu, przeglądając informacje znajdujące się w temacie “Program narzędziowy wiersza komend manageprofiles (w przypadku profili produktu Business Space)” na stronie 177. Określ wartości, które mają zostać podane dla profilu. Przejrzyj wartości domyślne, aby sprawdzić, czy są one odpowiednie dla profilu. Na przykład można użyć parametrów -templatePath, -enableAdminSecurity, -adminUserName, -adminPassword, -dbType, -dbUserId, dbPassword, -dbJDBCClasspath, -dbName, -bspaceSchema, -dbHostName, -dbServerPort i -dbDelayConfig.
3. Uruchom plik z poziomu wiersza komend. Poniżej przedstawiono prosty przykład:

```
manageProfiles -create -templatePath instalacyjny_katalog_główny/profileTemplates/BusinessSpace/d
-enableAdminSecurity true -adminUserName nazwa_administratora -adminPassword hasło_administrator
-dbType DB2_Universal -dbUserId ID_użytkownika_bazy_danych_db2 -dbPassword hasło_użytkownika_baz
-dbJDBCClasspath instalacyjny_katalog_główny/jdbcdrivers/DB2 -dbName nazwa_bazy_danych -bspaceSc
nazwa_schematu_bazy_danych -dbHostName nazwa_hosta -dbServerPort numer_portu -dbDelayConfig false
```

Komenda wyświetla status w trakcie działania. Należy poczekać na zakończenie operacji. W przypadku pliku odpowiedzi mają zastosowanie normalne zasady sprawdzania składni, ponieważ plik jest analizowany w sposób identyczny jak dowolny inny plik odpowiedzi. Poszczególne wartości w pliku odpowiedzi są traktowane jak parametry wiersza komend.

Tworzenie profili produktu Business Space dla konfiguracji wdrożenia sieciowego:

Aby utworzyć profile produktu Business Space dla środowiska wdrożenia sieciowego, możliwe jest użycie narzędzia Profile Management Tool lub programu narzędziowego wiersza komend manageprofiles.

Jeśli produkt Business Space jest skonfigurowany jako część profilu produktu, te zadania są opcjonalne.

Tworzenie profili produktu Business Space dla konfiguracji wdrożenia sieciowego za pomocą narzędzia Profile Management Tool:




Za pomocą narzędzia Profile Management Tool można utworzyć profile produktu Business Space dla konfiguracji wdrożenia sieciowego: tworzony jest profil menedżera wdrażania i profile niestandardowe (węzły zarządzane).

- Należy przejrzeć kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- W przypadku korzystania z narzędzia Profile Management Tool z graficznym interfejsem użytkownika Motif w systemie operacyjnym Solaris domyślna wielkość okna narzędzia Profile Management Tool może być zbyt mała do wyświetlenia wszystkich komunikatów i przycisków.

Tej procedury należy użyć, jeśli jest tworzony profil produktu Business Space dla konfiguracji wdrożenia sieciowego. Należy utworzyć profile menedżera wdrażania i profile niestandardowe dla węzłów zarządzanych. W poniższych krokach opisano zarówno opcję Zaawansowane tworzenie profilu, jak i Typowe tworzenie profilu.




Jeśli produkt Business Space został skonfigurowany jako część profilu produktu, to zadanie jest opcjonalne.

1. Utwórz profil menedżera wdrażania.

- a. Uruchom narzędzie Profile Management Tool.
Należy użyć jednej z następujących komend:
-   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
 -  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`
- b. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.
Zostanie otwarta karta Profile.
Karta Profile zawiera listę profili utworzonych na danym komputerze. Do tworzenia nowych profili lub rozszerzania profili już istniejących można użyć narzędzia Profile Management Tool.
- c. Na karcie Profile kliknij opcję **Utwórz**.
W oddzielnym oknie zostanie otwarta strona Wybór środowiska.
- d. Na stronie Wybór środowiska rozwiń sekcję **Produkt Business Space oparty na technologii WebSphere**, wybierz opcję **Menedżer wdrażania produktu Business Space opartego na technologii WebSphere**, a następnie kliknij opcję **Dalej**.
- e. Na stronie Opcje tworzenia profilu zdecyduj, czy utworzyć profil autonomiczny za pomocą opcji **Typowe tworzenie profilu**, czy opcji **Zaawansowane tworzenie profilu**.
- f. Jeśli wybrano opcję **Typowe tworzenie profilu**, wykonaj następujące kroki:
- 1) Na panelu Zabezpieczenia administracyjne wprowadź nazwę i hasło użytkownika, potwierdź hasło, a następnie kliknij przycisk **Dalej**. Cała konfiguracja profilu, w tym opcje profilu i baza danych, są domyślnie skonfigurowane i wyświetlane na stronie Podsumowanie profilu.
 - 2) Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.
Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.
- Ostrzeżenie:** Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:
- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
 - **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.
- Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.
- g. Jeśli wybrano opcję **Zaawansowane tworzenie profilu**, wykonaj następujące kroki:
- 1) Na stronie Wdrażanie opcjonalnych aplikacji zaznacz odpowiednie pola wyboru, jeśli ma zostać wdrożona Konsola administracyjna i aplikacja domyślna.
 - 2) Na stronie Nazwa i położenie profilu wykonaj następujące kroki:
 - a) W polu Nazwa profilu wpisz unikalną nazwę lub zaakceptuj wartość domyślną. Każdy tworzony profil musi mieć nazwę. W przypadku, gdy istnieje więcej niż jeden profil, można je odróżnić na najwyższym poziomie

za pomocą tej nazwy. Jeśli wybrano opcję nieużywania nazwy domyślnej, w systemie Windows należy użyć krótkiej nazwy, ponieważ nazwy ścieżek mają ograniczoną długość.

- b) W polu Katalog profilu wpisz nazwę katalogu profilu lub użyj przycisku Przeglądaj, aby przejść do katalogu profilu. Określony katalog będzie zawierać pliki definiujące środowisko wykonawcze (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Katalog domyślny jest zależny od platformy:

-   `instalacyjny_katalog_główny/profiles/nazwa_profilu`
-  `instalacyjny_katalog_główny\profiles\nazwa_profilu`
gdzie `nazwa_profilu` to podana nazwa.

Pole katalogu profilu musi spełniać następujące wymagania:

- Nazwa profilu (`nazwa_profilu`) musi być unikalna.
 - Podany katalog musi być pusty.
 - Identyfikator użytkownika musi mieć uprawnienia do katalogu.
 - Musi istnieć wystarczająca ilość miejsca do utworzenia profilu.
- c) Opcjonalnie: jeśli tworzony profil ma być używany jako profil domyślny, należy zaznaczyć pole wyboru **Ustaw ten profil jako domyślny**. To pole wyboru zostanie wyświetlone tylko wtedy, gdy w systemie istnieje profil. Komendy będą działać automatycznie z profilem domyślnym. Pierwszy profil tworzony na stacji roboczej jest profilem domyślnym. Profil domyślny jest domyślnym miejscem docelowym dla komend wykonywanych z poziomu katalogu bin w instalacyjnym katalogu głównym produktu. Gdy na stacji roboczej istnieje tylko jeden profil, każda komenda jest wykonywana względem tego profilu. Jeśli istnieje więcej niż jeden profil, niektóre komendy wymagają określenia profilu będącego ich celem.

- d) Kliknij przycisk **Dalej**.

- 3) Na stronie Nazwy węzłów i hostów wykonaj następujące czynności na potrzeby tworzonego profilu:

- a) W polu Nazwa węzła wpisz nazwę węzła lub zaakceptuj wartość domyślną. Nazwy węzłów powinny być jak najkrótsze, ale jednocześnie każda z nich musi być unikalna w środowisku wdrażania.
- b) W polu Nazwa hosta wpisz nazwę hosta lub zaakceptuj wartość domyślną.
- c) W polu Nazwa komórki wpisz nazwę komórki lub zaakceptuj wartość domyślną.

Kliknij przycisk **Dalej**, aby wyświetlić stronę Zabezpieczenia administracyjne.

- 4) Na stronie Zabezpieczenia administracyjne wprowadź nazwę i hasło użytkownika oraz potwierdź hasło. Kliknij przycisk **Dalej**.

- 5) Na stronie Certyfikat bezpieczeństwa (część 1) określ, czy mają być tworzone nowe certyfikaty, czy mają zostać zaimportowane istniejące certyfikaty. Wykonaj następujące czynności:

- Aby utworzyć nowy domyślny certyfikat osobisty i nowy główny certyfikat podpisywania, wybierz opcję **Utwórz nowy domyślny certyfikat osobisty i Utwórz nowy główny certyfikat podpisywania**, a następnie kliknij przycisk **Dalej**.
- Aby zaimportować istniejące certyfikaty, wybierz opcję **Importuj istniejący domyślny certyfikat osobisty i Importuj istniejący główny osobisty certyfikat podpisywania**, a następnie podaj następujące informacje:
 - W polu Ścieżka wprowadź ścieżkę do katalogu dla istniejącego certyfikatu.

- W polu Hasło wpisz hasło dla certyfikatu.
- W polu Typ magazynu kluczy wybierz typ magazynu kluczy dla importowanego certyfikatu.
- W polu Alias magazynu kluczy wybierz alias magazynu kluczy dla importowanego certyfikatu.
- Kliknij przycisk **Dalej**.

W przypadku importowania certyfikatu osobistego jako domyślnego certyfikatu osobistego należy zaimportować główny certyfikat, za pomocą którego podpisano certyfikat osobisty. W przeciwnym razie narzędzie Profile Management Tool dodaje osobę podpisującą dla certyfikatu osobistego do pliku `trust.p12`. W przypadku importowania domyślnego certyfikatu osobistego lub głównego certyfikatu podpisywania należy określić ścieżkę i hasło, a następnie wybrać typ oraz alias magazynu kluczy dla każdego importowanego certyfikatu.

- 6) Na stronie Certyfikat bezpieczeństwa (część 2) sprawdź, czy informacje o certyfikacie są poprawne, i kliknij przycisk **Dalej**, aby wyświetlić stronę Przypisywanie wartości portów.

Tworząc certyfikaty, można użyć wartości domyślnych lub zmodyfikować je na potrzeby tworzenia nowych certyfikatów. Domyślny certyfikat osobisty jest domyślnie ważny przez rok i jest podpisany przez główny certyfikat podpisywania. Główny certyfikat podpisywania jest certyfikatem samopodpisanym, który domyślnie jest ważny przez 15 lat. Domyślne hasło magazynu kluczy dla głównego certyfikatu podpisywania to WebAS. To hasło należy zmienić. Hasło nie może zawierać żadnych znaków z zestawu znaków dwubajtowych (DBCS), ponieważ tych znaków nie obsługują niektóre typy magazynów kluczy, takie jak PKCS12. Obsługiwane typy magazynów kluczy są zależne od dostawców zawartych w pliku `java.security`.

W przypadku tworzenia lub importowania jednego bądź obu certyfikatów są tworzone następujące pliki kluczy:

- `key.p12`: zawiera domyślny certyfikat osobisty.
- `trust.p12`: zawiera certyfikat osoby podpisującej z domyślnego certyfikatu głównego.
- `root-key.p12`: zawiera główny certyfikat podpisywania.
- `default-signers.p12`: zawiera certyfikaty osób podpisujących dodawane do każdego nowego pliku kluczy tworzonego po zainstalowaniu i uruchomieniu serwera. Domyślnie w tym pliku kluczy znajdują się informacje o osobie podpisującej domyślny certyfikat główny i certyfikat osoby podpisującej serwera DataPower®.
- `deleted.p12`: zawiera certyfikaty usunięte za pomocą zadania `deleteKeyStore`, aby można je było odzyskać w razie potrzeby.
- `ltpa.jceks`: zawiera domyślne klucze LTPA (Lightweight Third-Party Authentication) serwera używane przez serwery w danym środowisku do wzajemnej komunikacji.

W przypadku tworzenia lub importowania certyfikatów wszystkie te pliki mają takie same hasło. Może to być hasło domyślne lub określone przez użytkownika. Importowany certyfikat jest dodawany do pliku `key.p12` lub pliku `root-key.p12`. Jeśli zostaną zaimportowane certyfikaty, które nie zawierają żądanych informacji, należy kliknąć przycisk **Wstecz**, aby zaimportować inny certyfikat.

- 7) Na stronie Przypisywanie wartości portów sprawdź, czy porty określone dla profilu są unikalne, a następnie kliknij przycisk **Dalej**.

Narzędzie Profile Management Tool wykrywa porty aktualnie używane przez inne produkty IBM WebSphere i wyświetla zalecane wartości portów, które nie

powodują konfliktu z już istniejącymi. Jeśli są używane inne aplikacje, które korzystają z określonych portów, należy sprawdzić, czy porty nie powodują konfliktów. Jeśli na stronie Wdrażanie aplikacji opcjonalnych nie wybrano opcji wdrażania Konsoli administracyjnej, jej porty nie będą dostępne na stronie Przypisywanie wartości portów. Porty są rozpoznawane jako używane, jeśli zostały przypisane do profilu utworzonego podczas instalacji przeprowadzanej przez bieżącego użytkownika lub jeśli są one aktualnie używane.

Mimo że narzędzie sprawdza poprawność portów w momencie uzyskiwania dostępu do strony Przypisywanie wartości portów, mogą występować konflikty portów, które wynikają z ustawień wybranych na kolejnych stronach narzędzia Profile Management Tool. Porty nie zostaną przypisane do momentu zakończenia procesu tworzenia profilu. Jeśli zachodzi podejrzenie wystąpienia konfliktu portów, po utworzeniu profilu można to sprawdzić.

Sprawdzając plik katalog_główny_profilu/properties/portdef.props, należy określić porty używane podczas tworzenia profilu. W tym pliku znajdują się klucze i wartości użyte podczas ustawiania portów. W przypadku wykrycia konfliktów portów można je ponownie przypisać ręcznie. Aby ponownie przypisać porty, należy zapoznać się z tematem Aktualizowanie portów istniejącego profilu, który znajduje się w Centrum informacyjnym produktu WebSphere Application Server Network Deployment. Przy użyciu opisanego w tym temacie skryptu ws_ant należy uruchomić plik updatePorts.ant.


- 8) W przypadku przeprowadzania instalacji na platformie Linux lub Windows użytkownikowi będącemu administratorem lub z uprawnieniami grupy administratorów zostanie wyświetlona strona definicji usługi systemu Linux lub Windows. Na stronie Definicja usługi należy wskazać, czy usługa systemu Windows lub Linux będzie uruchamiała serwer procesów, a następnie należy kliknąć opcję **Dalej**, aby wyświetlić stronę Definicja serwera WWW.

Windows Strona Definicja usługi systemu Windows jest otwierana dla platformy Windows tylko wtedy, gdy ID użytkownika instalującego usługę systemu Windows ma uprawnienia grupy administratorów. Jeśli profil został skonfigurowany jako usługa systemu Windows, produkt uruchamia usługi systemu Windows dla procesów uruchomionych za pomocą komendy startServer lub startManager. Jeśli na przykład serwer lub menedżer wdrażania został skonfigurowany jako usługa systemu Windows i zostanie wydana komenda startServer lub startManager, komenda wasservice uruchomi zdefiniowane usługi.

Ważne: W przypadku logowania jako określone konto użytkownika należy podać ID i hasło użytkownika uruchamiającego usługę oraz typ uruchamiania (typ domyślny to Ręcznie). Identyfikator użytkownika nie może zawierać spacji, musi należeć do grupy Administratorzy oraz mieć uprawnienia użytkownika zaawansowanego pozwalające na logowanie w trybie usługi. Jeśli ID użytkownika należy do grupy Administratorzy, narzędzie Profile Management Tool nadaje mu uprawnienia użytkownika zaawansowanego, jeśli jeszcze ich nie ma. W ramach procesu usuwania profilu można usunąć usługę systemu Windows dodaną podczas tworzenia profilu.

Windows **Uwagi dotyczące protokołu IPv6 w przypadku uruchamiania profili jako usługi systemu Windows:** profile utworzone w celu działania jako usługa systemu Windows nie mogą zostać uruchomione w przypadku użycia protokołu IPv6, jeśli usługa została skonfigurowana do działania jako system lokalny. Aby włączyć protokół IPv6, należy utworzyć zmienną środowiskową specyficzną dla użytkownika. Ponieważ ta zmienna środowiskowa jest zmienną użytkownika, a nie zmienną systemu lokalnego, tylko usługa systemu Windows działająca jako ten konkretny użytkownik może uzyskać dostęp do tej zmiennej środowiskowej. Gdy nowy profil jest tworzony i konfigurowany w celu działania

jako usługa systemu Windows, ta usługa jest domyślnie ustawiana do działania jako system lokalny. Jeśli jest podejmowana próba uruchomienia usługi systemu Windows, ta usługa nie może uzyskać dostępu do zmiennej środowiskowej użytkownika określającej protokół IPv6, w związku z czym podejmowana jest następnie próba użycia protokołu IPv4. W takim przypadku serwer nie zostanie poprawnie uruchomiony. Aby rozwiązać ten problem, podczas tworzenia profilu należy określić, że usługa systemu Windows jest uruchamiana nie jako system lokalny, tylko jako ten sam identyfikator użytkownika, w ramach którego zdefiniowano zmienną środowiskową określającą protokół IPv6.

 Strona Definicja usługi systemu Linux jest wyświetlana tylko wtedy, gdy bieżący system operacyjny jest obsługiwana wersją systemu Linux, a bieżący użytkownik ma odpowiednie uprawnienia. Produkt podejmuje próbę uruchomienia usług systemu Linux dla procesów uruchamianych przez komendę `startServer` lub `startManager`. Jeśli na przykład serwer lub menedżer wdrażania został skonfigurowany jako usługa systemu Linux i zostanie wydana komenda `startServer` lub `startManager`, komenda `wasservice` uruchomi zdefiniowane usługi. Domyślnie produkt nie jest wybrany do działania jako usługa systemu Linux. Aby utworzyć usługę, użytkownik uruchamiający narzędzie Profile Management Tool musi być administratorem. Jeśli narzędzie Profile Management Tool zostanie uruchomione po zalogowaniu z użyciem identyfikatora użytkownika innego niż administrator, strona Definicja usługi systemu Linux nie zostanie wyświetlona, więc nie będzie można utworzyć usługi. Należy określić nazwę użytkownika, który uruchamia usługę. Aby usunąć usługę systemu Linux, użytkownik musi być administratorem lub mieć uprawnienia pozwalające na usunięcie usługi. W przeciwnym razie jest tworzony skrypt usuwania, za pomocą którego administrator może usunąć usługę w imieniu użytkownika.

- 9) Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.

Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.

Ostrzeżenie: Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:




- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
- **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.

Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.

2. Uruchom profil menedżera wdrażania.




Menedżer wdrażania należy uruchomić za pomocą komendy `startServer` z poziomu katalogu `katalog_główny_profilu/bin`.

Należy użyć następującej składni:




-   `startServer.sh nazwa_serwera`
-  `startServer.bat nazwa_serwera`

Więcej informacji dotyczących komendy `startServer` zawiera temat Komenda `startServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

3. Utwórz profile niestandardowe (węzły zarządzane).

- a. Uruchom narzędzie Profile Management Tool.
Należy użyć jednej z następujących komend:
-   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
 -  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`
- b. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.
Zostanie otwarta karta Profile.
Karta Profile zawiera listę profili utworzonych na danym komputerze. Do tworzenia nowych profili lub rozszerzania profili już istniejących można użyć narzędzia Profile Management Tool.
- c. Na karcie Profile kliknij opcję **Utwórz**.
W oddzielnym oknie zostanie otwarta strona Wybór środowiska.
- d. Na stronie Wybór środowiska rozwiń sekcję **Produkt Business Space oparty na technologii WebSphere**, wybierz opcję **Profil niestandardowy produktu Business Space opartego na technologii WebSphere**, a następnie kliknij opcję **Dalej**.
- e. Na stronie Opcje tworzenia profilu zdecyduj, czy utworzyć profil autonomiczny za pomocą opcji **Typowe tworzenie profilu**, czy opcji **Zaawansowane tworzenie profilu**.
- f. Jeśli wybrano opcję **Typowe tworzenie profilu**, wykonaj następujące kroki:
- 1) Na stronie Stowarzyszanie wybierz opcję stowarzyszania danego węzła z menedżerem wdrażania albo w ramach bieżącej procedury tworzenia danego profilu, albo w przyszłości za pomocą komendy addNode (niezależnie od procedury tworzenia profilu). Zaznacz lub usuń zaznaczenie pola wyboru **Stowarzysz ten węzeł później** i kliknij przycisk **Dalej**.
 - 2) Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.
Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.
- Ostrzeżenie:** Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:
- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
 - **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.
- Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.
- g. Jeśli wybrano opcję **Zaawansowane tworzenie profilu**, wykonaj następujące kroki:
- 1) Na stronie Nazwa i położenie profilu wykonaj następujące kroki:
 - a) W polu Nazwa profilu wpisz unikalną nazwę lub zaakceptuj wartość domyślną. Każdy tworzony profil musi mieć nazwę. W przypadku, gdy istnieje więcej niż jeden profil, można je odróżnić na najwyższym poziomie za pomocą tej nazwy. Jeśli wybrano opcję nieużywania nazwy domyślnej, w systemie Windows należy użyć krótkiej nazwy, ponieważ nazwy ścieżek mają ograniczoną długość.

b) W polu Katalog profilu wpisz nazwę katalogu profilu lub użyj przycisku Przeglądaj, aby przejść do katalogu profilu. Określony katalog będzie zawierał pliki definiujące środowisko wykonawcze (takie jak komendy, pliki konfiguracyjne oraz pliki dzienników). Katalog domyślny jest zależny od platformy:

-   `instalacyjny_katalog_główny/profiles/nazwa_profilu`
-  `instalacyjny_katalog_główny\profiles\nazwa_profilu`
gdzie `nazwa_profilu` to podana nazwa.

Pole katalogu profilu musi spełniać następujące wymagania:

- Nazwa profilu (`nazwa_profilu`) musi być unikalna.
 - Podany katalog musi być pusty.
 - Identyfikator użytkownika musi mieć uprawnienia do katalogu.
 - Musi istnieć wystarczająca ilość miejsca do utworzenia profilu.
- c) Opcjonalnie: jeśli tworzony profil ma być używany jako profil domyślny, należy zaznaczyć pole wyboru **Ustaw ten profil jako domyślny**. To pole wyboru zostanie wyświetlone tylko wtedy, gdy w systemie istnieje profil. Komendy będą działać automatycznie z profilem domyślnym. Pierwszy profil tworzony na stacji roboczej jest profilem domyślnym. Profil domyślny jest domyślnym miejscem docelowym dla komend wykonywanych z poziomu katalogu bin w instalacyjnym katalogu głównym produktu. Gdy na stacji roboczej istnieje tylko jeden profil, każda komenda jest wykonywana względem tego profilu. Jeśli istnieje więcej niż jeden profil, niektóre komendy wymagają określenia profilu będącego ich celem.

d) Kliknij przycisk **Dalej**.

2) Na stronie Nazwy węzłów i hostów wykonaj następujące czynności na potrzeby tworzonego profilu:

- a) W polu Nazwa węzła wpisz nazwę węzła lub zaakceptuj wartość domyślną. Nazwy węzłów powinny być jak najkrótsze, ale jednocześnie każda z nich musi być unikalna w środowisku wdrażania.
- b) W polu Nazwa hosta wpisz nazwę hosta lub zaakceptuj wartość domyślną.
- c) W polu Nazwa komórki wpisz nazwę komórki lub zaakceptuj wartość domyślną.

Kliknij przycisk **Dalej**, aby wyświetlić stronę Zabezpieczenia administracyjne.

3) Na stronie Stowarzyszenie wybierz opcję stowarzyszenia danego węzła z menedżerem wdrażania albo w ramach bieżącej procedury tworzenia danego profilu, albo w przyszłości za pomocą komendy `addNode` (niezależnie od procedury tworzenia profilu). Zaznacz lub usuń zaznaczenie pola wyboru **Stowarzysz ten węzeł później** i kliknij przycisk **Dalej**.

4) Na stronie Certyfikat bezpieczeństwa (część 1) określ, czy mają być tworzone nowe certyfikaty, czy mają zostać zaimportowane istniejące certyfikaty. Wykonaj następujące czynności:

- Aby utworzyć nowy domyślny certyfikat osobisty i nowy główny certyfikat podpisywania, wybierz opcję **Utwórz nowy domyślny certyfikat osobisty i Utwórz nowy główny certyfikat podpisywania**, a następnie kliknij przycisk **Dalej**.
- Aby zaimportować istniejące certyfikaty, wybierz opcję **Importuj istniejący domyślny certyfikat osobisty i Importuj istniejący główny osobisty certyfikat podpisywania**, a następnie podaj następujące informacje:
 - W polu Ścieżka wprowadź ścieżkę do katalogu dla istniejącego certyfikatu.

- W polu Hasło wpisz hasło dla certyfikatu.
- W polu Typ magazynu kluczy wybierz typ magazynu kluczy dla importowanego certyfikatu.
- W polu Alias magazynu kluczy wybierz alias magazynu kluczy dla importowanego certyfikatu.
- Kliknij przycisk **Dalej**.

W przypadku importowania certyfikatu osobistego jako domyślnego certyfikatu osobistego należy zaimportować główny certyfikat, za pomocą którego podpisano certyfikat osobisty. W przeciwnym razie narzędzie Profile Management Tool dodaje osobę podpisującą dla certyfikatu osobistego do pliku `trust.p12`. W przypadku importowania domyślnego certyfikatu osobistego lub głównego certyfikatu podpisywania należy określić ścieżkę i hasło, a następnie wybrać typ oraz alias magazynu kluczy dla każdego importowanego certyfikatu.

- 5) Na stronie Certyfikat bezpieczeństwa (część 2) sprawdź, czy informacje o certyfikacie są poprawne, i kliknij przycisk **Dalej**, aby wyświetlić stronę Przypisywanie wartości portów.

Tworząc certyfikaty, można użyć wartości domyślnych lub zmodyfikować je na potrzeby tworzenia nowych certyfikatów. Domyślny certyfikat osobisty jest domyślnie ważny przez rok i jest podpisany przez główny certyfikat podpisywania. Główny certyfikat podpisywania jest certyfikatem samopodpisanym, który domyślnie jest ważny przez 15 lat. Domyślne hasło magazynu kluczy dla głównego certyfikatu podpisywania to WebAS. To hasło należy zmienić. Hasło nie może zawierać żadnych znaków z zestawu znaków dwubajtowych (DBCS), ponieważ tych znaków nie obsługują niektóre typy magazynów kluczy, takie jak PKCS12. Obsługiwane typy magazynów kluczy są zależne od dostawców zawartych w pliku `java.security`.

W przypadku tworzenia lub importowania jednego bądź obu certyfikatów są tworzone następujące pliki kluczy:

- `key.p12`: zawiera domyślny certyfikat osobisty.
- `trust.p12`: zawiera certyfikat osoby podpisującej z domyślnego certyfikatu głównego.
- `root-key.p12`: zawiera główny certyfikat podpisywania.
- `default-signers.p12`: zawiera certyfikaty osób podpisujących dodawane do każdego nowego pliku kluczy tworzonego po zainstalowaniu i uruchomieniu serwera. Domyślnie w tym pliku kluczy znajdują się informacje o osobie podpisującej domyślny certyfikat główny i certyfikat osoby podpisującej serwera DataPower®.
- `deleted.p12`: zawiera certyfikaty usunięte za pomocą zadania `deleteKeyStore`, aby można je było odzyskać w razie potrzeby.
- `ltpa.jceks`: zawiera domyślne klucze LTPA (Lightweight Third-Party Authentication) serwera używane przez serwery w danym środowisku do wzajemnej komunikacji.

W przypadku tworzenia lub importowania certyfikatów wszystkie te pliki mają takie same hasło. Może to być hasło domyślne lub określone przez użytkownika. Importowany certyfikat jest dodawany do pliku `key.p12` lub pliku `root-key.p12`. Jeśli zostaną zaimportowane certyfikaty, które nie zawierają żądanych informacji, należy kliknąć przycisk **Wstecz**, aby zaimportować inny certyfikat.

- 6) Na stronie Podsumowanie profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu.

Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono tworzenie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil.**

Ostrzeżenie: Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:




- **Narzędzie Profile Management Tool utworzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
- **Narzędzie Profile Management Tool nie może utworzyć profilu** - ten komunikat wskazuje, że proces tworzenia profilu zakończył się całkowitym niepowodzeniem.

Na stronie Zakończono tworzenie profilu wskazany jest plik dziennika, który można przejrzeć w celu rozwiązania problemów.

4. Zaloguj się w Konsoli administracyjnej menedżera wdrażania.
5. W zależności od tego, czy produkt Business Space ma zostać wdrożony w klastrze, czy na serwerach zarządzanych, wykonaj jedną z następujących czynności:
 - Dla klastra:
 - a. Utwórz klaster serwera aplikacji.
 - b. Dodaj co najmniej jeden element klastra do klastra (są to wcześniej utworzone profile niestandardowe produktu Business Space).
 - Dla każdego serwera zarządzanego:
 - a. Utwórz serwer aplikacji.
 - b. Wybierz węzeł serwera zarządzanego będący wcześniej utworzonym profilem produktu Business Space.
6. Zatrzymaj profil menedżera wdrażania.

Menedżer wdrażania można zatrzymać za pomocą komendy `stopServer` uruchamianej z poziomu katalogu `katalog_główny_profilu/bin`.

Należy użyć następującej składni:

-  `Linux`  `UNIX` `stopServer.sh nazwa_serwera -username nazwa_użytkownika -password hasło`
-  `Windows` `stopServer.bat nazwa_serwera -username nazwa_użytkownika -password hasło`

Jeśli w profilu nie włączono zabezpieczeń, parametry `-username` i `-password` nie są konieczne.

Więcej informacji dotyczących komendy `stopServer` zawiera temat Komenda `stopServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

7. Przejdź do katalogu `instalacyjny_katalog_główny/BusinessSpace/config.bspace/MetadataFiles` i w zależności od typu bazy danych, która będzie używana dla produktu Business Space, skopiuj odpowiedni plik do katalogu roboczego. Nie zmieniaj rozszerzenia tego pliku - rozszerzeniem musi być `.properties`.
 - a. Zmodyfikuj kopię tego pliku i zmień wartości na odpowiadające używanej bazie danych. Należy zwrócić szczególną uwagę na właściwość `wasHome` i upewnić się, że jest ona poprawna.
 - b. Zapisz plik po zakończeniu edytowania informacji o bazie danych.

Po utworzeniu profili i skonfigurowaniu informacji dotyczących bazy danych dla profili można skonfigurować produkt Business Space w używanym środowisku, wykonując następujące kroki.

1. Dla każdego klastra lub serwera zarządzanego uruchom komendę `installBusinessSpace` w celu zainstalowania plików archiwum korporacyjnego (EAR) produktu Business Space w środowisku wykonawczym. Należy podać parametr **clusterName** lub parametry **nodeName** i **serverName** w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
2. Dla każdego klastra lub serwera zarządzanego uruchom komendę `configureBusinessSpace`, podając parametr **clusterName** lub parametry **nodeName** i **serverName** w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Określ także parametr **bspacedbDesign**. Wartością tego parametru powinna być ścieżka do pliku właściwości bazy danych, który był wcześniej edytowany. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
3. Zapisz konfigurację narzędzia `wsadmin`.
4. Utwórz i skonfiguruj bazę danych produktu Business Space. Patrz temat “Konfigurowanie bazy danych produktu Business Space” na stronie 205.
5. Uruchom menedżer wdrażania.
6. Uruchom klastry lub serwery zarządzane.

Tworzenie profili produktu Business Space dla konfiguracji wdrożenia sieciowego za pomocą programu narzędziowego wiersza komend `manageprofiles`:

Za pomocą programu narzędziowego wiersza komend `manageprofiles` możliwe jest tworzenie profili menedżera wdrażania i profili niestandardowych (węzły zarządzane) dla konfiguracji wdrożenia sieciowego produktu Business Space.

Przed uruchomieniem programu narzędziowego wiersza komend `manageprofiles` należy upewnić się, że wykonano następujące czynności:

- Przejrzano kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- Przejrzano przykładowe komendy służące do tworzenia profilu.
- Sprawdzone, czy program narzędziowy wiersza komend `manageprofiles` nie został już uruchomiony dla tego samego profilu. W przypadku wyświetlenia komunikatu o błędzie należy ustalić, czy trwa tworzenie lub rozszerzanie innego profilu. Jeśli tak, należy poczekać do chwili zakończenia tego działania.

W tym zadaniu opisano sposób użycia programu narzędziowego wiersza komend `manageprofiles` do utworzenia profili produktu Business Space dla konfiguracji wdrożenia sieciowego produktu Business Space. Aby utworzyć profil przy użyciu programu narzędziowego wiersza komend `manageprofiles`, wykonaj następujące kroki.

1. Utwórz profil menedżera wdrażania.
 - a. Znajdź szablon `dmgr.bspace` dla profili menedżera wdrażania produktu Business Space, który definiuje menedżery wdrażania. Menedżer wdrażania udostępnia pojedynczy interfejs administracyjny dla logicznej grupy serwerów na jednej lub większej liczbie stacji roboczych.
Szablony dla poszczególnych profili znajdują się w katalogu `instalacyjny_katalog_główny/profileTemplates/BusinessSpace`.
 - b. Określ, jakie parametry są wymagane do utworzenia profilu, przeglądając informacje znajdujące się w temacie “Program narzędziowy wiersza komend `manageprofiles` (w przypadku profili produktu Business Space)” na stronie 177. Określ wartości, które mają zostać podane dla profilu. Przejrzyj wartości domyślne, aby sprawdzić, czy są one odpowiednie dla profilu. Na przykład można dołączyć parametry `-templatePath`, `-serverType`, `-enableAdminSecurity`, `-adminUserName` i `-adminPassword`.

- c. Uruchom plik z poziomu wiersza komend. Poniżej przedstawiono prosty przykład:



```
manageProfiles -create -templatePath instalacyjny_katalog_główny/profileTemplates/BusinessSpace
-serverType DEPLOYMENT_MANAGER -enableAdminSecurity true -adminUserName ID_administratora
```

Komenda wyświetla status w trakcie działania. Należy poczekać na zakończenie operacji. W przypadku pliku odpowiedzi mają zastosowanie normalne zasady sprawdzania składni, ponieważ plik jest analizowany w sposób identyczny jak dowolny inny plik odpowiedzi. Poszczególne wartości w pliku odpowiedzi są traktowane jak parametry wiersza komend.

2. Uruchom profil menedżera wdrażania.

Menedżer wdrażania należy uruchomić za pomocą komendy `startServer` z poziomu katalogu `katalog_główny_profilu/bin`.

Należy użyć następującej składni:

-  `startServer.sh nazwa_serwera`
-  `startServer.bat nazwa_serwera`

Więcej informacji dotyczących komendy `startServer` zawiera temat Komenda `startServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

3. Utwórz profile niestandardowe (węzły zarządzane).

- a. Znajdź szablon `managed.bspace` dla profili niestandardowych produktu Business Space, które (jeśli są stowarzyszone z menedżerem wdrażania) definiują węzły zarządzane. Jeśli zdecydowano, że rozwiązanie wymaga środowiska wdrażania, środowisko wykonawcze musi mieć co najmniej jeden węzeł zarządzany. Profil niestandardowy zawiera pusty węzeł, którego działanie jest możliwe po stowarzyszeniu z komórką menedżera wdrażania. Po stowarzyszeniu profil niestandardowy zmienia się w węzeł zarządzany. Nie należy stowarzyszać węzła, chyba że ma on zostać stowarzyszony z menedżerem wdrażania, którego wersja jest taka sama (lub nowsza) jak wersja tworzonego profilu niestandardowego.

Szablony dla poszczególnych profili znajdują się w katalogu `instalacyjny_katalog_główny/profileTemplates/BusinessSpace`.

- b. Określ, jakie parametry są wymagane do utworzenia profilu, przeglądając informacje znajdujące się w temacie “Program narzędziowy wiersza komend `manageprofiles` (w przypadku profili produktu Business Space)” na stronie 177. Określ wartości, które mają zostać podane dla profilu. Przejrzyj wartości domyślne, aby sprawdzić, czy są one odpowiednie dla profilu. Na przykład można dołączyć parametry `-templatePath`, `-dmgrAdminUserName`, `-dmgrAdminPassword`, `-dmgrPort` i `-dmgrHost`.

- c. Uruchom plik z poziomu wiersza komend. Poniżej przedstawiono prosty przykład:

```
manageProfiles -create -templatePath instalacyjny_katalog_główny/profileTemplates/BusinessSpace
-dmgrAdminUserName ID_administratora_menedżera_wdrażania -dmgrAdminPassword hasło_administratora
-dmgrPort port_menedżera_wdrażania -dmgrHost nazwa_hosta_menedżera_wdrażania
```

Komenda wyświetla status w trakcie działania. Należy poczekać na zakończenie operacji. W przypadku pliku odpowiedzi mają zastosowanie normalne zasady sprawdzania składni, ponieważ plik jest analizowany w sposób identyczny jak dowolny inny plik odpowiedzi. Poszczególne wartości w pliku odpowiedzi są traktowane jak parametry wiersza komend.

4. Zaloguj się w Konsoli administracyjnej menedżera wdrażania.




5. W zależności od tego, czy produkt Business Space ma zostać wdrożony w klastrze, czy na serwerach zarządzanych, wykonaj jedną z następujących czynności:

- Dla klastra:
 - a. Utwórz klastr serwera aplikacji.
 - b. Dodaj co najmniej jeden element klastra do klastra (są to wcześniej utworzone profile niestandardowe produktu Business Space).

- Dla każdego serwera zarządzanego:
 - a. Utwórz serwer aplikacji.
 - b. Wybierz węzeł serwera zarządzanego będący wcześniej utworzonym profilem produktu Business Space.
- 6. Zatrzymaj profil menedżera wdrażania.

Menedżer wdrażania można zatrzymać za pomocą komendy `stopServer` uruchamianej z poziomu katalogu `katalog_główny_profilu/bin`.

Należy użyć następującej składni:

-   `stopServer.sh nazwa_serwera -username nazwa_użytkownika -password hasło`
-  `stopServer.bat nazwa_serwera -username nazwa_użytkownika -password hasło`

Jeśli w profilu nie włączono zabezpieczeń, parametry `-username` i `-password` nie są konieczne.

Więcej informacji dotyczących komendy `stopServer` zawiera temat Komenda `stopServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

7. Przejdź do katalogu `instalacyjny_katalog_główny/BusinessSpace/config.bspace/MetadataFiles` i w zależności od typu bazy danych, która będzie używana dla produktu Business Space, skopiuj odpowiedni plik do katalogu roboczego. Nie zmieniaj rozszerzenia tego pliku - rozszerzeniem musi być `.properties`.
 - a. Zmodyfikuj kopię tego pliku i zmień wartości na odpowiadające używanej bazie danych. Należy zwrócić szczególną uwagę na właściwość `wasHome` i upewnić się, że jest ona poprawna.
 - b. Zapisz plik po zakończeniu edytowania informacji o bazie danych.

Po utworzeniu profili i skonfigurowaniu informacji dotyczących bazy danych dla profili można skonfigurować produkt Business Space w używanym środowisku, wykonując następujące kroki.

1. Dla każdego klastra lub serwera zarządzanego uruchom komendę `installBusinessSpace` w celu zainstalowania plików archiwum korporacyjnego (EAR) produktu Business Space w środowisku wykonawczym. Należy podać parametr `clusterName` lub parametry `nodeName` i `serverName` w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
2. Dla każdego klastra lub serwera zarządzanego uruchom komendę `configureBusinessSpace`, podając parametr `clusterName` lub parametry `nodeName` i `serverName` w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Określ także parametr `bspacedbDesign`. Wartością tego parametru powinna być ścieżka do pliku właściwości bazy danych, który był wcześniej edytowany. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
3. Zapisz konfigurację narzędzia `wsadmin`.
4. Utwórz i skonfiguruj bazę danych produktu Business Space. Patrz temat “Konfigurowanie bazy danych produktu Business Space” na stronie 205.
5. Uruchom menedżer wdrażania.
6. Uruchom klastry lub serwery zarządzane.

Rozszerzanie profili produktu Business Space dla konfiguracji autonomicznej:

Aby rozszerzyć profile produktu Business Space dla środowiska autonomicznego, możliwe jest użycie narzędzia Profile Management Tool lub programu narzędziowego wiersza komend `manageprofiles`.

Jeśli produkt Business Space jest skonfigurowany jako część profilu produktu, te zadania są opcjonalne.

Rozszerzanie profili produktu Business Space dla konfiguracji autonomicznej za pomocą narzędzia Profile Management Tool:

Za pomocą narzędzia Profile Management Tool można rozszerzać profile autonomiczne produktu Business Space.

Należy zrozumieć pojęcia dotyczące profili, w tym różnice między profilami autonomicznymi, wdrożenia sieciowego i niestandardowymi. Należy także zrozumieć różnice między opcją Typowe rozszerzanie profilu i opcją Zaawansowane rozszerzanie profilu, w tym potrafić określić, w których scenariuszach należy użyć danej opcji. Opcja Typowe rozszerzanie profilu umożliwia rozszerzenie profilu przy użyciu domyślnych ustawień konfiguracji. Opcja Zaawansowane rozszerzanie profilu umożliwia określenie własnych wartości konfiguracji dla rozszerzanego profilu.




- Należy przejrzeć kompletną listę wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- W przypadku korzystania z narzędzia Profile Management Tool z graficznym interfejsem użytkownika Motif w systemie operacyjnym Solaris domyślna wielkość okna narzędzia Profile Management Tool może być zbyt mała do wyświetlenia wszystkich komunikatów i przycisków.
- Jeśli planowane jest użycie pliku projektu bazy danych na potrzeby informacji dotyczących bazy danych produktu Business Space, należy wykonać kroki znajdujące się w sekcji “Tworzenie pliku właściwości projektu bazy danych produktu Business Space” na stronie 204.

Tej procedury należy użyć, jeśli jest rozszerzany profil produktu Business Space dla konfiguracji autonomicznej. W poniższych krokach opisano zarówno opcję Zaawansowane tworzenie profilu, jak i Typowe tworzenie profilu.

Jeśli produkt Business Space został rozszerzony jako część profilu produktu, to zadanie jest opcjonalne.

1. Uruchom narzędzie Profile Management Tool.

Należy użyć jednej z następujących komend:

-   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
-  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`

Zostanie otwarta strona Powitanie.

2. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.

Zostanie otwarta karta Profile.

Karta Profile zawiera listę profili znajdujących się aktualnie na danym komputerze. W tej procedurze przyjęto założenie, że istniejący profil serwera aplikacji zostanie rozszerzony o produkt Business Space w konfiguracji autonomicznej.

3. Wybierz profil, który ma zostać rozszerzony, i kliknij opcję **Rozszerz**. Przycisku **Rozszerz** nie można wybrać, jeśli rozszerzenie profilu nie jest możliwe.

W oddzielnym oknie zostanie otwarta strona Wybór rozszerzenia.

4. Jeśli profil może zostać rozszerzony do produktu Business Space, na stronie Wybór rozszerzenia jest dostępna opcja **Profil autonomiczny**. Kliknij przycisk **Dalej**.

5. Na stronie Opcje rozszerzania profilu zdecyduj, czy rozszerzyć profil autonomiczny za pomocą opcji **Typowe rozszerzanie profilu**, czy opcji **Zaawansowane rozszerzanie profilu**.

Opcja Typowe rozszerzanie profilu umożliwia rozszerzenie profilu przy użyciu domyślnych ustawień konfiguracji. Opcja Zaawansowane rozszerzanie profilu umożliwia określenie własnych wartości konfiguracji dla rozszerzanego profilu.

6. Jeśli wybrano opcję **Typowe rozszerzanie profilu**, wykonaj następujące kroki:
 - a. Na stronie Zabezpieczenia administracyjne wprowadź ponownie ID i hasło administratora dla rozszerzanego profilu.
 - b. Na stronie Podsumowanie operacji rozszerzania profilu kliknij opcję **Rozszerz**, aby rozszerzyć profil, lub opcję **Wstecz** w celu zmiany parametrów profilu.

Postęp rozszerzania jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu rozszerzania profilu zostanie wyświetlona strona Zakończono rozszerzanie profilu z komunikatem **Narzędzie Profile Management Tool pomyślnie rozszerzyło profil**.

Ostrzeżenie: Jeśli podczas rozszerzania profilu zostaną wykryte błędy, zamiast komunikatu o pomyślnym zakończeniu operacji mogą zostać wyświetlone inne komunikaty. Na przykład:

- **Narzędzie Profile Management Tool rozszerzyło profil, ale wystąpiły błędy** - ten komunikat oznacza, że proces rozszerzania profilu zakończył się, ale w jego trakcie wygenerowano błędy.
- **Narzędzie Profile Management Tool nie może rozszerzyć profilu** - ten komunikat oznacza, że operacja rozszerzania profilu zakończyła się całkowitym niepowodzeniem.

Na stronie Zakończono rozszerzanie profilu jest umieszczone wskazanie dotyczące pliku dziennika, który można przejrzeć w celu rozwiązania problemów.

7. Jeśli wybrano opcję **Zaawansowane rozszerzanie profilu**, wykonaj następujące kroki:
 - a. Na stronie Zabezpieczenia administracyjne wprowadź ponownie ID i hasło administratora dla rozszerzanego profilu.
 - b. Jeśli ma zostać użyty plik projektu, który został wcześniej utworzony w celu skonfigurowania baz danych dla rozszerzonego profilu, należy wykonać poniższe kroki zamiast używać stron Konfiguracja bazy danych.
 - 1) Wybierz opcję **Użyj pliku projektu bazy danych** w celu skonfigurowania bazy danych.
 - 2) Kliknij przycisk **Przeglądaj**.
 - 3) Podaj pełną ścieżkę do pliku projektu.
 - 4) Kliknij przycisk **Dalej**.
 - c. Jeśli nie użyto pliku projektu bazy danych, na stronie Konfiguracja bazy danych wykonaj następujące czynności:
 - 1) Z listy Wybierz bazę danych wybierz bazę danych, która zostanie użyta przez profil.
 - 2) Zaznacz pole wyboru **Nadpisz domyślny katalog danych wyjściowych dla skryptów bazy danych**, jeśli ma zostać ustawiony katalog, do którego są zapisywane skrypty SQL używane do tworzenia tabel baz danych. Jeśli to pole wyboru nie zostanie zaznaczone, skrypty zostaną zapisane w katalogu domyślnym.
 - 3) Kliknij przycisk **Dalej**, aby wyświetlić stronę Konfiguracja bazy danych (część 2).

Informacje znajdujące się na stronie Konfiguracja bazy danych (część 2) różnią się w zależności od wartości wybranych z listy Wybór produktu bazy danych na stronie Konfiguracja bazy danych.

- d. Na stronie Konfiguracja bazy danych (część 2) dokończ konfigurację bazy danych. W zależności od bazy danych należy określić nazwę użytkownika i hasło na potrzeby uwierzytelniania w bazie danych, informacje dotyczące sterownika JDBC, a także host, port oraz schemat.
- e. Na stronie Podsumowanie operacji rozszerzania profilu kliknij opcję **Rozszerz**, aby rozszerzyć profil, lub opcję **Wstecz** w celu zmiany parametrów profilu.
Postęp rozszerzania jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu rozszerzania profilu zostanie wyświetlona strona Zakończono rozszerzanie profilu z komunikatem **Narzędzie Profile Management Tool pomyślnie rozszerzyło profil**.

Ostrzeżenie: Jeśli podczas rozszerzania profilu zostaną wykryte błędy, zamiast komunikatu o pomyślnym zakończeniu operacji mogą zostać wyświetlone inne komunikaty. Na przykład:

- **Narzędzie Profile Management Tool rozszerzyło profil, ale wystąpiły błędy** - ten komunikat oznacza, że proces rozszerzania profilu zakończył się, ale w jego trakcie wygenerowano błędy.
- **Narzędzie Profile Management Tool nie może rozszerzyć profilu** - ten komunikat oznacza, że operacja rozszerzania profilu zakończyła się całkowitym niepowodzeniem.

Na stronie Zakończono rozszerzanie profilu jest umieszczone wskazanie dotyczące pliku dziennika, który można przejrzeć w celu rozwiązania problemów.

Jeśli miało miejsce rozszerzanie do profilu ze skonfigurowanymi wcześniej zabezpieczeniami z repozytorium użytkowników, które nie jest domyślną opcją repozytoriów stowarzyszonych, należy sprawdzić plik `ConfigServices.properties` w celu dopasowania parametru `MashupAdminForOOBSpace`. Patrz temat "Wybieranie repozytorium użytkowników dla produktu Business Space" na stronie 228.

Rozszerzanie profili produktu Business Space dla konfiguracji autonomicznej za pomocą programu narzędziowego wiersza komend manageprofiles:

Istnieje możliwość rozszerzania profili autonomicznych produktu Business Space z poziomu wiersza komend przy użyciu programu narzędziowego wiersza komend manageprofiles.

Przed uruchomieniem programu narzędziowego wiersza komend manageprofiles w celu rozszerzenia profilu upewnij się, że wykonano następujące czynności:

- Przejrzano kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- Przejrzano przykładowe komendy służące do tworzenia profilu.
- Sprawdzone, czy program narzędziowy wiersza komend manageprofiles nie został już uruchomiony dla tego samego profilu. W przypadku wyświetlenia komunikatu o błędzie należy ustalić, czy trwa tworzenie lub rozszerzanie innego profilu. Jeśli tak, należy poczekać do chwili zakończenia tego działania.
- Wyłączono wszystkie serwery powiązane z profilem, który ma zostać rozszerzony.
- Określono, czy profil, który ma zostać rozszerzony, został już stowarzyszony z menedżerem wdrażania. Jeśli tak, profilu nie można rozszerzać przy użyciu programu narzędziowego wiersza komend manageprofiles.

- Określono szablon, za pomocą którego utworzono istniejący profil (menedżer wdrażania, profil autonomiczny albo zarządzany). Szablon użyty do utworzenia profilu można określić, wyświetlając rejestr profili znajdujący się w pliku *instalacyjny_katalog_główny/properties/profileRegistry.xml*. Tego pliku nie wolno modyfikować. Należy go użyć jedynie w celu wyświetlenia szablonów. Na potrzeby tej procedury przyjęto, że jest rozszerzany profil autonomiczny serwera Process Server.

Aby rozszerzyć profil produktu Business Space dla konfiguracji autonomicznej przy użyciu programu narzędziowego wiersza komend manageprofiles, wykonaj następujące kroki.

Jeśli produkt Business Space został rozszerzony jako część profilu produktu, to zadanie jest opcjonalne.

1. Znajdź szablon profilu default.bspace dla profili autonomicznych produktu Business Space, który definiuje serwery autonomiczne.

Szablony dla poszczególnych profili znajdują się w katalogu *instalacyjny_katalog_główny/profileTemplates/BusinessSpace*.

Parametr **augment** umożliwia dokonanie zmian w istniejącym profilu przy użyciu szablonu rozszerzania. Parametr **augment** powoduje, że program narzędziowy wiersza komend manageprofiles aktualizuje lub rozszerza profil zidentyfikowany w parametrze **-profileName** przy użyciu szablonu określonego w parametrze **-templatePath**. Szablony rozszerzania, które mogą być używane, są określane na podstawie zainstalowanych w danym środowisku produktów IBM i ich wersji. Należy upewnić się, że podano pełną ścieżkę do pliku dla parametru **-templatePath**, ponieważ podanie względnej ścieżki do pliku spowoduje, że wskazany profil nie zostanie w pełni rozszerzony.

2. Uruchom plik z poziomu wiersza komend. Nie podawaj parametru **-profilePath**. Poniżej przedstawiono prosty przykład:

```
manageProfiles -augment -profileName nazwa_profilu -templatePath
instalacyjny_katalog_główny/profileTemplates/BusinessSpace/default.bspace -cellName nazwa_komórki
-nodeName nazwa_węzła -enableAdminSecurity true -adminUserName admin
-adminPassword admin -dbType DB2_Universal -dbUserId ID_użytkownika_bazy_danych
-dbPassword hasło_bazy_danych -dbJDBCClasspath instalacyjny_katalog_główny/jdbcdrivers/DB2
-dbName nazwa_bazy_danych -bSpaceSchema schemat_bazy_danych -dbHostName
nazwa_hosta_bazy_danych -dbServerPort port_bazy_danych -dbDelayConfig false
```

Po zakończeniu działania komendy status jest zapisywany w oknie konsoli.

Jeśli miało miejsce rozszerzenie do profilu ze skonfigurowanymi wcześniej zabezpieczeniami z repozytorium użytkowników, które nie jest domyślną opcją repozytoriów stowarzyszonych, należy sprawdzić plik *ConfigServices.properties* w celu dopasowania parametru *MashupAdminForOOBSpace*. Patrz temat “Wybieranie repozytorium użytkowników dla produktu Business Space” na stronie 228.

Rozszerzanie profili produktu Business Space dla konfiguracji wdrożenia sieciowego:

Aby rozszerzyć profile produktu Business Space dla konfiguracji wdrożenia sieciowego, możliwe jest użycie narzędzia Profile Management Tool lub programu narzędziowego wiersza komend manageprofiles.

Jeśli produkt Business Space jest skonfigurowany jako część profilu produktu, te zadania są opcjonalne.

Rozszerzanie profili produktu Business Space dla konfiguracji wdrożenia sieciowego za pomocą narzędzia Profile Management Tool:

Za pomocą narzędzia Profile Management Tool można rozszerzać profile produktu Business Space dla środowiska wdrożenia sieciowego.

Należy zrozumieć pojęcia dotyczące profili, w tym różnice między profilami autonomicznymi, wdrożenia sieciowego i niestandardowymi. Należy także zrozumieć różnice między opcją Typowe rozszerzanie profilu i opcją Zaawansowane rozszerzanie profilu, w tym potrafić określić, w których scenariuszach należy użyć danej opcji. Opcja Typowe rozszerzanie profilu umożliwia rozszerzenie profilu przy użyciu domyślnych ustawień konfiguracji. Opcja Zaawansowane rozszerzanie profilu umożliwia określenie własnych wartości konfiguracji dla rozszerzanego profilu.


- Należy przejrzeć kompletną listą wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- W przypadku korzystania z narzędzia Profile Management Tool z graficznym interfejsem użytkownika Motif w systemie operacyjnym Solaris domyślna wielkość okna narzędzia Profile Management Tool może być zbyt mała do wyświetlenia wszystkich komunikatów i przycisków.

Tej procedury należy użyć, jeśli jest rozszerzany profil produktu Business Space dla konfiguracji wdrożenia sieciowego. W poniższych krokach opisano zarówno opcję Zaawansowane rozszerzanie profilu, jak i Typowe rozszerzanie profilu. Na potrzeby tej procedury przyjęto, że istnieje profil menedżera wdrażania i profile niestandardowe (węzły zarządzane), które mają zostać rozszerzone do produktu Business Space.

Jeśli produkt Business Space został rozszerzony jako część profilu produktu, to zadanie jest opcjonalne.

1. Rozszerz profil menedżera wdrażania.
 - a. Uruchom narzędzie Profile Management Tool.

Należy użyć jednej z następujących komend:

 -   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
 -  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`
 - b. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.

Zostanie otwarta karta Profile.

Karta Profile zawiera listę profili utworzonych na danym komputerze. Do tworzenia nowych profili lub rozszerzania profili już istniejących można użyć narzędzia Profile Management Tool.
 - c. Na karcie Profile kliknij opcję **Rozszerz**.

W oddzielnym oknie zostanie otwarta strona Wybór rozszerzenia.
 - d. Na stronie Wybór rozszerzenia rozwiń sekcję **Produkt Business Space oparty na technologii WebSphere**, wybierz opcję **Menedżer wdrażania produktu Business Space**, a następnie kliknij opcję **Dalej**.
 - e. Na stronie Opcje rozszerzania profilu zdecyduj, czy rozszerzyć profil autonomiczny za pomocą opcji **Typowe rozszerzanie profilu**, czy opcji **Zaawansowane rozszerzanie profilu**.
 - f. Na panelu Zabezpieczenia administracyjne wprowadź nazwę i hasło użytkownika, potwierdź hasło, a następnie kliknij przycisk **Dalej**. Cała konfiguracja profilu, w tym opcje profilu, są domyślnie konfigurowane i wyświetlane na stronie Podsumowanie operacji rozszerzania profilu.
 - g. Na stronie Podsumowanie operacji rozszerzania profilu kliknij opcję **Rozszerz**, aby rozszerzyć profil, lub opcję **Wstecz** w celu zmiany parametrów profilu.

Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono rozszerzanie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil.**

Ostrzeżenie: Jeśli podczas rozszerzania profilu zostaną wykryte błędy, zamiast komunikatu o pomyślnym zakończeniu operacji mogą zostać wyświetlone inne komunikaty. Na przykład:




- **Narzędzie Profile Management Tool rozszerzyło profil, ale wystąpiły błędy** - ten komunikat oznacza, że proces rozszerzania profilu zakończył się, ale w jego trakcie wygenerowano błędy.
- **Narzędzie Profile Management Tool nie może rozszerzyć profilu** - ten komunikat oznacza, że operacja rozszerzania profilu zakończyło się całkowitym niepowodzeniem.

Na stronie Zakończono rozszerzanie profilu jest umieszczone wskazanie dotyczące pliku dziennika, który można przejrzeć w celu rozwiązania problemów.

2. Uruchom profil.

Uruchom profil za pomocą komendy `startServer` uruchamianej z poziomu katalogu *katalog_główny_profilu/bin*.

Należy użyć następującej składni:




-   `startServer.sh nazwa_serwera`
-  `startServer.bat nazwa_serwera`

Więcej informacji dotyczących komendy `startServer` zawiera temat Komenda `startServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

3. Rozszerz profile niestandardowe (węzły zarządzane).

a. Uruchom narzędzie Profile Management Tool.

Należy użyć jednej z następujących komend:

-   `instalacyjny_katalog_główny/bin/ProfileManagement/pmt.sh`
-  `instalacyjny_katalog_główny\bin\ProfileManagement\pmt.bat`

b. Na stronie Powitanie kliknij opcję **Uruchom narzędzie Profile Management Tool** lub wybierz kartę Profile Management Tool.

Zostanie otwarta karta Profile.

Karta Profile zawiera listę profili utworzonych na danym komputerze. Do tworzenia nowych profili lub rozszerzania profili już istniejących można użyć narzędzia Profile Management Tool.

c. Na karcie Profile kliknij opcję **Rozszerz**.

W oddzielnym oknie zostanie otwarta strona Wybór rozszerzenia.

d. Na stronie Wybór rozszerzenia rozwiń sekcję **Produkt Business Space oparty na technologii WebSphere**, wybierz opcję **Profil niestandardowy produktu Business Space**, a następnie kliknij przycisk **Dalej**.

e. Na stronie Opcje rozszerzania profilu zdecyduj, czy utworzyć profil autonomiczny za pomocą opcji **Typowe tworzenie profilu**, czy opcji **Zaawansowane tworzenie profilu**.

f. Na stronie Stowarzyszenie wybierz opcję stowarzyszenia danego węzła z menedżerem wdrażania albo w ramach bieżącej procedury tworzenia danego profilu, albo w przyszłości za pomocą komendy `addNode` (niezależnie od procedury tworzenia profilu). Zaznacz lub usuń zaznaczenie pola wyboru **Stowarzysz ten węzeł później** i kliknij przycisk **Dalej**.

- g. Na stronie Podsumowanie operacji rozszerzania profilu kliknij przycisk **Utwórz**, aby utworzyć profil, albo przycisk **Wstecz**, aby zmienić parametry tego profilu. Postęp konfiguracji jest wyświetlany w oknie Postęp konfiguracji profilu. Po zakończeniu tworzenia profilu zostanie wyświetlona strona Zakończono rozszerzanie profilu zawierająca komunikat **Narzędzie Profile Management Tool pomyślnie utworzyło profil**.

Ostrzeżenie: Jeśli podczas tworzenia profilu wykryto błędy, zamiast komunikatu o powodzeniu mogą zostać wyświetlone inne komunikaty, na przykład:




- **Narzędzie Profile Management Tool rozszerzyło profil, ale wystąpiły błędy** - ten komunikat wskazuje, że zakończyło się tworzenie profilu, ale zostały wygenerowane błędy.
- **Narzędzie Profile Management Tool nie może rozszerzyć profilu** - ten komunikat wskazuje, że tworzenie profilu zakończyło się całkowitym niepowodzeniem.

Na stronie Zakończono rozszerzanie profilu jest umieszczone wskazanie dotyczące pliku dziennika, który można przejrzeć w celu rozwiązania problemów.

4. Zaloguj się w Konsoli administracyjnej menedżera wdrażania.
5. Opcjonalne: Jeśli nie istnieje jeszcze klastr lub serwery zarządzane, należy wykonać w środowisku jeden z poniższych kroków:
 - Dla klastra:
 - a. Utwórz klastr serwera aplikacji.
 - b. Dodaj co najmniej jeden element klastra do klastra (są to wcześniej utworzone profile niestandardowe produktu Business Space).
 - Dla każdego serwera zarządzanego:
 - a. Utwórz serwer aplikacji.
 - b. Wybierz węzeł serwera zarządzanego będący wcześniej utworzonym profilem produktu Business Space.
6. Zatrzymaj profil menedżera wdrażania.

Menedżer wdrażania można zatrzymać za pomocą komendy `stopServer` uruchamianej z poziomu katalogu `katalog_główny_profilu/bin`.

Należy użyć następującej składni:

-   `stopServer.sh nazwa_serwera -username nazwa_użytkownika -password hasło`
-  `stopServer.bat nazwa_serwera -username nazwa_użytkownika -password hasło`

Jeśli w profilu nie włączono zabezpieczeń, parametry `-username` i `-password` nie są konieczne.

Więcej informacji dotyczących komendy `stopServer` zawiera temat Komenda `stopServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

7. Przejdź do katalogu `instalacyjny_katalog_główny/BusinessSpace/config.bspace/MetadataFiles` i w zależności od typu bazy danych, która będzie używana dla produktu Business Space, skopiuj odpowiedni plik do katalogu roboczego. Nie zmieniaj rozszerzenia tego pliku - rozszerzeniem musi być `.properties`.
 - a. Zmodyfikuj kopię tego pliku i zmień wartości na odpowiadające używanej bazie danych. Należy zwrócić szczególną uwagę na właściwość `washome` i upewnić się, że jest ona poprawna.
 - b. Zapisz plik po zakończeniu edytowania informacji o bazie danych.

Po utworzeniu profili i skonfigurowaniu informacji dotyczących bazy danych dla profili można skonfigurować produkt Business Space w używanym środowisku, wykonując następujące kroki.

1. Dla każdego klastra lub serwera zarządzanego uruchom komendę `installBusinessSpace` w celu zainstalowania plików archiwum korporacyjnego (EAR) produktu Business Space w środowisku wykonawczym. Należy podać parametr **clusterName** lub parametry **nodeName** i **serverName** w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
2. Dla każdego klastra lub serwera zarządzanego uruchom komendę `configureBusinessSpace`, podając parametr **clusterName** lub parametry **nodeName** i **serverName** w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Określ także parametr **bspacedbDesign**. Wartością tego parametru powinna być ścieżka do pliku właściwości bazy danych, który był wcześniej edytowany. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
3. Zapisz konfigurację narzędzia `wsadmin`.
4. Utwórz i skonfiguruj bazę danych produktu Business Space. Patrz temat “Konfigurowanie bazy danych produktu Business Space” na stronie 205.
5. Uruchom menedżer wdrażania.
6. Uruchom klastry lub serwery zarządzane.

Jeśli miało miejsce rozszerzenie do profilu ze skonfigurowanymi wcześniej zabezpieczeniami z repozytorium użytkowników, które nie jest domyślną opcją repozytoriów stowarzyszonych, należy sprawdzić plik `ConfigServices.properties` w celu dopasowania parametru `MashupAdminForOOBSpace`. Patrz temat “Wybieranie repozytorium użytkowników dla produktu Business Space” na stronie 228.

Rozszerzanie profili produktu Business Space dla konfiguracji wdrożenia sieciowego za pomocą programu narzędziowego wiersza komend `manageprofiles`:

Istnieje możliwość rozszerzania profili produktu Business Space dla konfiguracji wdrożenia sieciowego z poziomu wiersza komend przy użyciu programu narzędziowego wiersza komend `manageprofiles`.

Przed uruchomieniem programu narzędziowego wiersza komend `manageprofiles` w celu rozszerzenia profilu upewnij się, że wykonano następujące czynności:

- Przejrzano kompletną listę wymagań wstępnych dotyczących tworzenia lub rozszerzania profilu znajdującą się w temacie Pojęcia związane z profilami w Centrum informacyjnym serwera WebSphere Application Server.
- Przejrzano przykładowe komendy służące do tworzenia profilu.
- Sprawdzone, czy program narzędziowy wiersza komend `manageprofiles` nie został już uruchomiony dla tego samego profilu. W przypadku wyświetlenia komunikatu o błędzie należy ustalić, czy trwa tworzenie lub rozszerzanie innego profilu. Jeśli tak, należy poczekać do chwili zakończenia tego działania.
- Wyłączono wszystkie serwery powiązane z profilem, który ma zostać rozszerzony.
- Określono, czy profil, który ma zostać rozszerzony, został już stowarzyszony z menedżerem wdrażania. Jeśli tak, profilu nie można rozszerzać przy użyciu programu narzędziowego wiersza komend `manageprofiles`.
- Określono szablon, za pomocą którego utworzono istniejący profil (menedżer wdrażania, profil autonomiczny albo zarządzany). Szablon użyty do utworzenia profilu można określić, wyświetlając rejestr profili znajdujący się w pliku `instalacyjny_katalog_główny/properties/profileRegistry.xml`. Tego pliku nie wolno

modyfikować. Należy go użyć jedynie w celu wyświetlenia szablonów. Na potrzeby tej procedury przyjęto, że jest rozszerzany produkt Business Space oparty na profilu menedżera wdrażania produktu WebSphere.

Aby rozszerzyć profil produktu Business Space dla konfiguracji wdrożenia sieciowego przy użyciu programu narzędziowego wiersza komend `manageprofiles`, należy wykonać poniższe kroki. Na potrzeby tej procedury przyjęto, że istnieje profil menedżera wdrażania i profile niestandardowe (węzły zarządzane), które mają zostać rozszerzone do produktu Business Space.

Jeśli produkt Business Space został rozszerzony jako część profilu produktu, to zadanie jest opcjonalne.

1. Rozszerz profil menedżera wdrażania.

- a. Znajdź szablon `dmgr.bspace` dla profili menedżera wdrażania produktu Business Space, który definiuje menedżery wdrażania. Menedżer wdrażania udostępnia pojedynczy interfejs administracyjny dla logicznej grupy serwerów na jednej lub większej liczbie stacji roboczych.

Szablony dla poszczególnych profili znajdują się w katalogu *instalacyjny_katalog_główny/profileTemplates/BusinessSpace*.

- b. Określ, jakie parametry są wymagane do rozszerzenia profilu, przeglądając informacje znajdujące się w temacie “Program narzędziowy wiersza komend `manageprofiles` (w przypadku profili produktu Business Space)” na stronie 177. Określ wartości, które mają zostać podane dla profilu. Przejrzyj wartości domyślne, aby sprawdzić, czy są one odpowiednie dla profilu.

Parametr **augment** umożliwia dokonanie zmian w istniejącym profilu przy użyciu szablonu rozszerzania. Parametr **augment** powoduje, że program narzędziowy wiersza komend `manageprofiles` aktualizuje lub rozszerza profil zidentyfikowany w parametrze **-profileName** przy użyciu szablonu określonego w parametrze **-templatePath**. Szablony rozszerzania, które mogą być używane, są określane na podstawie zainstalowanych w danym środowisku produktów IBM i ich wersji. Należy upewnić się, że podano pełną ścieżkę do pliku dla parametru **-templatePath**, ponieważ podanie względnej ścieżki do pliku spowoduje, że wskazany profil nie zostanie w pełni rozszerzony.

- c. Uruchom plik z poziomym wierszem komend. Poniżej przedstawiono prosty przykład:




```
manageProfiles -augment -profileName nazwa_profilu
               -templatePath instalacyjny_katalog_główny/profileTemplates/BusinessSpace/dmgr.bspace
               -serverType DEPLOYMENT_MANAGER -cellName nazwa_komórki_zarządzania
               -nodeName nazwa_węzła_zarządzania -enableAdminSecurity true
               -adminUserName nazwa_administratora -adminPassword hasło_administratora
```

Komenda wyświetla status w trakcie działania. Należy poczekać na zakończenie operacji.

2. Uruchom profil menedżera wdrażania.

Uruchom profil za pomocą komendy `startServer` uruchamianej z poziomu katalogu *katalog_główny_profilu/bin*.

Należy użyć następującej składni:

-   `startServer.sh nazwa_serwera`
-  `startServer.bat nazwa_serwera`

Więcej informacji dotyczących komendy `startServer` zawiera temat Komenda `startServer` w Centrum informacyjnym produktu WebSphere Application Server 7.0.

3. Rozszerz profile niestandardowe (węzły zarządzane).

- a. Znajdź szablon managed.bspace dla profili niestandardowych produktu Business Space, które (jeśli są stowarzyszone z menedżerem wdrażania) definiują węzły zarządzane. Jeśli zdecydowano, że rozwiązanie wymaga środowiska wdrażania, środowisko wykonawcze musi mieć co najmniej jeden węzeł zarządzany. Profil niestandardowy zawiera pusty węzeł, którego działanie jest możliwe po stowarzyszeniu z komórką menedżera wdrażania. Po stowarzyszeniu profil niestandardowy zmienia się w węzeł zarządzany. Nie należy stowarzyszać węzła, chyba że ma on zostać stowarzyszony z menedżerem wdrażania, którego wersja jest taka sama (lub nowsza) jak wersja tworzonego profilu niestandardowego.

Szablony dla poszczególnych profili znajdują się w katalogu *instalacyjny_katalog_główny/profileTemplates/BusinessSpace*.

- b. Określ, jakie parametry są wymagane do rozszerzenia profilu, przeglądając informacje znajdujące się w temacie “Program narzędziowy wiersza komend manageprofiles (w przypadku profilu produktu Business Space)” na stronie 177. Określ wartości, które mają zostać podane dla profilu. Przejrzyj wartości domyślne, aby sprawdzić, czy są one odpowiednie dla profilu.

Parametr **augment** umożliwia dokonanie zmian w istniejącym profilu przy użyciu szablonu rozszerzania. Parametr **augment** powoduje, że program narzędziowy wiersza komend manageprofiles aktualizuje lub rozszerza profil zidentyfikowany w parametrze **-profileName** przy użyciu szablonu określonego w parametrze **-templatePath**. Szablony rozszerzania, które mogą być używane, są określane na podstawie zainstalowanych w danym środowisku produktów IBM i ich wersji. Należy upewnić się, że podano pełną ścieżkę do pliku dla parametru **-templatePath**, ponieważ podanie względnej ścieżki do pliku spowoduje, że wskazany profil nie zostanie w pełni rozszerzony.

- c. Uruchom plik z poziomu wiersza komend. Poniżej przedstawiono prosty przykład:



```
manageProfiles -augment -profileName nazwa_profilu
               -templatePath instalacyjny_katalog_główny/profileTemplates/BusinessSpace/managed.bspace
               -dmgrAdminUserName nazwa_administratora -dmgrAdminPassword hasło_administratora
               -dmgrPort port_menedżera_wdrażania -dmgrHost nazwa_hosta_menedżera_wdrażania -cellName
               nazwa_komórki_zarządzania -nodeName nazwa_węzła
```


Komenda wyświetla status w trakcie działania. Należy poczekać na zakończenie operacji.

4. Zaloguj się w Konsoli administracyjnej menedżera wdrażania.
5. Opcjonalne: Jeśli nie istnieje jeszcze klastr lub serwery zarządzane, należy wykonać w środowisku jeden z poniższych kroków:
 - Dla klastra:
 - a. Utwórz klastr serwera aplikacji.
 - b. Dodaj co najmniej jeden element klastra do klastra (są to wcześniej utworzone profile niestandardowe produktu Business Space).
 - Dla każdego serwera zarządzanego:
 - a. Utwórz serwer aplikacji.
 - b. Wybierz węzeł serwera zarządzanego będący wcześniej utworzonym profilem produktu Business Space.
6. Zatrzymaj profil menedżera wdrażania.

Menedżer wdrażania można zatrzymać za pomocą komendy stopServer uruchamianej z poziomu katalogu *katalog_główny_profilu/bin*.

Należy użyć następującej składni:

-   stopServer.sh nazwa_serwera -username nazwa_użytkownika -password hasło

-  stopServer.bat nazwa_serwera -username nazwa_uzytkownika -password haslo

Jeśli w profilu nie włączono zabezpieczeń, parametry -username i -password nie są konieczne.

Więcej informacji dotyczących komendy stopServer zawiera temat Komenda stopServer w Centrum informacyjnym produktu WebSphere Application Server 7.0.

- Przejdź do katalogu *instalacyjny_katalog_glowny/BusinessSpace/config.bspace/MetadataFiles* i w zależności od typu bazy danych, która będzie używana dla produktu Business Space, skopiuj odpowiedni plik do katalogu roboczego. Nie zmieniaj rozszerzenia tego pliku - rozszerzeniem musi być `.properties`.
 - Zmodyfikuj kopię tego pliku i zmień wartości na odpowiadające używanej bazie danych. Należy zwrócić szczególną uwagę na właściwość `wasHome` i upewnić się, że jest ona poprawna.
 - Zapisz plik po zakończeniu edytowania informacji o bazie danych.

Po utworzeniu profili i skonfigurowaniu informacji dotyczących bazy danych dla profili można skonfigurować produkt Business Space w używanym środowisku, wykonując następujące kroki.

- Dla każdego klastra lub serwera zarządzanego uruchom komendę `installBusinessSpace` w celu zainstalowania plików archiwum korporacyjnego (EAR) produktu Business Space w środowisku wykonawczym. Należy podać parametr `clusterName` lub parametry `nodeName` i `serverName` w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
- Dla każdego klastra lub serwera zarządzanego uruchom komendę `configureBusinessSpace`, podając parametr `clusterName` lub parametry `nodeName` i `serverName` w zależności od sposobu skonfigurowania topologii wdrożenia sieciowego. Określ także parametr `bspacedbDesign`. Wartością tego parametru powinna być ścieżka do pliku właściwości bazy danych, który był wcześniej edytowany. Patrz temat “Konfigurowanie produktu Business Space przy użyciu wiersza komend” na stronie 202.
- Zapisz konfigurację narzędzia `wsadmin`.
- Utwórz i skonfiguruj bazę danych produktu Business Space. Patrz temat “Konfigurowanie bazy danych produktu Business Space” na stronie 205.
- Uruchom menedżer wdrażania.
- Uruchom klastry lub serwery zarządzane.

Jeśli miało miejsce rozszerzenie do profilu ze skonfigurowanymi wcześniej zabezpieczeniami z repozytorium użytkowników, które nie jest domyślną opcją repozytoriów stowarzyszonych, należy sprawdzić plik `ConfigServices.properties` w celu dopasowania parametru `MashupAdminForOOBSpace`. Patrz temat “Wybieranie repozytorium użytkowników dla produktu Business Space” na stronie 228.

Program narzędziowy wiersza komend `manageprofiles` (w przypadku profili produktu Business Space):




Program narzędziowy wiersza komend `manageprofiles` służy do tworzenia profilu, który jest zestawem plików definiujących środowisko wykonawcze dla menedżera wdrażania, węzła zarządzanego lub serwera autonomicznego. Programu można użyć do utworzenia obszaru biznesowego opartego na profilu produktu WebSphere. Jeśli obszar biznesowy skonfigurowano jako część profilu produktu, ta informacja jest opcjonalna.

Profil definiuje środowisko wykonawcze i obejmuje wszystkie pliki, które w czasie wykonywania mogą być zmieniane przez procesy serwera.

Program narzędziowy wiersza komend `manageprofiles` i jego graficzny interfejs użytkownika, czyli narzędzie Profile Management Tool, to jedyne narzędzia umożliwiające tworzenie profili lub środowisk wykonawczych. Za pomocą programu narzędziowego wiersza komend `manageprofiles` można też rozszerzać i usuwać profile.

Plik komendy znajduje się w katalogu *instalacyjny_katalog_główny/bin*. Plik komendy to skrypt o nazwie `manageprofiles.sh` dla platform Linux i UNIX lub `manageprofiles.bat` dla platform Windows.

Program narzędziowy wiersza komend `manageprofiles` tworzy dziennik dla każdego utworzonego, usuwanego lub rozszerzanego profilu. Dzienniki znajdują się w następujących katalogach (w zależności od platformy):

-   *instalacyjny_katalog_główny/logs/manageprofiles*
-  *instalacyjny_katalog_główny\logs\manageprofiles*

Pliki mają następujące nazwy:

- *nazwa_profilu_create.log*
- *nazwa_profilu_augment.log*
- *nazwa_profilu_delete.log*

Szablony dla poszczególnych profili znajdują się w katalogu *instalacyjny_katalog_główny/profileTemplates/BusinessSpace*. W tym katalogu znajdują się różne katalogi odpowiadające poszczególnym typom profili. Te katalogi to ścieżki wskazywane podczas używania programu narzędziowego wiersza komend `manageprofiles` z opcją `-templatePath`. Jeśli istnieją szablony profili znajdujące się poza instalacyjnym katalogiem głównym, również można je określić. W przypadku produktu Business Space należy użyć następujących szablonów:

- `default.bspace`: przeznaczony dla profilu serwera autonomicznego produktu Business Space, który definiuje serwer autonomiczny.
- `dmgr.bspace`: przeznaczony dla profilu menedżera wdrażania produktu Business Space, który definiuje menedżer wdrażania.
- `managed.bspace`: przeznaczony dla niestandardowego profilu produktu Business Space, który po stowarzyszeniu z menedżerem wdrażania definiuje węzeł zarządzany.

Składnia

Program narzędziowy wiersza komend `manageprofiles` umożliwia wykonywanie następujących czynności:

- Tworzenie profilu (parametr `-create`)
- Rozszerzanie profilu (parametr `-augment`)

Ograniczenie: Użycie profili, w przypadku których cofnięto rozszerzenie (parametr `-unaugment`), nie jest obsługiwane.

- Usuwanie profilu (parametr `-delete`)
- Usuwanie wszystkich profili (parametr `-deleteAll`)
- Wyświetlanie listy wszystkich profili (parametr `-listProfiles`)
- Uzyskiwanie nazwy istniejącego profilu na podstawie jego nazwy (parametr `-getName`)
- Uzyskiwanie nazwy istniejącego profilu na podstawie jego ścieżki (parametr `-getPath`)
- Sprawdzanie poprawności rejestru profili (parametr `-validateRegistry`)
- Sprawdzanie poprawności i aktualizowanie rejestru profili (parametr `-validateAndUpdateRegistry`)
- Uzyskiwanie domyślnej nazwy profilu (parametr `-getDefaultName`)

- Ustawianie domyślnej nazwy profilu (parametr `-setDefaultName`)
- Tworzenie kopii zapasowej profilu (parametr `-backupProfile`)
- Odtwarzanie profilu (parametr `-restoreProfile`)
- Używanie pliku odpowiedzi zawierającego informacje wymagane do uruchomienia programu narzędziowego wiersza komend `manageprofiles` (parametr `-response`)

Szczegółową pomoc obejmującą wykaz wymaganych parametrów dla poszczególnych czynności realizowanych przy użyciu programu narzędziowego wiersza komend `manageprofiles` można uzyskać, stosując parametr **-help**. Oto przykład użycia parametru `-help` dla programu narzędziowego wiersza komend `manageprofiles` z parametrem **-augment** w systemach operacyjnych Windows: `manageprofiles.bat -augment -help`. Dane wyjściowe tej komendy określają, które parametry są wymagane, a które są opcjonalne.

Wyniki komendy

Po zakończeniu działania komendy wyświetlany jest komunikat podobny do jednego z poniższych. Treść komunikatu zależy od tego, czy utworzono, usunięto, czy rozszerzono profil.

- **INSTCONFSUCCESS**: Operacja tworzenia profilu powiodła się.
- **INSTCONFFAILED**: Operacja tworzenia profilu nie powiodła się.
- **INSTCONFPARTIALSUCCESS**: Niektóre niekrytyczne działania konfiguracyjne wykonywane po instalacji nie powiodły się.

W niektórych przypadkach ten sam komunikat jest wyświetlany więcej niż raz. Na przykład wiersz z komunikatem **INSTCONFSUCCESS** jest wyświetlany w wierszu komend trzy razy. Więcej informacji na ten temat można znaleźć w sekcji Pliki dzienników instalacji i tworzenia profili.

Parametry

Podczas tworzenia profilu produktu Business Space należy używać tylko parametrów udokumentowanych w Centrum informacyjnym produktu Business Space. W przypadku wszystkich parametrów jest rozróżniana wielkość liter.

-adminUserName *identyfikator_administratora*

Określa identyfikator użytkownika na potrzeby zabezpieczeń administracyjnych. Ten parametr jest wymagany w przypadku rozszerzania istniejącego profilu z włączonymi zabezpieczeniami administracyjnymi.

-adminPassword *hasło_administratora*

Określa hasło dla identyfikatora użytkownika zabezpieczeń administracyjnych określonego za pomocą parametru `-adminUserName`. Ten parametr jest wymagany w przypadku rozszerzania istniejącego profilu z włączonymi zabezpieczeniami administracyjnymi.

-augment

Parametr `augment` umożliwia dokonanie zmian w istniejącym profilu przy użyciu szablonu rozszerzania. Parametr `augment` powoduje, że program narzędziowy wiersza komend `manageprofiles` aktualizuje lub rozszerza profil zidentyfikowany w parametrze `-profileName` przy użyciu szablonu określonego w parametrze `-templatePath`. Szablony rozszerzania, które mogą być używane, są określane na podstawie zainstalowanych w danym środowisku produktów IBM i ich wersji.

Ważne: Nie należy ręcznie modyfikować plików znajdujących się w katalogu `katalog_instalacyjny/profileTemplates`. Na przykład w przypadku zmiany portów podczas tworzenia profilu należy użyć narzędzia Profile Management Tool albo

argumentów `-startingPort` lub `-portsFile` programu narzędziowego wiersza komend `manageprofiles`, a nie modyfikować plik w katalogu szablonu profilu. Dla parametru `-templatePath` należy określić pełną ścieżkę do pliku. Przykład: `manageprofiles(.bat)(.sh) -augment -profileName nazwa_profilu -templatePath pełna_ścieżka_do_szablonu`

-backupProfile

Tworzy kopię zapasową systemu plików dla folderu profilu i metadanych profilu w pliku rejestru profili.

-backupFile *nazwa_pliku_kopii_zapasowej*

Tworzy kopię zapasową pliku rejestru profili w określonym pliku. Jako wartość *nazwa_pliku_kopii_zapasowej* należy podać pełną ścieżkę do pliku.

-bspacedbDesign *plik_projektu_bazy_danych*

Określa ścieżkę do pliku projektu bazy danych produktu Business Space. Przykładowe pliki projektów znajdują się w katalogu *instalacyjny_katalog_główny/BusinessSpace/config.bspace/MetadataFiles*.

-bspaceSchemaName *nazwa_schematu_bazy_danych*

Nazwa schematu bazy danych. Jeśli nie zostanie podana żadna wartość, w przypadku większości typów baz danych będzie używana wartość `IBMBUSSP`.

-cellName *nazwa_komórki*

Określa nazwę komórki profilu. Dla każdego profilu należy użyć unikalnej nazwy komórki. Rozszerzając profil, należy określić komórkę oryginalnego profilu. Wartość domyślna tego parametru jest oparta na kombinacji krótkiej nazwy hosta, stałej `Cell` i liczby końcowej, na przykład:

```
if (DMgr)
    shortHostNameCellnumer_komórki
else
    shortHostNameNodenumer_węzłaCell
```

, gdzie *numer_komórki* to kolejna liczba, począwszy od 01, a *numer_węzła* to numer węzła użyty do zdefiniowania nazwy węzła. Wartość tego parametru nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: `*`, `?`, `"`, `<`, `>`, `..`, `/`, `\` i `|`.

-create

Tworzy profil. Aby uzyskać konkretne informacje na temat tworzenia profilu, należy określić komendę `manageprofiles -create -templatePath pełna_ścieżka_do_pliku_szablonu -help`. Dostępne są następujące szablony:

- `default.bspace`: przeznaczony dla profilu serwera autonomicznego produktu Business Space, który definiuje serwer autonomiczny.
- `dmgr.bspace`: przeznaczony dla profilu menedżera wdrażania produktu Business Space, który definiuje menedżer wdrażania.
- `managed.bspace`: przeznaczony dla niestandardowego profilu produktu Business Space, który po stowarzyszeniu z menedżerem wdrażania definiuje węzeł zarządzany.
-

-dbBSPassword *hasło_bazy_danych_produkту_Business_Space*

Ten parametr jest potrzebny, jeśli podczas tworzenia profilu wprowadzone zostały określone przez użytkownika nazwa i hasło użytkownika, a wartością parametru `dbType` jest `ORACLE`. Wartość domyślna to `dbPassword`.

-dbBSPassword

-dbBSPassword *identyfikator_użytkownika_bazy_danych_produkту_Business_Space*

Ten parametr jest potrzebny, jeśli podczas tworzenia profilu wprowadzone zostały określone przez użytkownika nazwa i hasło użytkownika. Wartość domyślna to `IBMBUSSP`.

-dbConnectionLocation *położenie_db2*

Położenie bazy danych DB2 for z/OS.

-dbCreateNew

Wskazuje, czy zostanie utworzona nowa baza danych, czy też zostanie ponownie wykorzystana istniejąca baza danych. Poprawne wartości to **true** (prawda) lub **false** (fałsz). Wartością domyślną jest **true**.

-dbDelayConfig

Wskazuje, czy tworzenie tabel ma zostać przeprowadzone dopiero po utworzeniu profilu. Poprawne wartości to **true** (prawda) lub **false** (fałsz). Wartość domyślna to **false**. Jeśli jest używana zdalna baza danych, ustawienie tego parametru na wartość **true** umożliwia opóźnienie wykonywania skryptów bazy danych.

-dbDriverType *typ_sterownika_bazy_danych*

Typ sterownika bazy danych. Poprawny tylko dla baz danych Oracle. W przypadku bazy danych Oracle należy określić wartość **ORACLE**. W przypadku baz danych innych niż Oracle wartość zostaje ustawiona automatycznie na podstawie systemu operacyjnego serwera. Serwery zainstalowane w systemie operacyjnym z/OS używają typu 2. Serwery zainstalowane w pozostałych systemach operacyjnych używają typu 4.

-dbDriverVersion *wersja_sterownika_bazy_danych*

Wersja sterownika bazy danych. Poprawny tylko w przypadku produktu Microsoft SQL Server. W przypadku bazy danych SQL Server należy określić wartość 1.2 dla sterownika Microsoft SQL JDBC w wersji 1.2 lub wartość 2.0 dla sterownika Microsoft SQL JDBC w wersji 2.0. Jeśli wartość nie zostanie określona, automatycznie przyjmowana jest wartość domyślna 2.0.

-dbHostName *nazwa_hosta_bazy_danych*

Nazwa hosta lub adres IP serwera bazy danych. Wartość domyślna to **localhost**.

-dbJDBCClasspath *położenie_sterownika_jdbc*

Położenie plików sterownika JDBC. Aby uzyskać dostęp do bazy danych Oracle, należy zainstalować sterownik ojdbc6.jar. Baza danych Oracle 10g nie zawiera sterownika ojdbc6.jar. Można go pobrać z serwisu WWW Oracle.

-dbName *nazwa_bazy_danych*

Nazwa bazy danych produktu. Domyślnie wartość ta jest ustawiana na **orcl** dla baz danych Oracle, a dla wszystkich innych obsługiwanych baz danych na **BSPACE**.

-dbOutputScriptDir *katalog_wyjściowy_bazy_danych*

Położenie wyeksportowanych skryptów bazy danych. Dostępny tylko po wybraniu opcji Zastąp katalog docelowy dla wygenerowanych skryptów. Wartość musi być ścieżką bezwzględną. Jeśli zostanie ustawiona ścieżka względna, skrypty SQL nie zostaną wyeksportowane ani wykonane, co może spowodować wystąpienie wielu wyjątków podczas uruchamiania serwera.

-dbPassword *hasło_bazy_danych*

Hasło wymagane na potrzeby uwierzytelniania w bazach danych.

-dbServerPort *numer_portu_bazy_danych*

Numer portu serwera bazy danych. W zależności od używanej bazy danych można określić inny numer portu zamiast domyślnego numeru portu.

-dbStorageGroup *grupa_pamięci_masowych_bazy_danych*

Nazwa grupy pamięci masowych dla baz danych DB2 for z/OS.

-dbSysPassword *hasło_sys*

Ten parametr jest wymagany, jeśli parametr **dbDelayConfig** ustawiono na wartość **false**, a wartością parametru **dbType** jest **ORACLE**.

-dbSysUserId *identyfikator_użytkownika_sys*

Ten identyfikator musi mieć uprawnienia SYSDBA. Nie należy używać użytkownika wewnętrznego sys bazy danych Oracle. Ten parametr jest wymagany, jeśli parametr dbDelayConfig ustawiono na wartość false, a wartością parametru dbType jest ORACLE.

-dbType *typ_bazy_danych*

Typ bazy danych. Należy ustawić jedną z poniższych wartości jako typ produktu bazodanowego używanego z produktem Business Space.

- DB2 Universal = DB2_Universal
- DB2 DataServer = DB2_DataServer
- DB2 Universal for z/OS = DB2UDBOS390
- Oracle = Oracle
- Microsoft SQL Server = MSSQLSERVER_MICROSOFT lub MSSQLSERVER_DATADIRECT

-dbUserId *identyfikator_użytkownika_bazy_danych*

Identyfikator użytkownika dla wszystkich typów bazy danych. Określa identyfikator użytkownika, który ma uprawnienia do tworzenia i usuwania baz danych. Źródło danych produktu WebSphere używa tego identyfikatora do uwierzytelniania połączenia z bazą danych. W przypadku baz danych DB2 określa on identyfikator użytkownika bazy danych, do którego będą należeć tabele bazy danych. W przypadku baz danych DB2 for z/OS ten parametr określa identyfikator użytkownika, który ma uprawnienia do tworzenia i usuwania baz danych. Ten parametr jest wymagany. Ważne: wartość parametru -dbUserId musi być poprawnym identyfikatorem autoryzowanego użytkownika bazy danych. Więcej informacji na temat identyfikatorów autoryzowanych użytkowników zawiera sekcja Authorization IDs and authorization names (Identyfikatory autoryzowanych użytkowników i nazwy autoryzacji) na stronie ograniczeń dotyczących właściwości bazy danych DB2.

-debug

Włącza funkcję debugowania narzędzia Apache Ant, które jest używane przez program narzędziowy wiersza komend manageprofiles.

-defaultPorts

Przypisuje do profilu domyślne lub podstawowe wartości portów.

Tego parametru nie należy używać w przypadku korzystania z parametrów -startingPort lub -portsFile.

Jeśli nie zostanie określony parametr -startingPort, parametr -defaultPorts lub parametr -portsFile, podczas tworzenia profilu program narzędziowy wiersza komend manageprofiles będzie używać automatycznie wygenerowanego zestawu zalecanych portów. Zalecane wartości portów mogą się różnić od domyślnych wartości portów w zależności od dostępności portów domyślnych.

Uwaga: Tego parametru nie należy używać w przypadku korzystania z szablonu profilu zarządzanego.

-delete

Usuwa profil.

Usunięcie profilu nie powoduje usunięcia katalogu profilu. Jeśli na przykład utworzono profil w katalogu /usr/WebSphere/AppServer/profiles/AppSrvr01, katalog nie zostanie usunięty po usunięciu profilu.

Ten katalog można usunąć lub pozostawić. Katalog *katalog_główny_profilu/logs* zawiera jednak informacje o deinstalowaniu profilu. Można na przykład zachować plik *_nodeuninst.log*, aby określić przyczynę problemów podczas procedury deinstalacji.

Jeśli usuwany jest profil, który ma zarejestrowane szablony rozszerzania w rejestrze profili, działania cofania rozszerzania są wykonywane automatycznie.

-deleteAll

Usuwa wszystkie zarejestrowane profile.

Usunięcie profilu nie powoduje usunięcia katalogu profilu. Jeśli na przykład utworzono profil w katalogu `/usr/WebSphere/AppServer/profiles/AppSrvr01`, katalog pozostanie po usunięciu profilu.

Ten katalog można usunąć lub pozostawić. Katalog `katalog_główny_profilu/logs` zawiera jednak informacje o deinstalowaniu profilu. Można na przykład zachować plik `_nodeuninst.log`, aby określić przyczynę problemów podczas procedury deinstalacji.

Jeśli usuwany jest profil, który ma zarejestrowane szablony rozszerzania w rejestrze profili, działania cofania rozszerzania są wykonywane automatycznie.

-dmgrAdminUserName nazwa_użytkownika

Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, należy podać poprawną nazwę użytkownika.

-dmgrAdminPassword hasło

Jeśli w menedżerze wdrażania włączono zabezpieczenia administracyjne, dla nazwy użytkownika należy określić hasło.

-dmgrHost nazwa_hosta_menedżera_wdrażania

Identyfikuje stację roboczą, na której działa menedżer wdrażania. W celu stowarzyszenia profilu niestandardowego podczas jego tworzenia lub rozszerzania należy określić ten parametr wraz z parametrem **dmgrPort**. Ten parametr jest dostępny w przypadku szablonu profili `managed.bspace`.

Nazwą hosta może być długa lub krótka nazwa DNS albo adres IP stacji roboczej menedżera wdrażania.

Gdy ten opcjonalny parametr zostanie określony, program narzędziowy wiersza komend `manageprofiles` podejmuje próbę stowarzyszenia węzła niestandardowego z komórką menedżera wdrażania podczas tworzenia profilu niestandardowego. Ten parametr jest ignorowany podczas tworzenia profilu menedżera wdrażania lub profilu serwera autonomicznego.

Jeśli węzeł niestandardowy zostanie stowarzyszony w momencie, gdy menedżer wdrażania nie działa, w dziennikach zostanie umieszczony indyktor instalacji o wartości `INSTCONFFAILED` informujący o niepowodzeniu wykonywania operacji. Użycie wynikowego profilu niestandardowego nie będzie możliwe. Konieczne jest przeniesienie katalogu profilu niestandardowego poza repozytorium profilu (główny katalog instalacji profilu) przed utworzeniem następnego profilu niestandardowego o takiej samej nazwie.

Jeśli zmieniono domyślny typ konektora JMX, nie można wykonać stowarzyszenia za pomocą programu narzędziowego wiersza komend `manageprofiles`. Zamiast niej należy użyć komendy `addNode`.

Wartością domyślną tego parametru jest `localhost`. Wartość tego parametru musi mieć postać poprawnej nazwy hosta, a ponadto nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\` i `|`. Połączenie z menedżerem wdrażania musi być także dostępne w przypadku parametru `dmgrPort`.

-dmgrPort numer_portu_menedżera_wdrażania

Identyfikuje port SOAP menedżera wdrażania. W celu stowarzyszenia profilu niestandardowego podczas jego tworzenia lub rozszerzania należy określić ten parametr wraz z parametrem **dmgrHost**. Menedżer wdrażania musi działać i być dostępny.

Jeśli zmieniono domyślny typ konektora JMX, nie można wykonać stowarzyszenia za pomocą programu narzędziowego wiersza komend `manageprofiles`. Zamiast niej należy użyć komendy `addNode`.

Wartością domyślną tego parametru jest `8879`. Wskazany numer portu musi być dodatnią liczbą całkowitą, a połączenie z menedżerem wdrażania musi być dostępne w przypadku parametru `-dmgrHost`.

-enableAdminSecurity true | false

Włącza zabezpieczenia administracyjne. Poprawne wartości to `true` lub `false`. Wartość domyślna to `false`. Jeśli tworzone są profile dla środowiska wdrażania, konieczne jest ustawienie tego parametru na wartość `true`. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Jeśli parametr `enableAdminSecurity` ustawiono na wartość `true`, konieczne jest także określenie parametrów `-adminUserName` i `-adminPassword` wraz z ich wartościami. Jeśli podczas instalacji serwera aplikacji zainstalowano przykłady, niezbędne jest również określenie parametru `-samplesPassword` podczas tworzenia profilu, dla którego włączono zabezpieczenia administracyjne. Jeśli parametr `-samplesPassword` nie zostanie określony po włączeniu zabezpieczeń administracyjnych, profil zostanie utworzony pomyślnie, ale próba uruchomienia przykładów spowoduje umieszczenie informacji o wyjątkach i niepowodzeniach w dzienniku wyjścia systemowego serwera.

> Linux

-enableService true | false

Włącza tworzenie usługi systemu Linux. Poprawne wartości to `true` lub `false`. Wartością domyślną tego parametru jest `false`. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Uruchomienie programu narzędziowego wiersza komend `manageprofiles` z opcją `-enableService` ustawioną na wartość `true` spowoduje utworzenie usługi systemu Linux wraz z profilem, jeśli komenda zostanie uruchomiona przez administratora. Jeśli program narzędziowy wiersza komend `manageprofiles` zostanie uruchomiony przez użytkownika innego niż administrator, profil zostanie utworzony, ale bez usługi systemu Linux. Usługa systemu Linux nie zostanie utworzona, ponieważ użytkownik inny niż administrator nie ma wystarczającego uprawnienia do skonfigurowania tej usługi. Po zakończeniu tworzenia profilu wyświetlany jest wynik `INSTCONPARTIALSUCCESS`, a dziennik tworzenia profilu `instalacyjny_katalog_główny/logs/manageprofiles/nazwa_profilu_create.log` zawiera komunikat wskazujący, że bieżący użytkownik nie ma wystarczającego uprawnienia do skonfigurowania usługi systemu Linux.

-federateLater true | false

Wskazuje, czy profil zarządzany zostanie stowarzyszony podczas jego tworzenia, czy też zostanie stowarzyszony w późniejszym czasie przy użyciu komendy `addNode`. Jeśli tworzony jest profil produktu Business Space, nie należy podawać wartości, ale użyć wartości domyślnej `true`.

-getDefaultName

Zwraca nazwę profilu domyślnego.

-getName

Pobiera nazwę profilu zarejestrowanego dla danego parametru `-profilePath`.

-getPath

Pobiera położenie w systemie plików dla profilu o podanej nazwie. Wymaga parametru `profileName`.

-help

Wyświetla składnię komendy.

-hostName nazwa_hosta

Określa nazwę hosta, na którym tworzony jest profil. Nie należy go podawać podczas

rozszerzenia istniejącego profilu. Nazwa powinna być zgodna z nazwą hosta określoną podczas początkowego instalowania produktu. Wartością domyślną tego parametru jest długa forma nazwy DNS (Domain Name System). Ten parametr jest wymagany tylko do tworzenia profilu. Wartość tego parametru musi być poprawną nazwą hosta IPv6 i nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: *, ?, ", <, >, ,, /, \ i |.

-importPersonalCertKS *ścieżka_do_magazynu_kluczy*

Określa ścieżkę do pliku kluczy, który jest używany do importowania certyfikatu osobistego podczas tworzenia profilu. Certyfikat osobisty to domyślny certyfikat osobisty serwera.

W przypadku importowania certyfikatu osobistego jako domyślnego certyfikatu osobistego należy zaimportować główny certyfikat, za pomocą którego podpisano certyfikat osobisty. W przeciwnym razie program narzędziowy manageprofiles dodaje klucz publiczny certyfikatu osobistego do pliku trust.p12 i tworzy główny certyfikat podpisywania.

Parametr -importPersonalCertKS wyklucza się wzajemnie z parametrem -personalCertDN. Jeśli nie zostanie utworzony ani zaimportowany certyfikat osobisty, zostanie on utworzony domyślnie.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha -importPersonal, konieczne jest określenie ich wszystkich.

-importPersonalCertKSType *typ_magazynu_kluczy*

Określa typ pliku kluczy określonego za pomocą parametru -importPersonalCertKS. Poprawne wartości to JCEKS, CMSKS, PKCS12, PKCS11 i JKS. Lista ta może jednak ulec zmianie w zależności od dostawcy w pliku java.security.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha -importPersonal, konieczne jest określenie ich wszystkich.

-importPersonalCertKSPassword *hasło_magazynu_kluczy*

Określa hasło pliku kluczy określonego za pomocą parametru -importPersonalCertKS.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha -importPersonal, konieczne jest określenie ich wszystkich.

-importPersonalCertKSAlias *alias_magazynu_kluczy*

Określa alias certyfikatu znajdującego się w pliku kluczy, który określono w parametrze -importPersonalCertKS. Certyfikat jest dodawany do domyślnego pliku kluczy serwera i służy jako domyślny certyfikat osobisty serwera.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha -importPersonal, konieczne jest określenie ich wszystkich.

-importSigningCertKS *ścieżka_do_magazynu_kluczy*

Określa ścieżkę do pliku kluczy, który jest używany do importowania certyfikatu głównego podczas tworzenia profilu. Certyfikat główny to certyfikat używany jako domyślny certyfikat główny serwera. Parametr -importSigningCertKS wyklucza się wzajemnie z parametrem -signingCertDN. Jeśli nie zostanie utworzony ani zaimportowany główny certyfikat podpisywania, taki certyfikat zostanie utworzony domyślnie.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha -importSigning, konieczne jest określenie ich wszystkich.

-importSigningCertKSType *ścieżka_do_magazynu_kluczy*

Określa typ pliku kluczy określonego za pomocą parametru -importSigningCertKS. Poprawne wartości to JCEKS, CMSKS, PKCS12, PKCS11 i JKS. Lista ta może jednak ulec zmianie w zależności od dostawcy w pliku java.security.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha `-importSigning`, konieczne jest określenie ich wszystkich.

-importSigningCertKSPassword *hasło_magazynu_kluczy*

Określa hasło pliku kluczy określonego za pomocą parametru `-importSigningCertKS`.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha `-importSigning`, konieczne jest określenie ich wszystkich.

-importSigningCertKSAlias *alias_magazynu_kluczy*

Określa alias certyfikatu znajdującego się w pliku kluczy, który określono w parametrze `-importSigningCertKS`. Certyfikat zostaje dodany do domyślnego głównego magazynu kluczy serwera i służy jako domyślny certyfikat główny serwera.

Jeśli są określane jakiegokolwiek parametry rozpoczynające się od łańcucha `-importSigning`, konieczne jest określenie ich wszystkich.

-isDefault

Określa, że profil zidentyfikowany przez towarzyszący parametr `-profileName` stanie się profilem domyślnym po zarejestrowaniu. Podczas wykonywania komend dotyczących profilu domyślnego nie jest konieczne użycie atrybutu `-profileName` komendy.

-keyStorePassword *hasło_magazynu_kluczy*

Określa hasło, które ma być używane dla wszystkich plików kluczy tworzonych podczas tworzenia profilu. Pliki kluczy są tworzone dla domyślnego certyfikatu osobistego i głównego certyfikatu podpisywania.

-listAugments




Wyświetla listę zarejestrowanych rozszerzeń profilu znajdującego się w rejestrze profilu. Wraz z parametrem `-listAugments` należy określić parametr `-profileName`.

-listProfiles

Wyświetla listę wszystkich zdefiniowanych profili.

-nodeName *nazwa_węzła*

Określa nazwę węzła, który zostanie utworzony przy użyciu nowego profilu. Należy użyć unikalnej wartości w komórce lub na stacji roboczej. Każdy profil, który współużytkuje ten sam zestaw plików binarnych produktu, musi mieć unikalną nazwę węzła. Rozszerzając profil, należy określić węzeł oryginalnego profilu.

   Wartość domyślna tego parametru jest oparta na krótkiej nazwie hosta, typie profilu i liczbie końcowej, na przykład:

```
if (Dmgr)
  krótka_nazwa_hostaCellManagernumer_węzła
else
  krótka_nazwa_hostaNodenumer_węzła
```

, gdzie *numer_węzła* to kolejna liczba, począwszy od 01.

Wartość tego parametru nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: *, ?, ", <, >, ,, /, \ i |.

-omitAction *funkcja1 funkcja2... funkcjaN*

Opcjonalny parametr, który wyklucza funkcje profilu.

Każdy szablon profilu jest wstępnie zdefiniowany przy użyciu określonych funkcji opcjonalnych. Opcja `samplesInstallAndConfig` jest dostępna tylko wtedy, gdy produkt został zainstalowany z wybranymi aplikacjami przykładowymi. Poniższe funkcje opcjonalne mogą być używane z parametrem `-omitAction` dla następujących szablonów profili:

- **domyślny** - serwer aplikacji
 - `deployAdminConsole`

- samplesInstallAndConfig
- defaultAppDeployAndConfig
- **dmgr** - menedżer wdrażania
 - deployAdminConsole

-personalCertDN *nazwa_wyróżniająca*

Określa nazwę wyróżniającą certyfikatu osobistego, który jest tworzony podczas tworzenia profilu. Nazwę wyróżniającą należy umieścić w znakach cudzysłowu. Ten domyślny certyfikat osobisty znajduje się w pliku kluczy serwera. Parametr `-importPersonalCertKSType` wyklucza się wzajemnie z parametrem `-personalCertDN`. Patrz parametry `-personalCertValidityPeriod` i `-keyStorePassword`.

-personalCertValidityPeriod *okres_ważności*

Opcjonalny parametr określający czas ważności (w latach) domyślnego certyfikatu osobistego. Jeśli ten parametr nie zostanie określony wraz z parametrem `-personalCertDN`, domyślny certyfikat osobisty będzie ważny przez jeden rok.

-portsFile *ścieżka_do_pliku*

Opcjonalny parametr określający ścieżkę do pliku, który definiuje ustawienia portu dla nowego profilu. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Tego parametru nie należy używać w przypadku korzystania z parametrów `-startingPort` lub `-defaultPorts`.

Jeśli nie zostanie określony parametr `-startingPort`, parametr `-defaultPorts` lub parametr `-portsFile`, podczas tworzenia profilu program narzędziowy wiersza komend `manageprofiles` będzie używać automatycznie wygenerowanego zestawu zalecanych portów. Zalecane wartości portów mogą się różnić od domyślnych wartości portów w zależności od dostępności portów domyślnych.

-profileName *nazwa_profilu*

Określa nazwę profilu. Podczas tworzenia profilu należy użyć wartości unikalnej.

Każdy profil, który współużytkuje ten sam zestaw plików binarnych produktu, musi mieć unikalną nazwę. Domyślna nazwa profilu jest oparta na typie profilu i liczbie końcowej, na przykład:

```
typ_profilu
numer_profilu
```

, gdzie *typ_profilu* to wartość taka jak `AppSrv`, `Dmgr` lub `Custom`, a *numer_profilu* to kolejna liczba, która powoduje utworzenie unikalnej nazwy profilu.

Wartość tego parametru nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\` i `|`. Wybrana nazwa profilu nie może być już w użyciu.


-profilePath *katalog_główny_profilu*

Określa pełną ścieżkę do profilu, która w Centrum informacyjnym jest znana jako *katalog_główny_profilu*.

Na przykład:

```
-profilePath katalog_główny_profilu
```

Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go ustawiać podczas rozszerzania istniejącego profilu.

 **Platformy Windows:** jeśli pełna ścieżka zawiera spację, należy umieścić wartość w cudzysłowach.

Wartość domyślna jest oparta na katalogu *instalacyjny_katalog_główny*, podkatalogu profilu i nazwie pliku.

Na przykład wartość domyślna dla tworzenia profili to:

```
WS_WSPROFILE_DEFAULT_PROFILE_HOME/nazwa_profilu
```

, gdzie wartość `WS_WSPROFILE_DEFAULT_PROFILE_HOME` jest zdefiniowana w pliku `wasprofile.properties` w katalogu `instalacyjny_katalog_główny/properties`.

Wartość tego parametru musi stanowić poprawną ścieżkę dla systemu docelowego i nie może być już używana.

Użytkownik musi mieć uprawnienia do zapisu w tym katalogu.

-response *plik_odpowiedzi*

Umożliwia dostęp do wszystkich funkcji API z poziomu wiersza komend przy użyciu programu narzędziowego wiersza komend `manageprofiles`.

Sterowanie interfejsem wiersza komend może odbywać się przy użyciu pliku odpowiedzi, który zawiera argumenty wejściowe dla danej komendy w pliku właściwości w formacie klucza i wartości. Poniżej przedstawiono przykładowy plik odpowiedzi dla operacji tworzenia (`create`):

```
create
profileName=testResponseFileCreate
profilePath=katalog_główny_profilu
templatePath=instalacyjny_katalog_główny/profileTemplates/default
nodeName=nazwa_węzła
cellName=nazwa_komórki
hostName=nazwa_hosta
omitAction=działanie_opcjonalne1, działanie_opcjonalne2
```

Windows Platformy Windows: w instrukcji ścieżki w systemie operacyjnym Windows mogą być używane ukośniki (/) lub ukośniki odwrotne (\). Jeśli w instrukcji ścieżki są używane ukośniki odwrotne, konieczne jest użycie podwójnych ukośników odwrotnych w pliku odpowiedzi, aby rozpoznał on poprawnie ścieżkę. Poniżej przedstawiono przykład pliku odpowiedzi dla operacji tworzenia (`create`), który używa podwójnych ukośników odwrotnych:

```
create
templatePath=C:\\WebSphere\\AppServer\\profileTemplates\\BusinessSpace\\default.bspace
```

Dodając właściwości oznaczające nazwy wyróżniające dla certyfikatów, należy poprzedzać przecinki podwójnymi ukośnikami odwrotnymi (\\). Należy zauważyć, że separatorem oddzielającym klucz (`personalCertDN`) od wartości jest nie znak równości, lecz spacja. Wynika to z faktu, że znak równości występuje wewnątrz wartości tej właściwości. Poniżej przedstawiono przykład instrukcji opisującej certyfikat w pliku odpowiedzi, w której zastosowano podwójne ukośniki odwrotne:

```
personalCertDN
cn=nazwa_komputera.przyrostek_dnx.com\\,ou=nazwa_komputera
Node04Cell\\,ou=nazwa_komputeraNode04\\,o=IBM\\,c=US
```

Aby określić, które argumenty wejściowe są wymagane dla różnych typów szablonów profili i działań, należy użyć programu narzędziowego wiersza komend `manageprofiles` z parametrem **-help**.

-restoreProfile

Odtwarza kopię zapasową profilu. Tego parametru należy używać z parametrem `-backupFile`.

-samplesPassword *hasło_przykładów*

Tworzy hasło, które ma być używane dla przykładów. Hasło służy do ograniczania dostępu do przykładów aplikacji WWW zainstalowanych podczas instalacji serwera aplikacji.

-serverType DEPLOYMENT_MANAGER

Określa typ profilu zarządzania. Należy określić wartość `DEPLOYMENT_MANAGER` dla profilu zarządzania. Ten parametr jest wymagany podczas tworzenia profilu zarządzania.

Linux -serviceUserName identyfikator_użytkownika_usługi

Określa ID użytkownika używany podczas tworzenia usługi systemu Linux, dzięki czemu usługa systemu Linux będzie uruchamiana w ramach tego ID użytkownika. Usługa systemu Linux jest uruchamiana po każdym zalogowaniu użytkownika o tym identyfikatorze.

-setDefaultName

Ustawia profil domyślny na jeden z istniejących profili. Tego parametru należy używać z parametrem `-profileName`, na przykład:

```
manageprofiles(.bat)(.sh) -setDefaultName -profileName nazwa_profilu
```

-signingCertDN nazwa_wyróżniająca

Określa nazwę wyróżniającą głównego certyfikatu podpisywania, który jest tworzony podczas tworzenia profilu. Nazwę wyróżniającą należy umieścić w znakach cudzysłowu. Ten domyślny certyfikat osobisty znajduje się w pliku kluczy serwera. Parametr `-importSigningCertKS` wyklucza się wzajemnie z parametrem `-signingCertDN`. Jeśli nie zostanie utworzony ani zaimportowany główny certyfikat podpisywania, taki certyfikat zostanie utworzony domyślnie. Patrz parametry `-signingCertValidityPeriod` i `-keyStorePassword`.

-signingCertValidityPeriod okres_ważności

Opcjonalny parametr określający czas ważności (w latach) głównego certyfikatu podpisywania. Jeśli ten parametr nie zostanie określony wraz z parametrem `-signingCertDN`, główny certyfikat podpisywania będzie ważny przez 20 lat.

-startingPort port_początkowy

Określa początkowy numer portu w celu generowania i przypisywania wszystkich portów dla profilu.

Tego parametru nie należy ustawiać podczas rozszerzania istniejącego profilu. Wartości portów są przypisywane kolejno, począwszy od wartości `-startingPort`, z pominięciem już używanych portów. System rozpoznaje i rozstrzyga porty, które są aktualnie używane, a także określa przypisania portów w celu uniknięcia konfliktów portów.

Tego parametru nie należy używać w połączeniu z parametrami `-defaultPorts` i `-portsFile`.

Jeśli nie zostanie określony parametr `-startingPort`, parametr `-defaultPorts` lub parametr `-portsFile`, podczas tworzenia profilu program narzędziowy wiersza komend `manageprofiles` będzie używać automatycznie wygenerowanego zestawu zalecanych portów. Zalecane wartości portów mogą się różnić od domyślnych wartości portów w zależności od dostępności portów domyślnych.

Uwaga: Tego parametru nie należy używać w przypadku korzystania z szablonu profilu zarządzanego.

-templatePath ścieżka_do_szablonów

Określa ścieżkę do katalogu z plikami szablonów w instalacyjnym katalogu głównym. W katalogu `profileTemplates` znajdują się różne katalogi, które odpowiadają poszczególnym typom profili. Katalogi te różnią się w zależności od typu zainstalowanego produktu. Katalogi profili to ścieżki, które można wskazać podczas korzystania z opcji `-templatePath`. Możliwe jest określenie szablonów profili znajdujących się poza instalacyjnym katalogiem głównym, jeśli takie szablony istnieją.

Należy używać ścieżek bezwzględnych. Ten parametr musi istnieć jako katalog i musi wskazywać poprawny katalog szablonów. W produkcie Business Space należy używać następujących szablonów:

- **default.bspace**: przeznaczony dla profilu serwera autonomicznego produktu Business Space, który definiuje serwer autonomiczny.
- **dmgr.bspace**: przeznaczony dla profilu menedżera wdrażania produktu Business Space, który definiuje menedżer wdrażania.
- **managed.bspace**: przeznaczony dla niestandardowego profilu produktu Business Space, który po stowarzyszeniu z menedżerem wdrażania definiuje węzeł zarządzany.

-validateAndUpdateRegistry

Sprawdza wszystkie profile wymienione w rejestrze profili w celu określenia, czy profile są obecne w systemie plików. Powoduje usunięcie wszystkich brakujących profili z rejestru. Zwraca listę brakujących profili, które zostały usunięte z rejestru.

-validateRegistry

Sprawdza wszystkie profile wymienione w rejestrze profili w celu określenia, czy profile są obecne w systemie plików. Zwraca listę brakujących profili.

-validatePorts

Określa porty, które powinny zostać sprawdzone w celu upewnienia się, że nie są zarezerwowane lub używane. Ten parametr pomaga zidentyfikować porty, które nie są używane. Jeśli zostanie określone, że port jest w użyciu, nastąpi zatrzymanie tworzenia profilu, a następnie zostanie wyświetlony komunikat o błędzie. Tego parametru można użyć w dowolnym momencie w wierszu komendy tworzenia (create). Zalecane jest użycie tego parametru wraz z parametrem `-portsFile`.

-webFormConfig true | false

Wskazuje, czy produkt Business Space został skonfigurowany w taki sposób, aby używał serwera IBM Forms Server w celu pracy z widgetami zarządzania czynnościami personelu. Wartością domyślną tego parametru jest `false`. Wartość `true` jest używana do konfigurowania produktu Business Space w celu korzystania z serwera IBM Forms Server. Parametry **webFormConfig** i **webFormInstallRoot** są wymagane do skonfigurowania serwera IBM Forms Server. Ten parametr jest poprawny tylko w przypadku profili serwerów autonomicznych.

Uwaga: Konfiguracja serwera IBM Forms Server używająca tych parametrów jest poprawna tylko w przypadku lokalnych instalacji serwera IBM Forms Server.

-webServerCheck true | false


Wskazuje, czy mają zostać skonfigurowane definicje serwera WWW. Poprawne wartości to `true` lub `false`. Wartością domyślną tego parametru jest `false`. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerHostname nazwa_hosta_serwera_WWW

Nazwa hosta serwera. Wartością domyślną tego parametru jest długa nazwa hosta lokalnej stacji roboczej. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerInstallPath nazwa_ścieżki_instalacji_serwera_WWW

Ścieżka instalacji lokalnego lub zdalnego serwera WWW. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Wartość domyślna tego parametru jest zależna od systemu operacyjnego lokalnej stacji roboczej oraz od wartości parametru `webServerType`. Na przykład: 

`webServerType=IHS`: wartość parametru `webServerInstallPath` jest ustawiana domyślnie na `/usr/IBM/HTTPServer`

`webServerType=IIS`: wartość parametru `webServerInstallPath` jest ustawiana domyślnie na `n\`

`webServerType=SUNJAVASYSTEM`: wartość parametru `webServerInstallPath` jest ustawiana domyślnie na `/opt/sun/webserver`

webServerType=DOMINO: wartość parametru webServerInstallPath jest ustawiana domyślnie na ?
webServerType=APACHE: wartość parametru webServerInstallPath jest ustawiana domyślnie na ?
webServerType=HTTPSERVER_ZOS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n/a

HP-UX

webServerType=IHS: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/IBM/HTTPServer
webServerType=IIS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n\|a
webServerType=SUNJAVASYSTEM: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/sun/webserver
webServerType=DOMINO: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=APACHE: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=HTTPSERVER_ZOS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n/a

> Linux

webServerType=IHS: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/IBM/HTTPServer
webServerType=IIS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n\|a
webServerType=SUNJAVASYSTEM: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/sun/webserver
webServerType=DOMINO: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=APACHE: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=HTTPSERVER_ZOS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n/a

Solaris

webServerType=IHS: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/IBM/HTTPServer
webServerType=IIS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n\|a
webServerType=SUNJAVASYSTEM: wartość parametru webServerInstallPath jest ustawiana domyślnie na /opt/sun/webserver
webServerType=DOMINO: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=APACHE: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=HTTPSERVER_ZOS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n/a

> Windows

webServerType=IHS: wartość parametru webServerInstallPath jest ustawiana domyślnie na C:\Program Files\IBM\HTTPServer
webServerType=IIS: wartość parametru webServerInstallPath jest ustawiana domyślnie na C:\
webServerType=SUNJAVASYSTEM: wartość parametru webServerInstallPath jest ustawiana domyślnie na C:\
webServerType=DOMINO: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=APACHE: wartość parametru webServerInstallPath jest ustawiana domyślnie na
webServerType=HTTPSERVER_ZOS: wartość parametru webServerInstallPath jest ustawiana domyślnie na n/a

-webServerName *nazwa_serwera_WWW*

Nazwa serwera WWW. Wartością domyślną tego parametru jest **webserver1**. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerOS *system_operacyjny_serwera_WWW*

System operacyjny serwera WWW. Poprawne wartości to: **windows**, **linux**, **solaris**, **aix**, **hpux**, **os390** i **os400**. Tego parametru należy używać z parametrem **webServerType**.

Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerPluginPath *ścieżka_do_wtyczek_serwera_WWW*

Ścieżka do wtyczek używanych przez serwer WWW. Wartością domyślną tego parametru jest *instalacyjny_katalog_główny/plugins*. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerPort *port_serwera_WWW*

Wskazuje port, który będzie używany w celu uzyskania dostępu do serwera WWW. Wartością domyślną tego parametru jest **80**. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

-webServerType *typ_serwera_WWW*

Typ serwera WWW. Poprawne wartości to: IHS, SUNJAVASYSTEM, IIS, DOMINO, APACHE i HTTPSERVER_ZOS. Tego parametru należy używać z parametrem **webServerOS**. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Windows **-winserviceAccountType** *specifieduser | localsystem*

Typ konta właściciela usługi systemu Windows tworzonej dla profilu. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Poprawne wartości to **specifieduser** lub **localsystem**. Wartość **localsystem** powoduje uruchomienie usługi systemu Windows w ramach konta lokalnego użytkownika, który tworzy profil. Wartością domyślną tego parametru jest **system**.

Windows **-winserviceCheck** *true | false*

Parametr może mieć wartość **true** lub **false**. Należy określić wartość **true**, aby utworzyć usługę systemu Windows dla procesu serwera, który jest tworzony w ramach profilu. Aby usługa systemu Windows nie była tworzona, należy określić wartość **false**. Wartością domyślną tego parametru jest **false**.

Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Windows **-winservicePassword** *haslo_uslugi_systemu_Windows*

Należy podać hasło dla określonego użytkownika lub konta lokalnego, do którego będzie należeć usługa systemu Windows. Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Windows **-winserviceStartupType** *manual | automatic | disabled*

Poprawne wartości dla uruchamiania usługi systemu Windows to:

- manual
- automatic
- disabled

Wartość domyślna tego parametru to **manual**.

Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Windows **-winserviceUserName**

identyfikator_uzytkownika_uslugi_systemu_Windows

Należy określić ID użytkownika, aby system operacyjny Windows mógł zweryfikować identyfikator tego użytkownika jako identyfikator, w przypadku którego możliwe jest tworzenie usługi systemu Windows. Identyfikator użytkownika musi należeć do grupy administratorów i mieć następujące zaawansowane uprawnienia użytkownika:

- Działanie jako element systemu operacyjnego
- Logowanie w trybie usługi

Wartością domyślną tego parametru jest nazwa bieżącego użytkownika. Wartość tego parametru nie może zawierać spacji ani żadnych niepoprawnych znaków, takich jak: *, ?, ", <, >, ,, /, \ i |. Określony użytkownik musi mieć odpowiednie uprawnienia do tworzenia usługi systemu Windows. Konieczne jest określenie poprawnego hasła dla wybranej nazwy użytkownika.

Tego parametru należy używać tylko podczas tworzenia profili. Nie należy go podawać podczas rozszerzania istniejącego profilu.

Konfigurowanie produktu Business Space jako części kreatora konfiguracji środowiska wdrażania

Konfiguracja produktu Business Space oraz konfiguracja usługi REST (Representational State Transfer) widgetów w produkcie Business Space jest automatycznie uwzględniana w kreatorze konfiguracji środowiska wdrażania. Użytkownik może zdecydować o tym, jakie usługi REST mają zostać skonfigurowane.

Zanim rozpoczniesz tę czynność, musisz wykonać następujące czynności:

- Zainstaluj produkt.
- Utwórz profil i upewnij się, że wskazano pełną nazwę hosta dla profilu.
- Włącz zabezpieczenia, jeśli ma zostać skonfigurowane bezpieczne środowisko dla produktu Business Space.

W przypadku konfigurowania menedżera wdrażania oraz profili niestandardowych jest to najprostszy sposób skonfigurowania produktu Business Space.

1. W Konsoli administracyjnej kliknij opcję **Serwery > Środowiska wdrażania > Nowe**. Przeprowadzenie procesu tworzenia środowiska wdrażania będzie możliwe dzięki serii odpowiednich stron kreatora.
2. Zdefiniuj nowe środowisko wdrażania lub zaimportuj plik zawierający definicje środowiska wdrażania. Użytkownik może utworzyć środowisko wdrażania w oparciu o jeden z wzorców dostarczonych przez IBM lub utworzyć niestandardowe środowisko wdrażania.
3. Na stronie Wzorce środowiska wdrażania wybierz jeden ze wzorców środowiska wdrażania.
4. Na stronie Wybór węzłów wskaż węzły, które mają zostać częścią środowiska wdrażania.
5. Na stronie Klastry określ liczbę elementów klastra z poszczególnych węzłów w celu przypisania do konkretnych funkcji środowiska wdrażania.
6. Na stronie Baza danych skonfiguruj źródło danych dla produktu Business Space - jeden z komponentów wymienionych w tabeli. Możliwe jest zmodyfikowanie opisu, przetestowanie połączenia oraz ustawienie produktu bazodanowego, który ma być używany w charakterze dostawcy. Na tej stronie nie można zaznaczyć pola wyboru **Utwórz table** dla produktu Business Space. Tabele bazy danych dla produktu Business Space należy skonfigurować ręcznie. Lista systemów baz danych zawiera wszystkie bazy danych obsługiwane przez poszczególne komponenty.
7. Na stronie Zabezpieczenia skonfiguruj aliasy uwierzytelniania używane przez produkt WebSphere podczas uzyskiwania dostępu do bezpiecznych komponentów. Na tej stronie można zmienić nazwę i hasło użytkownika aliasu uwierzytelniania. Aliasy te służą do uzyskiwania dostępu do bezpiecznych komponentów, ale nie umożliwiają uzyskiwania dostępu do źródeł danych.
8. W przypadku konfiguracji produktu IBM Business Process Manager podaj informacje wymagane do skonfigurowania miejsca docelowego wdrażania aplikacji na potrzeby obsługi wdrażania komponentów produktu Business Process Choreographer. Określ kontekstowe katalogi główne, zabezpieczenia oraz wartości sesji poczty elektronicznej menedżera czynności personelu używane przez kreator do konfigurowania produktu Business Process Choreographer dla tego środowiska wdrażania.
9. W przypadku konfiguracji produktu IBM Business Process Manager skonfiguruj menedżer reguł biznesowych, aby możliwe było jego uruchomienie w klastrze lub na serwerze.
10. Na stronie Usługi REST skonfiguruj usługi dla widgetów, które mają być dostępne w produkcie Business Space dla środowiska wykonawczego.

- Wpisz numer portu oraz host lub host wirtualny wymagany przez klient do komunikacji z serwerem lub klastrem. W środowisku klastrowym jest to zazwyczaj nazwa hosta oraz port serwera równoważenia obciążenia.
- Jeśli pola hosta i portu pozostaną puste, jako wartości domyślne zostaną przyjęte wartości hosta oraz portu HTTP elementu klastra. W przypadku środowiska z równoważeniem obciążenia należy później zmienić wartości domyślne na nazwę hosta wirtualnego i port serwera równoważenia obciążenia. Koniecznie należy wpisać pełną nazwę hosta.
- Jeśli będzie to konieczne, należy ustawić opis dla widgetów.

11. Na następnej stronie kliknij opcję **Zakończ** lub **Zakończ i generuj środowisko**.
12. Uruchom skrypty w celu skonfigurowania tabel bazy danych dla produktu Business Space, zanim zostanie uruchomione środowisko wdrażania lub klastry. Więcej informacji zawiera sekcja Konfigurowanie tabel bazy danych produktu Business Space.

Wskazówka: Produkt Business Space używa komponentu proxy w celu nawiązywania połączeń z usługami REST. W niektórych przypadkach, jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia między produktem Business Space a usługami REST w zależności od wydajności serwerów usługi REST. Więcej informacji zawiera temat Zmianie ustawień limitu czasu dla proxy Ajax produktu Business Space.

Konfigurowanie produktu Business Space na potrzeby środowisk wdrożenia sieciowego

W przypadku środowiska rozproszonego lub środowiska wdrożenia sieciowego należy skonfigurować produkt Business Space przy użyciu Konsoli administracyjnej lub komend.

W przypadku używania menedżera wdrażania oraz profili niestandardowych należy skonfigurować punkty końcowe usługi REST (Representational State Transfer), skonfigurować produkt Business Space, zarejestrować punkty końcowe usługi REST, a następnie skonfigurować tabele bazy danych.

Konfigurowanie usług REST:

W przypadku korzystania ze środowiska serwera autonomicznego lub jeśli środowisko wykonawcze jest konfigurowane za pomocą kreatora środowiska wdrażania, usługi REST (Representational State Transfer) są automatycznie konfigurowane i włączane. W przypadku innych środowisk do skonfigurowania usług REST należy użyć Konsoli administracyjnej.

Jeśli widżety mają być dostępne w produkcie Business Space, należy skonfigurować usługi REST dla tych widżetów. Następnie należy zarejestrować punkty końcowe usługi REST, aby produkt Business Space powiązał widżety z punktami końcowymi oraz aby widżety zostały wyświetlone na palecie i udostępnione do użycia.

Wszystkie usługi REST można skonfigurować dla konkretnego serwera lub klastra. Ewentualnie można wybrać poszczególne usługi do skonfigurowania. Konfiguracją każdej usługi można zarządzać, wyświetlając wszystkie usługi dla dostawcy usług lub wyświetlając wszystkie usługi dla środowiska.

Usługi REST są zwykle prezentowane w komponencie REST Gateway. Niektóre usługi REST są implementowane przy użyciu dedykowanej dla nich aplikacji systemowej. Aplikacja Brama usług REST włącza wspólne usługi REST systemu. Aplikacja Brama usług REST jest tworzona podczas konfigurowania usług REST.

W środowiskach klastrowych wszystkie czynności administracyjne i konfiguracyjne dla usług REST są wykonywane w aplikacji Menedżer wdrażania bramy usług REST w menedżerze wdrażania. Aplikacja Menedżer wdrażania bramy usług REST jest używana z następującymi widgetami:

- Przeglądarka modułów
- Zespół modułu
- Właściwości modułu
- Brama proxy
- Poprawność modułu
- Poprawność systemu

Konfigurowanie wszystkich usług REST w Konsoli administracyjnej:

Wszystkie usługi REST (Representational State Transfer) dla danego środowiska można skonfigurować za pomocą strony Usługi REST w Konsoli administracyjnej.

Przed wykonaniem tej czynności należy zainstalować produkt WebSphere do zarządzania procesami biznesowymi.

Wdrażanie usług REST jest przeprowadzane automatycznie w profilu serwera autonomicznego. W przypadku innych typów konfiguracji strona Konsoli administracyjnej umożliwi użytkownikowi skonfigurowanie usług REST dla wszystkich widgetów w produkcie Business Space. Na stronie Usługi REST można wyświetlać wszystkie usługi związane z danym środowiskiem oraz włączać i wyłączać poszczególne z nich.

Konieczne jest także zarejestrowanie punktów końcowych usług REST w produkcie Business Space. Następnie produkt Business Space tworzy powiązania między widgetami i tymi punktami końcowymi, a widgety są wyświetlane do użycia na palecie. Aby upewnić się, że punkty końcowe usług REST są zarejestrowane w produkcie Business Space, należy zapoznać się z tematem Konfigurowanie produktu Business Space i rejestrowanie punktów końcowych usług REST za pomocą Konsoli administracyjnej.

Aby skonfigurować wiele instancji tego samego punktu końcowego usługi REST, należy ręcznie dokonać edycji pliku punktów końcowych oraz pliku metadanych widgetów. Więcej informacji na ten temat zawiera sekcja Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi.

Aplikacja Brama usług REST włącza wspólne usługi REST systemu. Aplikacja Brama usług REST jest tworzona podczas konfigurowania usług REST.

1. Kliknij opcję **Usługi > Usługi REST > Usługi REST**.

Zostanie otwarta strona Usługi REST, na której wymienione są wszystkie usługi REST w środowisku użytkownika.

2. W sekcji **Zasięg** wybierz wartość **Wszystkie**, aby wyświetlić wszystkie usługi REST w środowisku, bądź wybierz serwer lub klastr, w którym włączone zostały usługi REST. Jeśli brakuje pewnych usług REST, które powinny być wyświetlane w wybranym zasięgu, należy włączyć aplikację Brama usług REST albo odpowiednich dostawców usług REST na serwerze lub w klastrze. Więcej informacji można znaleźć w sekcji Konfigurowanie usług REST dla serwera, klastra lub komponentu.

3. W każdym wierszu tabeli zawierającej usługi REST dla dostawcy zaznacz pole wyboru **Włączona**, aby włączyć daną usługę REST, lub usuń zaznaczenie pola wyboru **Włączona**, aby wyłączyć daną usługę REST.

4. W kolumnie **Opis** wprowadź zrozumiałe opisy dla każdej usługi, która ma zostać włączona.

5. Kliknij przycisk **OK**, aby zatwierdzić zmiany wprowadzone w usługach.
 - Skonfiguruj produkt Business Space.
 - Skonfiguruj tabele bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrożenia sieciowego).
 - Zarejestruj punkty końcowe usługi REST.
 - Jeśli w przypadku wielu instancji punktów końcowych usługi (na przykład wtedy, gdy praca jest partycjonowana w dwóch klastrach) w widgetach mają być wyświetlane dane z każdego klastra, ręcznie włącz dodatkowe widgety dla każdego dodatkowego klastra.
 - Skonfiguruj zabezpieczenia produktu Business Space.

Konfigurowanie usług REST w dostawcy usług:

W tym temacie opisano konfigurowanie usług Representational State Transfer (REST) w dostawcy usług za pomocą strony Konsoli administracyjnej służącej do konfiguracji dostawców usług REST.

Przed wykonaniem tej czynności należy zainstalować produkt WebSphere do zarządzania procesami biznesowymi.

Wdrażanie usług REST jest przeprowadzane automatycznie w profilu serwera autonomicznego. W przypadku innych typów konfiguracji usługi REST dla wszystkich widgetów produktu Business Space można skonfigurować za pomocą Konsoli administracyjnej. Na stronie Konsoli administracyjnej służącej do konfiguracji dostawców usług REST można wyświetlić wszystkie usługi dla wybranego dostawcy usług, a także niezależnie włączyć lub wyłączyć każdą usługę. Strona ta pozwala na zarządzanie konfiguracją poszczególnych usług, umożliwiając pracę ze wszystkimi usługami dostawcy usług.

Konieczne jest także zarejestrowanie punktów końcowych usług REST w produkcie Business Space. Następnie produkt Business Space tworzy powiązania między widgetami i tymi punktami końcowymi, a widgety są wyświetlane do użycia na palecie. Aby upewnić się, że punkty końcowe usługi REST są zarejestrowane w produkcie Business Space, należy zapoznać się z tematem Konfigurowanie produktu Business Space i rejestrowanie punktów końcowych usług REST za pomocą Konsoli administracyjnej.

Aby skonfigurować wiele instancji tego samego punktu końcowego usługi REST, należy ręcznie dokonać edycji pliku punktów końcowych oraz pliku metadanych widgetów. Więcej informacji na ten temat zawiera sekcja Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi.

Aplikacja Brama usług REST włącza wspólne usługi REST systemu. Aplikacja Brama usług REST jest tworzona podczas konfigurowania usług REST.

Dostępni są następujący dostawcy usług REST skonfigurowani w przedstawionym zasięgu:

- **Brama usług REST:** aby dodać bramę usług REST dla danego zasięgu, należy wybrać opcję **Serwery > Typy serwerów > mój_serwer > Integracja biznesowa > Usługi REST** lub **Serwery > Klastry > mój_klaster > Integracja biznesowa > Usługi REST**. Następnie należy skonfigurować dostawcę bramy usług REST dla danego serwera lub klastra.
- **Menedżer wdrażania bramy usług REST:** dostawca bramy usług REST w menedżerze wdrażania jest konfigurowany automatycznie podczas tworzenia profilu menedżera wdrażania produktu IBM Business Process Manager lub WebSphere Enterprise Service Bus. Ten dostawca udostępnia administracyjne usługi REST używane przez widgety Przeglądarka modułów, Administrowanie modułem, Monitor poprawności i Gateway proxy.

1. Kliknij opcję **Usługi > Usługi REST > Dostawcy usług REST**.
Zostanie otwarta strona Dostawcy usług REST z wyświetlonymi wszystkimi dostawcami usług REST.
2. Kliknij odsyłacz dostawcy, aby skonfigurować usługi dla grupy usług REST zarządzanych przez tego dostawcę.
Zostanie otwarta strona konfiguracji dostawców usług REST z wyświetlonymi wszystkimi usługami REST dostawcy.
3. Z listy **Protokół** wybierz protokół dla wszystkich usług REST, które mają zostać skonfigurowane, aby były dostępne w produkcie Business Space. Skonfiguruj pełną ścieżkę adresu URL, wybierając opcję **https://** lub **http://**, a następnie wypełniając pola **Nazwa hosta lub hosta wirtualnego w środowisku z równoważeniem obciążenia i Port**. Użyj pełnej nazwy hosta.
Jeśli żądania usług REST mają być przekazywane bezpośrednio do serwera aplikacji, należy wpisać nazwę hosta i port serwera aplikacji. Aby żądania usług REST były przekazywane do serwera proxy lub serwera HTTP znajdującego się „przed” jednym lub wieloma serwerami aplikacji, należy wpisać nazwę hosta i port skonfigurowanego wcześniej serwera proxy lub serwera HTTP. W przypadku środowiska z systemem równoważenia obciążenia lub serwerem proxy między przeglądarką a produktem Business Space i usługami REST należy upewnić się, że wartości podane dla protokołu, hosta i portu są zgodne z wartościami w adresie URL wprowadzanym w przeglądarce w celu uzyskania dostępu do produktu Business Space.
4. W każdym wierszu tabeli zawierającej usługi REST dla dostawcy zaznacz pole wyboru **Włączona**, aby włączyć daną usługę REST, lub usuń zaznaczenie pola wyboru **Włączona**, aby wyłączyć daną usługę REST.
5. W kolumnie **Opis** wprowadź zrozumiały opis dla każdej usługi, która ma zostać włączona.
6. Kliknij przycisk **OK**, aby zatwierdzić zmiany wprowadzone w usługach.
 - Skonfiguruj produkt Business Space.
 - Skonfiguruj tabele bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrożenia sieciowego).
 - Zarejestruj punkty końcowe usługi REST.
 - Jeśli w przypadku wielu instancji punktów końcowych usługi (na przykład wtedy, gdy praca jest partycjonowana w dwóch klastrach) w widgetach mają być wyświetlane dane z każdego klastra, ręcznie włącz dodatkowe widgety dla każdego dodatkowego klastra.
 - Skonfiguruj zabezpieczenia produktu Business Space.

Konfigurowanie usług REST dla serwera, klastra lub komponentu:

Usługi REST (Representational State Transfer) dla serwera, klastra lub komponentu należy skonfigurować przy użyciu strony Usługi REST w Konsoli administracyjnej.

Przed wykonaniem tej czynności należy zainstalować produkt WebSphere do zarządzania procesami biznesowymi.

Wdrażanie usług REST jest przeprowadzane automatycznie w profilu serwera autonomicznego. W przypadku innych typów konfiguracji strona Usługi REST w Konsoli administracyjnej umożliwia skonfigurowanie usług dla serwera, klastra lub komponentu.

W wyniku wykonania tej czynności zostanie skonfigurowana aplikacja dostawcy usług REST dla konkretnego serwera lub klastra. Aplikację dostawcy należy skonfigurować przed udostępnieniem usług REST na serwerze lub w klastrze. Więcej informacji na temat dostawców usług REST zawiera temat Konfigurowanie usług REST w dostawcy usług.

Konieczne jest także zarejestrowanie punktów końcowych usług REST w produkcie Business Space. Następnie produkt Business Space tworzy powiązania między widgetami i tymi punktami końcowymi, a widgety są wyświetlane do użycia na palcie. Aby upewnić się, że punkty końcowe usługi REST są zarejestrowane w produkcie Business Space, należy zapoznać się z tematem Konfigurowanie produktu Business Space i rejestrowanie punktów końcowych usług REST za pomocą Konsoli administracyjnej.

Aby skonfigurować wiele instancji tego samego punktu końcowego usługi REST, należy ręcznie dokonać edycji pliku punktów końcowych oraz pliku metadanych widgetów. Więcej informacji zawiera temat Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi.

Aplikacja Brama usług REST włącza wspólne usługi REST systemu. Aplikacja Brama usług REST jest tworzona podczas konfigurowania usług REST.

1. Kliknij jedną z następujących opcji.
 - W przypadku usług REST na serwerze kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere > nazwa_serwera > Integracja biznesowa > Usługi REST**.
 - W przypadku usług REST w klastrze kliknij opcję **Serwery > Klastry > Klastry serwerów aplikacji WebSphere > nazwa_klastra > Integracja biznesowa > Usługi REST**.

Zostanie wyświetlona strona Usługi REST zawierająca wszystkie domyślne usługi REST, które można skonfigurować dla widgetów produktu Business Space do użycia z produktem lub komponentem (menedżerem przepływów biznesowych lub menedżerem czynności personelu). Jeśli usługa REST została już skonfigurowana, zostanie wyświetlony odpowiedni komunikat.

2. Z listy **Protokół** wybierz protokół dla wszystkich usług REST, które mają zostać skonfigurowane, aby były dostępne w produkcie Business Space. Skonfiguruj pełną ścieżkę adresu URL, wybierając opcję **https://** lub **http://**, a następnie wypełniając pola **Nazwa hosta lub hosta wirtualnego w środowisku z równoważeniem obciążenia i Port**. Użyj pełnej nazwy hosta.

Jeśli żądania usług REST mają być przekazywane bezpośrednio do serwera aplikacji, należy wpisać nazwę hosta i port serwera aplikacji. Aby żądania usług REST były przekazywane do serwera proxy lub serwera HTTP znajdującego się „przed” jednym lub wieloma serwerami aplikacji, należy wpisać nazwę hosta i port skonfigurowanego wcześniej serwera proxy lub serwera HTTP. W przypadku środowiska z systemem równoważenia obciążenia lub serwerem proxy między przeglądarką a produktem Business Space i usługami REST należy upewnić się, że wartości podane dla protokołu, hosta i portu są zgodne z wartościami w adresie URL wprowadzanym w przeglądarce w celu uzyskania dostępu do produktu Business Space. Takie samo ograniczenie ma zastosowanie we wszystkich środowiskach, w których są używane widgety produktu Business Space obsługujące technologie Flex.

3. W tabeli usług REST w każdym wierszu zaznacz pole wyboru **Włączona**, aby włączyć poszczególne usługi REST, lub usuń zaznaczenie pola wyboru **Włączona**, aby wyłączyć poszczególne usługi REST.
4. W tabeli usług REST w polu **Opis** wpisz znaczący opis dla każdej usługi REST.
5. Kliknij przycisk **OK**, aby zatwierdzić zmiany wprowadzone w usługach.

Aby później zmodyfikować konfigurację usługi REST, można ponownie przejść na stronę Usługi REST lub użyć innych stron Konsoli administracyjnej do zarządzania konfiguracją punktów końcowych usługi REST. Strona Dostawcy usług REST umożliwia wybranie dostawcy usługi, który ma zostać skonfigurowany. Strona Usługi REST, do której dostęp można uzyskać, wybierając opcję **Usługi > Usługi REST**, umożliwia skonfigurowanie wszystkich usług REST w środowisku użytkownika.

- Skonfiguruj produkt Business Space.
- Skonfiguruj tabele bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrożenia sieciowego).
- Zarejestruj punkty końcowe usługi REST.
- Jeśli w przypadku wielu instancji punktów końcowych usługi (na przykład wtedy, gdy praca jest partycjonowana w dwóch klastrach) w widgetach mają być wyświetlane dane z każdego klastra, ręcznie włącz dodatkowe widgety dla każdego dodatkowego klastra.
- Skonfiguruj zabezpieczenia produktu Business Space.

Konfigurowanie usług REST za pomocą wiersza komend:

Wszystkie widgety wymagane przez produkt użytkownika są instalowane z produktem Business Space oparty na technologii WebSphere. Usługi REST (Representational State Transfer) dla widgetów muszą zostać skonfigurowane, włączone i zarejestrowane w produkcie Business Space, zanim zespół użytkownika będzie mógł używać widgetów w produkcie Business Space. Jeśli nie jest używana strona Usługi REST w Konsoli administracyjnej, należy użyć komendy `updateRESTGatewayService`.

Przed wykonaniem tej czynności należy zainstalować produkt WebSphere do zarządzania procesami biznesowymi.

Wdrażanie usług REST jest przeprowadzane automatycznie w profilu serwera autonomicznego. W przypadku innych typów konfiguracji strona Usługi REST w Konsoli administracyjnej lub komenda `updateRESTGatewayService` umożliwi skonfigurowanie usług dla aplikacyjnych interfejsów programistycznych (interfejsów API) usług REST dla wszystkich widgetów produktu użytkownika w produkcie Business Space.

Konieczne jest także zarejestrowanie punktów końcowych usług REST w produkcie Business Space. Następnie produkt Business Space tworzy powiązania między widgetami i tymi punktami końcowymi, a widgety są wyświetlane do użycia na palecie.

Aby skonfigurować wiele instancji tego samego punktu końcowego usługi REST, należy ręcznie dokonać edycji pliku punktów końcowych oraz pliku metadanych widgetów. Więcej informacji zawiera temat *Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi*.

1. Otwórz okno komend.

Komenda `wsadmin` jest dostępna w katalogu `katalog_główny_profilu/bin` w środowisku serwera autonomicznego lub w katalogu `katalog_główny_profilu_menedżera_wdrażania/bin` w środowisku wdrożenia sieciowego.

2. W wierszu komend wpisz komendę `wsadmin`, aby uruchomić środowisko `wsadmin`.

3. Przy użyciu komendy `updateRESTGatewayService` skonfiguruj usługi REST, określając klastr lub serwer i węzeł. Parametr **-enable** jest opcjonalny. Jeśli nie zostanie podany, domyślnie zostanie przyjęta wartość `true`.

4. Uruchom komendę `save`.

W następującym przykładzie użyto języka Jython do uruchomienia komendy `updateRESTGatewayService` i zapisania zmian. Przykład ten konfiguruje usługi REST w klastrze.

```
AdminTask.updateRESTGatewayService(['[-clusterName
nazwa_klastra]'])
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updateRESTGatewayService {-clusterName
nazwa_klastra}
$AdminConfig save
```

- Skonfiguruj produkt Business Space.
- Skonfiguruj tabele bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrożenia sieciowego).
- Zarejestruj punkty końcowe usługi REST.
- Jeśli w przypadku wielu instancji punktów końcowych usługi (na przykład wtedy, gdy praca jest partycjonowana w dwóch klastrach) w widgetach mają być wyświetlane dane z każdego klastra, ręcznie włącz dodatkowe widgety dla każdego dodatkowego klastra.
- Skonfiguruj zabezpieczenia produktu Business Space.

Konfigurowanie produktu Business Space i rejestrowanie punktów końcowych REST za pomocą Konsoli administracyjnej:

Produkt Business Space oparty na technologii WebSphere można zainstalować i skonfigurować przy użyciu Konsoli administracyjnej.

Zanim rozpoczniesz tę czynność, musisz wykonać następujące czynności:

- Zainstaluj oprogramowanie i utwórz profil. Podczas instalacji produktu są instalowane pliki produktu Business Space na potrzeby konfigurowanych profili. Profil użytkownika nie zostanie skonfigurowany dla produktu Business Space do czasu jawnego skonfigurowania produktu Business Space w profilu.
- Włącz zabezpieczenia, jeśli ma zostać skonfigurowane bezpieczne środowisko dla produktu Business Space.
- Skonfiguruj usługi REST (Representational State Transfer). Jeśli użytkownik korzysta ze środowiska serwera autonomicznego lub konfiguruje środowisko wykonawcze za pomocą kreatora środowiska wdrażania, punkty końcowe usługi REST są konfigurowane i włączane automatycznie. W przypadku innych środowisk w celu skonfigurowania usług REST należy użyć strony usług REST w Konsoli administracyjnej. Jeśli widgety mają być dostępne w produkcie Business Space, należy skonfigurować usługi REST dla tych widжетów. Na stronie konfiguracji produktu Business Space w Konsoli administracyjnej należy zarejestrować punkty końcowe usługi REST, aby widgety zostały powiązane z punktami końcowymi przez produkt Business Space oraz aby były wyświetlane na palecie i dostępne do użycia.
- Aby skonfigurować produkt Business Space na serwerze lub w klastrze przy użyciu innego źródła danych niż źródło danych produktu, najpierw utwórz źródło danych w zasięgu serwera lub klastra, stosując poprawną nazwę JNDI interfejsu jdbc/mashupDS, a następnie skonfiguruj produkt Business Space przy użyciu Konsoli administracyjnej.
- W przypadku bazy danych Oracle: aby w tabelach produktu Business Space użyć schematu innego niż schemat używany przez bazę danych produktu, wykonaj następujące kroki w celu ręcznego utworzenia źródła danych przed otwarciem strony Konfiguracja produktu Business Space:
 1. Utwórz schemat przy użyciu oprogramowania bazy danych produktu.
 2. Przy użyciu Konsoli administracyjnej skonfiguruj dostawcę JDBC.
 3. Użyj Konsoli administracyjnej, aby utworzyć źródło danych pod nazwą JNDI interfejsu jdbc/mashupDS w zasięgu serwera lub klastra, w zależności od środowiska.
 4. Utwórz alias uwierzytelniania przy użyciu Konsoli administracyjnej. Jako nazwę użytkownika ustaw nazwę utworzonego schematu, a uwierzytelnianie ustaw zgodnie z konfiguracją produktu Oracle.
 5. Ustaw alias uwierzytelniania w źródle danych.

W przypadku używania środowisk wdrażania lub innej zaawansowanej konfiguracji profilu należy użyć Konsoli administracyjnej, aby skonfigurować produkt Business Space do pracy ze środowiskiem wykonawczym. Produkt Business Space to przeznaczony dla użytkowników biznesowych i oparty na przeglądarce graficzny interfejs użytkownika aplikacji działającej w skonfigurowanym profilu. W produkcie Business Space użytkownik oraz użytkownicy korzystający z aplikacji użytkownika mogą dostosowywać treść z produktów z oferty produktów do zarządzania procesami biznesowymi WebSphere.

1. Upewnij się, że Konsola administracyjna została uruchomiona.
2. Na panelu nawigacyjnym kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere** lub **Serwery > Klastry > Klastry serwerów aplikacji WebSphere**.
3. Wybierz nazwę docelowego serwera lub klastra.
4. Kliknij opcję **Konfiguracja produktu Business Space** w sekcji **Integracja biznesowa** na stronie Konfiguracja. Zostanie wyświetlona strona Konfiguracja produktu Business Space. Jeśli produkt Business Space został już skonfigurowany, można przeglądać tę stronę, ale nie można edytować pól.
5. Zaznacz pole wyboru **Zainstaluj usługę Business Space**.
6. W polu **Nazwa schematu bazy danych** wpisz nazwę schematu bazy danych, która ma być używana na potrzeby bazy danych produktu Business Space.

Uwaga: W przypadku bazy Oracle schemat ma taką samą nazwę jak nazwa użytkownika skonfigurowana w aliasie uwierzytelniania w źródle danych.

7. Jeśli w polu **Istniejące źródło danych produktu Business Space** nie zostało określone żadne źródło danych, przejdź do opcji **Utwórz źródło danych produktu Business Space za pomocą** i wybierz źródło danych łączące się z bazą danych, która ma być używana z produktem Business Space.

Wybór źródła danych z użyciem opcji **Utwórz źródło danych produktu Business Space za pomocą**: powoduje utworzenie źródła danych dla produktu Business Space z nazwą JNDI obiektu jdbc/mashupDS modelowanego w wybranym źródle danych.

Źródło danych produktu Business Space jest tworzone na serwerze lub w klastrze stanowiącym miejsce konfiguracji produktu Business Space, nawet jeśli źródło danych produktu znajduje się na innym serwerze lub w innym klastrze.

Wskazówka: Jeśli istniejące źródło danych, które ma być używane, nie jest wyświetlane, należy anulować stronę Konfiguracja produktu Business Space, skonfigurować bazę danych i żądane źródło danych, a następnie przejść ponownie na stronę Konfiguracja produktu Business Space w celu zakończenia procesu konfiguracji. Więcej informacji zawiera sekcja **Zanim rozpocznie**.

8. Kliknij przycisk **OK**.
9. Aby zarejestrować odpowiednie miejsce docelowe wdrażania (klastrer lub serwer) dla punktów końcowych usługi REST systemu w przypadku każdego z widgetów używanych w produkcie Business Space, kliknij opcję **Rejestracja punktów końcowych usług REST**.

Miejsce docelowe wybrane dla typu punktu końcowego usługi REST może spowodować ustawienie zasięgu danych wyświetlanych w niektórych widgetach. Możliwe jest także wybranie konkretnego klastra lub serwera w celu zwiększenia wydajności i dostępności.

Jeśli używane są widgety zarządzania czynnościami personelu, można wybrać więcej niż jednego dostawcę usług REST na serwer lub klastrer w wierszu określającym typy usług procesów i usług zadań. Należy wybrać dostawcę o nazwie **Name=Federated REST Services** (Stowarzyszone usługi REST), **Name=Business Process Choreographer REST services** (Usługi REST produktu Business Process Choreographer) lub **Name=BPD engine REST services** (Usługi REST mechanizmu BPD). Jeśli zadania i procesy są uruchamiane zarówno w produkcie Business Process Choreographer, jak i w mechanizmie BPD (business process definition), należy wybrać

stowarzyszone usługi REST. Jeśli używane są tylko procesy i zadania uruchamiane w produkcji Business Process Choreographer (modelowane w produkcji Integration Designer), należy wybrać usługi REST produktu Business Process Choreographer. Jeśli używane są tylko procesy i zadania uruchamiane w mechanizmie BPD (modelowane w produkcji Process Designer), należy wybrać mechanizm BPD.

Jeśli miejsce docelowe nie zostanie określone, punkt końcowy usługi REST tego typu nie zostanie zarejestrowany w produkcji Business Space i żadne widżety wymagające punktu końcowego usługi REST tego typu nie będą widoczne w produkcji Business Space.

10. Zapisz konfigurację.
11. Przed uruchomieniem środowiska wdrażania lub klastrów uruchom skrypty w celu skonfigurowania tabel bazy danych dla produktu Business Space. Skrypty zostały wygenerowane podczas wykonywania czynności konfiguracyjnych przez użytkownika. Więcej informacji na ten temat można znaleźć w sekcji Konfigurowanie bazy danych produktu Business Space.

Uwaga: W przypadku używania produktu Oracle hasło aliasu uwierzytelniania źródła danych produktu Business Space jest ustawione na taką samą wartość jak nazwa schematu produktu Business Space. Wartość domyślna dla schematu to IBMBUSSP. Podczas konfigurowania produktu Business Space można określić inny schemat w Konsoli administracyjnej lub w wierszu komend. W tym przypadku domyślne hasło jest takie samo jak określony schemat. Jeśli dla nazwy użytkownika produktu Business Space ma być używane inne hasło, należy użyć Konsoli administracyjnej w celu zaktualizowania zasobów JDBC. W tym celu należy znaleźć źródło danych jdbc/mashupDS. Wartość aliasu uwierzytelniania należy zmodyfikować tak, aby był zgodny z hasłem nazwy schematu produktu Business Space. Następnie należy zapisać zmiany i zrestartować serwer.

Uwaga: Produkt Business Space używa komponentu proxy w celu nawiązywania połączeń z usługami REST. W niektórych przypadkach, jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia między produktem Business Space a usługami REST w zależności od wydajności serwerów usługi REST. Więcej informacji zawiera temat Zmienianie ustawień limitu czasu dla proxy Ajax produktu Business Space.

Konfigurowanie produktu Business Space przy użyciu wiersza komend:

Produkt Business Space oparty na technologii WebSphere można skonfigurować przy użyciu komendy wsadmin. Komenda wsadmin może zostać użyta do wykonania tych samych czynności konfiguracyjnych dla produktu Business Space, które można wykonać w Konsoli administracyjnej.

Zanim rozpoczniesz tę czynność, musisz wykonać następujące czynności:

- Zainstaluj oprogramowanie produktu i utwórz profil. Podczas instalacji produktu są instalowane pliki produktu Business Space na potrzeby konfigurowanych profili. Profil użytkownika nie zostanie skonfigurowany dla produktu Business Space do czasu jawnego skonfigurowania produktu Business Space w profilu.
- Włącz zabezpieczenia, jeśli ma zostać skonfigurowane zabezpieczone środowisko dla produktu Business Space.
- Jeśli planowane jest użycie pliku projektu bazy danych na potrzeby informacji dotyczących bazy danych produktu Business Space, wykonaj kroki opisane w sekcji “Tworzenie pliku właściwości projektu bazy danych produktu Business Space” na stronie 204.
- Skonfiguruj usługi REST (Representational State Transfer). Jeśli użytkownik korzysta ze środowiska serwera autonomicznego lub konfiguruje środowisko wykonawcze za pomocą kreatora środowiska wdrażania, punkty końcowe usługi REST są konfigurowane i włączane automatycznie. W przypadku innych środowisk w celu skonfigurowania usług

REST należy użyć strony usług REST w Konsoli administracyjnej. Jeśli widgety mają być dostępne w produkcie Business Space, dla tych widжетów należy skonfigurować punkty końcowe usługi REST. Aby produkt Business Space powiązał widgety z punktami końcowymi, a same widgety zostały udostępnione do użycia na palecie, konieczne jest zarejestrowanie punktów końcowych usługi REST.

- Aby skonfigurować produkt Business Space na serwerze lub w klastrze przy użyciu źródła danych innego niż źródło danych produktu, najpierw utwórz źródło danych w zasięgu serwera lub klastra, używając poprawnej nazwy JNDI interfejsu jdbc/mashupDS (przed uruchomieniem komendy `configureBusinessSpace`).
- W przypadku bazy danych Oracle, aby użyć innego schematu dla tabel produktu Business Space niż schemat używany przez bazę danych produktu, przed uruchomieniem komend służących do instalowania i konfigurowania produktu Business Space wykonaj następujące kroki w celu ręcznego utworzenia źródła danych:
 - Przy użyciu Konsoli administracyjnej skonfiguruj dostawcę JDBC.
 - Użyj Konsoli administracyjnej, aby utworzyć źródło danych pod nazwą JNDI interfejsu jdbc/mashupDS w zasięgu serwera lub klastra, w zależności od środowiska.

Jeśli produkt Business Space ma zostać skonfigurowany przy użyciu skryptów utworzonych przez użytkownika, a nie za pomocą Konsoli administracyjnej, do skonfigurowania produktu Business Space można użyć wiersza komend.

W przypadku braku pewności, czy produkt Business Space jest już skonfigurowany, można uruchomić komendę `getBusinessSpaceDeployStatus`, aby sprawdzić, czy produkt Business Space skonfigurowano na serwerze, w klastrze lub w komórce. Więcej informacji na temat tej komendy zawiera sekcja Komenda `getBusinessSpaceDeployStatus`.

Aby skonfigurować produkt Business Space, wykonaj następujące kroki:

1. Otwórz okno komend.

Komenda `wsadmin` jest dostępna w katalogu `katalog_główny_profilu/bin` w środowisku serwera autonomicznego lub w katalogu `katalog_główny_profilu_menedżera_wdrażania/bin` w środowisku wdrożenia sieciowego.

2. W wierszu komend wpisz komendę `wsadmin`, aby uruchomić środowisko `wsadmin`.
3. Przy użyciu komendy `installBusinessSpace` zainstaluj w środowisku wykonawczym pliki archiwum korporacyjnego (EAR) produktu Business Space.
4. Przy użyciu komendy `configureBusinessSpace` skonfiguruj źródło danych dla produktu Business Space i skopiuj skrypty służące do konfigurowania tabel bazy danych do katalogu `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_węzła_nazwa_serwera/typ_bazy_danych/nazwa_bazy_danych` (w przypadku serwera autonomicznego) lub do katalogu `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_klastra/typ_bazy_danych/nazwa_bazy_danych` (w przypadku klastra).

Należy uruchomić skrypty służące do konfigurowania tabel bazy danych. Więcej informacji o skryptach zawiera temat “Konfigurowanie bazy danych produktu Business Space” na stronie 205.

Jeśli na potrzeby konfiguracji bazy danych jest używany plik projektu bazy danych, można skorzystać z parametru **-bspacedbDesign**, aby określić ten plik podczas uruchamiania komendy `configureBusinessSpace`.

5. Po wykonaniu każdej komendy uruchom komendę `AdminConfig.save` (Jython) lub komendę `$AdminConfig save` (Jacl).
6. Przed uruchomieniem środowiska wdrażania lub klastrów uruchom skrypty w celu skonfigurowania tabel bazy danych dla produktu Business Space. Więcej informacji zawiera temat Konfigurowanie tabel bazy danych produktu Business Space.

Konfigurowanie produktu Business Space obejmuje skonfigurowanie graficznego interfejsu użytkownika opartego na przeglądarce na potrzeby użytkowników biznesowych aplikacji działającej ze skonfigurowanym profilem. W produkcie Business Space użytkownik oraz użytkownicy korzystający z aplikacji użytkownika mogą dostosowywać treść z produktów z oferty produktów do zarządzania procesami biznesowymi WebSphere.

W poniższym przykładzie użyto języka Jython do uruchomienia komend `installBusinessSpace` i `configureBusinessSpace` w celu zainstalowania plików EAR i skonfigurowania źródła danych na potrzeby produktu Business Space w klastrze. Przykład określa schemat i bazę danych produktu, które mają być używane z produktem Business Space, jeśli zainstalowanych jest wiele produktów. W sytuacji, w której zainstalowany jest zarówno produkt IBM Business Process Manager, jak i IBM Business Monitor, ten przykład tworzy źródło danych produktu Business Space przy użyciu właściwości źródła danych produktu IBM Business Process Manager.

```
AdminTask.installBusinessSpace('[-clusterName mójKlaster -save true]')
AdminTask.configureBusinessSpace('[-clusterName
mójKlaster -schemaName mójSchemat -productTypeForDatasource
WPS -save true]')
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask installBusinessSpace {-clusterName mójKlaster -save true}
$AdminTask configureBusinessSpace {-clusterName
mójKlaster -schemaName mójSchemat -productTypeForDatasource
WPS -save true}
```

Wskazówka: Jeśli używana jest baza danych Oracle, hasło aliasu uwierzytelniania dla źródła danych produktu Business Space jest ustawione na taką samą nazwę, jak nazwa schematu produktu Business Space. Wartość domyślna dla schematu to `IBMBUSSP`. Podczas konfigurowania produktu Business Space można określić inny schemat w Konsoli administracyjnej lub w wierszu komend. W tym przypadku domyślne hasło jest takie samo jak określony schemat. Jeśli dla nazwy użytkownika produktu Business Space ma być używane inne hasło, należy użyć Konsoli administracyjnej w celu zaktualizowania zasobów JDBC. W tym celu należy znaleźć źródło danych `jdbc/mashupDS`. Wartość aliasu uwierzytelniania należy zmodyfikować tak, aby był zgodny z hasłem nazwy schematu produktu Business Space. Następnie należy zapisać zmiany i zrestartować serwer.

Po skonfigurowaniu produktu Business Space wykonaj następujące kroki, aby włączyć produkt Business Space dla środowiska wykonawczego użytkownika:

- Zarejestruj punkty końcowe za pomocą komendy `registerRESTserviceEndpoint`.
- Skonfiguruj zabezpieczenia, które mają być używane z produktem Business Space oraz widgetami używanymi przez zespół użytkownika. Więcej informacji na ten temat zawiera sekcja Konfigurowanie zabezpieczeń dla produktu Business Space.

Wskazówka: Produkt Business Space używa komponentu proxy w celu nawiązywania połączeń z usługami REST. W niektórych przypadkach, jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia między produktem Business Space a usługami REST w zależności od wydajności serwerów usługi REST. Więcej informacji zawiera temat Zmienianie ustawień limitu czasu dla proxy Ajax produktu Business Space.

Tworzenie pliku właściwości projektu bazy danych produktu Business Space:

Jeśli typ bazy danych produktu Business Space użytkownika jest inny niż domyślny, należy utworzyć plik właściwości projektu bazy danych, aby uprościć proces tworzenia bazy danych.

Szablony plików projektów dla każdego typu bazy danych są udostępnione w katalogu *instalacyjny_katalog_główny/BusinessSpace/config.bspace/MetadataFiles*; na przykład szablon pliku projektu dla bazy danych DB2 ma nazwę *BSpace_DB2-distributed.properties*.

1. Utwórz nowy plik, tworząc kopię pliku szablonu odpowiedniego dla używanej bazy danych.
2. Zmień wartości ustawień właściwości w pliku właściwości projektu bazy danych zgodnie z używaną konfiguracją. W pliku zamieszczono komentarze ułatwiające wybranie poprawnych wartości właściwości.

Należy podać pełną ścieżkę do pliku właściwości projektu bazy danych w jednym z następujących miejsc, w zależności od środowiska produktu i preferencji konfiguracji:

- Jeśli do konfigurowania produktu Business Space przy użyciu profilu używane jest narzędzie Profile Management Tool, należy wskazać plik projektu bazy danych, wybierając opcję **Użyj pliku projektu bazy danych**.
- Jeśli do konfigurowania produktu Business Space przy użyciu profilu używany jest program narzędziowy wiersza komend `manageprofiles`, należy wskazać plik projektu bazy danych za pomocą parametru **-bspacedbDesign**.
- Jeśli do konfigurowania produktu Business Space używana jest komenda `configureBusinessSpace`, należy wskazać plik projektu bazy danych za pomocą parametru **-bspacedbDesign**.

Konfigurowanie bazy danych produktu Business Space:

Tabele bazy danych produktu Business Space można zainstalować ręcznie na zdalnym serwerze bazy danych przy użyciu skryptów wygenerowanych przez program instalacyjny. Jeśli jest używane środowisko wdrażania lub jeśli baza danych jest zdalna, należy zainstalować te tabele po skonfigurowaniu produktu Business Space.

Przed wykonaniem tej czynności należy wykonać następujące czynności:

- Zainstaluj produkt.
- Utwórz profile i skonfiguruj serwery lub klastry na potrzeby produktu Business Space.
- W przypadku bazy danych Oracle: utwórz bazę danych.
- W przypadku produktu Microsoft SQL Server: ustaw uwierzytelnianie instancji produktu SQL Server. Sterownik JDBC produktu SQL Server obsługuje jedynie tryb mieszany uwierzytelniania. W związku z tym podczas tworzenia instancji produktu SQL Server uwierzytelnianie musi zostać ustawione na wartość **SQL Server i Windows**.
- W przypadku wszystkich baz danych należy się upewnić, że są one instalowane z użyciem uniwersalnego zestawu znaków UTF-8, jeśli produkt Business Space ma być używany w środowisku użytkownika.
- Upewnij się, że serwer aplikacji z produktem Business Space został zatrzymany.

Jeśli używana baza danych to DB2 for z/OS, a wymagane zasoby nie zostały jeszcze ustawione w ramach podstawowej instalacji produktu, przed rozpoczęciem tej czynności wykonaj następujące czynności dodatkowe:

- Utwórz bazę danych TEMP oraz obszar tabel TEMP, które będą zawierały zadeklarowane tabele tymczasowe używane do przetwarzania kursorów przewijalnych.
- Utwórz dedykowaną grupę STOGROUP, która będzie zawierać dane produktu Business Space.

Jeśli w przypadku bazy danych DB2 for z/OS ma zostać użyta inna grupa pamięci masowych (na przykład w sytuacji, gdy tabele bazy danych produktu Business Space nie mają być dodawane do tej samej bazy danych i grupy pamięci masowych co wspólna baza danych),

dokonaj edycji skryptu `createTablespace_BusinessSpace.sql`, a następnie go uruchom po skonfigurowaniu produktu Business Space, ale przed skonfigurowaniem tabel bazy danych produktu Business Space.

- Otwórz w edytorze plik `createTablespace_BusinessSpace.sql` dostępny w następującym położeniu: `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_węzła_nazwa_serwera/typ_bazy_danych/nazwa_bazy_danych` dla serwera autonomicznego lub `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_klastra/typ_bazy_danych/nazwa_bazy_danych` dla klastra, gdzie `typ_bazy_danych` to DB2zOS.
- Zmień wartość parametru VCAT z @VCAT@ na nazwę lub alias katalogu funkcji zintegrowanego wpisywania do katalogu dla grupy pamięci masowych, która będzie używana.

Jeśli używana jest baza danych DB2 9.x i ma zostać poprawiona wydajność, dokonaj edycji pliku `createTablespace_BusinessSpace.sql`. Plik

`createTablespace_BusinessSpace.sql` jest dostępny w następującym położeniu:

`katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_węzła_nazwa_serwera/typ_bazy_danych/nazwa_bazy_danych` dla serwera autonomicznego lub `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_klastra/typ_bazy_danych/nazwa_bazy_danych` dla klastra.

- Zmień wartość `IMMEDIATE SIZE 8000 PAGESIZE 32K` na `IMMEDIATE SIZE 8000 AUTOMATIC PAGESIZE 32K`.
- Dodaj wiersz `PREFETCHSIZE AUTOMATIC` po wierszu `EXTENTSIZE 16`, a pod wierszami `CREATE SYSTEM TEMPORARY TABLESPACE @TSDIR@TMPTP` i `CREATE REGULAR TABLESPACE @TSDIR@REGTP`.

Skrypt `configBusinessSpaceDB` służy do konfigurowania tabel dla produktu Business Space z określoną bazą danych. Aby utworzyć table w istniejącej bazie danych, ale innej niż określona, należy użyć w produkcie skryptu `createDBTables` zamiast skryptu `configBusinessSpaceDB`.

Aby skonfigurować table bazy danych dla produktu Business Space, wykonaj następujące kroki.

1. Upewnij się, że używany identyfikator użytkownika ma wystarczające uprawnienia do tworzenia tabel.
2. Znajdź skrypt w profilu, który był ostatnio konfigurowany, a następnie zapisz ten skrypt w położeniu w tym samym systemie, w którym działa baza danych.
 - W przypadku wszystkich baz danych oprócz bazy danych DB2 for z/OS należy znaleźć skrypt `configBusinessSpaceDB.bat` lub `configBusinessSpaceDB.sh`.
 - W przypadku produktu WebSphere Enterprise Service Bus for z/OS, jeśli table bazy danych produktu Business Space mają być konfigurowane ze wszystkimi innymi obiektami baz danych, należy znaleźć skrypt `createDB.sh`.
 - Jeśli w przypadku bazy danych DB2 for z/OS nie zostanie uruchomiony skrypt `createDB.sh`, pliki produktu Business Space należy uruchamiać pojedynczo. Należy znaleźć pliki `createDatabase.sql`, `createStorageGroup_BusinessSpace.sql`, `createTablespace_BusinessSpace.sql` oraz `createTable_BusinessSpace.sql`.

Domyślnie skrypty znajdują się w następującym katalogu: `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_węzła_nazwa_serwera/typ_bazy_danych/nazwa_bazy_danych` dla serwera autonomicznego lub `katalog_główny_profilu/dbscripts/BusinessSpace/nazwa_klastra/typ_bazy_danych/nazwa_bazy_danych` dla klastra. Zaktualizowane skrypty (wraz z informacjami wprowadzonymi podczas tworzenia profilu) znajdują się w profilu dla serwera lub klastra, który był ostatnio konfigurowany. Jeśli został użyty kreator konfiguracji środowiska wdrażania, to skrypty

znajdują się w profilu menedżera wdrażania. Podczas konfigurowania zdalnej bazy danych należy skopiować skrypty z systemu, w którym zainstalowano produkt, do lokalizacji w systemie zdalnym.

3. **Dla produktu WebSphere Enterprise Service Bus for z/OS:** w przypadku konfigurowania produktu DB2 for z/OS można użyć skryptu `createDB.sh` w celu skonfigurowania tabel bazy danych produktu Business Space wraz ze wszystkimi innymi obiektami bazy danych w jednej bazie danych. Więcej informacji zawiera temat Tworzenie obiektów bazy danych DB2 za pomocą skryptu `createDB.sh` znajdujący się w dokumentacji produktu WebSphere Enterprise Service Bus for z/OS.

4. Otwórz wiersz komend i w zależności od platformy uruchom jedną z następujących komend:

Skopiuj folder z plikami wsadowymi i skryptami do tego samego położenia, w którym znajduje się baza danych, a następnie uruchom komendę w tym położeniu. Identyfikator użytkownika musi mieć przypisane uprawnienia dostępu do interpretera wiersza komend dla danego typu bazy danych oraz uprawnienia do uruchamiania komend.

-   **Na platformach Linux, UNIX i z/OS:**
`configBusinessSpaceDB.sh`




-  **Na platformach Windows:** `configBusinessSpaceDB.bat`

W przypadku baz danych DB2 i SQL Server należy użyć opcjonalnego parametru `-createDB`, jeśli zamiast istniejącej bazy danych ma zostać utworzona i użyta inna baza danych.

Ograniczenie: W przypadku używania produktu SQL Server po uruchomieniu skryptu bazy danych w pliku `systemout.log` zostaną umieszczone następujące ostrzeżenia o błędach: ... Ostrzeżenie! Maksymalna długość klucza to 900 bajtów Te ostrzeżenia można zignorować, jeśli jako rejestr użytkowników używane są repozytoria stowarzyszone. Jeśli jest używany autonomiczny rejestr LDAP, należy upewnić się, że liczba znaków we wszystkich pozycjach nazw wyróżniających użytkowników w organizacji nie przekracza limitu wynoszącego 131 znaków. Jeśli liczba znaków w dowolnej nazwie wyróżniającej użytkownika przekroczy 131 znaków, należy zmienić rejestr kont użytkowników, wybierając opcję repozytoriów stowarzyszonych.

W przypadku produktu DB2 for z/OS należy uruchomić poniższe pliki w podanej kolejności:

- `createDatabase.sql`
- `createStorageGroup_BusinessSpace.sql`
- `createTablespace_BusinessSpace.sql`
- `createTable_BusinessSpace.sql`

5.    W przypadku korzystania z baz danych DB2 i DB2 for z/OS utwórz powiązanie interfejsu wiersza komend z bazą danych produktu Business Space za pomocą następujących komend:

```
db2 connect to nazwa_bazy_danych
db2 bind katalog_instalacyjny_DB2\bnd\@db2cli.lst blocking all grant public
db2 connect reset
```

, gdzie:

Zmienna `nazwa_bazy_danych` jest nazwą bazy danych produktu Business Space.

Zmienna `katalog_instalacyjny_DB2` określa katalog, w którym zainstalowano bazę danych DB2.

6. W przypadku ponownego tworzenia bazy danych produktu Business Space po jej wcześniejszym usunięciu konieczne jest zaimportowanie szablonów i obszarów produktu Business Space przed użyciem środowiska Business Space. Wykonaj kroki przedstawione

w sekcji Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.

- Zaktualizuj punkty końcowe widgetów, które mają być dostępne w produkcie Business Space.
- Skonfiguruj zabezpieczenia produktu Business Space i widgety, które są używane przez zespół.

Rejestrowanie punktów końcowych usługi REST widgetu produktu Business Space przy użyciu wiersza komend:

Jeśli produkt Business Space jest konfigurowany za pomocą Konsoli administracyjnej, należy zarejestrować punkty końcowe usługi REST (Representational State Transfer) w celu umożliwienia zespołowi korzystania z widgetów w produkcie Business Space. Jeśli punkty końcowe nie zostaną zarejestrowane w Konsoli administracyjnej przy użyciu stron Konfiguracja produktu Business Space i Rejestracja punktów końcowych usługi REST systemu, można je zarejestrować przy użyciu komendy `registerRESTServiceEndpoint`.

Przed wykonaniem tej czynności należy wykonać następujące czynności:

- Zainstaluj produkt.
- Skonfiguruj usługi REST dla widgetów używanych w produkcie Business Space przy użyciu strony Usługi REST w Konsoli administracyjnej lub komendy `updateRESTGatewayService`. Jeśli użytkownik dysponuje środowiskiem serwera autonomicznego lub jeśli konfiguruje środowisko wykonawcze za pomocą kreatora środowiska wdrażania, usługi REST są konfigurowane i włączane automatycznie.
- Skonfiguruj produkt Business Space za pomocą strony Konfiguracja produktu Business Space Konsoli administracyjnej lub komend `installBusinessSpace` i `configureBusinessSpace`.
- Skonfiguruj tabele bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrożenia sieciowego).

Usługi REST są rejestrowane automatycznie, jeśli użytkownik dysponuje środowiskiem serwera autonomicznego, a produkt Business Space został skonfigurowany przy użyciu Konsoli administracyjnej lub narzędzia Profile Management Tool, bądź jeśli środowisko wykonawcze zostało skonfigurowane przy użyciu kreatora środowiska wdrażania. W przeciwnym razie użytkownik musi sam skonfigurować i zarejestrować usługi REST.

Zarejestrowanie punktów końcowych usług REST dla wszystkich widgetów w produkcie Business Space jest możliwe za pomocą strony Rejestracja punktów końcowych usługi REST systemu w Konsoli administracyjnej oraz komendy `registerRESTServiceEndpoint`. Następnie produkt Business Space automatycznie tworzy powiązania widgetów z tymi punktami końcowymi, co pozwala na wyświetlenie tych widgetów do użycia na palecie produktu Business Space.

Komenda `registerRESTServiceEndpoint` pozwala na zarejestrowanie zbioru punktów końcowych dla danego dostawcy, miejsca docelowego wdrażania lub wszystkich unikalnych punktów końcowych w komórce. Przy użyciu tej komendy można zarejestrować punkty końcowe usług REST, które znajdują się w tej samej komórce co produkt Business Space.

1. Otwórz okno komend.

Komenda `wsadmin` jest dostępna w katalogu `katalog_główny_profilu/bin` w środowisku serwera autonomicznego lub w katalogu `katalog_główny_profilu_menedżera_wdrażania/bin` w środowisku wdrożenia sieciowego.

2. W wierszu komend wpisz komendę `wsadmin`, aby uruchomić środowisko `wsadmin`.

3. Użyj komendy `registerRESTServiceEndpoint`, aby zarejestrować punkty końcowe usług REST dla wszystkich widgetów produktu Business Space.
4. Po każdej komendzie wykonaj komendę `save`.

W następującym przykładzie użyto języka Jython do uruchomienia komendy `registerRESTServiceEndpoint` i późniejszego zapisania zmian. Ta komenda rejestruje w produkcie Business Space wszystkie usługi REST, które są skonfigurowane i włączone w klastrze.

```
AdminTask.registerRESTServiceEndpoint('[-clusterName  
nazwa_klastra_uslug_REST -businessSpaceClusterName  
nazwa_klastra_produkту_Business_Space]')  
AdminConfig.save()
```

gdzie *nazwa_klastra_uslug_REST* jest nazwą klastra, w którym skonfigurowano usługi REST, a *nazwa_klastra_produkту_Business_Space* jest nazwą klastra, w którym wdrożono produkt Business Space.

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask registerRESTServiceEndpoint  
{-clusterName nazwa_klastra_uslug_REST  
-businessSpaceClusterName  
nazwa_klastra_produkту_Business_Space}  
$AdminConfig save
```

gdzie *nazwa_klastra_uslug_REST* jest nazwą klastra, w którym skonfigurowano usługi REST, a *nazwa_klastra_produkту_Business_Space* jest nazwą klastra, w którym wdrożono produkt Business Space.

Parametry **appName**, **webModuleName**, **type**, **name**, **version**, **nodeName**, **serverName** i **clusterName** są opcjonalne.

Jeśli parametry **type**, **appName** i **webModuleName** nie zostaną określone, zarejestrowane zostaną wszystkie unikalne punkty końcowe usługi REST skonfigurowane w danym miejscu docelowym wdrażania.

Jeśli nie zostanie określony żaden z tych parametrów, zarejestrowane zostaną wszystkie unikalne punkty końcowe usługi REST skonfigurowane w dowolnym miejscu docelowym wdrażania.

Wskazówka: Produkt Business Space używa komponentu proxy w celu nawiązywania połączeń z usługami REST. W niektórych przypadkach, jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia między produktem Business Space a usługami REST w zależności od wydajności serwerów usługi REST. Więcej informacji zawiera temat Zmianianie ustawień limitu czasu dla proxy Ajax produktu Business Space.

Konfigurowanie serwera proxy lub serwera równoważenia obciążenia pod kątem użycia z produktem Business Space:

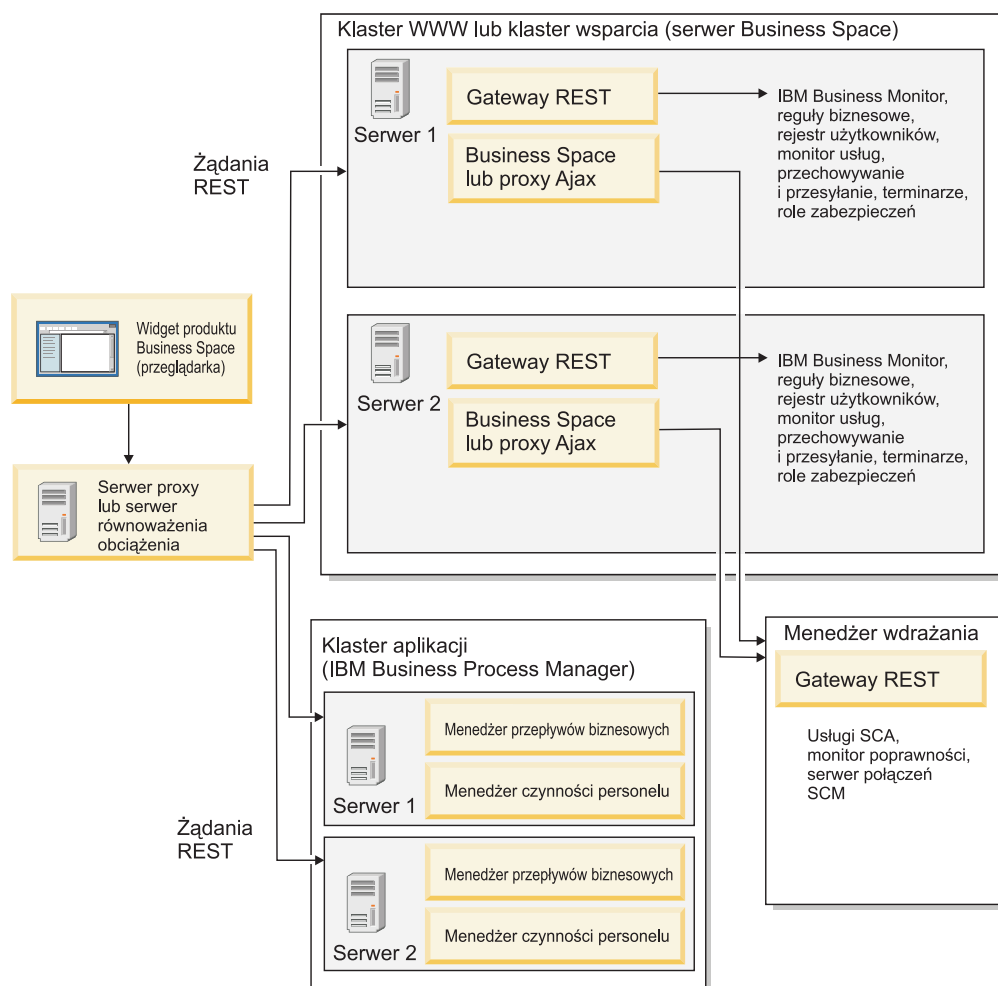
W przypadku używania produktu Business Space w środowisku z serwerem proxy lub serwerem równoważenia obciążenia należy skonfigurować środowisko użytkownika. Pozwoli to na poprawne działanie produktu Business Space oraz widgetów.

W środowisku wdrażania sieciowego lub w środowisku klastrowym ze względów bezpieczeństwa oraz na potrzeby równoważenia obciążenia może być konieczne skonfigurowanie serwera proxy lub serwera HTTP. Przychodzące żądania HTTP nie są kierowane bezpośrednio do serwera aplikacji. Zamiast tego są kierowane do serwera proxy, który może je rozesłać do wielu serwerów aplikacji obsługujących żądanie.

Zamiast serwera proxy lub „przed” nim można używać innych serwerów kierujących, na przykład serwera IBM HTTP Server.

Ważne: Serwer proxy (lub alternatywny serwer kierujący) jest wymagany do równoważenia obciążenia przez rozdzielanie żądań HTTP między dwa lub więcej elementów klastra. Serwer proxy umożliwia klientom uzyskiwanie dostępu do aplikacji w obrębie tej topologii.

W środowisku z serwerem równoważenia obciążenia lub serwerem proxy między przeglądarką, produktem Business Space i usługami REST należy upewnić się, że wartości wyznaczone dla protokołu usług REST, hosta i portu są zgodne z wartościami w adresie URL wprowadzanym w przeglądarce w celu uzyskania dostępu do produktu Business Space. Na stronie dostawców usługi REST w Konsoli administracyjnej należy sprawdzić, czy wszyscy dostawcy (na przykład menedżer przepływów biznesowych i menedżer czynności personelu) mają ustawiony poprawny protokół, host i port. Więcej informacji na temat modyfikowania usług REST zawiera temat Konfigurowanie usług REST w dostawcy usług.



Rysunek 1. Typowa topologia

Jeśli jest używany serwer IBM HTTP Server, należy wykonać dodatkowe kroki związane z odwzorowaniem w celu sprawdzenia, czy moduły zostały odwzorowane na serwer WWW, a także czy aliasy hosta zostały skonfigurowane.

Jeśli jest używany serwer proxy WebSphere Application Server, należy się upewnić, że wszystkie moduły zostały włączone dla tego serwera proxy.

W przypadku używania konfiguracji odwrotnego proxy dla serwera HTTP należy odwzorować adresy URL dla produktu Business Space i widgetów.

Konfigurowanie produktu IBM HTTP Server na potrzeby produktu Business Space:

W przypadku używania produktu IBM HTTP Server należy wykonać dodatkowe kroki dotyczące odwzorowania, aby produkt Business Space działał w środowisku użytkownika.

Przed skonfigurowaniem produktu IBM HTTP Server na potrzeby współpracy z produktem Business Space wykonaj następujące kroki:

- Zainstaluj produkt IBM HTTP Server.
- Włącz protokół SSL (Secure Sockets Layer) dla produktu IBM HTTP Server.
- Dodaj definicję serwera WWW dla produktu IBM HTTP Server do serwera aplikacji.
Podczas instalacji wtyczki produktu IBM HTTP Server na komputerze serwera WWW proces instalacji generuje skrypt `configureserver_WWW`. Skrypt `configureserver_WWW` służy do odwzorowywania modułów aplikacji WWW na serwer WWW. Oznacza to, że ten skrypt należy uruchomić po wygenerowaniu środowiska wdrażania.

1. Upewnij się, że moduły zostały odwzorowane na serwer WWW. W przypadku każdej aplikacji wymaganej przez produkt Business Space należy sprawdzić, czy serwer WWW jest jednym z wybranych miejsc docelowych.

- a. Zaloguj się do Konsoli administracyjnej jako administrator.
- b. Kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.
- c. Na panelu Aplikacje korporacyjne kliknij nazwę aplikacji.

Należy sprawdzić następujące aplikacje. Na liście może się znajdować jedna lub kilka aplikacji, zależnie od tego, które produkty są używane z produktem Business Space.

- **BPMAdministrationWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - **BusinessSpaceHelpEAR_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **BSpaceEAR_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **BSpaceForms_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **HumanTaskManagementWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktów IBM Business Process Manager i IBM Business Monitor)
 - **Brama usług REST** (w przypadku wszystkich produktów)
 - **Menedżer wdrażania bramy usług REST** (w przypadku produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - **mm.was_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **WBMDashboardWeb_nazwa_węzła_nazwa_serwera** (w przypadku produktu IBM Business Monitor)
 - **wesbWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktu WebSphere Enterprise Service Bus)
- d. W przypadku każdej aplikacji na karcie Konfiguracja w obszarze Moduły kliknij opcję **Zarządzaj modułami**.
 - e. Na stronie Zarządzanie modułami aplikacji upewnij się, że jednym z wybranych miejsc docelowych dla poszczególnych modułów użytkownika jest serwer WWW.

- W tabeli sprawdź kolumnę Serwer dla każdego modułu, aby upewnić się, że serwer WWW jest jednym z wybranych miejsc docelowych dla poszczególnych modułów użytkownika. Na przykład w przypadku aplikacji mm.was_nazwa_węzła_nazwa_serwera znajdź serwer WWW, który ma zostać wyświetlony w kolumnie Serwer:
WebSphere:cell=qaxs41Cell02,node=qaxs41Node03,server=httpsrserver
WebSphere:cell=qaxs41Cell02,cluster=Golden.WebApp.
 - Jeśli konieczne jest dodanie serwera WWW, zaznacz pole wyboru obok nazwy modułu. Następnie na liście Klastry i serwery zaznacz przy użyciu klawisza Ctrl wiele miejsc docelowych. Aby na przykład serwer WWW obsługiwał aplikację użytkownika, naciśnij klawisz Ctrl, a następnie wybierz razem klaster serwerów aplikacji oraz serwer WWW. Kliknij przycisk **Zastosuj**, przycisk **OK**, a następnie przycisk **Zapisz** w celu zapisania wprowadzonych zmian.
2. Sprawdź, czy alias nazwy hosta **default_host** zawiera poprawne informacje dla każdego elementu klastra, serwera WWW lub serwera proxy.
 - a. Zaloguj się do Konsoli administracyjnej jako administrator.
 - b. Kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere**.
 - c. Dla poszczególnych elementów klastra kliknij nazwę serwera aplikacji, aby wyświetlić numer portu dla nazwy portu **WC_defaulthost**.
 - W obszarze Komunikacja należy rozwinąć pozycję **Porty**.
 - Należy zapamiętać numer portu o nazwie **WC_defaulthost**.
 - d. W lewym obszarze nawigacyjnym Konsoli administracyjnej kliknij opcję **Środowisko > Hosty wirtualne**.
 - e. Kliknij nazwę **default_host**.
 - f. W obszarze Właściwości dodatkowe kliknij opcję **Aliasy hosta**.
 - g. Jeśli nazwa hosta oraz numer portu dla elementów klastra nie są wyświetlane na liście, kliknij opcję **Nowy** w celu dodania brakującej pozycji do listy. Znak wieloznaczny * (znak gwiazdki) jest obsługiwany w przypadku nazwy hosta.
 - h. Jeśli zostanie dodana nowa pozycja, kliknij opcję **Zapisz**, a następnie opcję **Synchronizuj**.

Konfigurowanie serwera proxy produktu WebSphere Application Server na potrzeby produktu Business Space:

Jeśli jest używany serwer proxy serwera WebSphere Application Server, aby produkt Business Space działał w środowisku użytkownika należy upewnić się, że włączone są wszystkie moduły serwera proxy.

Przed skonfigurowaniem serwera proxy serwera WebSphere Application Server do pracy z produktem Business Space należy wykonać następujące kroki:

1. Upewnienie się, że zastosowano najnowszą wersję produktu WebSphere Application Server.
2. Utworzenie serwera proxy. W tym celu należy kliknąć opcję **Serwery > Typy serwerów > Serwery proxy WebSphere**. Więcej informacji zawiera temat Konfigurowanie serwera proxy w Centrum informacyjnym serwera WebSphere Application Server.
3. Upewnienie się, że wybrano protokół HTTP.
 1. Upewnij się, że moduły są odwzorowane na serwer proxy serwera WebSphere Application Server. W przypadku każdej aplikacji wymaganej przez produkt Business Space należy sprawdzić, czy moduły zostały włączone na potrzeby serwera proxy.
 - a. Zaloguj się do Konsoli administracyjnej jako administrator.
 - b. Wybierz opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**.

- c. Na panelu Aplikacje korporacyjne wybierz nazwę aplikacji.
Należy sprawdzić następujące aplikacje. Na liście może się znajdować jedna lub kilka aplikacji, zależnie od tego, które produkty są używane z produktem Business Space.
 - **BPMAdministrationWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - **BusinessSpaceHelpEAR_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **BSpaceEAR_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **BSpaceForms_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **HumanTaskManagementWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktów IBM Business Process Manager i IBM Business Monitor)
 - **Brama usług REST** (w przypadku wszystkich produktów)
 - **Menedżer wdrażania bramy usług REST** (w przypadku produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - **mm.was_nazwa_węzła_nazwa_serwera** (w przypadku wszystkich produktów)
 - **WBMDashboardWeb_nazwa_węzła_nazwa_serwera** (w przypadku produktu IBM Business Monitor)
 - **wesbWidgets_nazwa_węzła_nazwa_serwera** (w przypadku produktu WebSphere Enterprise Service Bus)
 - d. Dla każdej aplikacji na karcie **Konfiguracja** w obszarze **Moduły** kliknij opcję **Zarządzaj modułami**.
 - e. Na stronie Zarządzanie modułami dla aplikacji kliknij każdy moduł i wybierz opcję **Konfiguracja serwera proxy modułu WWW**.
 - f. Upewnij się, że jest wybrana opcja **Włącz serwer proxy**.
2. Sprawdź, czy alias nazwy hosta **default_host** zawiera poprawne informacje dla każdego elementu klastra, serwera WWW lub serwera proxy.
 - a. Zaloguj się do Konsoli administracyjnej jako administrator.
 - b. Wybierz opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere**.
 - c. Dla każdego elementu klastra wybierz nazwę serwera aplikacji, aby wyświetlić numer portu dla nazwy portu **WC_defaulthost**.
 - W obszarze Komunikacja należy rozwinąć pozycję **Porty**.
 - Należy zanotować numer portu dla nazwy portu **WC_defaulthost**.
 - d. W obszarze nawigacyjnym znajdującym się po lewej stronie Konsoli administracyjnej wybierz opcję **Środowisko > Hosty wirtualne**.
 - e. Kliknij opcję **default_host**.
 - f. W obszarze Właściwości dodatkowe kliknij opcję **Alias hosta**.
 - g. Jeśli nazwa hosta i numer portu danego elementu klastra nie są wyświetlane na liście, kliknij opcję **Nowy**, aby dodać do listy brakującą pozycję. W nazwie hosta można użyć znaku wieloznacznego * (gwiazdka).
 - h. Jeśli zostanie dodany nowy wpis, kliknij przycisk **Zapisz**, a następnie opcję **Synchronizuj**.
 3. Aby użyć protokołu HTTP, skonfiguruj serwer proxy serwera WebSphere Application Server.
 - a. Zaloguj się do Konsoli administracyjnej jako administrator.
 - b. Wybierz opcję **Serwery > Typy serwerów > Serwery proxy WebSphere** i wybierz wcześniej utworzony serwer proxy.
 - c. Rozwiń pozycję **Ustawienia serwera proxy HTTP** i kliknij opcję **Ustawienia serwera proxy**.

- d. Kliknij opcję **Właściwości niestandardowe** i dodaj nową właściwość o nazwie `cache.query.string` i wartości `true`.
- e. Kliknij przycisk **Zapisz** i zrestartuj serwer proxy.

Odwzorowywanie adresów URL produktu Business Space na serwer odwrotnego proxy:

Jeśli podczas konfigurowania serwera HTTP na potrzeby współdziałania z produktem Business Space istnieje konfiguracja odwrotnego proxy dla serwera HTTP, należy odwzorować adresy URL dla produktu Business Space oraz widgetów używanych przez zespół użytkownika.

1. Dokonaj edycji pliku konfiguracyjnego serwera HTTP.
2. Odwzoruj wszystkie adresy URL dla produktu Business Space oraz widgetów, z którymi pracują użytkownicy biznesowi w rozwiązaniu środowiska wykonawczego.

Adresy URL dla ogólnego środowiska produktu Business Space (wszystkie produkty):

- `/BusinessSpace/*`
- `/mum/*`
- `/help/*`
- `/BSpaceWebformsProxy/*`
- `/themes/*`
- `/pageBuilder2/*`

Dodatkowe adresy URL dla widgetów produktu IBM Business Monitor:

- `/BusinessDashboard/*`
- `/DashboardABX/*`
- `/monitorServerComponent/*`
- `/mobile/*`
- `/rest/*`
- `/p2pd/*`
- `/AlphabloxServer/*`
- `/AlphabloxAdmin/*`
- `/AlphabloxTooling/*`
- `/BloxBuilder/*`

Dodatkowe adresy URL dla widgetów produktu IBM Business Process Manager:

- `/BSpaceWidgetsHM/*`
- `/SecurityManagerWidgets/*`
- `/BSpaceWidgetsBCM/*`
- `/rest/*`
- `/PolymorphicWidget/*`
- `/scaWidget/*`
- `/ServiceMonitorGraphWidget/*`
- `/StoreAndForward/*`

Dodatkowe adresy URL dla widgetów produktu WebSphere Enterprise Service Bus:

- `/BSpaceWidgetsHM/*`
- `/rest/*`
- `/PolymorphicWidget/*`
- `/scaWidget/*`
- `/ServiceMonitorGraphWidget/*`
- `/StoreAndForward/*`

Włączanie funkcji API stowarzyszania w wielu miejscach docelowych wdrażania:

Funkcja API stowarzyszania umożliwia wyświetlanie procesów i zadań utworzonych w produktach Process Designer i Integration Designer na tej samej liście zadań. Jeśli środowisko zawiera wiele klastrów w tej samej komórce lub wiele komórek, należy ręcznie skonfigurować domeny stowarzyszenia za pomocą komend.

Zasięg tematu: Ten temat ma zastosowanie do następujących produktów:

- IBM Business Process Manager Advanced

Przed wykonaniem tej czynności należy wykonać następujące czynności:

- Zainstaluj produkt.
- Utwórz profile i skonfiguruj produkt Business Space w miejscu docelowym wdrażania (na serwerze lub w klastrze).
- Skonfiguruj tabele bazy danych (w przypadku używania zdalnej bazy danych lub środowiska wdrażania).

Funkcja API stowarzyszania jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend wsadmin.

1. Otwórz okno komend.

Komenda wsadmin jest dostępna w katalogu *katalog_główny_profilu/bin* w środowisku serwera autonomicznego lub w katalogu *katalog_główny_profilu_menedżera_wdrażania/bin* w środowisku wdrożenia sieciowego.

2. W wierszu komend wpisz komendę wsadmin, aby uruchomić środowisko wsadmin.
3. Użyj komendy createBPMApiFederationDomain, aby utworzyć domenę stowarzyszenia, a następnie wykonaj krok addTarget, aby dokonać stowarzyszenia tej domeny w jednym lub wielu miejscach docelowych wdrażania.

Parametr name musi mieć unikalną wartość *nazwa_domeny_stowarzyszenia*.

W następującym przykładzie dodano domenę stowarzyszenia o nazwie *niestandardowa_domena_stowarzyszenia*, która dokonuje stowarzyszenia na serwerze (nazwa węzła: *mój_węzeł*, nazwa serwera: *mój_serwer*) i w klastrze (o nazwie *mój_klaster*).

- Przykład kodu Jython:

```
AdminTask.createBPMApiFederationDomain(['-nodeName nazwa_węzła  
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia  
-addTarget [{"mój_węzeł mój_serwer"} [{"mój_klaster"}]])
```

- Przykład kodu Jacl:

```
$AdminTask createBPMApiFederationDomain {-nodeName nazwa_węzła  
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia  
-addTarget [{"mój_węzeł mój_serwer"} {"mój_klaster}}
```

W razie konieczności zmodyfikowania konfiguracji funkcji API stowarzyszania dostępne są inne komendy.

- Jeśli ma zostać usunięta domena stowarzyszenia wraz z zawartymi w niej miejscami docelowymi, należy użyć komendy deleteBPMApiFederationDomain.
- Do wyświetlania listy wszystkich domen stowarzyszenia służy komenda listBPMApiFederationDomains.
- Do dodawania miejsc docelowych do domeny stowarzyszenia oraz do ich usuwania służy komenda modifyBPMApiFederationDomain.

- Do wyświetlania szczegółów domeny stowarzyszenia służy komenda `showBPMApiFederationDomain`.

Włączanie widgetów produktu Business Space dla środowisk międzykomórkowych:

Pliki punktów końcowych należy edytować ręcznie, jeśli produkt Business Space jest uruchomiony w innej komórce niż ta, w której są uruchomione usługi REST, lub jeśli widgety znajdują się w innych komórkach niż produkt Business Space.

Przed wykonaniem tej czynności muszą być wykonane następujące czynności:

- Zainstalowanie produktu.
- Utworzenie profili i skonfigurowanie produktu Business Space w miejscu docelowym wdrażania (na serwerze lub w klastrze).
- Skonfigurowanie tabel bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrażania).

Wszystkie widgety wymagane dla danego produktu są instalowane z produktem Business Space, ale zanim zespół będzie mógł używać w produkcie Business Space punktów końcowych wymaganych przez widgety, należy je skonfigurować i zarejestrować. Punkty końcowe można skonfigurować i zarejestrować, używając stron Konsoli administracyjnej. Jeśli jednak produkt i usługi REST są zainstalowane w innej komórce niż produkt Business Space, należy zmodyfikować pliki punktów końcowych usług REST w taki sposób, aby uzyskiwały one dostęp do usług REST, umożliwiając tym samym poprawne działanie widgetów w produkcie Business Space.

W zależności od zainstalowanych produktów i widgetów używanych w produkcie Business Space należy zmodyfikować co najmniej jeden z poniższych plików punktów końcowych:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor z produktem IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (w przypadku widgetów Administrowanie strategią mediacji, Przeglądarka usług oraz Gateway proxy), `bpmAdministrationEndpoints.xml` (w przypadku widgetów administracyjnych)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (w przypadku widgetów administracyjnych), `wesbWidgetEndpoints.xml` (w przypadku widgetów Administrowanie strategią mediacji, Przeglądarka usług oraz Gateway proxy), `HumanTaskManagementEndpoints.xml` (w przypadku procesów biznesowych oraz czynności personelu), `bospaceWFSEndpoints.xml` (w przypadku używania produktu Lotus Webform Server z widgetami zarządzania czynnościami personelu)
- Wszystkie produkty: `wsumEndpoint.xml` (w przypadku przypisania użytkownika)

Użytkownik, który jest administratorem, może rejestrować punkty końcowe i włączać widgety, wykonując następujące kroki.

1. Skopiuj widgety z komórki, w której zostały zainstalowane, do komórki, w której produkt Business Space jest konfigurowany podczas instalacji. Widgety znajdują się w katalogu `instalacyjny_katalog_główny\BusinessSpace\widgets`, skąd można je kopiować do folderu tymczasowego.
2. Uruchom komendę `installBusinessSpaceWidgets`, aby móc instalować, wdrażać i rejestrować wyznaczone widgety znajdujące się w katalogu `instalacyjny_katalog_główny\BusinessSpace\widgets`.
 - a. Sprawdź, czy serwer docelowy (w przypadku środowiska serwera autonomicznego) lub menedżer wdrażania (w przypadku środowiska wdrożenia sieciowego) jest zainstalowany i skonfigurowany, a następnie otwórz w tym profilu okno komend.

- Komenda wsadmin znajduje się w katalogu `profiles\nazwa_profilu\bin`.
- b. W wierszu komend wpisz komendę wsadmin, aby uruchomić środowisko wsadmin.
 - c. Uruchom komendę `installBusinessSpaceWidgets`. W przypadku środowiska klastrowego należy określić parametr **-clusterName**. W przypadku środowiska serwera autonomicznego należy określić parametry **-serverName** i **-nodeName**. Parametr **-widgets** należy określić przy użyciu pełnej ścieżki do katalogu lub pliku zawierającego widżety.
3. Znajdź pliki punktów końcowych w katalogu `instalacyjny_katalog_główny\BusinessSpace\registryData\endpoints`. W przypadku klastra należy sprawdzić, czy używany jest serwer aplikacji, na którym został utworzony profil menedżera wdrażania. Wszystkie nazwy plików mają zakończenie `Endpoints.xml` lub `Endpoint.xml`.
 4. Wykonaj kopię zapasową każdego skonfigurowanego pliku punktów końcowych.
 5. Utwórz następujący katalog w profilu menedżera wdrażania pierwszej komórki (jeśli nie ma jeszcze takiego katalogu): `katalog_główny_profilu\BusinessSpace\registryData\` (gdzie `katalog_główny_profilu` oznacza zwykle katalog `instalacyjny_katalog_główny\profiles\nazwa_profilu` lub `instalacyjny_katalog_główny\pf\nazwa_profilu`) i skopiuj do tego katalogu plik rejestracji punktów końcowych.
 6. Skonfiguruj odpowiednio punkty końcowe, edytując ich pliki. Każdy punkt końcowy w pliku punktów końcowych jest wyznaczany przez blok `<tns:Endpoint>`. Należy zidentyfikować blok, który ma zostać zmieniony.

Wskazówka: Jeśli nie ma potrzeby aktywowania niektórych punktów końcowych, można je usunąć z pliku dla większej przejrzystości.

Położenie identyfikowane przez punkt końcowy jest określone w bloku `<tns:url>`. Ta wartość jest ścieżką w module WWW określoną jako pełny lub względny adres URL HTTP. Domyślnie adres URL jest względny. Można go zastąpić pełną ścieżką URL, np. `https://host_wirtualny.com:port_wirtualny/rest/bpm/htm` lub `http://host1:9445/WBPublishingDRAFT/`, gdzie protokół, host i port definiują sposób uzyskania dostępu do modułu WWW produktu.

Aby znaleźć numer portu serwera, wykonaj następujące kroki:

- Zaloguj się w Konsoli administracyjnej produktu .
- Kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere**.
- Kliknij serwer, którego numer portu ma zostać znaleziony, a następnie rozwiń sekcję **Porty**.

Wszystkie aplikacje używają tego samego portu, który jest określony przy użyciu parametru **wc_defaulthost** (niezabezpieczony host) lub parametru **wc_defaulthost_secure** (zabezpieczony host).

Uwaga: W przypadku używania serwera HTTP w celu uzyskiwania dostępu do modułów WWW na potrzeby równoważenia obciążenia należy używać ustawień nazwy hosta i portu serwera HTTP.

7. W komórce, w której skonfigurowany jest serwer Business Space, uruchom komendę `updateBusinessSpaceWidgets`, aby zaktualizować adresy URL punktów końcowych po zmodyfikowaniu plików XML punktów końcowych.
 - a. Dla danego profilu użytkownika otwórz okno komend. Komenda wsadmin znajduje się w katalogu `profiles\nazwa_profilu\bin`. W przypadku środowiska klastrowego należy uruchomić komendę w katalogu `katalog_główny_profilu_menedżera_wdrażania\bin`. W przypadku środowiska z serwerem autonomicznym należy uruchomić komendę z poziomu katalogu `katalog_główny_profilu\bin`.
 - b. W wierszu komend wpisz komendę wsadmin, aby uruchomić środowisko wsadmin.

- c. Uruchom komendę `updateBusinessSpaceWidgets`. W przypadku środowiska klastrowego należy określić parametr **-clusterName**. W przypadku środowiska serwera autonomicznego należy określić parametry **-serverName** i **-nodeName**. Parametr **-endpoints** należy określić przy użyciu pełnej ścieżki do katalogu zawierającego pliki punktów końcowych widgetów lub pełnej ścieżki do konkretnego pliku punktu końcowego.

8. Zrestartuj serwer.

Poniżej przedstawiono przykładowy plik punktów końcowych dla widgetów produktu IBM Business Monitor.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- START NON-TRANSLATABLE -->
<tns:BusinessSpaceRegistry
  xmlns:tns="http://com.ibm.bspace/BusinessSpaceRegistry"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
  BusinessSpaceRegistry.xsd ">

  <tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Położenie usług pomocniczych dla widgetów programu Monitor
  </tns:description>
  </tns:Endpoint>

</tns:BusinessSpaceRegistry>
<!-- END NON-TRANSLATABLE -->
```

- Po uruchomieniu komendy `installBusinessSpaceWidgets` lub komendy `updateBusinessSpaceWidgets` należy samodzielnie wykonać kroki aktualizacji szablonów i obszarów produktu Business Space. Więcej informacji zawiera temat Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.
- Jeśli punkty końcowe usługi mają wiele instancji (na przykład w przypadku partycjonowania pracy na dwóch klastrach) i zachodzi potrzeba wyświetlenia w widgetach danych z każdego klastra, należy ręcznie aktywować dodatkowe widgety dla każdego dodatkowego klastra. Należy zmodyfikować zarówno pliki punktów końcowych widgetów, jak i pliki katalogów widgetów. Więcej informacji na ten temat zawiera sekcja Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi.
- Jeśli włączono zabezpieczenia środowiska, należy się upewnić, że zostały poprawnie skonfigurowane do pracy z produktem Business Space.

Włączanie widgetów produktu Business Space do pracy z wieloma punktami końcowymi:

Jeśli w przypadku skonfigurowanej pojedynczej instancji produktu Business Space wymagane jest utworzenie kolejnej instancji punktów końcowych usługi w środowisku, należy skonfigurować produkt Business Space tak, aby w widgetach mogły być wyświetlane dane z wielu punktów końcowych usługi. Należy dokonać edycji dwóch plików: pliku punktów końcowych, który służy do rejestrowania punktów końcowych w produkcie Business Space, oraz pliku katalogu widgetów, który zawiera definicje widgetów.

Przed wykonaniem tej czynności muszą być wykonane następujące czynności:

- Zainstalowanie produktu.
- Utworzenie serwera lub klastra oraz skonfigurowanie go na potrzeby produktu Business Space.
- Skonfigurowanie tabel bazy danych (jeśli jest używana zdalna baza danych lub środowisko wdrażania).
- Skonfigurowanie dodatkowych usług REST (Representational State Transfer) dla dodatkowych widgetów.

W środowisku wdrażania może występować partycjonowanie pracy. Na przykład mogą istnieć dwa klastry, z których jeden przetwarza dane działu księgowości, a drugi dane działu ubezpieczeń. Jednak punkt końcowy usługi obsługuje tylko jeden klaster. Aby uzyskać dostęp do obu partycji pracy z produktu Business Space, należy zarejestrować dwa oddzielne widgety (po jednym dla każdej partycji pracy). Pozwoli to uzyskać dostęp do obu tych partycji z poziomu produktu Business Space. Na przykład w katalogu może się znajdować widget Lista czynności personelu dotycząca księgowości oraz widget Lista czynności dotycząca ubezpieczenia (oba o tym samym rzeczywistym kodzie listy czynności personelu).

Należy ręcznie dokonać edycji pliku punktów końcowych oraz pliku katalogu widgetów.

Pliki punktów końcowych widgetów są dostarczane z każdym produktem i dodawane podczas instalacji produktu. Należy dokonać edycji co najmniej jednego z następujących plików punktów końcowych na podstawie zainstalowanych produktów oraz widgetów używanych z produktem Business Space:

- IBM Business Monitor: `monitorEndpoints.xml`
- IBM Business Monitor z produktem IBM Cognos Business Intelligence: `cognosEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (w przypadku widgetów Administrowanie strategią mediacji, Przeglądarka usług oraz Gateway proxy), `bpmAdministrationEndpoints.xml` (w przypadku widgetów administracyjnych)
- IBM Business Process Manager: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (w przypadku widgetów administracyjnych), `wesbWidgetEndpoints.xml` (w przypadku widgetów Administrowanie strategią mediacji, Przeglądarka usług oraz Gateway proxy), `HumanTaskManagementEndpoints.xml` (w przypadku procesów biznesowych oraz czynności personelu), `bospaceWFSEndpoints.xml` (w przypadku używania produktu Lotus Webform Server z widgetami zarządzania czynnościami personelu)
- Wszystkie produkty: `wsumEndpoint.xml` (w przypadku przypisania użytkownika)

Pliki katalogów widgetów zawierają definicje widgetów dla produktu użytkownika. Należy dokonać edycji co najmniej jednego z następujących plików widgetów na podstawie zainstalowanych produktów oraz widgetów używanych z produktem Business Space:

- IBM Business Monitor: `catalog_WBMonitor.xml`
- WebSphere Enterprise Service Bus: `catalogProxyGateway.xml` i `catalog_ServiceAdmin.xml`
- IBM Business Process Manager: `catalog_BPMAAdministration.xml`, `catalog_BusinessRules.xml`, `catalog_ServiceAdmin.xml` i `catalog_HumanTaskManagement.xml`

Zarówno pliki punktów końcowych, jak i pliki katalogów widgetów znajdują się w katalogu *instalacyjny_katalog_główny\BusinessSpace\registryData*. Pliki punktów końcowych znajdują się w podkatalogu *endpoints*, a pliki katalogów znajdują się w podkatalogu *catalogs*.

Katalog *instalacyjny_katalog_główny*\BusinessSpace\registryData\ zawiera pliki szablonów punktów końcowych oraz katalogów widgetów dla produktu użytkownika. Potrzebne pliki można skopiować jako szablon, a następnie dodać własne zmiany.

1. Aby utworzyć wiele instancji widgetu, zainstaluj aplikacje udostępniające widgetom unikalną nazwę aplikacji oraz kontekstowy katalog główny dla każdej instancji widgetu.
 - a. Wdróż aplikację widgetu w miejscu docelowym wdrażania produktu Business Space (na tym samym serwerze lub w tym samym klastrze, w którym jest uruchomiona aplikacja **BSpaceEAR_serwer_węzeł**) dla poszczególnych instancji widgetu. Zależnie od używanych produktów należy wdrożyć co najmniej jeden z następujących plików EAR (Enterprise Archive):
 - BPMAAdministrationWidgets_*nazwa_węzła_nazwa_serwera* (dla produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - HumanTaskManagementWidgets_*nazwa_węzła_nazwa_serwera* (dla produktów IBM Business Process Manager i IBM Business Monitor)
 - WBMDashboardWeb_*nazwa_węzła_nazwa_serwera* (dla produktu IBM Business Monitor)
 - wesbWidgets_*nazwa_węzła_nazwa_serwera* (dla produktu WebSphere Enterprise Service Bus)
 - b. Podczas wdrażania zaktualizuj nazwę aplikacji oraz nazwy kontekstowych katalogów głównych modułu WWW tak, aby były unikalne. Zanotuj nazwy używanych kontekstowych katalogów głównych.
2. Dokonaj edycji nowych punktów końcowych usługi REST dla dodatkowych miejsc docelowych wdrażania aplikacji (serwera lub klastra z wdrożoną aplikacją usług REST). Utwórz plik punktów końcowych w celu dodania punktów końcowych usługi.
 - a. Znajdź pliki punktów końcowych w katalogu *instalacyjny_katalog_główny*\BusinessSpace\registryData\endpoints. Skopiuj plik szablonów punktów końcowych, a następnie usuń wszystkie punkty końcowe, które nie mają zostać zmienione.
 - b. Dokonaj edycji pliku punktów końcowych, a następnie dodaj dodatkowy punkt końcowy usługi rozpoczynający się od elementu <tns:Endpoint> z unikalnym identyfikatorem (<tns:id>) oraz adresem URL dla nowego punktu końcowego (<tns:url>), ale z tą samą wersją, a także opcjonalnie ze wszystkimi ustawieniami narodowymi oryginalnego punktu końcowego. Typ (<tns:type>) musi mieć taką samą wartość, jak identyfikator (<tns:id>). Nazwę oraz opis można zmienić. Na przykład Lista czynności dotycząca ubezpieczeń mojego zespołu.
 - c. Podczas dodawania punktów końcowych zwróć uwagę na następujące informacje:
 - Identyfikator <tns:id>: identyfikatorem może być dowolny łańcuch, ale musi on być unikalny dla wszystkich zarejestrowanych punktów końcowych. Należy się upewnić, że ten identyfikator jest unikalny podczas dodawania dodatkowych punktów końcowych.
 - Typ <tns:type>: typ musi mieć taką samą wartość co identyfikator <tns:id>.
 - Adres URL <tns:url>: jeśli adres URL punktu końcowego usługi jest względny, przyjmuje się, że punkt końcowy usługi REST znajduje się w tym samym położeniu, co serwer produktu Business Space. Jeśli adres URL jest względny, należy się upewnić, że jest on taki sam, jak kontekstowy katalog główny, który został wdrożony przez użytkownika, ale ze wskazaniem katalogu początkowego i końcowego, na przykład: <tns:url>/BSpaceWidgetsWPS2/</tns:url>. Jeśli punkt końcowy znajduje się w systemie zdalnym, należy zaktualizować to pole przy użyciu bezwzględnego adresu URL, ale ze wskazaniem katalogu końcowego.
 - Opis <tns:description>: należy wpisać znaczący opis zawierający szczegółowe informacje dotyczące rodzaju zestawu danych przetwarzanego przez ten punkt końcowy. Opis może być oparty na klastrze przetwarzającym zestaw danych lub

rodzaju zestawu danych, na przykład: Lista czynności personelu dotyczących roszczenia wynikającego z kontraktu ubezpieczenia lub Lista czynności personelu dotyczących danych rozliczeniowych.

d. Zapisz zmiany.

Przykładowy punkt końcowy usługi znajdujący się w pliku `monitorEndpoints.xml`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>/rest/</tns:url>
  <tns:description>Położenie usług pomocniczych dla widgetów programu
Monitor
</tns:description>
</tns:Endpoint>
```

3. W pliku punktów końcowych dodaj punkt końcowy widgetu dla poszczególnych instancji widgetu.

a. Dokonaj edycji pliku punktów końcowych utworzonego w kroku 2. Dodaj kolejny punkt końcowy widgetu rozpoczynający się od elementu `<tns:Endpoint>` z unikalnym identyfikatorem (`<tns:id>`). Typ (`<tns:type>`) musi mieć taką samą wartość, jak identyfikator (`<tns:id>`). Adres URL nowego punktu końcowego (`<tns:url>`) powinien być taki sam, jak kontekstowy katalog główny wdrożony w kroku 1, ale ze wskazaniem katalogu początkowego i końcowego, na przykład: `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`. Dodawany punkt końcowy widgetu powinien zawierać tę samą wersję co oryginalny punkt końcowy oraz opcjonalnie jego wszystkie ustawienia narodowe. Nazwę oraz opis można zmienić.

b. Podczas dodawania punktów końcowych zwróć uwagę na następujące informacje:

- Identyfikator `<tns:id>`: identyfikatorem może być dowolny łańcuch, ale musi on być unikalny dla wszystkich zarejestrowanych punktów końcowych. Należy się upewnić, że ten identyfikator jest unikalny podczas dodawania dodatkowych punktów końcowych.
- Typ `<tns:type>`: typ musi mieć taką samą wartość co identyfikator `<tns:id>`.
- Adres URL `<tns:url>`: w przypadku punktu końcowego widgetu należy się upewnić, że adres URL jest taki sam, jak wdrożony kontekstowy katalog główny, ale ze wskazaniem katalogu początkowego i końcowego, na przykład: `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`.
- Opis `<tns:description>`: należy wpisać znaczący opis zawierający szczegółowe informacje dotyczące rodzaju zestawu danych przetwarzanego przez ten punkt końcowy. Opis może być oparty na klastrze przetwarzającym zestaw danych lub rodzaju zestawu danych, na przykład: Lista czynności personelu dotyczących roszczenia wynikającego z kontraktu ubezpieczenia lub Lista czynności personelu dotyczących danych rozliczeniowych.

c. Zapisz zmiany.

Przykładowy punkt końcowy widgetu znajdujący się w pliku `monitorEndpoints.xml`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:id>
  <tns:type>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>/newMonitorWidgetContextRoot/</tns:url>
  <tns:description>Położenie widgetów programu Monitor</tns:description>
</tns:Endpoint>
```

4. Utwórz plik katalogu widgetów w celu dodania nowych definicji widgetów.

a. Znajdź plik katalogu widgetów w katalogu `instalacyjny_katalog_główny\BusinessSpace\registryData\catalogs`. Skopiuj plik szablonu katalogu. W przypadku nowej nazwy pliku należy użyć następującego standardu: `catalog_widget.xml` (bez spacji w nazwie pliku), gdzie `widget` to wartość identyczna, jak wartość identyfikatora elementu `<catalog>` w pliku. Należy usunąć

wszystkie elementy <category>, które nie mają zostać zmienione. W przypadku kategorii, z którą pracuje użytkownik, należy usunąć wszystkie elementy <entry>, które nie mają zostać zmienione.

- b. Dodaj element <entry> o unikalnym identyfikatorze, na przykład `id="{com.ibm.bspace.widget}identyfikator_widgetu` oraz unikalnej nazwie, na przykład `unique-name="{com.ibm.bspace.widget}nazwa_widgetu`. Nie trzeba usuwać pozostałych definicji.
- c. Zmień tytuł oraz opis, aby udostępnić nowy widget jako odrębny widget w produkcie Business Space, podając zarys rodzaju nowego punktu końcowego. Na przykład można nadać widgetowi nazwę Lista czynności dotycząca ubezpieczeń mojego zespołu, korzystając z elementu <title>. Tytuł powinien ułatwić użytkownikom biznesowym wybór właściwego widgetu. Opis powinien pomóc użytkownikom biznesowym w zrozumieniu rodzaju danych oraz funkcji wybieranego widgetu.
- d. Dokonaj edycji nowego pliku XML katalogu widgetów w celu utworzenia odwołania do nowego punktu końcowego widgetu: zmień definicję tak, aby była zgodna z identyfikatorem <tns:id> punktu końcowego widgetu dodanego w kroku 3.a.

Na przykład zmień ją na następującą: ...

```
<definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId2/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
```

...

- e. Upewnij się, że w elemencie <metadata> pliku katalogu element `endpoint://` jest zgodny z typem oraz identyfikatorem w pliku punktów końcowych (<tns:type> oraz <tns:id>).
- f. Upewnij się, że w elemencie <metadata> pliku katalogu element "refVersion" : jest zgodny z wersją w pliku punktów końcowych (<tns:version>).
- g. Zapisz zmiany.

Przykładowy plik katalogu widgetów:

```
< entry id="{com.ibm.wbimonitor}instances"
unique-name="{com.ibm.wbimonitor}instances">
  <title>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="pl">Instancje</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </title>
  <description>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="pl">Instancje</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </description>
  <shortDescription>
    <!-- END NON-TRANSLATABLE -->
    <nls-string xml:lang="pl">Ten widget służy do wyświetlania panelu kontrolnego z
dostępnym kontekstem monitorowania w poszczególnych instancjach lub zdefiniowanych przez
użytkownika grupach instancji kontekstu.</nls-string>
    <!-- START NON-TRANSLATABLE -->
  </shortDescription>
  < definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId
/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
  <content>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
thumb_instances.gif</content>
  < preview>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
prev_instances.gif</preview>
  <previewThumbnail>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/
img/prev_instances.gif</previewThumbnail>
  <help>endpoint://{com.ibm.bspace}bSpaceWidgetHelpRootId/topic/
com.ibm.bspace.help.wdg.mon.doc/topics/help_instance_whatIs.html</help>
  <icon>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
icon_instances.gif</icon>
  <metadata name="com.ibm.mashups.builder.autoWiringEnabled">true
</metadata>
  <metadata name="com.ibm.bspace.version">7.0.0.0</metadata>
  <metadata name="com.ibm.bspace.owner">International Business
Machines Corp.</metadata>
  <metadata name="com.ibm.bspace.serviceEndpointRefs">
```

```
[[{"name":"serviceUrlRoot", "required":"true",  
"refId":"endpoint://{com.ibm.wbimonitor}monitorServiceRootId",  
"refVersion":"1.0.0.0"}]</metadata>  
</entry>
```

5. Umieść nowy plik punktów końcowych oraz nowy plik katalogu w skompresowanym pliku, a następnie uruchom komendę `updateBusinessSpaceWidgets` z parametrem **-widgets** w celu określenia położenia pliku skompresowanego.
 - Po uruchomieniu komendy `updateBusinessSpaceWidgets` należy ręcznie zaktualizować szablony oraz obszary produktu Business Space. Więcej informacji zawiera temat Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.
 - Jeśli produkt Business Space działa w innej komórce niż usługi REST, należy ręcznie dokonać edycji plików punktów końcowych.
 - Jeśli włączono zabezpieczenia środowiska, należy się upewnić, że zostały poprawnie skonfigurowane do pracy z produktem Business Space.

Konfigurowanie widgetów dla wielu produktów:

Widżety produktu Business Space można dodawać lub konfigurować dla produktu w obszarze Business Space, który został już skonfigurowany przy użyciu innego produktu, za pomocą komendy `installBusinessSpaceWidgets`.

Przed wykonaniem tej czynności należy wykonać następujące czynności:

- Wykonanie wszystkich kroków instalacji i konfiguracji produktu Business Space oraz skonfigurowanie tego produktu.
- Wykonanie wszystkich kroków instalacji i konfiguracji dodatkowego produktu.

Istnieje możliwość zainstalowania więcej niż jednego produktu współpracującego z produktem Business Space oraz, po zainstalowaniu drugiego produktu, skonfigurowania widgetów dla obu produktów. Jeśli jednak drugi produkt zostanie zainstalowany po wcześniejszym skonfigurowaniu produktu Business Space z widgetami dla pierwszego produktu, w celu dodania i skonfigurowania widgetów drugiego produktu na potrzeby współpracy z tym samym produktem Business Space należy użyć komendy `installBusinessSpaceWidgets`.

W przypadku rozszerzenia autonomicznego widżety są instalowane automatycznie. Na przykład widżety są instalowane w przypadku utworzenia profilu autonomicznego produktu IBM Business Process Manager, skonfigurowania serwera dla produktu Business Space, zainstalowania programu IBM Business Monitor oraz rozszerzenia wcześniej skonfigurowanego serwera o program IBM Business Monitor.

1. Upewnij się, że profil menedżera wdrażania został uruchomiony i działa, a następnie w tym profilu otwórz okno komend.
Komenda `wsadmin` znajduje się w katalogu `profiles/nazwa_profilu/bin`.
2. W wierszu komend wpisz komendę `wsadmin`, aby uruchomić środowisko `wsadmin`.
3. Przy użyciu komendy `installBusinessSpaceWidgets` zainstaluj, wdróż i zarejestruj określone widżety znajdujące się w katalogu `instalacyjny_katalog_główny/BusinessSpace/widgets`.

W następującym przykładzie przy użyciu kodu Jython uruchomiono komendę `installBusinessSpaceWidgets` w celu zainstalowania widgetów dla programu IBM Business Monitor na potrzeby współpracy ze środowiskiem produktu Business Space, które zostało wcześniej skonfigurowane dla produktu IBM Business Process Manager.

```
AdminTask.installBusinessSpaceWidgets('[-nodeName
nazwa_węzła
-serverName nazwa_serwera -widgets
instalacyjny_katalog_główny\BusinessSpace\widgets\WBM\widgets_WBMonitor.zip]')
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask
installBusinessSpaceWidgets {-nodeName nazwa_węzła
-serverName nazwa_serwera -widgets
instalacyjny_katalog_główny\BusinessSpace\widgets\WBM\widgets_WBMonitor.zip}
```

Aby po skonfigurowaniu widgetów włączyć produkt Business Space dla środowiska wykonawczego użytkownika, wykonaj następujące kroki:

- Po uruchomieniu komendy `installBusinessSpaceWidgets` lub `updateBusinessSpaceWidgets` wykonaj ręczne kroki w celu zaktualizowania szablonów i obszarów produktu Business Space. Więcej informacji zawiera temat Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.
- Skonfiguruj usługi REST. Więcej informacji zawiera temat Konfigurowanie usług REST.
- Zarejestruj punkty końcowe REST. Więcej informacji zawiera temat Konfigurowanie produktu Business Space i rejestrowanie punktów końcowych REST za pomocą Konsoli administracyjnej.
- Sprawdź, czy zabezpieczenia zostały poprawnie skonfigurowane na potrzeby współpracy z produktem Business Space oraz widgetami używanymi przez zespół. Więcej informacji na ten temat można znaleźć w sekcji Konfigurowanie zabezpieczeń dla produktu Business Space.

Konfigurowanie konkretnych widgetów do pracy w produkcie Business Space

Niektóre widgety dostarczane z produktem wymagają dodatkowych kroków konfiguracyjnych, zanim będzie możliwe użycie ich w produkcie Business Space.

Produkt do zarządzania procesami biznesowymi zawiera wiele widgetów, a niektóre z nich wymagają dodatkowej konfiguracji, aby komunikować się z rozwiązaniem opartym na produkcie Business Space.

Konfigurowanie monitora usług:

Jeśli jest tworzony nowy serwer i do mierzenia czasu odpowiedzi i przepustowości żądań dla usług wywołanych przez moduł SCA lub prezentowanych w tym module ma być używany widget Monitor usług w produkcie Business Space, w Konsoli administracyjnej należy skonfigurować i włączyć monitorowanie usług.

Wymagana rola zabezpieczeń dla tej czynności: jeśli włączono zabezpieczenia administracyjne, należy zalogować się przy użyciu roli administracyjnej, aby wykonać tę czynność.

Monitor usług ma architekturę klient/serwer.

- Agent monitora usług: mierzy przepustowość i czas odpowiedzi dla operacji i wysyła dane pomiarów do serwera monitora usług.
- Serwer monitora usług: zbiera i agreguje pomiary czasu odpowiedzi i przepustowości ze wszystkich działających agentów monitora usług, a także oblicza i zapisuje statystyki.

W środowisku wdrażania serwer działa w klastrze pomocniczym, a agent - w klastrze aplikacji na serwerze, na którym wdrożono moduł. W środowisku serwera autonomicznego zarówno serwer, jak i agent działają na serwerze autonomicznym.

Ważne: Jeśli dostęp do produktu Business Space jest uzyskiwany przy użyciu zewnętrznego serwera HTTP, należy upewnić się, że na tym serwerze HTTP skonfigurowano obsługę zakodowanych ukośników. Szczegółowe informacje na ten temat zawiera dokumentacja serwera HTTP.

1. Zaloguj się do Konsoli administracyjnej przy użyciu uprawnień administratora.
2. Skonfiguruj serwer monitora usług.
 - a. Z poziomu konsoli kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere > nazwa_serwera > Monitor usług**.
 - b. Na stronie Monitor usług kliknij opcję **Włącz monitor usług**.
 - c. Przejrzyj wartości domyślne wielkości bufora monitora usług oraz limitu wielkości zapytania i w razie potrzeby dokonaj ich zmiany.
 - d. Określ cele monitorowania usług. Są to agenty monitora usług, z których dane mają być zbierane.

Tabela 6. Monitorowanie

| Cele monitorowania | Kroki do wykonania |
|---|---|
| Monitorowanie wszystkich działających agentów monitora usług | Należy się upewnić, że jest zaznaczona opcja Wszystkie włączone agenty monitorowania usług . |
| Monitorowanie konkretnego podzbioru działających agentów monitora usług | <ol style="list-style-type: none"> 1. Należy usunąć zaznaczenie opcji Wszystkie włączone agenty monitorowania usług. Zostanie wyświetlona tabela gromadzenia. Jeśli jest to nowa konfiguracja, tabela jest pusta. 2. Należy kliknąć przycisk Dodaj. Zostanie wyświetlona strona Przeglądanie docelowych miejsc wdrożenia. 3. Z tabeli gromadzenia na stronie Przeglądanie docelowych miejsc wdrożenia wybierz docelowe miejsce wdrożenia, którego agent ma być monitorowany. 4. Należy kliknąć przycisk OK, aby wrócić do strony Serwer monitora usług. 5. Należy powtórzyć kroki od 2 do 4 do momentu dodania wszystkich agentów, które mają być monitorowane. |

- e. Na stronie Serwer monitora usług kliknij przycisk **OK**. Konfiguracja zostanie zapisana i jest stosowana natychmiast.
3. Skonfiguruj agent monitora usług.
 - a. Z poziomu konsoli kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere > nazwa_serwera > Agent monitora usług**.
 - b. Na stronie Agent monitora usług kliknij opcję **Włącz agent monitora usług**.
 - c. Przejrzyj wartości domyślne konfiguracji agenta i w razie potrzeby dokonaj ich zmiany.
 - d. Kliknij przycisk **OK**.

Konfigurowanie zabezpieczeń produktu Business Space

Jeśli produkt Business Space oparty na technologii WebSphere jest używany ze środowiskiem użytkownika, należy rozważyć opcje zabezpieczeń dotyczące sposobu pracy zespołu użytkownika z artefaktami w produkcie Business Space. Aby włączyć zabezpieczenia produktu Business Space, należy skonfigurować zabezpieczenia aplikacji i wyznaczyć repozytorium użytkowników. Aby zdefiniować administratorów produktu Business Space, należy przypisać użytkownikom rolę administratora.

Aby uzyskać najlepsze wyniki, zabezpieczenia należy włączyć przed skonfigurowaniem produktu Business Space. Jeśli zabezpieczenia zostaną włączone później, na stronie Zabezpieczenia globalne Konsoli administracyjnej należy włączyć zarówno zabezpieczenia administracyjne, jak i zabezpieczenia aplikacji. Ta strona umożliwi także określenie repozytorium kont użytkowników, w tym zmianę domyślnej opcji repozytoriów stowarzyszonych, tak aby było używane inne repozytorium użytkowników. Aby określić użytkowników z uprawnieniami do wykonywania czynności administracyjnych produktu Business Space w środowisku tego produktu, należy przypisać rolę administratora produktu Business Space. W przypadku konkretnego środowiska może być wymagana inna konfiguracja zabezpieczeń.

Ważne: Domyślnie konfiguracja proxy Ajax używana z widgetami produktu Business Space nie ogranicza dostępu do żadnych adresów IP. Dla wygody użytkownika proxy Ajax jest domyślnie skonfigurowane tak, aby było otwarte. Taka sytuacja stanowi zagrożenie dla bezpieczeństwa w przypadku środowiska produkcyjnego. Aby skonfigurować proxy Ajax tak, aby umożliwiała wyświetlanie treści tylko z wybranych serwisów lub blokowało treść z tych serwisów, należy wykonać kroki opisane w temacie Blokowanie adresów IP przy użyciu proxy Ajax produktu Business Space.

Włączanie zabezpieczeń dla produktu Business Space:

Jeśli ma być używane zabezpieczone środowisko, przed przystąpieniem do konfigurowania produktu Business Space należy włączyć zabezpieczenia. W razie konieczności można jednak włączyć te zabezpieczenia ręcznie w późniejszym czasie. Aby włączyć zabezpieczenia dla produktu Business Space, należy włączyć zarówno zabezpieczenia aplikacji, jak i zabezpieczenia administracyjne.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Produkt Business Space został wstępnie skonfigurowany w celu zapewnienia uwierzytelniania oraz autoryzacji dostępu. Podczas próby uzyskania dostępu do adresów URL produktu Business Space użytkownikom zostaje wyświetlona prośba o uwierzytelnienie. Nieuwierzytelnieni użytkownicy zostają przekierowani do strony logowania. Dostęp do produktu Business Space można uzyskiwać przy użyciu protokołów HTTP lub HTTPS. W przypadku używania serwera WWW, takiego jak produkt IBM HTTP Server, serwer ten należy skonfigurować na potrzeby obsługi protokołu HTTPS.

Jeśli istnieje obawa o bezpieczeństwo haseł z powodu braku zabezpieczeń SSL, należy rozważyć wyłączenie dostępu dla protokołu HTTP przy użyciu serwera WebSphere Application Server. Więcej informacji na temat zabezpieczeń zawiera sekcja Konfigurowanie, włączanie i migrowanie zabezpieczeń w Centrum informacyjnym serwera WebSphere Application Server.

Aby można było włączyć dostęp z uwierzytelnianiem do produktu Business Space, wymagane są skonfigurowany rejestr użytkowników oraz włączone zabezpieczenia aplikacji.

Autoryzacja dotycząca obszarów oraz treści strony w produkcie Business Space jest obsługiwana wewnętrznie względem produktu Business Space w ramach zarządzania obszarami.

1. Szczegółowe instrukcje dotyczące zabezpieczeń zawiera dokumentacja zabezpieczeń produktu.
2. W przypadku aplikacji Business Space na stronie Zabezpieczenia globalne w Konsoli administracyjnej wybierz następujące opcje: **Włącz zabezpieczenia administracyjne** oraz **Włącz zabezpieczenia aplikacji**.
3. Aby włączyć lub usunąć zabezpieczenia po skonfigurowaniu produktu Business Space przy użyciu profilu użytkownika, należy zmodyfikować właściwość `noSecurityAdminInternalUserOnly` w pliku `ConfigServices.properties`.

Właściwość `noSecurityAdminInternalUserOnly` określa identyfikator administratora produktu Business Space, gdy zabezpieczenia są wyłączone. W przypadku gdy zabezpieczenia są wyłączone, konfiguracja produktu Business Space domyślnie ustawia tę właściwość na wartość **BPMAdministrator**. Gdy zabezpieczenia są włączone, właściwość ta jest domyślnie ustawiana na identyfikator administratora serwera aplikacji. Aby włączyć lub usunąć zabezpieczenia po skonfigurowaniu produktu Business Space, należy posłużyć się identyfikatorem administratora serwera aplikacji.

- a. Zmodyfikuj właściwość `noSecurityAdminInternalUserOnly` w pliku `ConfigServices.properties`, ustawiając ją na identyfikator administratora serwera aplikacji. Plik `ConfigServices.properties` znajduje się w ścieżce `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties` (w przypadku serwera autonomicznego) lub w ścieżce `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties` (w przypadku klastra).
- b. Przy użyciu klienta skryptowego `wsadmin` uruchom komendę `updatePropertyConfig`.

- Dla serwera autonomicznego:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-serverName
nazwa_serwera -nodeName
nazwa_węzła
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask
updatePropertyConfig {-serverName
nazwa_serwera -nodeName nazwa_węzła
-propertyFileName
"katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Dla klastra:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-clusterName nazwa_klastra
-propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```

$AdminTask updatePropertyConfig {-clusterName nazwa_klastra
-propertyFileName
  "katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save

```

c. Zrestartuj serwer.

d. Zaloguj się do produktu Business Space i ponownie przypisz właścicieli obszarów domyślnych do nowego identyfikatora administratora.

- Gdy zabezpieczenia administracyjne oraz zabezpieczenia aplikacji zostaną włączone, podczas logowania do produktu Business Space będzie wyświetlana prośba o podanie ID użytkownika oraz hasła. Zalogowanie się będzie wymagać użycia poprawnego ID użytkownika oraz hasła z wybranego rejestru użytkowników. Po włączeniu zabezpieczeń administracyjnych przy każdym ponownym przejściu do Konsoli administracyjnej należy się zalogować przy użyciu ID użytkownika z uprawnieniami administracyjnymi.
- Jeśli ustawienie repozytorium konta użytkownika ma zostać zmienione z domyślnego dla profilu produktu użytkownika, należy wykonać czynności opisane w sekcji Wybieranie repozytorium konta użytkownika.
- Jeśli istnieje środowisko międzykomórkowe, w którym produkt Business Space jest zdalny względem lokalizacji uruchomionego produktu użytkownika, a węzły nie znajdują się w tej samej komórce, należy skonfigurować certyfikaty pojedynczego logowania (SSO) i Secure Sockets Layer (SSL). Należy postępować zgodnie z instrukcjami zawartymi w sekcji “Konfigurowanie funkcji pojedynczego logowania oraz protokołu SSL na potrzeby produktu Business Space” na stronie 232.
- Aby wyznaczyć użytkownika, który będzie wykonywać czynności administratora produktu Business Space w środowisku produktu Business Space, należy zapoznać się z sekcją “Przypisywanie roli administratora produktu Business Space” na stronie 242.

Wybieranie repozytorium użytkowników dla produktu Business Space:

Domyślna opcja repozytorium kont użytkowników dla profili to Repozytoria stowarzyszone. Typ repozytorium kont użytkowników można zmienić, jeśli jest to wymagane w środowisku użytkownika.

Przed wykonaniem tej czynności muszą być wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Aby można było włączyć dostęp z uwierzytelnianiem do produktu Business Space, wymagane są skonfigurowany rejestr użytkowników oraz włączone zabezpieczenia aplikacji. Informacje o zabezpieczeniach aplikacji zawiera temat “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.

Uwagi dotyczące używania rejestru kont użytkowników z produktem Business Space:

- W zależności od typu używanej konfiguracji LDAP ustawienia użytkownika mogą mieć wpływ na możliwość poprawnego dostępu do produktu Business Space. Należy się upewnić, że filtry użytkowników, filtry grup oraz ustawienia odwzorowania zostały poprawnie skonfigurowane. Więcej informacji na ten temat zawiera sekcja Konfigurowanie filtrów wyszukiwania w katalogu LDAP (Lightweight Directory Access Protocol) w dokumentacji serwera WebSphere Application Server.
- W zależności od typu używanej konfiguracji repozytorium stowarzyszonego ustawienia użytkownika mogą mieć wpływ na możliwość poprawnego dostępu do produktu Business

Space. Należy upewnić się, że dziedziny są poprawnie skonfigurowane. Więcej informacji na ten temat zawiera sekcja Zarządzanie dziedzina w konfiguracji repozytorium stowarzyszonego w dokumentacji serwera WebSphere Application Server.

- Zabezpieczenia LDAP są domyślnie skonfigurowane tak, aby do wyszukiwania w produkcie Business Space była używana właściwość logowania uid (ID użytkownika). Jeśli zabezpieczenia LDAP użytkownika zostaną zmienione, aby dla właściwości logowania było używane inne unikalne pole LDAP, na przykład mail (adres e-mail), należy zmodyfikować właściwość userIdKey w pliku ConfigServices.properties, aby wyszukiwanie działało w produkcie Business Space. Należy wykonać czynności opisane poniżej w kroku 3.
- W przypadku używania bazy danych Microsoft SQL Server oraz **autonomicznego rejestru LDAP** należy się upewnić, że nazwa wyróżniająca użytkownika nie zawiera więcej niż 450 znaków. Jeśli co najmniej jedna nazwa wyróżniająca użytkownika ma więcej niż 450 znaków, należy wybrać opcję **Repozytoria stowarzyszone** dla rejestru kont użytkowników.
- W przypadku używania opcji **Repozytoria stowarzyszone** widgety i środowisko udostępniają dodatkowe możliwości, takie jak rozszerzone możliwości wyszukiwania. Podczas wyszukiwania użytkowników w celu współużytkowania obszarów i stron zasięg wyszukiwania obejmuje pocztę elektroniczną, pełną nazwę użytkownika oraz identyfikator użytkownika.

1. Na stronie Konsoli administracyjnej Zabezpieczenia globalne w obszarze **Repozytorium kont użytkowników** wybierz opcję **Repozytoria stowarzyszone, Lokalny system operacyjny, Autonomiczny rejestr LDAP** lub **Autonomiczny rejestr niestandardowy**.

2. Zrestartuj serwer.

3. Aby jako domyślne repozytorium użytkowników ustawić repozytorium inne niż **repozytorium stowarzyszone**, zmodyfikuj właściwość MashupAdminForOOBSpace w pliku ConfigServices.properties w celu wyznaczenia poprawnego identyfikatora użytkownika (właściwość UID repozytorium użytkowników) jako poprawnego identyfikatora administratora.

- a. Skopiuj zmodyfikowany plik do pustego folderu w systemie. Plik ConfigServices.properties znajduje się w ścieżce *katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties* (w przypadku serwera autonomicznego) lub w ścieżce *katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties* (w przypadku klastra).

b. Przy użyciu klienta skryptowego wsadmin uruchom komendę updatePropertyConfig.

- Dla serwera autonomicznego:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-serverName nazwa_serwera -nodeName nazwa_węzła  
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
```

```
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask  
updatePropertyConfig {-serverName  
nazwa_serwera -nodeName nazwa_węzła  
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
```

```
$AdminConfig save
```

- Dla klastra:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-clusterName
nazwa_klastra -propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask
updatePropertyConfig {-clusterName nazwa_klastra -propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- c. Zaloguj się do produktu Business Space i ponownie przypisz właścicieli obszarów domyślnych do nowego identyfikatora administratora.
4. W przypadku używania repozytorium LDAP z unikalnym polem LDAP dla właściwości logowania, na przykład mail (adres e-mail) zamiast uid (identyfikator użytkownika), zmodyfikuj właściwość `userIdKey` w pliku `ConfigServices.properties`, aby wyszukiwanie działało w produkcie Business Space.
 - a. Znajdź plik `ConfigServices.properties` w ścieżce `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties` w przypadku serwera autonomicznego lub w ścieżce `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties` w przypadku klastra.
 - b. Zmień wartość atrybutu `userIdKey` z `uid` (identyfikator użytkownika), tak aby odpowiadał właściwości logowania repozytorium użytkowników LDAP, na przykład `mail` (adres e-mail).
 - c. Skopiuj zmodyfikowany plik do pustego folderu w systemie.
 - d. Przy użyciu klienta skryptowego `wsadmin` uruchom komendę `updatePropertyConfig`.

- Dla serwera autonomicznego:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-serverName
nazwa_serwera -nodeName nazwa_węzła
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask
updatePropertyConfig {-serverName
nazwa_serwera -nodeName nazwa_węzła
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```

- Dla klastra:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig('[-clusterName nazwa_klastra
-propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"]')
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName nazwa_klastra  
-propertyFileName
```

```
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"  
$AdminConfig save
```

5. Aby ograniczyć logowanie do produktu Business Space do podzbioru użytkowników i grup, można zmienić odwzorowanie roli zabezpieczeń Java EE produktu Business Space.
 - a. Zaktualizuj odwzorowanie na użytkownika/grupę dla dwóch aplikacji korporacyjnych: **BSpaceEAR_węzeł_serwer** i **mm.was_węzeł_serwer** (w przypadku środowiska serwera autonomicznego) lub **BSpaceEAR_klaster** i **mm.was_klaster** (w przypadku środowiska wdrożenia sieciowego).
 - b. Kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**, a następnie wybierz powyższe dwie aplikacje.
 - c. W panelu po prawej stronie w obszarze Właściwości szczegółowe wybierz opcję **Odwzorowanie roli zabezpieczeń na użytkownika/grupę**.
 - d. Zmień odwzorowanie ról **businessspaceusers** oraz **Allauthenticated** z dwóch aplikacji, usuwając najpierw podmiot specjalny.
 - e. Kliknij opcję **Odwzoruj podmioty specjalne**, a następnie wybierz opcję **Brak**.
 - f. Kliknij opcję **Odwzoruj użytkowników** lub **Odwzoruj grupy**, a następnie przypisz każdą rolę do wybranych użytkowników lub grup.

Zmiana roli zabezpieczeń Java EE nie wpływa na funkcję wyszukiwania użytkownika/grupy w produkcie Business Space.

6. Zrestartuj serwer.
7. Zaloguj się do produktu Business Space i ponownie przypisz właścicieli obszarów domyślnych do nowego identyfikatora administratora.
 - Aby ustawić autoryzację dotyczącą stron i obszarów w produkcie Business Space, podczas tworzenia stron i obszarów produktu Business Space można zarządzać autoryzacją.
 - Aby wyznaczyć użytkownika, który będzie wykonywać czynności administratora produktu Business Space w środowisku produktu Business Space, należy zapoznać się z sekcją “Przypisywanie roli administratora produktu Business Space” na stronie 242.

Uwaga:

Jeśli plik `SystemOut.log` zawiera poniższe błędy, rejestr użytkowników może zawierać dodatkowe atrybuty, których nie można przetworzyć:

```
00000046 SystemErr R Caused  
by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E  
Wartość właściwości secretary nie jest poprawna w przypadku obiektu  
uid=xxx,c=pl,ou=yyy,o=ibm.com.  
00000046 SystemErr R at com.ibm.ws.wim.adapter.Ldap.LdapAdapter.setPropertyValue  
(LdapAdapter.java:3338)
```

W celu pominięcia tych atrybutów w pliku `ConfigServices.properties` należy ustawić poniższe atrybuty:

```
com.ibm.mashups.user.userProfile = LIMITED  
com.ibm.mashups.user.groupProfile = LIMITED
```

Plik `ConfigServices.properties` znajduje się w ścieżce `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties` (w przypadku serwera autonomicznego) lub w ścieżce `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties` (w przypadku klastra). Po

zmodyfikowaniu pliku `ConfigServices.properties` przy użyciu klienta skryptowego wsadmin należy uruchomić komendę `updatePropertyConfig`, wykonując czynności opisane powyżej w kroku 4.d.

Uwaga:

Jeśli włączono zabezpieczenia Java EE w klastrze, należy wziąć pod uwagę zaostrenie strategii serwera w przypadku pozycji dotyczącej położenia systemu pomocy produktu Business Space.

Strategia położenia systemu pomocy produktu Business Space to:

```
grant codeBase "file:${was.install.root}/profiles/nazwa_profilu/temp/nazwa_węzła/" {  
  
permission java.security.AllPermission;  
  
};
```

Strategię należy zaostrzyć, zmieniając ją w następujący sposób:

```
grant codeBase "file:${was.install.root}/profiles/nazwa_profilu/temp/nazwa_węzła/  
nazwa_serwera/BusinessSpaceHelpEAR_nazwa_węzła_nazwa_serwera/  
BusinessSpaceHelp.war/" {  
  
permission java.security.AllPermission;  
  
};
```

Konfigurowanie funkcji pojedynczego logowania oraz protokołu SSL na potrzeby produktu Business Space:

W przypadku środowisk zdalnych, w których produkt Business Space oraz serwer produktu znajdują się w różnych komórkach, należy ręcznie skonfigurować funkcję pojedynczego logowania oraz protokół SSL (Secure Sockets Layer).

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
 - Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.
1. Jeśli produkt Business Space znajduje się w położeniu zdalnym względem położenia, w którym działa produkt użytkownika, a węzeł, w którym działa produkt Business Space, oraz węzeł z działającym produktem użytkownika nie znajdują się w tej samej komórce, wykonaj kroki ręcznie, aby upewnić się, że włączono funkcję pojedynczego logowania. Jeśli na przykład jest używany więcej niż jeden produkt, serwery znajdują się w różnych węzłach i wszystkie powinny współpracować z serwerem produktu Business Space, należy ręcznie skonfigurować funkcję pojedynczego logowania. Aby włączyć funkcję pojedynczego logowania, wykonaj następujące kroki:
 - a. W Konsoli administracyjnej dla każdego serwera otwórz stronę Zabezpieczenia globalne, klikając opcję **Zabezpieczenia > Zabezpieczenia globalne**. Rozwiń pozycję **Bezpieczeństwo WWW i SIP**, a następnie kliknij opcję **Pojedyncze logowanie (SSO)**, aby upewnić się, że zaznaczono pole wyboru **Włączone**.
 - b. Upewnij się, że wszystkie węzły używają tych samych informacji dotyczących **repozytorium kont użytkowników** (patrz krok 3).

- c. Wykonaj procedurę opisaną w temacie Importowanie i eksportowanie kluczy w Centrum informacyjnym serwera WebSphere Application Server.
2. W przypadku gdy w pliku punktów końcowych jest używany protokół HTTPS, punkt końcowy znajduje się w innym węźle niż produkt Business Space oraz certyfikat SSL to samopodpisany certyfikat SSL, zaimportuj ten certyfikat.
Należy się upewnić, że osoby podpisujące zostały skonfigurowane w odpowiednich magazynach zaufanych certyfikatów dla serwera produktu Business Space oraz serwera produktu. Więcej informacji można znaleźć w sekcji Bezpieczna komunikacja przy użyciu protokołu SSL (Secure Sockets Layer) Centrum informacyjnego produktu WebSphere Application Server.
Więcej informacji na temat funkcji pojedynczego logowania oraz protokołu SSL zawiera Centrum informacyjne serwera WebSphere Application Server.

Konfigurowanie zabezpieczeń dla systemowych usług REST:

Aby skonfigurować zabezpieczenia danych w widgetach na podstawie użytkowników i grup, należy zmodyfikować użytkowników odwzorowanych na aplikację bramy usług REST.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Sposób odwzorowania użytkowników na aplikację dostawcy usług REST ma wpływ na wszystkie usługi dostawcy.

Aby wyświetlić usługi, na które to działanie ma wpływ, należy wybrać opcję **Usługi > Usługi REST > Dostawcy usług REST** i wybrać odpowiednią aplikację dostawcy z listy dostawców.

1. Wybierz jedną z następujących opcji w Konsoli administracyjnej:
 - W przypadku środowiska serwera należy wybrać opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere > Brama usług REST**.
 - Ponadto w przypadku środowiska wdrożenia sieciowego należy wybrać opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere > Menedżer wdrażania bramy usług REST**.
2. W panelu po prawej stronie w obszarze Właściwości szczegółowe wybierz opcję **Odwzorowanie roli zabezpieczeń na użytkownika/grupę**.
3. Aby kontrolować dostęp do danych we wszystkich widgetach usług REST, należy dodać użytkowników i grupy do roli **RestServicesUser**.

Uwagi dotyczące zabezpieczeń widgetów produktu Business Space:

Zależnie od widgetów używanych w produkcie Business Space z produktem do zarządzania procesami biznesowymi można przypisać role grupy użytkowników administracyjnych w celu kontroli dostępu do danych widgetu lub przypisać dla widgetu dodatkową warstwę dostępu opartego na rolach.

Role grupy administracyjnej i widgety

Dostęp do danych widgetów można kontrolować za pomocą ról grupy administracyjnej i użytkowników przypisanych do tych ról. Aby określić, kogo przypisano do tych ról, należy

otworzyć Konsolę administracyjną i wybrać opcję **Użytkownicy i grupy > Role grupy administracyjnej** oraz grupę. Zostanie wyświetlona lista Role.

Reguły biznesowe i Zmienne biznesowe to dwa przykładowe widgety, które mogą wymagać dokonania zmian w rolach grupy administracyjnej.

W przypadku widgetu Poprawność systemu wszystkie następujące role grupy administracyjnej mają uprawnienia do monitorowania i umożliwiają uzyskanie dostępu do Konsoli administracyjnej (a zatem użytkownikom przypisanym do tych ról zezwalają na dostęp do danych widgetu Poprawność systemu):

- **Monitorujący**
- **Konfigurujący**
- **Operator**
- **Administrator**
- **Menedżer zabezpieczeń administracyjnych**
- **Wdrażający**
- **iscadmins**

Użytkownicy, którzy są odwzorowani na te role grupy administracyjnej, mają dostęp do danych widgetu Poprawność systemu. Użytkownicy, którzy nie są odwzorowani na te role, nie mogą uzyskać dostępu do danych widgetu Poprawność systemu.

Dostęp do widжетów oparty na rolach

Konfigurowanie serwera WebSEAL produktu Tivoli Access Manager do pracy z produktem Business Space:

Jeśli używany jest serwer WebSEAL produktu Tivoli Access Manager i użytkownik chce go używać z produktem Business Space, należy wykonać dodatkowe kroki konfiguracji.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Aby używać serwera WebSEAL produktu Tivoli Access Manager z produktem Business Space, należy skonfigurować zabezpieczenia produktu Tivoli Access Manager do używania zewnętrznego dostawcy JACC (Java Authorization Contract for Containers), skonfigurować serwer WebSEAL do używania produktu Tivoli Access Manager, skonfigurować serwer WebSEAL do używania serwera aplikacji produktu oraz skonfigurować połączenia hostów dla używanego środowiska.

1. Skonfiguruj produkt Tivoli Access Manager w celu włączenia zewnętrznego dostawcy JACC.
 - a. Wykonaj jeden z następujących kroków w zależności od tego, czy ma być używana Konsola administracyjna, czy komendy narzędzia wsadmin.
 - Aby przy użyciu Konsoli administracyjnej skonfigurować produkt Tivoli Access Manager w celu włączenia dostawcy JACC, wykonaj następujące kroki:
 - 1) Włącz zabezpieczenia globalne.
 - a) Wybierz opcję **Zabezpieczenia > Zabezpieczenia globalne**.

- b) Włącz **zabezpieczenia administracyjne, zabezpieczenia aplikacji i zabezpieczenia Java 2** na serwerze LDAP, na którym skonfigurowano produkt Tivoli Access Manager.
- c) Wybierz opcję **Zabezpieczenia globalne > LDAP**, wprowadź poniższe informacje i kliknij przycisk **OK**.

| Nazwa | Opis |
|-----------------------------------|--|
| Identyfikator użytkownika serwera | Należy wprowadzić ten sam identyfikator użytkownika, który wprowadzono dla nazwy wyróżniającej administratora w ustawieniach produktu Tivoli Access Manager. Przykład: użytkownik1 |
| Hasło użytkownika serwera | haslo_użytkownika_1 |
| Host | Serwer LDAP skonfigurowany do używania z produktem Tivoli Access Manager. |
| Port | Przykład: 389 |
| Podstawowa nazwa wyróżniająca | Przykład: o=ibm, c=pl |
| Nazwa wyróżniająca powiązania | Przykład: cn=SecurityMaster,secAuthority=Default |
| Hasło powiązania | Hasło użytkownika SecurityMaster |

- d) Należy zapisać konfigurację i zrestartować serwer.
- 2) Należy włączyć autoryzację zewnętrzną z produktem Tivoli Access Manager i dostawcą JACC.
- a) Należy wybrać opcję **Zabezpieczenia > Zabezpieczenia globalne > Zewnętrzni dostawcy autoryzacji**.
 - b) Z listy **Dostawca autoryzacji** należy wybrać opcję **Zewnętrzny dostawca JACC**, a następnie kliknąć opcję **Konfiguruj**. Właściwości domyślne produktu Tivoli Access Manager są poprawne. Wartości domyślnych nie należy zmieniać.
 - c) W obszarze **Właściwości dodatkowe** należy wybrać opcję **Właściwości produktu Tivoli Access Manager**. Należy wybrać opcję **Włącz osadzony produkt Tivoli Access Manager**, wprowadzić poniższe informacje, a następnie kliknąć przycisk **OK**.

| Nazwa | Wartość |
|---|--|
| Zbiór portów nasłuchiwania klientów | Ustawienie domyślne to 8900 - 8999. Należy je zmienić tylko wtedy, gdy mają być używane inne porty. |
| Serwer strategii (nazwa:port) | Należy określić zmienną <i>serwer_strategii:port</i> . Przykład: windomain3.rtp.raleigh.ibm.com:7135 |
| Serwery autoryzacji i priorytet (nazwa:port:priorytet) | Należy określić serwer autoryzacji, port i priorytet w formacie <i>serwer_autoryzacji:port:priorytet</i> . Przykład: windomain3.rtp.raleigh.ibm.com:7136:1 |
| Nazwa administratora | Należy pozostawić domyślną nazwę użytkownika jako sec_master , chyba że zostanie użyta inna nazwa administratora na serwerze Tivoli Access Manager. |
| Hasło administratora | domino123 |

| Nazwa | Wartość |
|--|--|
| Przyrostek nazwy wyróżniającej rejestru użytkowników | Należy wpisać nazwę, która ma zostać użyta dla serwera aplikacji. Przykład: o=ibm, c=pl |
| Domena zabezpieczeń | Dla opcji Domena zabezpieczeń należy pozostawić ustawioną wartość Domyślna . To ustawienie należy zmienić, jeśli nie jest używana domyślna domena na serwerze Tivoli Access Manager. To ustawienie należy zmienić, jeśli istnieje wiele domen utworzonych na serwerze Tivoli Access Manager, a użytkownik chce nawiązać połączenie z domeną inną niż domyślna lub chce użyć domeny innej niż domyślna. |
| Nazwa wyróżniająca administratora | Należy wpisać pełną nazwę użytkownika, Przykład: cn=użytkownik1,o=ibm,c=pl Uwaga: Jest to ten sam użytkownik co użytkownik określony przez opcję Identyfikator użytkownika serwera skonfigurowaną na panelu rejestru użytkowników LDAP. |

Serwer łączy się z serwerem produktu Tivoli Access Manager i tworzy kilka plików właściwości na serwerze aplikacji. Ten proces może trwać kilka minut. Jeśli wystąpi błąd, należy sprawdzić komunikaty w pliku SystemOut i rozwiązać problem.

- Aby użyć programu narzędziowego wsadmin do skonfigurowania produktu Tivoli Access Manager w celu włączenia dostawcy JACC, należy wykonać poniższe kroki. Poniższą procedurę należy wykonać raz na serwerze menedżera wdrażania. Parametry konfiguracyjne są przekazywane do serwerów zarządzanych, w tym agentów węzłów, gdy jest wykonywana synchronizacja. Serwery zarządzane wymagają zrestartowania, aby zmiany konfiguracji zostały zastosowane.

- 1) Należy sprawdzić, czy wszystkie serwery zarządzane, włącznie z agentami węzłów, są uruchomione.
- 2) Uruchom serwer.
- 3) Należy uruchomić program narzędziowy wiersza komend, uruchamiając komendę programu narzędziowego wsadmin z poziomu katalogu *instalacyjny_katalog_główny/bin*.
- 4) W wierszu komend programu narzędziowego wsadmin należy uruchomić komendę configureTAM, uwzględniając odpowiednie informacje z następującej tabeli:

Przykład kodu Jacl:

```
$AdminTask configureTAM -interactive
```

Przykład kodu Jython:

```
AdminTask.configureTAM('-interactive')
```

Następnie należy wpisać następujące informacje:

| Nazwa | Wartość |
|---|---|
| Nazwa węzła serwera produktu użytkownika | Należy określić pojedynczy węzeł lub wprowadzić znak gwiazdki (*), aby wybrać wszystkie węzły. |
| Serwer strategii produktu Tivoli Access Manager | Należy wpisać nazwę serwera strategii produktu Tivoli Access Manager oraz port połączenia. Należy użyć formatu <i>serwer_strategii:port</i> . Port komunikacyjny serwera strategii jest ustawiany podczas konfigurowania produktu Tivoli Access Manager. Domyślny port to 7135. |

| Nazwa | Wartość |
|---|--|
| Serwer autoryzacji produktu Tivoli Access Manager | Należy wpisać nazwę serwera autoryzacji produktu Tivoli Access Manager. Należy użyć formatu <i>serwer_autoryzacji:port:priorytet</i> . Port komunikacyjny serwera autoryzacji jest ustawiany podczas konfigurowania produktu Tivoli Access Manager. Domyślny port to 7136. Istnieje możliwość określenia wielu serwerów autoryzacji - wystarczy rozdzielić poszczególne wpisy przecinkami. Skonfigurowanie więcej niż jednego serwera autoryzacji jest użyteczne na potrzeby przełączania awaryjnego i umożliwia zwiększenie wydajności. Wartość priorytetu określa kolejność użycia serwerów autoryzacji. Przykład: <i>serwer_autoryzacji_1:7136:1,serwer_autoryzacji_2:7137:2</i> . Priorytet 1 jest wymagany podczas konfigurowania pojedynczego serwera autoryzacji. |
| Nazwa wyróżniająca administratora dla serwera produktu | Należy wpisać pełną nazwę wyróżniającą identyfikatora administratora zabezpieczeń dla serwera produktu. Przykład: <i>cn=wasadmin,o=organizacja,c=kraj</i> . Więcej informacji można uzyskać, korzystając z odsyłacza do strony pokrewnej. |
| Przyrostek nazwy wyróżniającej rejestru użytkowników produktu Tivoli Access Manager | Na przykład: <i>o=organizacja,c=kraj</i> |
| Nazwa administratora produktu Tivoli Access Manager | Należy wpisać identyfikator administratora produktu Tivoli Access Manager utworzony podczas konfigurowania produktu Tivoli Access Manager. Ten identyfikator to zazwyczaj <i>sec_master</i> . |
| Hasło administratora produktu Tivoli Access Manager | Należy wpisać hasło administratora produktu Tivoli Access Manager. |
| Domena zabezpieczeń produktu Tivoli Access Manager | Należy wpisać nazwę domeny zabezpieczeń produktu Tivoli Access Manager używanej do przechowywania użytkowników i grup. Jeśli podczas konfiguracji produktu Tivoli Access Manager nie jest jeszcze określona domena zabezpieczeń, należy kliknąć przycisk Wróć , aby zaakceptować wartość domyślną. |
| Zbiór portów nasłuchiwanie osadzonego produktu Tivoli Access Manager | Serwer produktu nasłuchuje na porcie TCP/IP w celu pobrania aktualizacji bazy danych autoryzacji z serwera strategii. Ponieważ w określonym węźle i na określonym komputerze może być uruchomionych wiele procesów, konieczne jest określenie dla nich listy portów. Należy określić porty używane jako porty nasłuchiwanie przez klienty produktu Tivoli Access Manager, rozdzielając wartości przecinkami. W przypadku określania zakresu portów należy oddzielić dwukropkiem najmniejszą wartość portu od największej, na przykład: <i>7999, 9990:9999</i> . |

| Nazwa | Wartość |
|--------|---|
| Odrocz | Jeśli ta opcja została ustawiona na wartość Tak, konfigurowanie serwera zarządzania jest odraczane do następnego restartu serwera. Jeśli ta opcja została ustawiona na wartość Nie, konfigurowanie serwera zarządzania jest wykonywane natychmiast. Serwery zarządzane są konfigurowane przy następnym restarcie. |

- 5) Po wprowadzeniu wszystkich wymaganych informacji należy wybrać opcję **F**, aby zapisać właściwości konfiguracyjne, lub opcję **C**, aby anulować proces konfigurowania i odrzucić wprowadzone informacje.

Przykład dla serwera SVTM TAM60:

```
wsadmin>$AdminTask configureTAM -interactive
Konfigurowanie osadzonego produktu Tivoli Access Manager
```

Ta komenda umożliwia skonfigurowanie osadzonego produktu Tivoli Access Manager w określonym węźle lub określonych węzłach serwera WebSphere Application Server.

```
Nazwa węzła serwera WebSphere Application Server (nodeName): *
*Serwer strategii produktu Tivoli Access Manager (policySvr):
  windomain3.rtp.raleigh.ibm.com:7135
*Serwery autoryzacji produktu Tivoli Access Manager (authSvrs):
  windomain3.rtp.raleigh.ibm.com:7136:1
*Nazwa wyróżniająca administratora serwera WebSphere Application Server (wasAdminDN):
  cn=was61admin,o=ibm,c=pl
*Przyrostek nazwy wyróżniającej rejestru użytkowników produktu Tivoli Access
Manager (dnSuffix):
  o=ibm,c=pl
Nazwa administratora produktu Tivoli Access Manager (adminUid):
  [sec_master]
*Hasło administratora produktu Tivoli Access Manager (adminPasswd):
  domino123
Domena zabezpieczeń produktu Tivoli Access Manager (secDomain): [Domyślna]
Zbiór portów nasłuchiwania osadzonego produktu Tivoli Access Manager (portSet): [9900:9900]
Odrocz (defer): [nie]
```

Konfigurowanie osadzonego produktu Tivoli Access Manager

F (Zakończ)
C (Anuluj)

```
Wybierz [F, C]: [F] F
WASX7278I: Wygenerowany wiersz komend: $AdminTask
configureTAM {-policySvr
  windomain3.rtp.raleigh.ibm.com:7135 -authSvrs
  windomain3.rtp.raleigh.ibm.com:7136:1 -wasAdminDN cn=wa
Parametry działania konfiguracyjnego osadzonego produktu Tivoli Access Manager
zostały zapisane pomyślnie. Zrestartuj wszystkie instancje serwera
WebSphere Application Server działające w węźle docelowym lub
węzłach docelowych dla narzędzia
wsadmin>
```

- 6) W Konsoli administracyjnej należy wybrać opcję **Zabezpieczenia > Zabezpieczenia globalne > Zewnętrzni dostawcy autoryzacji**. Następnie należy wybrać opcję **Autoryzacja zewnętrzna za pomocą dostawcy JACC** i kliknąć przycisk **OK**.
- 7) Należy przejść do głównego ekranu zabezpieczeń i kliknąć przycisk **OK**. Należy zapisać i zsynchronizować zmiany.
- 8) Należy zrestartować wszystkie procesy serwera w komórce.

- b. Jeśli przed włączeniem produktu Tivoli Access Manager zainstalowano aplikacje (na przykład jeśli włączono zabezpieczenia LDAP i zainstalowano zabezpieczone aplikacje, a także odwzorowano użytkowników i grupy na role zabezpieczeń), należy rozpropagować informacje dotyczące odwzorowania ról zabezpieczeń z deskryptorów wdrażania do serwera strategii produktu Tivoli Access Manager. Należy wykonać jeden z poniższych kroków zależnie od tego, czy ma zostać użyta Konsola administracyjna, czy komendy programu narzędziowego wsadmin.
 - Aby użyć komendy narzędzia wsadmin propagatePolicyToJACCProvider, należy zapoznać się z sekcją Propagowanie strategii zabezpieczeń zainstalowanych aplikacji do dostawcy JACC za pomocą skryptów narzędzia wsadmin.
 - Aby użyć Konsoli administracyjnej, należy zapoznać się z sekcją Propagowanie strategii zabezpieczeń i ról na potrzeby wcześniej wdrożonych aplikacji.
2. Skonfiguruj produkt WebSEAL do pracy z produktem Tivoli Access Manager.
- a. Upewnij się, że produkt WebSEAL został poprawnie zainstalowany i skonfigurowany.
 - b. Aby utworzyć zaufane konto użytkownika w produkcie Tivoli Access Manager, którego można użyć do skonfigurowania modułu TAI, wprowadź następujące komendy:


```
pdadmin -a sec_master -p domino123
pdadmin sec_master> user create -gsouser -no-password-policy taiuser
"cn=taiuser,ou=websphere,o=ibm,c=pl" taiuser taiuser ptaiuser
pdadmin sec_master> user modify taiuser password-valid yes
pdadmin sec_master> user modify taiuser account-valid yes
```
 - c. Utwórz przyłączenie między produktem WebSEAL oraz serwerem aplikacji produktu użytkownika przy użyciu opcji **-c iv_creds** dla przechwytywacza TAI++ i opcji **-c iv_user** dla przechwytywacza TAI. Wprowadź jedną z następujących komend w postaci jednego wiersza, stosując zmienne odpowiednie dla używanego środowiska:


```
W przypadku przechwytywacza TAI++
server task webseald-server create -t tcp -b supply -c iv_creds
-h nazwa_hosta -p numer_portu_serwera_aplikacji_websphere
/nazwa_przyłączenia
```

Wskazówka: Zmienna *nazwa_przyłączenia* musi rozpoczynać się od znaku /.
 - d. W pliku konfiguracyjnym produktu WebSEAL *katalog_instalacyjny_produkту_webseal/etc/webseald-default.conf* ustaw następujący parametr:


```
basicauth-dummy-passwd=hasło_użytkownika_produkту_webseal
```

Jeśli na przykład w produkcie Tivoli Access Manager zostały ustawione wartości taiuser/ptaiuser, należy ustawić następujący parametr: basicauth-dummy-passwd = ptaiuser

Jeśli wykorzystywane jest uwierzytelnianie przy użyciu formularza, należy ustawić następujące parametry:

```
forms-auth=both
ba-auth=none
```
3. Skonfiguruj produkt WebSEAL pod kątem współpracy z serwerem aplikacji produktu, włączając przechwytywacz TAI++ na serwerze.
- a. W Konsoli administracyjnej wybierz opcję **Zabezpieczenia globalne > Mechanizmy uwierzytelniania i utrata ważności**.
 - b. Rozwiń element **Bezpieczeństwo WWW i SIP** i wybierz opcję **Powiązanie zaufane**. Zaznacz pole wyboru i kliknij przycisk **Zastosuj**.

- c. Wybierz opcję **Przechwytywacze > TAMTrustAssociationInterceptorPlus > Właściwości niestandardowe** i dodaj następujące właściwości:

| Nazwa | Wartość |
|--|---|
| com.ibm.websphere.security.webseal.configURL | \${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties |
| com.ibm.websphere.security.webseal.id | iv-creds |
| com.ibm.websphere.security.webseal.loginId | taiuser (jeśli użytkownik taiuser/ptaiuser został utworzony w produkcie Tivoli Access Manager). |

- d. Zrestartuj komórkę serwera.
- e. Aby uzyskać dostęp do klienta, przejdź pod adres `https://nazwa_serwera_webseal:port_serwera_webseal/nazwa_przyłączenia/identyfikator_URI_WWW_klienta`.
4. Skonfiguruj przyłączenia hosta dla środowiska użytkownika, aby zostały wyświetlone widżety produktu Business Space. Wykonaj jeden z następujących kroków zależnie od tego, czy używane są przyłączenia hosta wirtualnego, czy przyłączenia hosta przezroczystego.
- W przypadku używania przyłączeń hosta wirtualnego należy utworzyć przyłączenie hosta wirtualnego. Dzięki użyciu przyłączenia hosta wirtualnego nie trzeba tworzyć oddzielnych przyłączeń.
 - a. Należy się upewnić, że host wirtualny został skonfigurowany. Przyłączenia hosta wirtualnego są zgodne z hostem oraz numerem portu i adresami przekazywania do hosta docelowego. Nie występuje filtrowanie adresów URL, a wszystkie zgodne żądania są przekazywane do hosta docelowego.
 - b. Należy się upewnić, że następujące aplikacje są dostępne dla tego samego hosta wirtualnego. Mogą to być niektóre lub wszystkie aplikacje zależnie od tego, jakie produkty są używane z produktem Business Space.
 - BPMAAdministrationWidgets_nazwa_węzła_nazwa_serwera (dla produktów WebSphere Enterprise Service Bus i IBM Business Process Manager)
 - BusinessSpaceHelpEAR_nazwa_węzła_nazwa_serwera (w przypadku wszystkich produktów)
 - BSpaceEAR_nazwa_węzła_nazwa_serwera (w przypadku wszystkich produktów)
 - BSpaceForms_nazwa_węzła_nazwa_serwera (w przypadku wszystkich produktów)
 - HumanTaskManagementWidgets_nazwa_węzła_nazwa_serwera (dla produktów IBM Business Process Manager i IBM Business Monitor)
 - PageBuilder2_nazwa_węzła_nazwa_serwera (w przypadku wszystkich produktów)
 - Brama usług REST (w przypadku wszystkich produktów)
 - Menedżer wdrażania bramy usług REST (w przypadku produktu WebSphere Enterprise Service Bus oraz produktu IBM Business Process Manager)
 - mm.was_nazwa_węzła_nazwa_serwera (w przypadku wszystkich produktów)
 - WBMDashboardWeb_nazwa_węzła_nazwa_serwera (dla produktu IBM Business Monitor)
 - wesbWidgets_nazwa_węzła_nazwa_serwera (dla produktu WebSphere Enterprise Service Bus)

Uwaga: Ta lista aplikacji obejmuje tylko aplikacje wymagane przez produkt Business Space. W przypadku scenariuszy bez produktu Business Space może być konieczne dodanie innych aplikacji do listy przy użyciu produktu Tivoli Access Manager WebSEAL.

- c. Należy uruchomić następującą komendę przy użyciu narzędzia pdadmin: `server task serwer_webseal virtualhost create -t transport -h host_docelowy [-p port] [-v nazwa_hosta_wirtualnego] etykieta_hosta_wirtualnego`

Użyj następujących informacji:

- Zmienna `serwer_webseal` to nazwa serwera WebSEAL, na którym zostanie utworzona definicja hosta wirtualnego.
- Zmienna `transport` to typ transportu. Poprawne wpisy to `tcp`, `ssl`, `tcpproxy` i `sslproxy`.
- Zmienna `host_docelowy` to host wymaganej aplikacji.
- Zmienna `nazwa_hosta_wirtualnego` jest używana do uzgadniania żądań HTTP z przyłączeniem hosta wirtualnego. Jeśli nie zostanie wprowadzona żadna wartość, domyślnie składa się ona z hosta docelowego i portu. Na przykład jeśli zmienna `nazwa_hosta_wirtualnego` zostanie ustawiona na wartość `mojhostwirtualny.ibm.com:80`, serwer WebSEAL dopasowuje adresy URL zawierające łańcuch `mojhostwirtualny.ibm.com:80` i kieruje je do hosta udostępnionego w komendzie pdadmin.
- Zmienna `etykieta_hosta_wirtualnego` to etykieta używana do identyfikowania pozycji w produkcie WebSEAL. Musi być ona unikalna.

Aby produkt Business Space działał zgodnie z oczekiwaniami, zarówno pozycja `ssl`, jak i pozycja `tcp` muszą zostać utworzone dla typu transportu. Gdy to samo przyłączenie hosta wirtualnego ma obsługiwać protokół SSL (Secure Sockets Layer) i TCP (Transmission Control Protocol), należy użyć opcji `-g etykieta_hosta_wirtualnego`, gdzie `etykieta_hosta_wirtualnego` to pierwotna etykieta hosta wirtualnego używana do współużytkowania konfiguracji. Ta opcja znajduje wcześniej utworzone przyłączenie hosta wirtualnego (utworzone wcześniej, gdzie wartość `etykieta_hosta_wirtualnego` jest zgodna z etykietą podaną przy użyciu opcji `-g`) i udostępnia konfigurację do współużytkowania. Druga pozycja nadal wymaga własnej zmiennej `etykieta_hosta_wirtualnego`, ale może współużytkować host docelowy, port, a także inne wartości. Jeśli opcja `-g` nie zostanie podana, nie można utworzyć drugiego hosta wirtualnego, ponieważ produkt WebSEAL będzie traktował host docelowy oraz port jako identyczne z wcześniej utworzonym przyłączeniem (co nie jest dozwolone).

- W przypadku używania przyłączeń hosta przezroczystego należy utworzyć serię przyłączeń przezroczystej ścieżki dla widgetów każdego produktu.
 - a. Należy uruchomić następującą komendę przy użyciu narzędzia pdadmin: `server task serwer_webseal create -t typ_transportu (ssl lub tcp) -x -h hostname ścieżka`
Na przykład można wpisać: `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`.
 - b. Należy utworzyć następujące kontekstowe katalogi główne dla produktu użytkownika: Odwzorowywanie adresów URL produktu Business Space dla odwrotnego serwera proxy.

5. Wykonaj dodatkowe kroki konfiguracyjne, aby rozwiązać problemy z informacjami cookie przeglądarki i hostami wirtualnymi.

- a. Aby rozwiązać problem ze zmianą nazwy informacji cookie produktu Business Space, dodaj następującą treść do pliku konfiguracyjnego produktu WebSEAL:

```
[preserve-cookie-names]
```

```
name = com.ibm.bspace.UserName
```

name = com.ibm.wbimonitor.UserName

- b. Opcjonalne: W przypadku używania hostów wirtualnych innych niż domyślne z kontekstowym katalogiem głównym mogą wystąpić problemy ze stronami produktu Business Space. Może być konieczne dodanie przyłączenia -j do kontekstowego katalogu głównego w celu zapobieżenia ponownemu zapisaniu przez przyłączenie kodu języka JavaScript na stronach produktu Business Space. Uruchom następującą komendę: `server task default-webseald create -f -h nazwa_hosta -p numer_portu -t tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/kontekst_główny`

Przypisywanie roli administratora produktu Business Space:

Produkt Business Space umożliwia przypisywanie użytkownikom roli administratora (lub administratora produktu Business Space). Administrator może wyświetlać, edytować i usuwać wszystkie obszary i strony, tworzyć szablony i zarządzać nimi, a także zmieniać prawa własności obszarów, zmieniając ID właściciela.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Rolę administratora użytkownika produktu Business Space należy przypisać przy użyciu następującej roli zabezpieczeń serwera aplikacji: **Administrator**. Ta metoda pozwala na elastyczne przypisywanie roli do dowolnej liczby użytkowników i grup istniejących w organizacji użytkownika. Nie wymaga ona tworzenia grupy administratorów w rejestrze użytkowników jedynie po to, aby stanowiła centralny punkt dla administratora produktu Business Space.

Jeśli istnieje już administrator przypisany z wcześniejszej wersji produktu Business Space niż wersja 7.5, zamiast tego można zmodyfikować administratora przy użyciu grupy użytkownika. Więcej informacji zawiera temat Przypisywanie administratora produktu Business Space na podstawie grupy użytkowników.

- Jeśli administratorzy produktu Business Space są konfigurowani przy użyciu roli administratora po raz pierwszy, wykonaj następujące kroki:
 1. Zaloguj się do Konsoli administracyjnej produktu.
 2. Kliknij opcję **Aplikacje > Typy aplikacji > Aplikacje korporacyjne WebSphere**, a następnie wybierz jedną z następujących aplikacji:
 - **mm.was_węzeł_serwer** (w przypadku środowiska serwera autonomicznego).
 - **mm.was_klaster** (w przypadku środowiska wdrożenia sieciowego).
 3. Kliknij opcję **Odwzorowanie roli zabezpieczeń na użytkownika/grupę**.
 4. Wybierz wiersz dla roli **Administrator**, a następnie kliknij przycisk **Odwzoruj użytkowników** lub przycisk **Odwzoruj grupy** w celu odwzorowania użytkowników lub grup na rolę Administrator.
 5. Kliknij przycisk **Zapisz**.
 6. Zrestartuj serwer.
- Jeśli wcześniej przypisano administratorów na podstawie grup użytkowników i ma być używany prostszy sposób zarządzania administratorami, czyli według roli, wykonaj następujące kroki:
 1. Otwórz plik konfiguracyjny.

- Serwer autonomiczny: *katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties*
 - Klaster: *katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties*
2. W pliku konfiguracyjnym zmień następujące wartości właściwości.
`com.ibm.mashups.adminGroupName = {com.ibm.mashups.J2EERole.Admin}`
`com.ibm.mashups.widget.attributes.configure.groups=`
 3. W środowisku programu narzędziowego wsadmin dla profilu uruchom komendę `updatePropertyConfig`.

- Dla serwera autonomicznego:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask
updatePropertyConfig {-serverName
nazwa_serwera -nodeName nazwa_węzła
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_" }
$AdminConfig save
```

- Dla klastra:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-clusterName nazwa_klastra
-propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName
nazwa_klastra -propertyFileName
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\
config\ConfigService.properties" -prefix "Mashups_" }
$AdminConfig save
```

4. Zrestartuj serwer.
5. Wykonując czynności opisane w powyższym kroku, przypisz użytkowników do roli administratora produktu Business Space.

Przypisywanie administratora produktu Business Space według grupy użytkownika:

Użytkowników produktu Business Space można przypisać tak, aby byli administratorami (lub administratorami produktu Business Space) na podstawie grup użytkowników. Ta metoda jest przydatna, jeśli pracowano w wersji wcześniejszej niż 7.5, a rola administratora została już zdefiniowana według grupy użytkowników.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Wskazówka: Jeśli grupy użytkowników były wcześniej używane do przypisywania ról administratora produktu Business Space, można zacząć używać prostszej metody przypisywania administratorów produktu Business Space według ról. Więcej informacji na ten temat można znaleźć w sekcji “Przypisywanie ról administratora produktu Business Space” na stronie 242.

Administrator może wyświetlać, edytować i usuwać wszystkie obszary i strony, tworzyć szablony i zarządzać nimi, a także zmieniać prawa własności obszarów, zmieniając ID właściciela.

Jeśli zabezpieczenia administracyjne są włączone podczas konfigurowania produktu Business Space, należy wziąć pod uwagę następujące informacje dotyczące grup i administratorów:

- Użytkownicy należący do specjalnej grupy użytkowników **administrators** mają domyślnie rolę administratora. Oznacza to, że przypisanie ról administratora jest obsługiwane przez przypisanie do grupy użytkowników.
- W przypadku środowiska z pojedynczym serwerem serwer produktu Business Space tworzy grupę użytkowników **administrators** w domyślnym rejestrze użytkowników. Identyfikator administratora podany podczas konfigurowania zostaje automatycznie dodany jako element tej grupy.
- W środowisku wdrożenia sieciowego grupa użytkowników **administrators** nie jest tworzona automatycznie. W celu utworzenia grupy użytkowników i dodania do tej grupy członków w domyślnym rejestrze użytkowników należy użyć skryptu `createSuperUser.py`.
- Jeśli zamiast domyślnego rejestru użytkowników zostanie użyty inny rejestr użytkowników (na przykład LDAP) lub zostanie użyty domyślny rejestr użytkowników, ale nie zostanie użyta grupa użytkowników **administrators**, należy wskazać grupę użytkowników, którzy będą pełnili rolę administratorów produktu Business Space. Należy się upewnić, że podana wartość może zostać rozpoznana przez rejestr użytkowników. Na przykład w przypadku rejestru LDAP można podać nazwę `cn=administrators,dc=firma,dc=com`. Więcej informacji na temat identyfikowania tej grupy użytkowników zawierają instrukcje dotyczące zmiany grupy administratorów w sekcji Co dalej.
- W przypadku produktu Business Space w produkcie WebSphere Portal grupa domyślna **wpsadmins** jest także używana dla ról administratora. Członkom tej grupy nadawana jest rola administratora produktu Business Space.

Uwaga: Aby używać produktu Business Space w produkcie WebSphere Portal konieczne jest włączenie zabezpieczeń.

Jeśli podczas konfigurowania produktu Business Space nie są włączone zabezpieczenia administracyjne, tylko specjalny ID użytkownika **BPMAdministrator** ma rolę administratora produktu Business Space.

W przypadku środowiska wdrożenia sieciowego należy uruchomić skrypt `createSuperUser.py` służący do przypisywania ról administratora: w celu utworzenia grupy użytkowników i dodania członków. Zanim uruchomisz skrypt, wykonaj następujące kroki:

- Upewnij się, że domyślna nazwa grupy **administrators** nie została zmieniona.
 - Użyj domyślnego repozytorium dla rejestru użytkowników.
 - Uruchom serwer menedżera wdrażania dla środowiska produktu Business Space, dla profilu, w którym zainstalowany jest produkt Business Space.
1. Znajdź skrypt `instalacyjny_katalog_główny\BusinessSpace\scripts\createSuperUser.py` służący do przypisywania ról administratora użytkownikowi.

2. Otwórz wiersz komend i przejdź do następującego katalogu: *katalog_główny_profilu*\bin, gdzie *katalog_główny_profilu* reprezentuje katalog profilu, w którym zainstalowano produkt Business Space.
3. Wpisz następującą komendę: `wsadmin -lang jython -f katalog_główny_profilu\BusinessSpace\scripts\createSuperUser.py krótka_nazwa_użytkownika hasło`. Gdzie *nazwa_skrócona_użytkownika* jest unikalnym identyfikatorem użytkownika w produkcie Virtual Member Manager (VMM), a *hasło* jest hasłem do produktu VMM dla tego użytkownika. Jeśli użytkownik istnieje w produkcie VMM, zostanie on dodany do grupy administratorów.

Uwaga: Jeśli ścieżka zawiera spację (na przykład, gdy ścieżka *instalacyjny_katalog_główny* to Mój katalog instalacyjny), nazwy ścieżek należy ująć w cudzysłów. Na przykład można wpisać następującą komendę: `wsadmin -lang jython -f "Mój katalog instalacyjny\BusinessSpace\scripts\createSuperUser.py" krótka_nazwa_użytkownika_w_produkcie_VMM`.

Aby otworzyć produkt Business Space, należy użyć następującego adresu URL: `http://host:port/BusinessSpace`, gdzie *host* to nazwa hosta, na którym działa serwer użytkownika, a *port* to numer portu serwera użytkownika.

Domyślną specjalną grupę użytkowników o nazwie **administrators** można zmienić. Aby sprawdzić bieżącą nazwę grupy lub zmienić ją na inną, należy wykonać poniższe kroki.

Sprawdź wartość pomiaru `com.ibm.mashups.adminGroupName` w pliku konfiguracyjnym:

- *katalog_główny_profilu*\BusinessSpace*nazwa_węzła**nazwa_serwera*\mm.runtime.prof\config\ConfigService.properties na serwerze autonomicznym lub
- *katalog_główny_profilu_menedżera_wdrażania*\BusinessSpace*nazwa_klastra*\mm.runtime.prof\config\ConfigService.properties w klastrze.

Aby zmienić grupę administracyjną, na serwerze autonomicznym wykonaj następujące kroki:

1. Zmodyfikuj pomiar `com.ibm.mashups.adminGroupName` w pliku konfiguracyjnym *katalog_główny_profilu*\BusinessSpace*nazwa_węzła**nazwa_serwera*\mm.runtime.prof\config\ConfigService.properties.
2. Uruchom komendę `updatePropertyConfig` w środowisku programu narzędziowego `wsadmin` profilu: `$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}`, a następnie uruchom komendę `$AdminConfig save`.
3. Zrestartuj serwer.

Aby zmienić grupę administracyjną, wykonaj w klastrze następujące kroki:

1. Zmodyfikuj pomiar `com.ibm.mashups.adminGroupName` w pliku konfiguracyjnym *katalog_główny_profilu_menedżera_wdrażania*\BusinessSpace*nazwa_klastra*\mm.runtime.prof\config\ConfigService.properties.
2. Uruchom komendę `updatePropertyConfig` w środowisku programu narzędziowego `wsadmin` profilu środowiska wdrażania: `$AdminTask updatePropertyConfig {-clusterName nazwa_klastra -propertyFileName "katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}`, a następnie uruchom komendę `$AdminConfig save`.
3. Zrestartuj menedżer wdrażania.

Aby zmienić administratora, gdy zabezpieczenia nie są włączone, wykonaj następujące kroki na serwerze autonomicznym:

1. Zmodyfikuj pomiar `noSecurityAdminInternalUserOnly` w pliku konfiguracyjnym `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties`.
2. Uruchom komendę `updatePropertyConfig` w środowisku programu narzędziowego `wsadmin` profilu: `$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}`, a następnie uruchom komendę `$AdminConfig save`.
3. Zrestartuj serwer.

Aby zmienić administratora, gdy zabezpieczenia nie są włączone, wykonaj następujące kroki w klastrze:

1. Zmodyfikuj pomiar `noSecurityAdminInternalUserOnly` w pliku konfiguracyjnym `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties`.
2. Uruchom komendę `updatePropertyConfig` w środowisku programu narzędziowego `wsadmin` profilu środowiska wdrażania: `$AdminTask updatePropertyConfig {-clusterName nazwa_klastra -propertyFileName "katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}`, a następnie uruchom komendę `$AdminConfig save`.
3. Zrestartuj menedżer wdrażania.

Uniemożliwianie użytkownikom tworzenia obszarów biznesowych:

Produkt Business Space można skonfigurować w taki sposób, aby obszary biznesowe mogły być tworzone tylko przez użytkowników logujących się przy użyciu roli administratora.

Domyślnie obszary biznesowe mogą być tworzone przez wszystkich użytkowników. Możliwe jest jednak zablokowanie produktu Business Space w taki sposób, aby obszary biznesowe były tworzone lub importowane tylko przez osoby, które logują się za pomocą identyfikatora administratora. Administratorzy (lub administratorzy produktu Business Space) mogą tworzyć obszary biznesowe i przekazywać prawa własności innym użytkownikom. Użytkownicy z przypisanym prawem własności do obszarów mogą następnie administrować nimi tak, jakby utworzyli je sami. Na przykład mogą oni określić, kto może wyświetlać i edytować obszar oraz jego właściwości. Mogą również dodawać strony.

Uwaga: Funkcja pozwalająca na uniemożliwienie użytkownikom tworzenia obszarów biznesowych jest niedostępna w przypadku produktu Business Space działającego na platformie Business Space.

W celu ograniczenia możliwości tworzenia obszarów biznesowych tylko do administratorów wykonaj następujące kroki:

1. Zmień wartość ustawienia `com.ibm.mashups.lockeddown` na `true` w pliku konfiguracyjnym:
 - Serwer autonomiczny: `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties`
 - Klaster: `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties`

Wartość domyślna `false` oznacza, że wszyscy użytkownicy mogą tworzyć obszary biznesowe. Gdy wartością jest `true`, obszary biznesowe mogą być tworzone wyłącznie przez administratorów.

2. Uruchom komendę `updatePropertyConfig` w środowisku narzędzia `wsadmin` profilu:

- Dla serwera autonomicznego:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła  
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła  
-propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera  
\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

- Dla klastra:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-clusterName nazwa_klastra -propertyFileName  
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName nazwa_klastra -propertyFileName  
"katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\  
config\ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

Gdy następnym razem użytkownicy zalogują się do produktu Business Space, nie będą mogli utworzyć obszaru biznesowego, chyba że zalogują się za pomocą identyfikatora administratora.

Włączanie funkcji wyszukiwania repozytoriów użytkowników bez używania znaków wieloznacznych:

Jeśli rejestr użytkowników został skonfigurowany tak, aby nie były używane znaki wieloznaczne, należy wykonać dodatkowe kroki konfiguracyjne w celu zapewnienia poprawnego działania funkcji wyszukiwania w produkcie Business Space, a także w przypadku widgetów służących do wyszukiwania w rejestrze użytkowników.

Przed wykonaniem tej czynności muszą zostać wykonane następujące czynności:

- Należy włączyć zabezpieczenia aplikacji i zabezpieczenia administracyjne. Więcej informacji na ten temat można znaleźć w sekcji “Włączanie zabezpieczeń dla produktu Business Space” na stronie 226.
- Należy sprawdzić, czy identyfikator użytkownika został zarejestrowany w rejestrze użytkowników produktu.

Domyślnie, gdy użytkownik produktu Business Space szuka użytkowników lub grup, wpisując co najmniej jeden znak, produkt Business Space automatycznie dodaje znaki wieloznaczne. Jeśli na przykład rejestrem użytkowników jest serwer LDAP, a użytkownik wpisze frazę `KOWA`, produkt Business Space przekształci tę frazę w zapytanie `*KOWA*` tak, aby zostały zwrócone nazwy podobne do następujących: `KOWA`, `KOWALSKI` i `PKOWA`. Jeśli jednak funkcja automatycznego dodawania znaków wieloznacznych nie jest pożądana (na przykład gdy nie zezwala na nią rejestr użytkowników), można wyłączyć tę funkcję.

Aby wyłączyć funkcję wyszukiwania z automatycznym dodawaniem znaków wieloznacznych dla środowiska użytkownika, wykonaj następujące kroki:

- W przypadku serwera autonomicznego wykonaj następujące kroki:
 1. Zaktualizuj plik konfiguracyjny *katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties*, ustawiając właściwość `com.ibm.mashups.user.stripWildcards=true`.
 2. Uruchom komendę `updatePropertyConfig` w środowisku narzędzia `wsadmin` profilu:
W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```


W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```
 3. Zrestartuj serwer.
- W przypadku klastra wykonaj następujące kroki:
 1. Zaktualizuj plik konfiguracyjny *katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties*, ustawiając właściwość `com.ibm.mashups.user.stripWildcards=true`.
 2. Z poziomu menedżera wdrażania uruchom komendę `updatePropertyConfig` w środowisku narzędzia `wsadmin` profilu:
W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-clusterName nazwa_klastra -propertyFileName "katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```


W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName nazwa_klastra -propertyFileName "katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```
 3. Zrestartuj menedżer wdrażania.

Konfigurowanie proxy Ajax produktu Business Space

Proxy Ajax produktu Business Space można dostosowywać do szczególnych wymagań, na przykład wprowadzając zmienne ustawienia limitów czasu lub blokując adresy IP w celu zabezpieczenia środowisk produkcyjnych.

Plik proxy Ajax `proxy-config.xml` znajduje się w następujących położeniach:

- Dla środowiska produktu Business Space dostarczanego z produktem do zarządzania procesami biznesowymi: *katalog_główny_profilu/BusinessSpace/nazwa_węzła/nazwa_serwera/mm.runtime.prof/config/proxy-config.xml*.

W przypadku problemów z proxy Ajax należy zapoznać się z notami technicznymi dotyczącymi stron zespolonych IBM, które znajdują się pod adresem <http://www-01.ibm.com/support/search.wss?tc=SSWP9P>.

Ważne: Domyślnie konfiguracja proxy Ajax używana z widgetami produktu Business Space nie ogranicza dostępu do żadnych adresów IP. Dla wygody użytkownika proxy Ajax jest domyślnie skonfigurowane tak, aby było otwarte. Taka sytuacja stanowi zagrożenie dla bezpieczeństwa w przypadku środowiska produkcyjnego. Aby skonfigurować proxy Ajax tak, aby umożliwiała wyświetlanie treści tylko z wybranych serwisów lub blokowało treść z tych serwisów, należy wykonać kroki opisane w temacie Blokowanie adresów IP przy użyciu proxy Ajax produktu Business Space.

1. Zmodyfikuj plik `proxy-config.xml` w odpowiedni sposób.

Jeśli na przykład zmieniane są ustawienia limitów czasu dla proxy Ajax produktu Business Space, należy zmodyfikować element `proxy:value` dla elementu `socket-timeout`.

2. Uruchom komendę `updateBlobConfig` przy użyciu klienta skryptowego `wsadmin`, wyznaczając parametry `-serverName` i `-nodeName` dla serwera autonomicznego lub `-clusterName` dla klastra, `-propertyFileName` z wartością ścieżki do pliku `proxy-config.xml` i `-prefix` z wartością `Mashups_`.

W poniższym przykładzie użyto języka Jython: `AdminTask.updateBlobConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu/BusinessSpace/nazwa_węzła/nazwa_serwera/mm.runtime.prof/config/proxy-config.xml" -prefix "Mashups_"'])`

W poniższym przykładzie użyto języka Jacl: `$AdminTask updateBlobConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu/BusinessSpace/nazwa_węzła/nazwa_serwera/mm.runtime.prof/config/proxy-config.xml" -prefix "Mashups_"}`

Zmianianie ustawień limitu czasu dla proxy Ajax produktu Business Space:

Produkt Business Space używa komponentu proxy na potrzeby nawiązywania połączenia z usługami REST użytkownika. Jeśli usługi REST nie odpowiadają, należy zaktualizować ustawienia limitu czasu połączenia z produktu Business Space do usług REST użytkownika zależnie od wydajności serwerów usługi REST.

Jeśli występują przekroczenia limitu czasu połączeń usługi REST, należy zaktualizować następujące ustawienia.

W przypadku używania środowiska produktu Business Space, które jest dostarczane z produktem do zarządzania procesami biznesowymi, wartość `socket-timeout` jest domyślnie ustawiona na 30 sekund. Należy ją zmienić na wartość odpowiednią dla sytuacji użytkownika.

W przypadku używania produktu Business Space z produktem WebSphere Portal wartość `socket-timeout` jest domyślnie ustawiona na 10 sekund. Należy ją zmienić na wartość odpowiednią dla sytuacji użytkownika (30 sekund w przypadku używania widgetów administracyjnych produktu IBM Business Process Manager).

1. Otwórz plik `proxy-config.xml`. Informacje dotyczące miejsca, w którym można znaleźć plik proxy Ajax, zawiera temat “Konfigurowanie proxy Ajax produktu Business Space” na stronie 248.
2. Zmień wartość elementu `proxy:value` dla elementu `socket-timeout`. Czas jest określany w milisekundach.

```
<proxy:meta-data>
  <proxy:name>socket-timeout</proxy:name>
  <proxy:value>30000</proxy:value>
</proxy:meta-data>
```

3. Zakończ konfigurację proxy Ajax, aby odpowiadała środowisku użytkownika. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie proxy Ajax produktu Business Space” na stronie 248.

Blokowanie adresów IP przy użyciu proxy Ajax produktu Business Space:

Proxy Ajax przekazuje żądania z widgetów do serwerów produktu i serwerów docelowych użytkownika, jeśli serwery te są zdalne względem serwera produktu Business Space. Domyślnie konfiguracja proxy Ajax nie ogranicza dostępu do żadnych adresów IP, co nie jest bezpieczne dla środowisk produkcyjnych. Proxy Ajax należy skonfigurować w taki sposób, aby były wyświetlane treści tylko z wybranych serwisów lub aby były blokowane treści z wybranych serwisów.

Ważne: Domyślnie konfiguracja proxy Ajax używana z widgetami produktu Business Space nie ogranicza dostępu do żadnych adresów IP. Dla wygody użytkownika proxy Ajax jest domyślnie skonfigurowane tak, aby było otwarte. Taka sytuacja stanowi zagrożenie dla bezpieczeństwa w przypadku środowiska produkcyjnego. Aby skonfigurować proxy Ajax do wyświetlania treści tylko z wybranych serwisów lub blokowania treści z wybranych serwisów, wykonaj następujące czynności.

Jeśli zachodzi potrzeba ograniczenia dostępu do konkretnych adresów IP, można dokonać edycji proxy Ajax w taki sposób, aby adresy IP były filtrowane w celu zezwalania na dostęp lub odmawiania dostępu. Reguły czarnej lub białej listy należy zdefiniować w pliku proxy-config.xml.

1. Otwórz plik proxy-config.xml. Informacje dotyczące miejsca, w którym można znaleźć plik proxy Ajax, zawiera temat “Konfigurowanie proxy Ajax produktu Business Space” na stronie 248.
2. Dodaj reguły filtrowania, które służą do zezwalania na dostęp lub odmawiania dostępu.

Aby zdefiniować regułę czarnej listy dla konkretnego adresu IP lub zestawu adresów, należy użyć elementu proxy:deny. Aby zdefiniować regułę białej listy dla konkretnego adresu IP lub zestawu adresów, należy użyć elementu proxy:allow. Reguły filtrowania są stosowane kolejno, przy czym ostatnia mająca zastosowanie reguła filtrowania ma pierwszeństwo przed wcześniejszymi regułami filtrowania.

```
<proxy-rules
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:proxy="http://www.ibm.com/xmlns/prod/sw/ajax/proxy-config/1.1">
<proxy:mapping contextpath="/proxy/*" />

<proxy:policy url="*" acf="none">
<proxy:actions>
<proxy:method>GET</proxy:method>
</proxy:actions>
</proxy:policy>

<proxy:ipfilter>
<proxy:deny>9.6.0.0/255.255.0.0</proxy:deny>
<proxy:allow>9.6.1.0/255.255.255.0</proxy:allow>
<proxy:deny>9.6.1.4</proxy:deny>
</proxy:ipfilter>
</proxy-rules>
```

W tym przykładzie filtr IP wykonuje następujące operacje filtrowania:

- blokuje wszystkie adresy IP 9.6.*.*
- zezwala na dostęp do adresów IP 9.6.1.*, ale blokuje konkretny adres IP 9.6.1.4

W tym przypadku proxy nie zezwala więc na dostęp do adresów IP 9.6.2.5 oraz 9.6.120.7 i w odpowiedzi wyświetla komunikat: BMWPX0018E: Określony adres IP hosta docelowego jest zabroniony przez regułę.

Proxy zezwala na dostęp do adresów IP 9.6.1.5 i 9.6.1.120, ale odmawia dostępu do adresu IP 9.6.1.4.

Dodając nowe reguły filtrowania, można je składać na kilka sposobów, jednak proxy zawsze stosuje je w określonej kolejności. Ostatnia zgodna reguła zawsze jest skuteczna, bez względu na to, jakie reguły zezwolenia na dostęp lub odmowy dostępu ją poprzedzają.

3. Zakończ konfigurację proxy Ajax, aby odpowiadała środowisku użytkownika. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie proxy Ajax produktu Business Space” na stronie 248.

Komendy (skrypty programu wsadmin) konfigurowania produktu Business Space

Aby uzyskać szczegóły dotyczące składni komendy, należy wyszukać obiekt skryptowy lub klasę komendy.

Aby otworzyć spis treści Centrum informacyjnego wskazujący położenie tych informacji uzupełniających, należy kliknąć przycisk **Pokaż w spisie treści** znajdujący się na ramce Centrum informacyjnego.

Komenda `configureBusinessSpace`:

Komenda `configureBusinessSpace` służy do konfigurowania bazy danych dla produktu Business Space opartego na technologii WebSphere.

Ta komenda konfiguruje źródło danych dla produktu Business Space i generuje skrypty, które tworzą i konfigurują tabele bazy danych.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
`AdminConfig.save()`
- W przypadku języka Jacl:
`$AdminConfig save`

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra dla konfiguracji. W celu skonfigurowania produktu Business Space w klastrze należy określić parametr **clusterName**.

Parametry opcjonalne

-dbName *nazwa_bazy_danych*

Określa bazę danych używaną dla produktu Business Space. Jeśli serwer aplikacji i baza danych DB2 znajdują się w tym samym obrazie systemu z/OS, parametr **-dbName** musi zostać podany.

-schemaName *nazwa_schematu*

Parametr opcjonalny, który określa schemat bazy danych dla konfiguracji bazy danych produktu Business Space. Wartość domyślna to **IBMBUSSP**.

-tablespaceDir *ścieżka_do_obszaru_tabel*

Parametr opcjonalny, który określa ścieżkę do katalogu lub przedrostek nazwy pliku dla plików używanych jako fizyczne położenie obszarów tabel. Wartość domyślna to **BSP**. Parametr jest poprawny dla baz danych DB2, Oracle i SQL Server (w przypadku innych baz danych jest ignorowany). W przypadku bazy danych SQL Server ten parametr dotyczy głównego pliku danych i plików dziennika.

-tablespaceNamePrefix *przedrostek_obszaru_tabel*

Parametr opcjonalny, który określa łańcuch przedrostka dodawany na początku nazw obszarów tabel, aby były one unikalne. Wartość domyślna to **BSP**. Jeśli przedrostek nazwy obszaru tabel zawiera więcej niż cztery znaki, zostanie obcięty do czterech znaków. Ten parametr jest poprawny dla baz danych DB2, DB2 z/OS 8, DB2 z/OS 9 i Oracle (w przypadku innych baz danych jest ignorowany).

-dbLocationName *nazwa_położenia_bazy_danych*

Parametr opcjonalny, który określa nazwę położenia bazy danych w systemie z/OS. Wartość domyślna to **BSP** lub nazwa bazy danych produktu. Parametr jest poprawny dla baz danych DB2 z/OS 8 i 9 (w przypadku innych baz danych jest ignorowany).

-storageGroup *grupa_pamięci_masowej*

Parametr opcjonalny, który określa grupę pamięci masowej w systemie z/OS dla produktu Business Space. Jeśli jest używany system z/OS, przed uruchomieniem wygenerowanych skryptów bazy danych konieczne jest ich zaktualizowanie. Więcej informacji o skryptach zawiera temat Konfigurowanie tabel bazy danych produktu Business Space.

-bspacedbDesign *nazwa_pliku_projektu_bazy_danych*

Parametr opcjonalny, który określa plik projektu bazy danych używany do definiowania wszystkich informacji konfiguracyjnych bazy danych, w tym schematu i katalogu obszaru tabel. Jeśli plik projektu bazy danych zostanie wskazany za pomocą parametru **-bspacedbDesign**, nie jest konieczne podawanie parametrów **-schemaName**, **-tablespaceDir** ani **-storageGroup**, chyba że istnieje potrzeba przesłonięcia konkretnych informacji konfiguracyjnych bazy danych znajdujących się w pliku projektu bazy danych.

Uwaga: Dla źródła danych produktu Business Space zawsze jest używana nazwa JNDI jdbc/mashupDS, w związku z czym nazwa JNDI w pliku projektu bazy danych nie jest używana. Jeśli źródło danych z nazwą JNDI jdbc/mashupDS już istnieje, komenda przerywa działanie przed skonfigurowaniem profilu, chyba że zostanie określony również parametr **-replaceDatasource true**.

-productTypeForDatasource *baza_danych_produkту*

Parametr opcjonalny, który określa właściwości do użycia podczas tworzenia źródła danych dla produktu Business Space. Podanie parametru **productTypeForDatasource** powoduje utworzenie źródła danych dla produktu Business Space o nazwie JNDI jdbc/mashupDS. Źródło jest modelowane na podstawie źródła danych zainstalowanego produktu, na przykład produktu IBM Process Server, WebSphere Enterprise Service Bus, IBM Business Monitor i WebSphere Business Compass. Poprawne wartości to: **WPS** (dla produktu IBM Business Process Manager lub WebSphere Enterprise Service Bus),

WPBS (dla produktu WebSphere Business Compass) i WBM (dla produktu IBM Business Monitor). Jeśli określony jest również parametr **bspacedbDesign**, to parametr **productTypeForDatasource** przesłania typ bazy danych i dostawcę JDBC, a nazwa JNDI w pliku projektu bazy danych nie jest używana.

Uwaga: Jeśli źródło danych z nazwą JNDI jdbc/mashupDS już istnieje, komenda przerywa działanie przed skonfigurowaniem profilu, chyba że zostanie określony również parametr `-replaceDatasource true`.

-replaceDatasource true|false

Parametr opcjonalny, który określa, czy komenda `configureBusinessSpace` jest uruchamiana, jeśli profil został już skonfigurowany. Wartość domyślna to `false`. Podczas konfigurowania profilu dla produktu Business Space tworzone jest źródło danych o nazwie JNDI jdbc/mashupDS. Jeśli źródło danych już istnieje, a komenda `configureBusinessSpace` zostanie uruchomiona bez określenia parametru `-replaceDatasource true`, nie zmieni ona konfiguracji. Jeśli zostanie podana wartość `true`, komenda usuwa źródło danych i jego dostawcę JDBC oraz tworzy nowe źródło danych, nowego dostawcę JDBC i nowe skrypty DDL.

-save true|false

Parametr, który określa, czy zmiany konfiguracji mają zostać zapisane. Wartość domyślna to `false`.

Przykłady

W poniższym przykładzie komenda `configureBusinessSpace` została użyta do skonfigurowania źródła danych produktu Business Space na serwerze.

- Przykład kodu Jython:

```
AdminTask.configureBusinessSpace(['-nodeName mój_węzeł -serverName mój_serwer'])
```

- Przykład kodu Jacl:

```
$AdminTask configureBusinessSpace {-nodeName mój_węzeł -serverName mój_serwer}
```

W poniższym przykładzie komenda `configureBusinessSpace` została użyta do skonfigurowania źródła danych produktu Business Space w klastrze i zapisania zmian.

- Przykład kodu Jython:

```
AdminTask.configureBusinessSpace(['-clusterName mój_klaster -save true'])
```

- Przykład kodu Jacl:

```
$AdminTask configureBusinessSpace {-clusterName mój_klaster -save true}
```

W poniższym przykładzie komenda `configureBusinessSpace` została użyta do skonfigurowania źródła danych produktu Business Space w klastrze przy użyciu nazwy schematu i źródła danych produktu określonych dla produktu IBM Process Server.

- Przykład kodu Jython:

```
AdminTask.configureBusinessSpace(['-clusterName mój_klaster -schemaName mój_klaster -productTypeForDatasource WPS -save true'])
```

- Przykład kodu Jacl:

```
$AdminTask configureBusinessSpace {-clusterName mój_klaster -schemaName mój_klaster -productTypeForDatasource WPS -save true}
```

W poniższym przykładzie komenda `configureBusinessSpace` została użyta do skonfigurowania źródła danych produktu Business Space w klastrze przy użyciu informacji bazy danych, które znajdują się w pliku projektu bazy danych.

- Przykład kodu Jython:

```
AdminTask.configureBusinessSpace('[-clusterName mój_klaster  
-bspacedbDesign "C:/Bspace_dbDesign.properties" -save true]')
```

- Przykład kodu Jacl:

```
$AdminTask configureBusinessSpace {-clusterName mój_klaster  
-bspacedbDesign "C:/Bspace_dbDesign.properties" -save true}
```

Komenda `createBPMApiFederationDomain`:

Komenda `createBPMApiFederationDomain` umożliwia konfigurowanie domen stowarzyszenia w środowisku z wieloma miejscami docelowymi wdrażania w taki sposób, aby na tej samej liście zadań można było wyświetlać procesy i zadania utworzone w produktach Process Designer i Integration Designer.

Komenda `createBPMApiFederationDomain` z krokiem `addTarget` tworzy domenę stowarzyszenia w celu stowarzyszenia zadań i procesów w co najmniej jednym miejscu docelowym wdrażania. Funkcja API stowarzyszenia umożliwia wyświetlanie procesów i zadań utworzonych w produktach Process Designer i Integration Designer na tej samej liście zadań. Funkcja API stowarzyszenia jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend `wsadmin` w celu utworzenia domen stowarzyszenia i zarządzania nimi. Krok `addTarget` umożliwia dodanie do domeny stowarzyszenia co najmniej jednego miejsca docelowego wdrażania. Funkcja API stowarzyszenia dokonuje stowarzyszenia wszystkich systemów w dodanych miejscach docelowych wdrażania.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Obiekt docelowy

Jest to zasięg, w którym zostanie utworzona domena stowarzyszenia. Obiekt docelowy może być używany zamiast parametrów `nodeName`, `serverName` i `clusterName`.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera, na którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `nodeName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest tworzona w zasięgu komórki.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła, w którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie

parametru **serverName**. Tego parametru nie należy określać w przypadku określenia parametru **clusterName** lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest tworzona w zasięgu komórki.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra, w którym powinna być administrowana domena stowarzyszenia. Tego parametru nie należy określać w przypadku określenia parametrów **nodeName** i **serverName** albo obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest tworzona w zasięgu komórki.

-name *nazwa_domeny_stowarzyszenia*

Nazwa nowej domeny stowarzyszenia tworzonej przez użytkownika. Ta nazwa musi być unikalna. Ten parametr jest zawsze wymagany.

Parametry wymagane w przypadku kroku addTarget

-targetCellName *nazwa_komórki*

Parametr określający nazwę komórki używanej jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, ale nie zostaną określone parametry **nodeName**, **serverName** i **clusterName**, funkcja API stowarzyszenia dokona stowarzyszenia we wszystkich systemach w komórce.

-targetNodeName *nazwa_węzła*

Parametr określający nazwę węzła używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach tego węzła. W przypadku określenia tego parametru konieczne jest określenie parametru **targetServerName**. Tego parametru nie należy określać w przypadku określenia parametru **targetClusterName**.

-targetServerName *nazwa_serwera*

Parametr określający nazwę serwera używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach na tym serwerze. W przypadku określenia tego parametru konieczne jest określenie parametru **targetNodeName**. Tego parametru nie należy określać w przypadku określenia parametru **targetClusterName**.

-targetClusterName *nazwa_klastra*

Parametr określający nazwę klastra używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach tego klastra. Tego parametru nie należy określać w przypadku określenia parametru **targetNodeName** lub **targetServerName**.

Przykłady

W poniższym przykładzie komenda createBPMApiFederationDomain została użyta w celu dodania domeny stowarzyszenia o nazwie *niestandardowa_domena_stowarzyszenia*, która dokonuje stowarzyszenia na serwerze (nazwa węzła: *mój_węzeł*, nazwa serwera: *mój_serwer*) i w klastrze (o nazwie *mój_klaster*).

- Przykład kodu Jython:

```
AdminTask.createBPMApiFederationDomain('[-nodeName nazwa_węzła  
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia  
-addTarget [{" mój_węzeł mój_serwer ""} [{" "" "" "" mój_klaster}]])')
```

- Przykład kodu Jacl:

```
$AdminTask createBPMApiFederationDomain {-nodeName nazwa_węzła  
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia  
-addTarget {"{"" mój_węzeł mój_serwer ""} {" "" "" "" mój_klaster}}
```

Komenda deleteBPMApiFederationDomain:

Komenda `deleteBPMApiFederationDomain` służy do usuwania domeny stowarzyszenia z uwzględnieniem zawartych w niej miejsc docelowych.

Ta komenda usuwa domenę stowarzyszenia wraz z zawartymi w niej miejscami docelowymi dla stowarzyszenia zadań i procesów w co najmniej jednym miejscu docelowym wdrażania. Funkcja API stowarzyszenia umożliwia wyświetlanie procesów i zadań utworzonych w produktach Process Designer i Integration Designer na tej samej liście zadań. Funkcja API stowarzyszenia jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend `wsadmin` w celu utworzenia domen stowarzyszenia i zarządzania nimi.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
`AdminConfig.save()`
- W przypadku języka Jacl:
`$AdminConfig save`

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Obiekt docelowy

Jest to zasięg, z którego zostanie usunięta domena stowarzyszenia. Obiekt docelowy może być używany zamiast parametrów `nodeName`, `serverName` i `clusterName`.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera, na którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `nodeName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła, w którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `serverName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra, w którym powinna być administrowana domena stowarzyszenia. Tego parametru nie należy określać w przypadku określenia parametrów `nodeName` i `serverName` albo obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-name *nazwa_domeny_stowarzyszenia*

Nazwa domeny stowarzyszenia, która ma zostać usunięta. Ta nazwa musi być unikalna. Ten parametr jest zawsze wymagany.

Przykłady

W poniższym przykładzie komenda `deleteBPMApiFederationDomain` została użyta do usunięcia domeny stowarzyszenia.

- Przykład kodu Jython:

```
AdminTask.deleteBPMApiFederationDomain(['-nodeName mój_węzeł -serverName mój_serwer -name moja_
```

- Przykład kodu Jacl:

```
$AdminTask deleteBPMApiFederationDomain {-nodeName mój_węzeł -serverName mój_serwer -name moja_
```

Komenda `getBusinessSpaceDeployStatus`:

Komenda `getBusinessSpaceDeployStatus` służy do sprawdzania, czy produkt Business Space oparty na technologii WebSphere został skonfigurowany w konkretnym miejscu docelowym wdrażania.

Ta komenda służy do sprawdzania, czy produkt Business Space został skonfigurowany na określonym serwerze, węzle lub klastrze. Jeśli nie zostały ustawione żadne parametry, komenda sprawdza, czy produkt Business Space został skonfigurowany w komórce.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera sprawdzanego pod kątem produktu Business Space.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła sprawdzanego pod kątem produktu Business Space.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra sprawdzanego pod kątem produktu Business Space.

Przykłady

W poniższym przykładzie komenda `getBusinessSpaceDeployStatus` została użyta w celu sprawdzenia, czy produkt Business Space został skonfigurowany na serwerze.

- Przykład kodu Jython:

```
AdminTask.getBusinessSpaceDeployStatus(['-nodeName mój_węzeł -serverName mój_serwer'])
```

- Przykład kodu Jacl:

```
$AdminTask getBusinessSpaceDeployStatus {-nodeName mój_węzeł -serverName mój_serwer}
```

W poniższym przykładzie komenda `getBusinessSpaceDeployStatus` została użyta w celu sprawdzenia, czy produkt Business Space został skonfigurowany w klastrze.

- Przykład kodu Jython:

```
AdminTask.getBusinessSpaceDeployStatus(['-clusterName mój_klaster'])
```

- Przykład kodu Jacl:

```
$AdminTask getBusinessSpaceDeployStatus {-clusterName mój_klaster}
```

W poniższym przykładzie komenda `getBusinessSpaceDeployStatus` została użyta w celu zwrócenia listy wszystkich miejsc docelowych wdrażania (serwerów i klastrów) skonfigurowanych dla produktu Business Space w komórce.

Jeśli komenda zostanie uruchomiona z poziomu katalogu `bin` znajdującego się w katalogu głównym profilu, zwróci ona listę wszystkich miejsc docelowych wdrażania (serwerów i klastrów) skonfigurowanych dla produktu Business Space w komórce.

Jeśli komenda zostanie uruchomiona z poziomu katalogu `bin` znajdującego się w katalogu głównym instalacji, zwróci ona listę wszystkich miejsc docelowych wdrażania (serwerów i klastrów) skonfigurowanych dla produktu Business Space w tym samym katalogu głównym instalacji.

- Przykład kodu Jython:

```
AdminTask.getBusinessSpaceDeployStatus()
```

- Przykład kodu Jacl:

```
$AdminTask getBusinessSpaceDeployStatus
```

Komenda `installBusinessSpace`:

Komenda `installBusinessSpace` służy do konfigurowania produktu Business Space opartego na technologii WebSphere w środowisku wykonawczym.

Komenda `installBusinessSpace` służy do instalowania plików archiwum korporacyjnego (EAR) produktu Business Space w środowisku wykonawczym.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła dla konfiguracji. Wymagany jest jeden z następujących parametrów: `serverName`, `nodeName` lub `clusterName`. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra dla konfiguracji. W celu skonfigurowania produktu Business Space w klastrze należy określić parametr **clusterName**.

Parametry opcjonalne

—noWidgets true|false

Jeśli dla tego parametru opcjonalnego zostanie ustawiona wartość `true`, nie będzie można zainstalować widgetów produktu w miejscu docelowym wdrażania. W celu zainstalowania widgetów należy użyć komendy `installBusinessSpaceWidgets` po pomyślnym zakończeniu konfigurowania produktu Business Space. Wartość domyślna to `false`.

—save true|false

Parametr opcjonalny określający, czy zmiany w konfiguracji zostaną zapisane. Wartość domyślna to `false`.

Przykłady

W poniższym przykładzie komenda `installBusinessSpace` została użyta w celu zainstalowania na serwerze plików EAR produktu Business Space.

- Przykład kodu Jython:

```
AdminTask.installBusinessSpace('[-nodeName mój_węzeł -serverName  
mój_serwer -save true]')
```

- Przykład kodu Jacl:

```
$AdminTask installBusinessSpace {-nodeName mój_węzeł -serverName  
mój_serwer -save true}
```

W poniższym przykładzie komenda `installBusinessSpace` została użyta w celu zainstalowania w klastrze plików EAR produktu Business Space.

- Przykład kodu Jython:

```
AdminTask.installBusinessSpace('[-clusterName mój_klaster -save true]')
```

- Przykład kodu Jacl:

```
$AdminTask installBusinessSpace {-clusterName mój_klaster -save true}
```

Komenda `installBusinessSpaceWidgets`:

Komenda `installBusinessSpaceWidgets` służy do instalowania, wdrażania i rejestrowania widgetów przeznaczonych do użytku z produktem Business Space opartym na technologii WebSphere.

Komenda `installBusinessSpaceWidgets` służy do instalowania, wdrażania i rejestrowania wyznaczonych widgetów znajdujących się w pliku skompresowanym lub pliku archiwum korporacyjnego (EAR). Jeśli widgety są już wdrożone, komenda `installBusinessSpaceWidgets` odświeża informacje binarne i rejestracyjne.

Struktura skompresowanego pliku widgetu obejmuje następujące elementy:

- `[ear\widgets_nazwa.ear]` - jeden lub więcej plików EAR
- `[catalog\catalog_nazwa.xml]`
- `[endpoints*.xml]` - punkty końcowe widgetu
- `[templates*.zip]` - szablony muszą się znajdować w pliku skompresowanym i muszą być zgodne z formatem szablonów produktu IBM Lotus Mashups
- `[help\eclipse\plugins*]`

Żadne foldery nie są wymagane. Puste foldery są poprawne.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła dla konfiguracji. Wymagany jest jeden z następujących parametrów: **serverName**, **nodeName** lub **clusterName**. W celu skonfigurowania widgetów produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra dla konfiguracji. W celu skonfigurowania widgetów produktu Business Space w klastrze należy określić parametr **clusterName**.

-widgets *ścieżka_do_widgetów*

Parametr określający jedną z następujących ścieżek:

- Pełna ścieżka do katalogu, w którym znajdują się skompresowane pliki lub pliki EAR zawierające widgety. Po określeniu katalogu zostaną zainstalowane wszystkie widgety zawarte we wszystkich skompresowanych plikach i plikach EAR z tego katalogu.
- Pełna ścieżka do pojedynczego skompresowanego pliku zawierającego widgety.
- Pełna ścieżka do pojedynczego pliku EAR zawierającego widgety.

-save true|false

Parametr określający, czy konfiguracja zostanie zapisana. Wartością domyślną jest `true`.

Parametry opcjonalne

-save true|false

Parametr określający, czy konfiguracja zostanie zapisana. Wartością domyślną jest `true`.

Przykłady

W poniższym przykładzie komenda `installBusinessSpaceWidgets` została użyta w celu zainstalowania, wdrożenia i zarejestrowania widgetów na serwerze.

- Przykład kodu Jython:

```
AdminTask.installBusinessSpaceWidgets(['-nodeName nazwa_węzła  
-serverName nazwa_serwera -widgets  
instalacyjny_katalog_główny/BusinessSpace/widgets/MyWidget.zip'])
```

- Przykład kodu Jacl:

```
$AdminTask installBusinessSpaceWidgets {-nodeName nazwa_węzła  
-serverName nazwa_serwera -widgets  
instalacyjny_katalog_główny/BusinessSpace/widgets/MyWidget.zip}
```

W poniższym przykładzie komenda `installBusinessSpaceWidgets` została użyta w celu zainstalowania, wdrożenia i zarejestrowania widgetów w klastrze.

- Przykład kodu Jython:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName nazwa_klastra  
-widgets X:/WPS/Temp]')
```

- Przykład kodu Jacl:

```
$AdminTask installBusinessSpaceWidgets {-clusterName nazwa_klastra  
-widgets X:/WPS/Temp}
```

W celu zaktualizowania szablonów i obszarów produktu Business Space po uruchomieniu komendy `installBusinessSpaceWidgets` lub `updateBusinessSpaceWidgets` wymagane jest ręczne wykonanie pewnych kroków. Więcej informacji zawiera temat Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.

Komenda `listBPMApiFederationDomains`:

Komenda `listBPMApiFederationDomains` służy do pokazywania wszystkich domen stowarzyszenia w środowisku użytkownika.

Ta komenda powoduje wyświetlenie wszystkich domen stowarzyszenia, które istnieją dla serwera lub klastra. Funkcja API stowarzyszenia umożliwia wyświetlanie procesów i zadań utworzonych w produktach Process Designer i Integration Designer na tej samej liście zadań. Funkcja API stowarzyszenia jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend `wsadmin` w celu utworzenia domen stowarzyszenia i zarządzania nimi.

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Obiekt docelowy

Zasięg, w którym ma być administrowana domena stowarzyszenia. Obiekt docelowy może być używany zamiast parametrów `nodeName`, `serverName` i `clusterName`.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera, na którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `nodeName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła, w którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `serverName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra, w którym powinna być administrowana domena stowarzyszenia. Tego parametru nie należy określać w przypadku określenia parametrów `nodeName` i `serverName` albo obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

Przykłady

W poniższym przykładzie komenda `listBPMApiFederationDomains` została użyta w celu pokazania wszystkich domen stowarzyszenia na serwerze.

- Przykład kodu Jython:

```
AdminTask.listBPMApiFederationDomains('[-nodeName  
mój_węzeł -serverName  
mój_serwer]')
```

- Przykład kodu Jacl:

```
$AdminTask listBPMApiFederationDomains {-nodeName mój_węzeł -serverName  
mój_serwer}
```

Komenda `modifyBPMApiFederationDomain`:

Komenda `modifyBPMApiFederationDomain` służy do dodawania miejsc docelowych do domeny stowarzyszenia lub ich usuwania przy użyciu kroków `addTarget` i `deleteTarget`.

Ta komenda umożliwia dodawanie miejsc docelowych do domeny stowarzyszenia i usuwanie miejsc docelowych z tej domeny. Funkcja API stowarzyszenia jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend `wsadmin` w celu utworzenia domen stowarzyszenia i zarządzania nimi. Krok `addTarget` umożliwia dodanie do domeny stowarzyszenia co najmniej jednego miejsca docelowego wdrażania. Krok `deleteTarget` umożliwia usunięcie z domeny stowarzyszenia co najmniej jednego miejsca docelowego wdrażania. Funkcja API stowarzyszenia dokonuje stowarzyszenia wszystkich systemów w dodanych miejscach docelowych wdrażania.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Obiekt docelowy

Zasięg, w którym ma być administrowana domena stowarzyszenia. Obiekt docelowy może być używany zamiast parametrów `nodeName`, `serverName` i `clusterName`.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera, na którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `nodeName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła, w którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `serverName`. Tego parametru nie należy określać w przypadku określenia

parametru **clusterName** lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-clusterName*nazwa_klastra*

Parametr określający nazwę klastra, w którym powinna być administrowana domena stowarzyszenia. Tego parametru nie należy określać w przypadku określenia parametrów **nodeName** i **serverName** albo obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-name*nazwa_domeny_stowarzyszenia*

Nazwa nowej domeny stowarzyszenia modyfikowanej przez użytkownika. Ta nazwa musi być unikalna. Ten parametr jest zawsze wymagany.

Parametry wymagane w przypadku kroków addTarget i deleteTarget

-targetCellName*nazwa_komórki*

Parametr określający nazwę komórki używanej jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, ale nie zostaną określone parametry nodeName, serverName i clusterName, funkcja API stowarzyszenia dokona stowarzyszenia we wszystkich systemach w komórce.

-targetNodeName*nazwa_węzła*

Parametr określający nazwę węzła używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach na tym serwerze. W przypadku określenia tego parametru konieczne jest określenie parametru targetServerName. Tego parametru nie należy określać w przypadku określenia parametru targetClusterName.

-targetServerName*nazwa_serwera*

Parametr określający nazwę serwera używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach na tym serwerze. W przypadku określenia tego parametru konieczne jest określenie parametru targetNodeName. Tego parametru nie należy określać w przypadku określenia parametru targetClusterName.

-targetClusterName*nazwa_klastra*

Parametr określający nazwę serwera używanego jako miejsce docelowe stowarzyszenia. Jeśli ten parametr zostanie określony, funkcja API stowarzyszenia dokona stowarzyszenia w systemach tego klastra. Tego parametru nie należy określać w przypadku określenia parametru targetNodeName lub targetServerName.

Przykłady

W poniższym przykładzie komenda modifyBPMApiFederationDomain została użyta w celu usunięcia miejsca docelowego wdrażania określonego jako *mój_węzeł*, *mój_serwer* oraz dodania nowego miejsca docelowego wdrażania *mój_nowy_węzeł*, *mój_nowy_serwer*.

- Przykład kodu Jython:

```
AdminTask.modifyBPMApiFederationDomain('[-nodeName
nazwa_węzła
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia
-deleteTarget [{"mój_węzeł mój_serwer ""}]')
-addTarget [{"mój_nowy_węzeł mój_nowy_serwer ""}]')
```

- Przykład kodu Jacl:

```

$AdminTask modifyBPMApiFederationDomain
{-nodeName nazwa_węzła
-serverName nazwa_serwera -name niestandardowa_domena_stowarzyszenia
-deleteTarget {" " mój_węzeł mój_serwer " "}}
-addTarget {" " mój_nowy_węzeł mój_nowy_serwer " "}}

```

Komenda registerRESTServiceEndpoint:

Komenda registerRESTServiceEndpoint służy do rejestrowania skonfigurowanych i włączonych punktów końcowych usługi REST (Representational State Transfer) w celu umożliwienia zespołowi korzystania z widgetów w produkcie Business Space.

Ta komenda służy do rejestrowania punktów końcowych usługi REST, co umożliwia poprawne połączenie produktu Business Space z widgetami produktu użytkownika. Przy użyciu tej komendy można zarejestrować punkty końcowe usług REST, które znajdują się w tej samej komórce co produkt Business Space.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
AdminConfig.save()
- W przypadku języka Jacl:
\$AdminConfig save

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji -conntype NONE podczas uruchamiania tej komendy.

Parametry wymagane

-clusterName*nazwa_klastra_uslug_REST*

Parametr określający nazwę klastra usługi REST. W celu zarejestrowania punktów końcowych usług REST dla klastra należy określić parametr **clusterName**.

-nodeName*nazwa_węzła_uslug_REST*

Parametr określający nazwę węzła usługi REST. W celu zarejestrowania punktów końcowych usług REST dla serwera należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-serverName*nazwa_serwera_uslug_REST*

Parametr określający nazwę serwera usługi REST. W celu zarejestrowania punktów końcowych usług REST dla serwera należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-businessSpaceClusterName*nazwa_klastra_produkту_Business_Space*

Nazwa klastra produktu Business Space. Jeśli w klastrze jest skonfigurowany produkt Business Space, należy określić parametr **businessSpaceClusterName**.

-businessSpaceNodeName*nazwa_węzła_produkту_Business_Space*

Nazwa węzła produktu Business Space. Jeśli na serwerze jest skonfigurowany produkt Business Space, należy określić zarówno parametr **businessSpaceServerName**, jak i parametr **businessSpaceNodeName**.

-businessSpaceServerName*nazwa_serwera_produkту_Business_Space*

Nazwa serwera produktu Business Space. Jeśli na serwerze jest skonfigurowany produkt Business Space, należy określić zarówno parametr **businessSpaceServerName**, jak i parametr **businessSpaceNodeName**.

Parametry opcjonalne

-appName*nazwa_aplikacji_dostawcy*

Nazwa aplikacji dostawcy usługi REST.

-name*nazwa_uslugi_REST*

Nazwa usługi REST.

-type *nazwa_typu_uslugi*

Typ usługi. Ten parametr jest opcjonalny. Jeśli ten parametr nie zostanie określony, zostaną zarejestrowane wszystkie unikalne punkty końcowe usługi REST skonfigurowane dla określonego dostawcy usługi REST w określonym miejscu docelowym wdrażania. W celu określenia konkretnego punktu końcowego usługi należy użyć wartości `<tns:type>` znajdującej się w pliku punktów końcowych dla danego widgetu. Pliki punktów końcowych znajdują się w katalogu `instalacyjny_katalog_główny\BusinessSpace\registryData\endpoints`. Na przykład plik `bpmAdministrationEndpoints.xml` zawiera wszystkie typy punktów końcowych usługi, które są używane przez widgety administracyjne. Element `<tns:type>` ma wartość `{com.ibm.bpm}SCA`:

```
<tns:Endpoint>
  <tns:id>{com.ibm.bpm}SCA</tns:id>
  <tns:type>{com.ibm.bpm}SCA</tns:type>
  <tns:version>6.2.0.0</tns:version>
  <tns:url>/rest/sca/v1</tns:url>
  <tns:description>Położenie zaplecza usług SCA REST
  dla widgetów Administrowanie modułem i widgetu Monitorowanie usług
</tns:description>
</tns:Endpoint>
```

W przypadku języka Jacl należy używać cudzysłowów dla wartości, na przykład: ...
`-type "{com.ibm.bpm}SCA"`

-version*nazwa_wersji*

Wersja dostawcy usługi REST.

-webModuleName*nazwa_modulu_WWW*

Nazwa modułu WWW dostawcy usługi REST.

Przykłady

W poniższym przykładzie użyto komendy `registerRESTServiceEndpoint`. Ta komenda rejestruje w produkcie Business Space wszystkie usługi REST, które są skonfigurowane i włączone w klastrze.

- Przykład kodu Jython:

```
AdminTask.registerRESTServiceEndpoint(['-clusterName
nazwa_klastra_uslug_REST -businessSpaceClusterName
nazwa_klastra_produkту_Business_Space'])
```

- Przykład kodu Jacl:

```
$AdminTask registerRESTServiceEndpoint {-clusterName
nazwa_klastra_uslug_REST -businessSpaceClusterName
nazwa_klastra_produkту_Business_Space}
```

Komenda `showBPMApiFederationDomain`:

Komenda `showBPMApiFederationDomain` służy do wyświetlania szczegółów domeny stowarzyszenia.

Ta komenda umożliwia wyświetlenie szczegółów skonfigurowanych miejsc docelowych oraz węzła, serwera i klastra dla określonej domeny stowarzyszenia. Funkcja API stowarzyszenia jest automatycznie konfigurowana z produktem jako część aplikacji bramy usług REST. Aby

zmienić tę konfigurację dla środowiska z wieloma miejscami docelowymi wdrażania, należy użyć komend `wsadmin` w celu utworzenia domen stowarzyszenia i zarządzania nimi.

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Obiekt docelowy

Zasięg, w którym ma być administrowana domena stowarzyszenia. Obiekt docelowy może być używany zamiast parametrów `nodeName`, `serverName` i `clusterName`.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera, na którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `nodeName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła, w którym powinna być administrowana domena stowarzyszenia. W przypadku określenia tego parametru konieczne jest określenie parametru `serverName`. Tego parametru nie należy określać w przypadku określenia parametru `clusterName` lub obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra, w którym powinna być administrowana domena stowarzyszenia. Tego parametru nie należy określać w przypadku określenia parametrów `nodeName` i `serverName` albo obiektu docelowego. Jeśli nie zostanie określone żadne miejsce docelowe wdrażania, domena stowarzyszenia jest administrowana w zasięgu komórki.

-name *nazwa_domeny_stowarzyszenia*

Nazwa domeny stowarzyszenia, która ma zostać pokazana. Ta nazwa musi być unikalna. Ten parametr jest zawsze wymagany.

Przykłady

W poniższym przykładzie komenda `showBPMApiFederationDomain` została użyta w celu wyświetlenia szczegółów domeny stowarzyszenia.

- Przykład kodu Jython:

```
AdminTask.showBPMApiFederationDomain(['-nodeName mój_węzeł -serverName  
mój_serwer -name moja_domena_stowarzyszenia'])
```

- Przykład kodu Jacl:

```
$AdminTask showBPMApiFederationDomain {-nodeName mój_węzeł -serverName  
mój_serwer -name moja_domena_stowarzyszenia}
```

Komenda `uninstallBusinessSpaceWidgets`:

Komenda `uninstallBusinessSpaceWidgets` umożliwia usuwanie widgetów i definicji widgetów z profilu, w tym usuwanie poszczególnych zasobów aplikacyjnych widgetów, takich jak aplikacja, katalog, punkty końcowe, obszary, szablony i pomoc.

Komenda `uninstallBusinessSpaceWidgets` usuwa pliki widgetów w wyznaczonym pliku skompresowanym lub pliku archiwum korporacyjnego (EAR). Struktura skompresowanego pliku widgetu obejmuje następujące elementy:

- `[ear\widgets_nazwa.ear]` - jeden lub więcej plików EAR
- `[catalog\catalog_nazwa.xml]`
- `[endpoints*.xml]` - punkty końcowe widgetu
- `[templates*.zip]` - szablony muszą się znajdować w pliku skompresowanym i muszą być zgodne z formatem szablonów produktu IBM Lotus Mashups
- `[help\eclipse\plugins*]`

Żadne foldery nie są wymagane. Puste foldery są poprawne.

Uwaga: Jeśli informacje o punktach końcowych usługi REST zostaną dostosowane przy użyciu innego narzędzia niż komenda `updateBusinessSpaceWidgets`, wprowadzone zmiany zostaną utracone po uruchomieniu komendy `uninstallBusinessSpaceWidgets`.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
`AdminConfig.save()`
- W przypadku języka Jacl:
`$AdminConfig save`

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła dla konfiguracji. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra dla konfiguracji. W celu skonfigurowania produktu Business Space w klastrze należy określić parametr **clusterName**.

-widgetsścieżka_do_widgetów

Parametr określający jedną z następujących ścieżek:

- Pełna ścieżka do katalogu zawierającego pliki skompresowane lub pliki EAR widgetów zawierające widgety. Po określeniu katalogu zostaną zainstalowane wszystkie widgety zawarte we wszystkich skompresowanych plikach i plikach EAR z tego katalogu.
- Pełna ścieżka do pojedynczego skompresowanego pliku zawierającego widgety.
- Pełna ścieżka do pojedynczego pliku EAR zawierającego widgety.

Parametry opcjonalne

-save true|false

Parametr, który określa, czy zmiany konfiguracji mają zostać zapisane. Wartością domyślną jest `true`.

Przykład

W następującym przykładzie komenda `uninstallBusinessSpaceWidgets` została użyta do usunięcia widgetów z klastra.

Uwaga: Przykłady służą tylko do celów demonstracyjnych. Zawierają zmienne i nie są przeznaczone do ponownego wykorzystania jako fragmenty kodu.

- Przykład kodu Jython:

```
AdminTask.uninstallBusinessSpaceWidgets('[-clusterName  
nazwa_klastra -widgets X:/WPS/Temp]')
```

- Przykład kodu Jacl:

```
$AdminTask uninstallBusinessSpaceWidgets {-clusterName  
nazwa_klastra -widgets X:/WPS/Temp}
```

Komenda `updateBusinessSpaceWidgets`:

Komenda `updateBusinessSpaceWidgets` umożliwia aktualizowanie skonfigurowanych wcześniej widgetów produktu Business Space oraz ich punktów końcowych, katalogów, szablonów i wtyczek pomocy.

Komenda `updateBusinessSpaceWidgets` aktualizuje pliki binarne, pliki katalogów, pliki punktów końcowych, szablony i wtyczki pomocy widgetów, które zostały wcześniej zainstalowane i skonfigurowane dla produktu Business Space.

Komenda `updateBusinessSpaceWidgets` aktualizuje pliki widgetów w wyznaczonym pliku skompresowanym lub pliku archiwum korporacyjnego (EAR). Struktura skompresowanego pliku widgetu obejmuje następujące elementy:

- `[ear\widgets_nazwa.ear]` - jeden lub więcej plików EAR
- `[catalog\catalog_nazwa.xml]`
- `[endpoints*.xml]` - punkty końcowe widgetu
- `[templates*.zip]` - szablony muszą się znajdować w pliku skompresowanym i muszą być zgodne z formatem szablonów produktu IBM Lotus Mashups
- `[help\eclipse\plugins*]`

Żadne foldery nie są wymagane. Puste foldery są poprawne.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:

```
AdminConfig.save()
```

- W przypadku języka Jacl:

```
$AdminConfig save
```

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-serverName *nazwa_serwera*

Parametr określający nazwę serwera dla konfiguracji. W celu skonfigurowania widgetów produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła dla konfiguracji. Wymagany jest jeden z

następujących parametrów: `serverName`, `nodeName` lub `clusterName`. W celu skonfigurowania widgetów produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName*nazwa_klastra*

Parametr określający nazwę klastra dla konfiguracji. W celu skonfigurowania produktu Business Space w klastrze należy określić parametr **clusterName**.

Parametry opcjonalne

-widgets*ścieżka_do_widgetów*

Parametr, który określa pełną ścieżkę do katalogu zawierającego pliki archiwum korporacyjnego (EAR) widgetów lub skompresowane pliki widgetów albo pełną ścieżkę do konkretnego pliku EAR lub skompresowanego pliku widgetów.

-endpoints*ścieżka_do_punktów_końcowych*

Parametr, który określa pełną ścieżkę do katalogu zawierającego pliki punktów końcowych widgetów lub pełną ścieżkę do konkretnego pliku punktów końcowych.

-catalogs*ścieżka_do_katalogu*

Parametr, który określa pełną ścieżkę do katalogu zawierającego pliki katalogów widgetów lub pełną ścieżkę do konkretnego pliku katalogu.

-templates*ścieżka_do_szablonów*

Parametr, który określa pełną ścieżkę do katalogu zawierającego pliki szablonów widgetów lub pełną ścieżkę do konkretnego pliku szablonu.

-helpplugins*ścieżka_do_pomocy*

Parametr, który określa pełną ścieżkę do katalogu zawierającego pliki wtyczek pomocy elektronicznej dla widgetów lub pełną ścieżkę do konkretnego pliku wtyczki pomocy elektronicznej dla widgetu.

--noWidget*true|false*

Wskazuje, że pliki EAR widgetów znajdujące się w skompresowanym pliku widgetów nie mają być aktualizowane.

--noEndpoint*true|false*

Wskazuje, że podane pliki punktów końcowych znajdujące się w skompresowanym pliku widgetów nie mają być aktualizowane.

--noCatalog*true|false*

Wskazuje, że pliki definicji katalogów znajdujące się w skompresowanym pliku widgetów nie mają być aktualizowane.

--noTemplate*true|false*

Wskazuje, że szablony znajdujące się w skompresowanym pliku widgetów nie mają być aktualizowane.

--noHelp*true|false*

Wskazuje, że pliki pomocy znajdujące się w skompresowanym pliku widgetów nie mają być aktualizowane.

--save *true|false*

Parametr określający, czy konfiguracja zostanie zapisana. Wartością domyślną jest *true*.

Przykłady

W następującym przykładzie za pomocą komendy `updateBusinessSpaceWidgets` aktualizowane są widgety w klastrze.

Przykład kodu Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-clusterName
nazwa_klastra
-widgets ścieżka_do_widgetów]')
```

Przykład kodu Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-clusterName
nazwa_klastra
-widgets ścieżka_do_widgetów}
```

W następującym przykładzie za pomocą komendy `updateBusinessSpaceWidgets` aktualizowane są widgety na serwerze.

Przykład kodu Jython:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName nazwa_węźła
-serverName nazwa_serwera -widgets
ścieżka_do_widgetów]')
```

Przykład kodu Jacl:

```
$AdminTask updateBusinessSpaceWidgets {-nodeName
nazwa_węźła
-serverName nazwa_serwera -widgets
ścieżka_do_widgetów}
```

W celu zaktualizowania szablonów i obszarów produktu Business Space po uruchomieniu komendy `installBusinessSpaceWidgets` lub `updateBusinessSpaceWidgets` wymagane jest ręczne wykonanie pewnych kroków. Więcej informacji zawiera temat Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów.

Komenda `updateRESTGatewayService`:

Komenda `updateRESTGatewayService` służy do aktualizowania usługi bramy REST (Representational State Transfer) w celu konfigurowania i włączania usług REST.

Ta komenda służy do aktualizowania usługi bramy REST w celu konfigurowania i włączania usług REST. Wdrażanie usług REST jest przeprowadzane automatycznie w profilu serwera autonomicznego. W przypadku innych typów konfiguracji strona usług REST w Konsoli administracyjnej lub komenda `updateRESTGatewayService` umożliwi skonfigurowanie usług REST dla wszystkich widgetów produktu użytkownika w produkcie Business Space.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
`AdminConfig.save()`
- W przypadku języka Jacl:
`$AdminConfig save`

Jeśli serwer aplikacji nie jest uruchomiony, należy użyć opcji `-conntype NONE` podczas uruchamiania tej komendy.

Parametry wymagane

-clusterName *nazwa_klastra*

Parametr określający nazwę klastra usługi REST. W celu skonfigurowania usług REST w klastrze należy określić parametr **clusterName**.

-nodeName *nazwa_węzła*

Parametr określający nazwę węzła usługi REST. W celu skonfigurowania usług REST na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-serverName *nazwa_serwera*

Parametr określający nazwę serwera usługi REST. W celu skonfigurowania usług REST na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-enable true | false

Wskazuje, czy usługa REST jest włączona. Poprawne wartości to true lub false.

Parametry opcjonalne

-type *nazwa_typu_usługi*

Typ usługi REST.

-version *nazwa_wersji*

Wersja usługi REST.

Przykłady

W poniższym przykładzie komenda updateRESTGatewayService została użyta do zaktualizowania usługi bramy REST w celu skonfigurowania i włączenia usług REST.

- Przykład kodu Jython:

```
AdminTask.updateRESTGatewayService(['-nodeName węzeł1 -serverName
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable
true'])
```

- Przykład kodu Jacl:

```
$AdminTask updateRESTGatewayService {-nodeName węzeł1 -serverName
server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable true}
```

Aktualizowanie szablonów i obszarów produktu Business Space po zainstalowaniu lub zaktualizowaniu widgetów:

Po uruchomieniu komendy installBusinessSpaceWidgets lub updateBusinessSpaceWidgets w środowisku klastrowym wymagane jest wykonanie pewnych czynności ręcznie w celu zaktualizowania szablonów i obszarów produktu Business Space.

Jeśli wcześniej użyto komendy installBusinessSpaceWidgets lub updateBusinessSpaceWidgets, należy wykonać poniższe dodatkowe kroki.

1. Jeśli produkt Business Space jest skonfigurowany w klastrze, wykonaj następujące kroki:
 - a. Zidentyfikuj profil niestandardowy dla pliku oobLoadedStatus.properties:
 - 1) W profilu menedżera wdrażania należy otworzyć plik *katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\mm.runtime.profl\config\ConfigService.properties*.
 - 2) Poszukaj nazwy komórki, węzła i serwera we właściwościach *com.ibm.mashups.directory.templates* lub *com.ibm.mashups.directory.spaces*.
Na przykład we właściwości *com.ibm.mashups.directory.templates = config/cells/Cell01/nodes/Node01/servers/Server1/mm/templates* można znaleźć profil niestandardowy za pomocą nazwy komórki Cell01 i nazwy węzła Node01.
 - 3) Należy użyć nazwy komórki, węzła i serwera w celu znalezienia profilu niestandardowego.
 - b. W profilu niestandardowym otwórz plik *katalog_główny_profilu_niestandardowego\BusinessSpace\nazwa_klastra*

mm.runtime.prof\public\oobLoadedStatus.properties i zaktualizuj właściwości importTemplates.txt lub importSpaces.txt:

```
importTemplates.txt=true  
importSpaces.txt=true
```

Jeśli baza danych produktu Business Space została utworzona po jego usunięciu lub jeśli z innego powodu konieczne jest przeładowanie kompozycji, należy także zaktualizować następującą właściwość:

```
importThemes.txt=true
```

- c. Resynchronizuj profil niestandardowy.
 - 1) Należy otworzyć Konsolę administracyjną i kliknąć opcję **Administrowanie systemem > Węzły**.
 - 2) Należy kliknąć opcję **Pełna resynchronizacja**.
 - d. Zrestartuj klaster.
2. Jeśli produkt Business Space jest skonfigurowany na serwerze zarządzanym, wykonaj następujące kroki:
- a. W profilu niestandardowym, w którym znajduje się serwer zarządzany, otwórz plik *katalog_główny_profilu_niestandardowego\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\public\oobLoadedStatus.properties* i zaktualizuj właściwości importTemplates.txt lub importSpaces.txt:

```
importTemplates.txt=true  
importSpaces.txt=true
```

Jeśli baza danych produktu Business Space została utworzona po jego usunięciu lub jeśli z innego powodu konieczne jest przeładowanie kompozycji, należy także zaktualizować następującą właściwość:

```
importThemes.txt=true
```
 - b. Resynchronizuj profil niestandardowy.
 - 1) Należy otworzyć Konsolę administracyjną i kliknąć opcję **Administrowanie systemem > Węzły**.
 - 2) Należy kliknąć opcję **Pełna resynchronizacja**.
 - c. Zrestartuj serwer.

Migrowanie produktu Business Space (czynności po migracji produktu)

Po przeprowadzeniu migracji produktu Business Space do wersji 7.5 należy wykonać pewne czynności dodatkowe dla tego produktu przed uruchomieniem serwerów lub klastrów.

Przed przystąpieniem do tej czynności należy przeprowadzić migrację klastra lub serwera produktu i sprawdzić, czy ta migracja zakończyła się powodzeniem.

Konieczne jest również przeprowadzenie migracji bazy danych używanej dla produktu Business Space. W celu przeprowadzenia migracji baz danych i danych należy postępować zgodnie z instrukcjami przeznaczonymi dla danego produktu.

W przypadku migracji z wcześniejszej wersji produktu, jeśli produkt Business Space jest już skonfigurowany, należy wykonać poniższe kroki po migracji a przed rozpoczęciem korzystania z produktu Business Space.

1. Jeśli w poprzedniej wersji znajdowały się niestandardowe widżety, wykonaj ręcznie czynności, aby widżety te działały w produkcie Business Space 7.5. Więcej informacji na ten temat zawiera sekcja Migrowanie widżetów niestandardowych.

Wskazówka: Migracja danych w wersji 7.0 wspomaga migrację katalogu widgetów i punktu końcowego widgetów niestandardowych, dlatego nie jest konieczne ponowne ich migrowanie ręczne.

2. Jeśli w środowisku w poprzedniej wersji produkt Business Space był uruchomiony w innej komórce niż ta, w której były uruchomione usługi REST, lub widgety znajdowały się w innych komórkach niż produkt Business Space, konieczna jest aktualizacja plików punktów końcowych. Więcej informacji na ten temat zawiera sekcja Włączanie widgetów produktu Business Space dla środowisk międzykomórkowych.
3. Jeśli w środowisku w poprzedniej wersji produkt IBM Forms Server był używany z widgetami zarządzania czynnościami personelu, wykonaj ręcznie czynności mające na celu umożliwienie działania produktu Business Space z produktem IBM Forms Server 4.0 i komponentem Webform Server.
 - a. Zainstaluj produkt IBM Forms Server 4.0.
 - b. W Konsoli administracyjnej produktu zaktualizuj następujące zmienne środowiskowe:
 - Zmień odwołania do interfejsu API 76 na 80, na przykład:
`#{LFS_API_DIR};#{LFS_API_DIR}/80/system;`
 - Zmień wartość zmiennej LFS_DIR na ścieżkę instalacji produktu IBM Forms Server 4.0, na przykład: `c:\Program Files\IBM Forms Server\4.0\WebformServer`

Więcej informacji na ten temat zawiera sekcja Konfigurowanie produktu IBM Forms Server na potrzeby widgetów zarządzania czynnościami personelu w produkcie Business Space.

4. Jeśli z poprzedniego środowiska produktu Business Space wyeksportowano obszary lub szablony, zaimportuj je do wersji 7.5 produktu Business Space, aby były dostępne do użycia. Więcej informacji na ten temat zawierają sekcje Importowanie obszarów i Importowanie szablonów.

Wskazówka: W przypadku migracji z wersji 6.x i szablonów należy najpierw zaimportować je jako obszary w menedżerze obszarów, a następnie przekształcić zaimportowane obszary w szablony, klikając opcję **Działania > Zapisz jako szablon**.

Po zakończeniu tych procedur migracji można używać produktu Business Space 7.5.

Wskazówka: Jeśli wcześniej był używany produkt Business Space 6.2, należy wyczyścić pamięć podręczną przeglądarki przed użyciem produktu Business Space 7.5. Operacja taka pomoże uniknąć niezamierzonego korzystania z kodu i obrazów produktu Business Space 6.2.

Konfigurowanie produktu Business Space do pracy z produktem Mashup Center

Jeśli produkt Business Space został skonfigurowany do pracy z produktem IBM Mashup Center, użytkownicy produktu Business Space mogą publikować szablony i strony w katalogu produktu Mashup Center, używać szablonów produktu Mashup Center do tworzenia obszarów oraz importować pojedyncze strony z produktu Mashup Center do produktu Business Space.

Aby używać produktu Business Space z produktem Mashup Center, niezbędna jest ważna licencja produktu Mashup Center. Produkt Business Space działa tylko z widgetami zarejestrowanymi w produkcie Business Space lub widgetami, które zostały opublikowane w produkcie Mashup Center.

Jeśli produkt Mashup Center (w tym komponent IBM InfoSphere MashupHub) nie jest uruchomiony na tym samym serwerze aplikacji, co produkt Business Space, należy włączyć pojedyncze logowanie między tymi dwoma serwerami aplikacji. W tym celu środowisko musi

używać repozytorium stowarzyszonego jako rejestru użytkowników. Więcej informacji zawierają tematy Importowanie kluczy LTPA i Eksportowanie kluczy LTPA w Centrum informacyjnym produktu WebSphere Application Server. Należy także skonfigurować certyfikaty SSL. Więcej informacji można znaleźć w sekcji Bezpieczna komunikacja przy użyciu protokołu SSL (Secure Sockets Layer) Centrum informacyjnego produktu WebSphere Application Server.

Aby umożliwić współpracę produktu Business Space z produktem Mashup Center, należy wykonać jedną z następujących procedur dla serwera autonomicznego lub środowiska klastrowego.

- W przypadku serwera autonomicznego wykonaj następujące kroki:
 1. Zmodyfikuj właściwość `com.ibm.mashups.hub.url` w pliku konfiguracyjnym `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties` i ustaw ją na adres URL komponentu MashupHub produktu Mashup Center (*protokół://host:port/mashuphub*).
 2. Uruchom komendę `updatePropertyConfig` w środowisku narzędzia `wsadmin` profilu:
W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"'])
AdminConfig.save()
```


W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"}
$AdminConfig save
```
 3. Otwórz plik konfiguracyjny `katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\Endpoints.properties` i zmień właściwość `oob.Widget.url` na adres URL produktu Mashup Center (*protokół://host:port*).
 4. Uruchom komendę `updatePropertyConfig` w środowisku narzędzia `wsadmin` profilu:
W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"'])
AdminConfig.save()
```


W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-serverName nazwa_serwera -nodeName nazwa_węzła -propertyFileName "katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\Endpoints.properties" -prefix "Mashups_"}
$AdminConfig save
```
 5. Zrestartuj serwer.
- W przypadku klastra wykonaj następujące kroki:
 1. Zmodyfikuj właściwość `com.ibm.mashups.hub.url` w pliku konfiguracyjnym `katalog_główny_profilu_menedżera_wdrażania\BusinessSpace\nazwa_klastra\`

mm.runtime.prof\config\ConfigService.properties i ustaw ją na adres URL komponentu MashupHub produktu Mashup Center (*protokół://host:port/mashuphub*).

2. Z poziomu menedżera wdrażania uruchom komendę updatePropertyConfig w środowisku narzędzia wsadmin profilu:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-clusterName nazwa_klastra  
-propertyFileName "katalog_główny_profilu_menedżera_wdrażania\  
BusinessSpace\nazwa_klastra\mm.runtime.prof\config\  
ConfigService.properties" -prefix "Mashups_"'])  
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName nazwa_klastra  
-propertyFileName "katalog_główny_profilu_menedżera_wdrażania\  
BusinessSpace\nazwa_klastra\mm.runtime.prof\config\  
ConfigService.properties" -prefix "Mashups_"}  
$AdminConfig save
```

3. Otwórz plik konfiguracyjny *katalog_główny_profilu\BusinessSpace\nazwa_węzła\nazwa_serwera\mm.runtime.prof\config\Endpoints.properties* i zmień właściwość oob.Widget.url na adres URL produktu Mashup Center (*protokół://host:port*).

4. Z poziomu menedżera wdrażania uruchom komendę updatePropertyConfig w środowisku narzędzia wsadmin profilu:

W poniższym przykładzie użyto języka Jython:

```
AdminTask.updatePropertyConfig(['-clusterName nazwa_klastra  
-propertyFileName "katalog_główny_profilu_menedżera_wdrażania\  
BusinessSpace\nazwa_klastra\mm.runtime.prof\config\Endpoints.properties"  
-prefix "Mashups_"'])  
AdminConfig.save()
```

W poniższym przykładzie użyto języka Jacl:

```
$AdminTask updatePropertyConfig {-clusterName nazwa_klastra  
-propertyFileName "katalog_główny_profilu_menedżera_wdrażania\  
BusinessSpace\nazwa_klastra\mm.runtime.prof\config\Endpoints.properties"  
-prefix "Mashups_"}  
$AdminConfig save
```

5. Zrestartuj menedżer wdrażania.

Konfigurowanie widgetów do pracy z produktem WebSphere Portal

Jeśli zespół używa produktu IBM WebSphere Portal, można skonfigurować produkt Business Space na potrzeby pracy w środowisku produktu WebSphere Portal.

Przed skonfigurowaniem widgetów do pracy z produktem WebSphere Portal należy wykonać następujące czynności:

- Zainstalowanie produktu WebSphere Portal w wersji 7.0.0.1 lub nowszej.
- Zainstalowanie i skonfigurowanie produktu IBM z dołączonym produktem Business Space 7.5.
- Skonfigurowanie produktu Business Space oraz usług REST (Representational State Transfer) tak, aby widgety mogły uzyskiwać dostęp do usług w czasie wykonywania. Więcej informacji można znaleźć w sekcji “Konfigurowanie usług REST” na stronie 194.

- Skonfigurowanie protokołu SSL i pojedynczego logowania. Więcej informacji można znaleźć w sekcji “Konfigurowanie funkcji pojedynczego logowania oraz protokołu SSL dla widgetów w produkcie WebSphere Portal” na stronie 280.
- Zakończenie konkretnych kroków konfiguracji dla widgetów użytkownika, jeśli jest to wymagane.
- Jeśli używane są widżety zarządzania czynnościami personelu w środowisku klastrowym, należy pamiętać o zainstalowaniu formularzy DOJO w tym samym węźle co widżety.

W trakcie konfigurowania widgetów produktu Business Space do pracy w produkcie WebSphere Portal należy wziąć pod uwagę następujące kwestie:

- Nie należy instalować produktu serwera w profilu produktu WebSphere Portal.

Ograniczenie: Nie wszystkie widżety produktu obsługują pracę w produkcie WebSphere Portal. Należy zapoznać się z obsługiwanyimi środowiskami produktu.

1. Utwórz odwołania do punktu końcowego na serwerze aplikacji produktu WebSphere Portal. Aby produkt Business Space działał prawidłowo w środowisku portalu WebSphere Portal, muszą zostać utworzone pozycje odwołań do produktu Business Space i do punktu końcowego specyficznego dla produktu. Punkty końcowe muszą być zdefiniowane na serwerze produktu WebSphere Portal, należy je jednak tworzyć zdalnie przy użyciu komendy `updateEndpointBindingsOnPortal` uruchamianej na serwerze produktu użytkownika.
 - a. Uruchom serwer produktu WebSphere Portal oraz serwer produktu użytkownika.
 - b. Skopiuj pliki punktów końcowych z produktu Business Space i produktu użytkownika do katalogu tymczasowego na komputerze z produktem, na przykład `c:/tmp/endpoints/`.

Pliki punktów końcowych znajdują się na serwerze produktu w katalogu *katalog_główny_profilu/BusinessSpace/nazwa_węzła/nazwa_serwera/mm.runtime.prof/endpoints/*. Należy skopiować tylko te pliki punktów końcowych, dla których konieczne jest utworzenie pozycji. Nie jest konieczne kopiowanie plików przetworzonych wcześniej przy użyciu komendy `updateEndpointBindingsOnPortal`.

- c. W środowiskach rozproszonych dokonaj edycji plików punktów końcowych tak, aby wskazywały poprawne adresy URL.

Ponieważ punkty końcowe są zarejestrowane na serwerze aplikacji, który udostępnia serwer produktu WebSphere Portal, wszystkie punkty końcowe muszą wskazywać zdalny serwer produktu Business Space. Punkty końcowe muszą zawierać pełną nazwę lub adres IP zdalnego hosta, na przykład:

```
<tns:Endpoint>
  <tns:id>{com.ibm.bspace}bpaceCommonWidgetRootId</tns:id>
  <tns:type>{com.ibm.bspace}bpaceCommonWidgetRootId</tns:type>
  <tns:version>1.0.0.0</tns:version>
  <tns:url>http://<Business_Space_Host>:<port>/BusinessSpace/</tns:url>
  <tns:description>Położenie wspólnych widgetów produktu Business Space</tns:description>
</tns:Endpoint>
```

Wykonaj kroki opisane w sekcji “Włączanie widgetów produktu Business Space dla środowisk międzykomórkowych” na stronie 216.

- d. Otwórz sesję narzędzia `wsadmin` na serwerze produktu. Należy uruchomić plik `wsadmin.bat` lub `wsadmin.sh` znajdujący się w katalogu *katalog_główny_profilu/bin/*. Sesja narzędzia `wsadmin` nawiązuje połączenie z wirtualną maszyną języka Java lokalnego serwera aplikacji produktu.
- e. W sesji narzędzia `wsadmin` uruchom komendę `updateEndpointBindingsOnPortal`. W środowisku wdrożenia sieciowego należy ją uruchomić z menedżera wdrażania.
 - Przykład kodu Jython:

```
AdminTask.updateEndpointBindingsOnPortal('[-nodeName
nazwa_węzła_produkту_Portal -serverName WebSphere_Portal
-endpointBindingDirectoryName
katalog_zawierający_pliki_punktów_końcowych -host
adres_IP_lub_nazwa_hosta_serwera_produkту_Portal -port
domyślny_port_SOAP_produkту_Portal_10025 -user
identyfikator_administratora_produkту_Portal -password
hasło_administratora_produkту_Portal]')
```

- Przykład kodu Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName
nazwa_węzła_produkту_Portal -serverName WebSphere_Portal
-endpointBindingDirectoryName
katalog_zawierający_pliki_punktów_końcowych -host
adres_IP_lub_nazwa_hosta_serwera_produkту_Portal -port
domyślny_port_SOAP_produkту_Portal_10025 -user
identyfikator_administratora_produkту_Portal -password
hasło_administratora_produkту_Portal}
```

- f. Zrestartuj serwer produktu WebSphere Portal.
- g. Zweryfikuj punkty końcowe, przechodząc do dostawcy środowiska zasobów o nazwie **Punkty końcowe stron zespolonych produktu WP**. Należy kliknąć opcję **Zasoby > Dostawcy środowiska zasobów > Właściwości niestandardowe**.
2. Skonfiguruj proxy Ajax na serwerze produktu WebSphere Portal. Aby zdalne adresy URL miały dostęp do serwera produktu użytkownika z serwera produktu WebSphere Portal, należy skonfigurować proxy Ajax.
 - a. Zaktualizuj istniejący plik proxy-config.xml o przedstawiony w temacie "Pozycje wymagane w pliku proxy-config.xml do skonfigurowania widgetów pod kątem współpracy z produktem WebSphere Portal" na stronie 282 fragment kodu z przykładową strategią proxy.
 - b. Uruchom skrypt checkin-wp-proxy-config.
W środowisku klastrowym skrypt należy uruchomić w węzle podstawowym.
ConfigEngine.[bat|sh] checkin-wp-proxy-config
-DProxyConfigFileName=ścieżka_do_katalogu/
nazwa_tymczasowego_pliku.proxy -DWasPassword=hasło_serwera_aplikacji
-DWasUserid=identyfikator_użytkownika_serwera_aplikacji
-DPortalAdminId=identyfikator_administratora_produkту_WebSphere_Portal
-DPortalAdminPwd=hasło_administratora_produkту_WebSphere_Portal, gdzie
ścieżka_do_katalogu/nazwa_tymczasowego_pliku.proxy to pełna ścieżka do
zmodyfikowanego pliku wp.proxy.config.xml.
Więcej informacji na temat konfiguracji proxy zawiera dokumentacja produktu
WebSphere Portal dostępna pod adresem http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Global_proxy_configuration_wp7.
 - c. W Konsoli administracyjnej uruchom ponownie aplikację o nazwie **Konfiguracja proxy AJAX**.
3. W produkcie WebSphere Portal zarejestruj widgety produktu Business Space.
Widgety produktu Business Space są rejestrowane przez produkt WebSphere Portal jako elementy iWidget. Jest to realizowane przy użyciu masowego importu z wykorzystaniem pliku katalogu widgetów specyficznego dla produktu WebSphere Portal z produktem użytkownika. Plik XML katalogu jest dostępny w katalogu głównym pliku archiwum WWW (WAR) produktu. Każdy produkt ma inny kontekstowy katalog główny.
Istnieją dwa typy widgetów: wspólne i specyficzne dla produktu.
Kontekstowy katalog główny wspólnych widgetów produktu Business Space to /BusinessSpace, a plik katalogu to catalog_commonWidgets_portal.xml. Jako adres

URL do pliku XML katalogu dla wspólnych widgetów produktu Business Space można na przykład wpisać adres `http://localhost:9080/BusinessSpace/catalog_commonWidgets_portal.xml`.

Następujące adresy URL są przykładami dla produktów do zarządzania procesami biznesowymi:

- IBM Business Monitor: `http://produkt_Business_Space_udostepniajacy_program_Monitor:port/BusinessDashboard/catalog.xml`
- IBM Business Monitor z produktem IBM Cognos Business Intelligence: `http://produkt_Business_Space_udostepniajacy_program_Monitor:port/CognosWidgets/catalog.xml`
- Widzety do zarządzania czynnościami personelu: `http://produkt_Business_Space_udostepniajacy_produkt_Business_Process_Manager:port/HumanTaskManagementWidgets/portal_catalog.xml`

- a. Aby zarejestrować elementy iWidget przy użyciu pliku XML katalogu produktu, z katalogu `profil_wp\ConfigEngine` uruchom następującą komendę:

```
ConfigEngine.[bat|sh] register-iwidget-definition
-DIWidgetCatalog=adres_URL_do_pliku_XML_katalogu
-DWasPassword=haslo -DWasUserid=identyfikikator
-DPortalAdminId=identyfikikator -DPortalAdminPwd=haslo
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

Przykład dla programu IBM Business Monitor:

```
ConfigEngine.bat register-iwidget-definition -DIWidgetCatalog=http://
localhost:9080/BusinessDashboard/catalog.xml -DWasPassword=admin
-DWasUserid=admin -DPortalAdminId=admin -DPortalAdminPwd=admin
-DRegistrationAspects=catalogTitlesOverule,considerWidgetParam,considerUniqueName
```

- b. Komunikat `Wartość zwracana:0` oznacza, że komenda została poprawnie wykonana. Więcej informacji na temat opcjonalnych komend zawiera dokumentacja produktu WebSphere Portal dostępna pod adresem `http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Task_registeriwidgetdefinition_wp7`.

4. Włącz używane przez widzety produktu Business Space pozycje menu, aby były one wyświetlane w produkcie WebSphere Portal: Pomoc, Odśwież i Wyślij widget. Dalsze informacje znajdują się po adresem `http://www-10.lotus.com/ldd/portalwiki.nsf/dx/Consolidated_Steps_for_Creating_Custom_Themes_in_WP7_`.

- a. Przy użyciu klienta webDAV dokonaj edycji kompozycji niestandardowej. Należy użyć następującego adresu URL webDAV: `http://nazwa_hosta_produktu_Portal:10039/wps/mycontenthandler/dav/fs-type1`.

- b. Przejdź do aktualizowanej kompozycji produktu WebSphere Portal. Na przykład aby zaktualizować kompozycję `moja_kompozycja`, przejdź do katalogu `/fs-type1/themes/moja_kompozycja/` i znajdź plik HTML zgodny z ustawieniami narodowymi. Pobierz go przy użyciu klienta webDAV i dokonaj jego edycji.

- 1) Znajdź wiersz ``.

- 2) Dodaj po tym wierszu następujący znacznik skryptu:

```
<script type="text/javascript">
    var com_ibm_bspace_endpoint = com.ibm.mashups.services.ServiceManager.getService
(com.ibm.mashups.enabler.services.ConfigService.SERVICE_NAME).getConfigObject
(com.ibm.mashups.enabler.services.ConfigConstants.ENDPOINT_CONFIG_PROVIDER).getValue
("{com.ibm.bspace}bSpaceServerRootId.url");
    var bSpaceURL = com.ibm.mm.enabler.utils.URLHelper.rewriteURL
(com_ibm_bspace_endpoint + "com/ibm/bSpace/common/util/widget/BSpacePortalThemeHelper.js")
    var bSpaceRemoteJS = document.createElement('script');
    bSpaceRemoteJS.setAttribute("type", "text/javascript");
```

```

bSpaceRemoteJS.setAttribute("language", "JavaScript");
bSpaceRemoteJS.setAttribute("src", bspaceURL);
document.getElementsByTagName("head")[0].appendChild(bSpaceRemoteJS);
</script>

```

- 3) Zapisz zmodyfikowany plik HTML przy użyciu klienta webDAV.
- c. Otwórz plik o nazwie `widgetActions.json`. Na przykład w kompozycji *moja_kompozycja* plik ten znajduje się w katalogu `/fs-type1/themes/moja_kompozycja/menuDefinitions/`.
- d. Dodaj do pliku następujące pozycje i zapisz go w produkcie WebSphere Portal przy użyciu klienta webDAV. Upewnij się, że wprowadzona liczba porządkowa (parametr `ordinal`) jest unikalna.

```

{
  bundlePackage: "com.ibm.bspace.bundles",
  bundleName: "Kompozycja",
  bundleKey: "theme_refresh",
  iconClass: "",
  ordinal: 160,
  enabled: true,
  visibilityFn: confirmBspaceRefreshMenuVisibility,
  actionFn: refreshBspaceWidgetImpl,
  id: "BspaceWidgetActions:widgetRefresh"
},
{
  bundlePackage: "com.ibm.bspace.bundles",
  bundleName: "Kompozycja",
  bundleKey: "theme_help",
  iconClass: "",
  ordinal: 150,
  enabled: true,
  metadata: {
    mode: com.ibm.mm.iwidget.Constants.mode.HELP
  },
  visibilityFn: confirmBspaceHelpMenuVisibility,
  actionFn: bspaceWidgetHelpMenuImpl,
  id: "BspaceWidgetActions:widgetHelp"
},
{
  bundlePackage: "com.ibm.bspace.bundles",
  bundleName: "Kompozycja",
  bundleKey: "theme_sendWidget_control",
  iconClass: "",
  ordinal: 170,
  enabled: true,
  visibilityFn: confirmBspaceSendWidgetVisibility,
  actionFn: bspaceWidgetSendWidgetImpl,
  id: "BspaceWidgetActions:sendWidget"
},

```

- e. Aby wyświetlić dodane pozycje menu, usuń pamięć podręczną przeglądarki i przeładuj widgety.

Po zakończeniu konfiguracji produktu Business Space do pracy z produktem WebSphere Portal należy wykonać następujące czynności:

- Jeśli używany jest program IBM Business Monitor z produktem IBM Cognos Business Intelligence, należy zaktualizować sekcję `ProxyServlet_Servlet` pliku `web.xml`. Więcej informacji znajduje się w dokumentacji programu IBM Business Monitor.
- Aby znaleźć określone elementy iWidget produktu Business Space, dodać je do strony produktu WebSphere Portal i rozpocząć pracę w środowisku produktu WebSphere Portal, kliknij opcję **Działania > Edytuj stronę**.
- Aby umożliwić wymianę zdarzeń między elementami iWidget i własnymi portletami na jednej stronie produktu WebSphere Portal oraz umożliwić zachowywanie stanów

nawigacyjnych widgetów po zmianie strony, strony zawierające widżety Business Space należy skonfigurować tak, aby używały agregacji po stronie klienta. Więcej informacji zawiera dokumentacja produktu WebSphere Portal.

Konfigurowanie funkcji pojedynczego logowania oraz protokołu SSL dla widgetów w produkcie WebSphere Portal

Aby widżety produktu użytkownika działały w produkcie WebSphere Portal, należy skonfigurować funkcję pojedynczego logowania między produktem WebSphere Portal oraz produktem użytkownika zawierającym widżety produktu Business Space, a także skonfigurować certyfikaty SSL (Secure Sockets Layer) tak, aby były wymieniane między produktem WebSphere Portal oraz produktem zawierającym widżety produktu Business Space.

Należy skonfigurować funkcję pojedynczego logowania dla serwerów produktu WebSphere Portal oraz produktu użytkownika zawierającego widżety produktu Business Space. Należy także nawiązać połączenie SSL między produktem WebSphere Portal oraz produktem użytkownika zawierającym widżety produktu Business Space. Wymaga to wymiany certyfikatów SSL osoby podpisującej między serwerami.

W przypadku serwera produktu WebSphere Portal oraz serwera produktu użytkownika w celu zalogowania się do Konsoli administracyjnej należy użyć tej samej nazwy użytkownika i hasła.

1. Skonfiguruj pojedyncze logowanie między produktem WebSphere Portal oraz produktem zawierającym widżety produktu Business Space.
 - a. Zaloguj się do Konsoli administracyjnej menedżera wdrażania produktu zawierającego widżety produktu Business Space.
 - b. Wykonaj kroki opisane w sekcji Importowanie i eksportowanie kluczy Centrum informacyjnego produktu WebSphere Application Server.
2. Skonfiguruj certyfikaty SSL tak, aby były wymieniane między serwerem produktu WebSphere Portal oraz serwerem produktu użytkownika zawierającego widżety produktu Business Space.

Należy upewnić się, że osoby podpisujące zostały skonfigurowane w odpowiednich magazynach zaufanych certyfikatów serwera WebSphere Portal oraz serwera produktu użytkownika. Więcej informacji można znaleźć w sekcji Bezpieczna komunikacja przy użyciu protokołu SSL (Secure Sockets Layer) Centrum informacyjnego produktu WebSphere Application Server.

Komenda `updateEndpointBindingsOnPortal`

Komenda `updateEndpointBindingsOnPortal` służy do tworzenia odwołań do punktów końcowych na serwerze aplikacji portalu WebSphere Portal, co umożliwi zespołowi korzystanie z widżetów produktu Business Space w portalu WebSphere Portal.

Ta komenda tworzy odwołania do punktów końcowych usługi REST (Representational State Transfer) na serwerze aplikacji portalu WebSphere Portal. Aby produkt Business Space działał prawidłowo w środowisku portalu WebSphere Portal, muszą zostać utworzone pozycje odwołań do produktu Business Space i do punktu końcowego specyficznego dla produktu. Widżety produktu Business Space są rejestrowane przez produkt WebSphere Portal jako elementy `iWidget`. Jest to realizowane przy użyciu masowego importu z wykorzystaniem pliku katalogu widgetów specyficznego dla produktu WebSphere Portal z produktem użytkownika. Plik XML katalogu jest dostępny w katalogu głównym pliku archiwum WWW (WAR) produktu. Każdy produkt ma inny kontekstowy katalog główny. Ta komenda działa tylko w przypadku dostawcy środowiska zasobów o nazwie **WP Mashup Endpoints** (Punkty końcowe strony zespolonej WP).

Przed uruchomieniem tej komendy należy zainstalować produkt WebSphere Portal 7.0.0.1 lub nowszy, skonfigurować produkt Business Space oraz usługi REST dla używanego produktu, a także skonfigurować protokół SSL i funkcję pojedynczego logowania. Więcej informacji na ten temat zawiera sekcja Konfigurowanie produktu Business Space w produkcie WebSphere Portal.

Po użyciu komendy zapisz zmiany w konfiguracji głównej przy użyciu jednej z następujących komend:

- W przypadku języka Jython:
AdminConfig.save()
- W przypadku języka Jacl:
\$AdminConfig save

Parametry wymagane

-serverName*nazwa_serwera_WebSphere_Portal*

Parametr określający nazwę serwera docelowego dla konfiguracji produktu WebSphere Portal. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-nodeName*nazwa_węzła_WebSphere_Portal*

Parametr określający nazwę węzła docelowego dla konfiguracji produktu WebSphere Portal. W celu skonfigurowania produktu Business Space na serwerze należy określić zarówno parametr **serverName**, jak i parametr **nodeName**.

-clusterName*nazwa_klastra_WebSphere_Portal*

Parametr określający nazwę klastra docelowego dla konfiguracji produktu WebSphere Portal. W celu skonfigurowania produktu Business Space w klastrze należy określić tylko parametr **clusterName**. Nie należy określać parametrów **serverName** ani **nodeName**.

-host*adres_IP_lub_nazwa_hosta_serwera_portalu*

Parametr określający adres IP lub nazwę hosta dla zdalnego serwera produktu WebSphere Portal.

-port*wartość_domyślna_portu_SOAP_portalu_10025*

Parametr określający nazwę portu SOAP dla zdalnego serwera produktu WebSphere Portal.

-userIdentifikator_administratora_portalu

Parametr określający identyfikator administratora dla zdalnego serwera produktu WebSphere Portal.

-password*hasło_administratora_portalu*

Parametr określający hasło administratora dla zdalnego serwera produktu WebSphere Portal.

-endpointBindingDirectoryName*katalog_zawierający_pliki_punktów_końcowych*

Parametr określający katalog, w którym znajdują się pliki punktów końcowych. Należy się upewnić, że w tym katalogu nie ma żadnych innych plików.

Przykłady

W poniższym przykładzie tworzone są odwołania do punktu końcowego na serwerze aplikacji produktu WebSphere Portal dla środowiska autonomicznego.

- Przykład kodu Jython:
AdminTask.updateEndpointBindingsOnPortal(['-nodeName
nazwa_węzła_produkту_Portal -serverName WebSphere_Portal
-endpointBindingDirectoryName katalog_zawierający_pliki_punktów_końcowych
-host adres_IP_lub_nazwa_hosta_serwera_produkту_Portal -port

```
domyślny_port_SOAP_produkту_Portal_10025 -user
identyfikator_administradora_produkту_Portal -password
hasło_administradora_produkту_Portal])
```

- Przykład kodu Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-nodeName
nazwa_węzła_produkту_Portal -serverName WebSphere_Portal
-endpointBindingDirectoryName katalog_zawierający_pliki_punktów_końcowych
-host adres_IP_lub_nazwa_hosta_serwera_produkту_Portal -port
domyślny_port_SOAP_produkту_Portal_10025 -user
identyfikator_administradora_produkту_Portal -password
hasło_administradora_produkту_Portal}
```

W poniższym przykładzie tworzone są odwołania do punktu końcowego na serwerze aplikacji produktu WebSphere Portal dla środowiska klastrowego.

- Przykład kodu Jython:

```
AdminTask.updateEndpointBindingsOnPortal(['-clusterName
nazwa_klastra_portalu -endpointBindingDirectoryName
katalog_zawierający_pliki_punktów_końcowych_w_systemie_lokalnym -host
adres_IP_lub_nazwa_hosta_serwera_portalu -port
wartość_domyślna_portu_SOAP_portalu_8879 -user
identyfikator_administradora_portalu -password hasło_administradora_portalu'])
```

- Przykład kodu Jacl:

```
$AdminTask updateEndpointBindingsOnPortal {-clusterName
nazwa_klastra_portalu -endpointBindingDirectoryName
katalog_zawierający_pliki_punktów_końcowych_w_systemie_lokalnym -host
adres_IP_lub_nazwa_hosta_serwera_portalu -port
wartość_domyślna_portu_SOAP_portalu_8879 -user
identyfikator_administradora_portalu -password hasło_administradora_portalu}
```

Pozycje wymagane w pliku proxy-config.xml do skonfigurowania widgetów pod kątem współpracy z produktem WebSphere Portal

W celu skonfigurowania proxy Ajax na serwerze produktu WebSphere Portal należy użyć przykładów pozycji, które są wymagane w pliku proxy-config.xml. Aby zezwolić na zdalne adresy URL odwołujące się do serwera produktu z poziomu serwera produktu WebSphere Portal, należy skonfigurować proxy Ajax.

Poniższy fragment kodu XML prezentuje strategię proxy wymaganą przez produkty do zarządzania procesami biznesowymi. Takie ustawienie jest wymagane w przypadku wszystkich zdalnych adresów URL, które mają być otwierane z użyciem proxy produktu WebSphere Portal (na przykład adresów serwera produktu Business Space oraz serwera zarządzania procesami biznesowymi). W miejsce łańcucha `<ZDALNY_ADRES_URL_PRODUKTU_BPM>` należy wstawić zdalny adres URL, który wymaga otwarcia z użyciem proxy produktu WebSphere Portal.

Wskazówka: Domyślnie wartość socket-timeout jest ustawiona na 10 sekund. Produkt Business Space używa komponentu proxy na potrzeby nawiązywania połączenia z usługami REST użytkownika. Jeśli usługi REST nie odpowiadają, wartość socket-timeout należy zmienić na odpowiednią do sytuacji (na przykład 30 sekund). Więcej informacji na ten temat można znaleźć w sekcji “Zmienianie ustawień limitu czasu dla proxy Ajax produktu Business Space” na stronie 249.

Jeśli istnieje wiele zdalnych serwerów lub adresów URL, do których dostęp ma być uzyskiwany po akceptacji przez proxy serwera produktu WebSphere Portal, należy dostosować konfigurację proxy za pomocą pozycji strategii dynamicznej. Strategia proxy

będzie inna w poszczególnych wdrożeniach. Różne metody konfigurowania proxy serwera produktu WebSphere Portal opisano w dokumentacji produktu WebSphere Portal.

Plik proxy-config.xml znajduje się w katalogu *instalacyjny_katalog_główny_produkту_WebSphere_Portal*\base\wp.proxy.config\installableApps\wp.proxy.config.ear\wp.proxy.config.war\WEB-INF.

Ważne: Przed wprowadzeniem do produktu WebSphere Portal zaktualizowany plik proxy-config.xml wymaga przejrzania i zatwierdzenia przez administratorów produktu WebSphere Portal.

```
<!-- Strategia proxy produktu BPM/Business Space -->

<proxy:policy url="ZDALNY_ADRES_URL_PRODUKTU_BPM" acf="none">
<proxy:actions>
<proxy:method>GET</proxy:method>
<proxy:method>HEAD</proxy:method>
<proxy:method>POST</proxy:method>
<proxy:method>DELETE</proxy:method>
<proxy:method>PUT</proxy:method>

</proxy:actions>
<proxy:cookies>
<proxy:cookie>LtpaToken</proxy:cookie>
<proxy:cookie>LtpaToken2</proxy:cookie>
<proxy:cookie>JSESSIONID</proxy:cookie>
<proxy:cookie>CRN</proxy:cookie>
<proxy:cookie>caf</proxy:cookie>
<proxy:cookie>cam_passport</proxy:cookie>
<proxy:cookie>cc_session</proxy:cookie>
<proxy:cookie>userCapabilities</proxy:cookie>
<proxy:cookie>usersessionid</proxy:cookie>
</proxy:cookies>
<proxy:headers>
<proxy:header>User-Agent</proxy:header>
<proxy:header>Accept*</proxy:header>
<proxy:header>Content*</proxy:header>
<proxy:header>Authorization*</proxy:header>
<proxy:header>X-Method-Override</proxy:header>
<proxy:header>Set-Cookie</proxy:header>
<proxy:header>If-Modified-Since</proxy:header>
<proxy:header>If-None-Match</proxy:header>
<proxy:header>X-Server</proxy:header>
<proxy:header>X-Update-Nonce</proxy:header>
<proxy:header>X-Requested-With</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualhost</proxy:header>
<proxy:header>com.ibm.lotus.openajax.virtualport</proxy:header>
<proxy:header>Slug</proxy:header>
<proxy:header>SOAPAction</proxy:header>
</proxy:headers>
</proxy:policy>

<proxy:meta-data>
<proxy:name>forward-http-errors</proxy:name>
<proxy:value>true</proxy:value>
</proxy:meta-data>
<proxy:meta-data>
<proxy:name>socket-timeout</proxy:name>
<proxy:value>30000</proxy:value>
</proxy:meta-data>
```

Konfigurowanie monitorowania czynności personelu

Model monitorowania czynności personelu jest wymagany do wyświetlenia czynności personelu na panelu kontrolnym przy użyciu widgetu Czynności personelu produktu IBM Business Monitor. Ten model i widget obsługują tylko te czynności personelu, które działają w procesie Business Process Execution Language (BPEL) w produkcie IBM Business Process Manager Advanced. Jeśli podczas tworzenia profilu nie zainstalowano modelu czynności personelu, model monitorowania czynności personelu można zainstalować i skonfigurować później przy użyciu Konsoli administracyjnej.

W tej sekcji opisano sposób instalowania pliku EAR, włączania zabezpieczeń monitorowania czynności personelu w produkcie IBM Business Process Manager Advanced i włączania zdarzeń.

Ręczne instalowanie modelu monitorowania czynności personelu

Jeśli podczas tworzenia profilu produktu IBM Business Monitor nie zainstalowano modelu monitorowania globalnych czynności personelu, można zainstalować go później. Plik `GlobalHTMMApplication.ear` jest już zapisany na dysku twardym, nawet jeśli podczas tworzenia profilu nie zainstalowano modelu monitorowania czynności personelu.

Aby zainstalować plik `GlobalHTMMApplication.ear` wymagany w celu używania modelu monitorowania czynności personelu, wykonaj następujące kroki:

1. W Konsoli administracyjnej kliknij opcję **Aplikacje > Modele monitorowania**. W tej tabeli znajduje się lista wszystkich obecnie zainstalowanych modeli monitorowania.
2. Kliknij przycisk **Instaluj**.
3. Wybierz opcję **Lokalny system plików** i kliknij przycisk **Przeglądaj**.
4. Przejdź do folderu zawierającego plik `.ear`: `katalog_główny_serwera_aplikacji/installableApps.wbm/monitorModels`, wybierz plik `GlobalHTMMApplication.ear` i kliknij opcję **Otwórz**.
5. Upewnij się, że opcja **Pytaj tylko jeśli wymagane są dodatkowe informacje** jest zaznaczona.
6. Kliknij przycisk **Dalej** i akceptuj wszystkie ustawienia domyślne, aż wyświetlona zostanie strona **Podsumowanie**.
7. Na stronie **Podsumowanie** sprawdź, czy wszystkie informacje są poprawne i kliknij przycisk **Zakończ**.
8. Opcjonalnie: Aby przejrzeć dokonane zmiany, kliknij opcję **Przejrzyj zmiany** przed ich zapisaniem lub usunięciem.
9. Kliknij opcję **Zapisz**, aby zapisać zmiany w konfiguracji głównej i zapisać model.

Po zainstalowaniu pliku EAR należy skonfigurować panele kontrolne przy użyciu informacji o połączeniu produktu Business Process Choreographer. Należy także odwzorować role w celu skonfigurowania zabezpieczeń dla użytkowników modelu monitorowania czynności personelu.

Włączanie zdarzeń dla monitorowania czynności personelu

Po skonfigurowaniu zabezpieczeń dla monitorowania czynności personelu należy włączyć generowanie zdarzeń autonomicznych czynności personelu lub wstawianych czynności personelu BPEL (Business Process Execution Language) przy użyciu produktu Integration Designer. Czynności te są następnie wdrażane na serwerze produktu IBM Business Process Manager Advanced.

Przed wykonaniem tej czynności należy wykonać następujące czynności:

- Skonfigurowanie zdalnej infrastruktury CEI na serwerze produktu IBM Business Process Manager Advanced - w przypadku serwera procesów działającego na serwerze zdalnym.
- Skonfigurowanie zabezpieczeń produktu IBM Business Process Manager Advanced.
- Odwzorowanie użytkowników i grup na role administratora systemu i monitora systemu

Aby upewnić się, że zdarzenia są generowane, należy włączyć generowanie zdarzeń dla infrastruktury CEI i wskazać format wersji 7.0 w produkcie IBM Integration Designer.

Uwaga: Model monitorowania czynności personelu nie obsługuje formatu wersji 6.0.2.

Zdarzenia należy włączać oddzielnie dla każdej autonomicznej czynności personelu i wstawianej czynności personelu BPEL.

Więcej informacji na temat włączania generowania zdarzeń można znaleźć w dokumentacji produktu w sekcji odsyłaczy do stron pokrewnych.

Konfigurowanie połączeń produktu Business Space w programie WebSphere Portal

Informacje o połączeniu produktu Business Space dla panelu kontrolnego produktu WebSphere Portal należy wprowadzić ręcznie. Instalator używa tych informacji w celu przetestowania połączenia i sprawdzenia, czy serwer IBM Business Process Manager Advanced działa poprawnie na potrzeby funkcji monitorowania czynności personelu.

Aby ręcznie wprowadzić informacje o połączeniu na potrzeby paneli kontrolnych, wykonaj następujące kroki:

1. Zaloguj się w Konsoli administracyjnej serwera WebSphere Application Server, na którym zainstalowano serwer programu IBM Business Monitor.
2. Na panelu nawigacyjnym kliknij opcję **Serwery > Typy serwerów > Serwery WWW > Server1**. Zostanie wyświetlony panel Konfiguracja.
3. W obszarze Infrastruktura serwera rozwiń pozycję **Java i zarządzanie procesami**, a następnie kliknij opcję **Definicja procesu**.
4. W obszarze Właściwości dodatkowe kliknij opcję **Wirtualna maszyna języka Java > Właściwości niestandardowe**.
5. Kliknij opcję **Nowy**, aby utworzyć nowe właściwości. Zostanie wyświetlony panel Właściwości ogólne.
6. Dodaj następujące dwie właściwości i wartości:
 - W polu **Nazwa** wprowadź wartość **DashboardBPCHost**. W polu **Wartość** wpisz nazwę hosta lub adres IP serwera Process Server. Kliknij przycisk **Zastosuj**.
 - W polu **Nazwa** wprowadź wartość **DashboardBPCRMIPort**. W polu **Wartość** wpisz numer portu programu startowego, na przykład 2813. Kliknij przycisk **Zastosuj**.
7. Kliknij przycisk **OK**, aby zapisać nowe właściwości.

Konfigurowanie połączeń dla portletowych paneli kontrolnych

Informacje o połączeniu produktu Business Process Choreographer na potrzeby portletowych paneli kontrolnych należy wprowadzić ręcznie. Instalator używa tych informacji w celu przetestowania połączenia i sprawdzenia, czy serwer WebSphere Portal działa poprawnie na potrzeby funkcji monitorowania czynności personelu.

Aby ręcznie wprowadzić informacje o połączeniu na potrzeby portletowych paneli kontrolnych, wykonaj następujące kroki:

1. Zaloguj się w Konsoli administracyjnej produktu WebSphere Portal.
2. Na panelu nawigacyjnym kliknij opcję **Serwery > Typy serwerów > Serwery aplikacji WebSphere > WebSphere_Portal**. Zostanie wyświetlony panel Konfiguracja.
3. W obszarze Infrastruktura serwera rozwiń pozycję **Java i zarządzanie procesami**, a następnie kliknij opcję **Definicja procesu**.
4. W obszarze Właściwości dodatkowe kliknij opcję **Wirtualna maszyna języka Java > Właściwości niestandardowe**.
5. Kliknij opcję **Nowy**, aby utworzyć nowe właściwości. Zostanie wyświetlony panel Właściwości ogólne.
6. Dodaj następujące dwie właściwości i wartości:
 - W polu **Nazwa** wprowadź wartość **DashboardBPCHost**. W polu **Wartość** wpisz nazwę hosta lub adres IP serwera Process Server. Kliknij przycisk **Zastosuj**.
 - W polu **Nazwa** wprowadź wartość **DashboardBPCRMIPort**. W polu **Wartość** wpisz numer portu programu startowego, na przykład **2813**. Kliknij przycisk **Zastosuj**.
7. Kliknij przycisk **OK**, aby zapisać nowe właściwości.

Konfigurowanie modelu monitorowania procesu globalnego

Model monitorowania procesu globalnego pozwala na monitorowanie dowolnego procesu BPEL i czynności personelu bez kroków wdrażania lub generowania modelu monitorowania. Procesy są wykrywane dynamicznie i śledzone na podstawie emitowanych zdarzeń. Zgromadzone dane mogą być wyświetlane w produkcie Business Space za pomocą widgetu Instancje, widgetu Kluczowe wskaźniki wydajności i widgetów raportowania.

Informacje dotyczące korzystania z modelu monitorowania procesu globalnego można znaleźć w sekcji Global Process Monitor (Monitor procesu globalnego) serwisu WWW Business Process Management Samples and Tutorials (Przykłady i kursy produktu Business Process Management) lub w artykule zamieszczonym w serwisie developerWorks dostępnym za pomocą odsyłacza do informacji pokrewnych.

Ręczne instalowanie modelu monitorowania procesu globalnego

Jeśli model monitorowania procesu globalnego nie został utworzony podczas tworzenia profilu programu IBM Business Monitor, można zainstalować go później, wykonując poniższe czynności. Plik **GlobalProcessMonitorV75.ear** jest już przechowywany na dysku twardym, nawet jeśli nie zainstalowano modelu monitorowania procesu globalnego podczas tworzenia profilu. Aby zainstalować ten plik, należy użyć Konsoli administracyjnej.

Aby zainstalować plik **GlobalProcessMonitorV75.ear**, wykonaj następujące kroki:

1. W Konsoli administracyjnej kliknij opcję **Aplikacje > Modele monitorowania**. W tej tabeli znajduje się lista wszystkich obecnie zainstalowanych modeli monitorowania.
2. Kliknij przycisk **Instaluj**.
3. Wybierz opcję **Lokalny system plików** i kliknij przycisk **Przeglądaj**.
4. Przejdź do folderu zawierającego plik **.ear** (katalog **główny_serwera_aplikacji/installableApps.wbm/monitorModels**), wybierz plik **GlobalProcessMonitorV75.ear** i kliknij przycisk **Otwórz**.
5. Upewnij się, że opcja **Pytaj tylko jeśli wymagane są dodatkowe informacje** jest zaznaczona.
6. Kliknij przycisk **Dalej** i akceptuj wszystkie ustawienia domyślne, aż wyświetlona zostanie strona Podsumowanie.

7. Na stronie Podsumowanie sprawdź, czy wszystkie informacje są poprawne i kliknij przycisk **Zakończ**.
8. Opcjonalnie: Aby przejrzeć dokonane zmiany, kliknij opcję **Przejrzyj zmiany** przed ich zapisaniem lub usunięciem.
9. Kliknij opcję **Zapisz**, aby zapisać zmiany w konfiguracji głównej i zapisać model.

Jeśli procesy przeznaczone do monitorowania będą uruchomione na tym samym serwerze, nie jest wymagane przeprowadzanie dalszej konfiguracji. W przeciwnym razie konieczne jest skonfigurowanie modelu monitorowania zarówno do odbierania zdarzeń ze zdalnej infrastruktury CEI (produkt IBM Business Process Manager), zgodnie z opisem zamieszczonym w sekcji Konfigurowanie sposobu odbierania zdarzeń, jak i do odbierania zdarzeń z lokalnej infrastruktury CEI (serwer produktu IBM Business Monitor), ponieważ model monitorowania procesu globalnego przesyła zdarzenia do siebie samego.

Włączanie zdarzeń dla modelu monitorowania procesu globalnego

Aby umożliwić monitorowi procesu globalnego śledzenie procesów oraz czynności personelu, konieczne jest włączenie generowania zdarzeń BPEL przy użyciu produktu Integration Designer. Włączone zdarzenia określają ilość informacji o uruchomionych procesach i czynnościach personelu dostępną dla programu IBM Business Monitor. Generowanie zdarzeń dla produktu Business Process Manager jest domyślnie włączone.

Poniższe sugestie stanowią ogólne zalecenia dotyczące zdarzeń BPEL do włączenia:

- Dla każdego procesu, który będzie monitorowany, należy włączyć wszystkie zdarzenia na poziomie procesu. Zwykle będzie to tylko kilka zdarzeń przesyłanych przez proces podczas wykonywania (rozpoczęcie, koniec, niepowodzenia oraz usunięcie).
- Dla każdej interesującej czynności (zwykle czynności personelu i wywołania) również należy włączyć wszystkie zdarzenia.
- Dla każdego działania personelu, które ma być monitorowane, należy przejść do karty Szczegóły w widoku Właściwości tego działania i odszukać odsyłacz do odpowiedniej czynności personelu (jeśli odsyłacz nie istnieje, należy kliknąć przycisk Otwórz, aby go utworzyć). Należy użyć odsyłacza do czynności personelu, przejść do karty Monitor zdarzeń w widoku Właściwości tej czynności, a następnie włączyć požądane zdarzenia kontrolowane.
- Jeśli monitorowany jest zarówno proces, jak i wywoływany przez niego podproces, należy włączyć wszystkie zdarzenia dla czynności wywołania, która łączy tę parę.
- Należy wyłączyć zdarzenia dla krótkotrwałych, zautomatyzowanych kroków.
- Należy włączyć wszystkie zdarzenia dla autonomicznych czynności personelu, które mają być monitorowane.
- Należy rozważyć włączenie wszystkich zdarzeń dla pętli, ponieważ pozwala to uzyskać historię iteracji pętli ze znacznikami czasu.
- Należy włączyć zdarzenia zmiany zmiennej dla zmiennych procesów, które mają być monitorowane, ale nie dla innych zmiennych procesu.

Więcej informacji na temat włączania generowania zdarzeń można znaleźć w dokumentacji produktu Integration Designer 7.5. Poniżej udostępniono odsyłacz.

Konfigurowanie paneli kontrolnych dla modelu monitorowania procesu globalnego

Model monitorowania procesu globalnego odbiera zdarzenia dotyczące procesów i czynności personelu działających w programie IBM Business Process Manager. Wykrywa on wdrożone procesy i definicje zadań na podstawie zdarzeń emitowanych podczas ich działania oraz

śledzi uruchomione procesy i czynności. Użytkownik może skonfigurować własny panel kontrolny dla tego modelu monitorowania przy użyciu widgetu Instancje, widgetu Kluczowe wskaźniki wydajności i widgetu raportowania lub użyć jednego z udostępnionych obszarów biznesowych jako punktu początkowego.

Dwie konfiguracje produktu Business Space są udostępnione w następujących miejscach:

- katalog_główny_serwera_aplikacji/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace.zip
- katalog_główny_serwera_aplikacji/installableApps.wbm/monitorModels/BusinessSpace/GlobalProcessMonitor_BusinessSpace_Advanced.zip

Obie konfiguracje mają tę samą ogólną strukturę, ale w wersji zaawansowanej są wyświetlane dodatkowe szczegóły techniczne, takie jak dokładność co do milisekundy oraz informacje o strefie czasowej w przypadku znaczników czasu, identyfikatory instancji procesu i zadania, historie migracji instancji procesu oraz liczniki zdarzeń kontrolowanych. W celu załadowania wybranej konfiguracji należy użyć funkcji Importuj w produkcie Business Space. Można jej używać takim stanie, w jakim jest, lub potraktować ją jako punkt początkowy konfigurowania personalizowanych widoków panelu kontrolnego.

Początkowo może być pomocne poznanie struktury kontekstu monitorowania tego modelu:

Definicja procesu

Wykonywanie procesu

Krok wykonania procesu

Wykonanie zadania pokrewnego

Zmienna wykonania procesu

Definicja kroku

Wykonanie kroku

Wykonanie zadania pokrewnego

Definicja zadania

Wykonanie zadania

Istnieją dodatkowe definicje kontekstów monitorowania dla danych, których nie można przechowywać w pomiarach, i tym samym wymagających potomnych kontekstów monitorowania. Należy je traktować jako kontenery danych, które są częścią swoich nadrzędnych kontekstów monitorowania. Nie są one przedstawione w powyższej strukturze, która zawiera tylko strukturę głównego kontekstu monitorowania tego modelu monitorowania.

Kontekst monitorowania Definicja procesu odpowiada szablonowi procesu wdrożonemu w programie IBM Business Process Manager. Monitoruje on ten szablon i udostępnia informacje o liczbie rozpoczętych, działających i zakończonych procesów, minimalnym, maksymalnym i średnim czasie działania itd. Nawigując w dół, do kontekstu monitorowania Wykonywanie procesu, można znaleźć informacje dotyczące konkretnego uruchomienia procesu (czas rozpoczęcia, bieżący stan, czas zakończenia itd.). Elementami podrzędnymi kontekstu Wykonywanie procesu są konteksty monitorowania dla poszczególnych kroków procesu (czynności, czynności personelu itd.) oraz zmienne procesu. Dla kroków będących czynnościami personelu udostępniono jeszcze jeden poziom eksplorowania umożliwiający wyświetlanie wykonań pokrewnej czynności personelu, w tym wszystkich podczynności, które mogły zostać dodane podczas wykonywania.

Z kontekstu monitorowania Definicja procesu można również nawigować niżej do jego kontekstów monitorowania Definicja kroku, co umożliwia poznanie wszystkich znanych kroków tego szablonu procesu. (Wykryte mogą być jedynie kroki, które zostały uruchomione przynajmniej raz i przesłały zdarzenia do programu IBM Business Monitor). Dalsza nawigacja w dół powoduje przejście na poziom Wykonanie kroku, na którym można znaleźć te same informacje, co na poziomie Krok wykonania procesu, jednak pogrupowane w inny

sposób. Znajdują się tutaj wszystkie wykonania danej definicji kroku, zamiast wszystkich kroków składających się na jedno uruchomienie procesu. Dla kroków będących czynnościami personelu udostępniono jeszcze jeden poziom eksplorowania umożliwiający wyświetlanie wykonań pokrewnej czynności personelu, w tym wszystkich podczynności, które mogły zostać dodane podczas wykonywania.

Podczas konfigurowania paneli kontrolnych, własnych paneli niestandardowych lub paneli dostarczonych można wybrać pomiary wyświetlane w widgetach. Wszystkie pomiary z przedrostkiem AUX w nazwie służą tylko do przetwarzania wewnętrznego i nie należy ich dodawać do panelu kontrolnego.

Rozdział 11. Instalowanie przykładu modelowego

Jednoserverowa wersja programu IBM Business Monitor jest dostarczana z przykładowym modelem udzielania kredytu hipotecznego ilustrującym zastosowanie niektórych funkcji programu IBM Business Monitor. Jeśli został utworzony profil autonomiczny, za pomocą konsoli Pierwsze kroki można zainstalować przykład modelowy Lepsze pożyczki.

Przykład modelowy Lepsze pożyczki znajduje się w następującym katalogu:

```
katalog_główny_serwera_aplikacji/installableApps.wbm/samples/mortgageLending/  
katalog_główny_serwera_aplikacji\installableApps.wbm\samples\mortgageLending\
```

Nazwa modelu to MortgageLendingBAMApplication.ear.

Jeśli został utworzony profil autonomiczny, można skorzystać z jednej z następujących metod.

- (Nie dotyczy systemu z/OS) Zainstaluj przykład modelowy za pomocą konsoli Pierwsze kroki.

1. Otwórz konsolę Pierwsze kroki z profilu autonomicznego, używając jednej z następujących opcji:
 - Na panelu Zakończono tworzenie profilu wybierz opcję **Uruchom konsolę Pierwsze kroki produktu IBM Business Monitor**.
 - Wybierz opcję **Start > Wszystkie programy > IBM > Business Monitor 7.5 > Profile > nazwa_profilu > Pierwsze kroki**.
 - Przejdź do katalogu katalog_główny_profilu\firststeps.wbm i uruchom komendę firststeps.bat.

Ważne: Aby zainstalować lub uruchomić konsolę Pierwsze kroki w systemach Windows 7, Windows Vista lub Windows Server 2008, konieczne jest zwiększenie uprawnień konta użytkownika systemu Microsoft Windows przez kliknięcie prawym przyciskiem myszy pliku firststeps.bat i wybranie opcji **Uruchom jako administrator**. Jest to wymagane zarówno w przypadku administratorów, jak i użytkowników innych niż administratorzy.

- Otwórz okno komend. Przejdź do katalogu katalog_główny_profilu/firststeps.wbm i uruchom komendę firststeps.sh.
2. W konsoli Pierwsze kroki wybierz opcję **Przykład modelowy**.

Uwaga: Jeśli włączono zabezpieczenia, zostanie wyświetlone zapytanie o ID użytkownika i hasło serwera WebSphere Application Server.

- Zainstaluj przykład modelowy za pomocą Konsoli administracyjnej. Kliknij opcję **Aplikacje > Modele monitorowania**. Kliknij opcję **Instaluj** i przejdź do pliku MortgageLendingBAMApplication.ear. Użyj domyślnych ustawień dla tej instalacji.

Po zakończeniu instalacji należy uruchomić serwer, a następnie otworzyć produkt Business Space w celu wyświetlenia obszaru Lepsze pożyczki. Konsola Pierwsze kroki udostępnia zarówno opcje uruchamiania serwera, jak i produktu Business Space.



Rozdział 12. Deinstalowanie produktu IBM Business Monitor

Program IBM Business Monitor można usunąć za pomocą opcji deinstalowania w programie Installation Manager.

Deinstalowanie produktu IBM Business Monitor

Opcja Deinstaluj w programie Installation Manager umożliwia deinstalowanie pakietów z pojedynczego miejsca instalacji. Można również zdeinstalować wszystkie zainstalowane pakiety z każdego miejsca instalacji.

Aby zdeinstalować pakiety, należy zalogować się do systemu za pomocą tego samego konta użytkownika co konto użyte do zainstalowania pakietów produktu. Nie można zdeinstalować pakietu, jeśli inny pakiet jest od niego zależny, chyba że pakiet ten został również wybrany do zdeinstalowania.

1. Zamknij programy zainstalowane za pomocą programu Installation Manager.
2. Zatrzymaj wszystkie działające serwery.
3. Uruchom program Installation Manager. Na stronie początkowej kliknij opcję **Deinstaluj**.
 W systemie Windows można również kliknąć opcję **Start > Programy > IBM > IBM Business Monitor > Deinstaluj**.
4. Na stronie Deinstalacja pakietów wybierz pakiet IBM Business Monitor i powiązane pakiety, a następnie kliknij przycisk **Dalej**.  Jeśli w poprzednim kroku wybrano opcję **Start > Programy > IBM > IBM Business Monitor > Deinstaluj**, produkt IBM Business Monitor zostanie wstępnie zaznaczony do deinstalacji na stronie Deinstalacja pakietów.
5. Na stronie Podsumowanie przejrzyj listę pakietów, które zostaną zdeinstalowane, a następnie kliknij przycisk **Deinstaluj**. Po zakończeniu procesu deinstalowania zostanie otwarta strona Zakończone.
6. Kliknij przycisk **Zakończ**, aby zakończyć pracę kreatora.

Gdy produkt IBM Business Monitor jest deinstalowany, wszystkie profile rozszerzone do produktu IBM Business Monitor są usuwane, w tym wszystkie profile produktu WebSphere Application Server, które zostały rozszerzone do produktu IBM Business Monitor. W przypadku profili autonomicznego serwera programu Monitor usługa IBM Cognos BI jest usuwana.

Przykładowe modele monitorowania nie zostaną zdeinstalowane w celu zachowania dostosowań modeli. Aby zdeinstalować te modele, zobacz temat Usuwanie modeli i danych monitorowania.

Linux

Jeśli jest planowana reinstalacja produktu IBM Business Monitor, należy usunąć pozostałe wpisy DB2 Express znajdujące się w pliku `/etc/service`. Jest to niezbędne, ponieważ nowa instalacja wymaga dostępnego portu 50000. Należy przeszukać plik `/etc/service` i usunąć wszystkie odwołania do produktu DB2 Express i portu 50000. Na przykład:

```
db2c_bpminst 50000/tcp
```

lub

```
db2c_db2inst1 50000/tcp
```

Usuwanie przykładu modelowego

Program IBM Business Monitor jest dostarczany z przykładem modelowym udzielania kredytu hipotecznego ilustrującym zastosowanie niektórych funkcji programu IBM Business Monitor. Model ten można zainstalować przy użyciu konsoli Pierwsze kroki.

Aby usunąć przykład modelowy:

1. Usunąć panel kontrolny Lepsze pożyczki przy użyciu menedżera obszarów.
2. Przy użyciu Konsoli administracyjnej serwera WebSphere Application Server usunąć szablony alertów.
3. Jeśli włączono zabezpieczenia, przy użyciu Konsoli administracyjnej serwera WebSphere Application Server usunąć rolę użytkownika.
4. Przy użyciu Konsoli administracyjnej serwera WebSphere Application Server wyczyścić model.



Drukowane w USA