Identity Console

Podręcznik administracji

Wrzesień 2022 r.

Informacje prawne

Spis treści

Informacje o niniejszym podręczniku i bibliotece

Podręcznik administracji zawiera informacje koncepcyjne dotyczące produktu NetIQ Identity Console (Identity Console). Podano w nim definicje terminów oraz przedstawiono scenariusze implementacji.

Najnowszą wersję *Podręcznika administracji NetIQ Identity Console* zawiera angielska wersja dokumentacji dostępna online w witrynie z dokumentacją NetIQ Identity Console.

Docelowi odbiorcy

Ten podręcznik jest przeznaczony dla administratorów sieci.

Inne informacje w bibliotece

Biblioteka udostępnia następujące zasoby informacyjne:

Podręcznik instalacji

Opisuje sposób instalacji oprogramowania Identity Console. Jest on przeznaczony dla administratorów sieci.

Informacje o firmie NetIQ Corporation

Jesteśmy globalnym przedsiębiorstwem zajmującym się tworzeniem oprogramowania. Nasze działania mają na celu sprostanie trzem podstawowym wyzwaniom związanym ze środowiskiem naszych Klientów: zmianom, złożoności i ryzyku — pragniemy pomóc im w przezwyciężeniu tych przeszkód.

Nasz punkt widzenia

Przystosowywanie się do zmian oraz zarządzanie złożonością i ryzykiem to nic nowego

Ze wszystkich wyzwań, jakim muszą sprostać nasi Klienci, te trzy są w istocie najważniejszymi czynnikami ograniczającymi możliwość kontroli fizycznych, wirtualnych i chmurowych środowisk obliczeniowych — ich analizowania i monitorowania oraz zarządzania nimi w bezpieczny sposób.

Krytyczne usługi biznesowe: lepiej i szybciej

Wierzymy, że zapewnienie organizacjom IT maksymalnego możliwego poziomu kontroli to jedyny sposób na zagwarantowanie im możliwości efektywnego i zharmonizowanego czasowo świadczenia usług. Nacisk związany ze zmianami i poziomem złożoności nasila się przez cały czas wraz z nieustanną ewolucją organizacji i rosnącą złożonością technologii niezbędnych do zarządzania nimi.

Nasza filozofia

Sprzedajemy inteligentne rozwiązania, nie samo oprogramowanie

W celu zapewnienia niezawodnej kontroli musimy najpierw poznać rzeczywiste sytuacje, z którymi organizacje IT stykają się każdego dnia. Tylko ta metoda działania pozwala opracować praktyczne, inteligentne rozwiązania IT gwarantujące uzyskanie sprawdzonych, wymiernych rezultatów. To znacznie bardziej satysfakcjonujące niż zwykła sprzedaż oprogramowania.

Sukces naszych Klientów to nasza pasja

Sukces naszych Klientów to punkt centralny naszej działalności biznesowej. Wiemy, że na każdym etapie powstawania produktu — od projektu po wdrożenie — potrzebują oni rozwiązań IT umożliwiających bezproblemową współpracę i integrację z już istniejącymi systemami, potrzebują stabilnego wsparcia i szkoleń powdrożeniowych, a wreszcie — kogoś, z kim naprawdę łatwo wprowadzić wymaganą zmianę. Końcowy rezultat może być tylko jeden: jeśli nasz Klient osiągnie sukces, osiągniemy go wszyscy.

Nasze rozwiązania

- Nadzór nad tożsamością i dostępem
- Zarządzanie dostępem

- Zarządzanie zabezpieczeniami
- Zarządzanie systemami i aplikacjami
- Zarządzanie obciążeniami
- Zarządzanie usługami

Kontakt ze wsparciem ds. sprzedaży

W razie pytań dotyczących produktów, cen i możliwości należy się skontaktować z lokalnym partnerem. Jeśli nie jest to możliwe, należy się skontaktować z naszym zespołem wsparcia ds. sprzedaży.

Świat:	www.netiq.com/about_netiq/officelocations.asp
Stany Zjednoczone i Kanada:	1-888-323-6768
Adres e-mail:	info@netiq.com
Witryna WWW:	www.netiq.com

Kontakt z usługami wsparcia Technical Support

W przypadku problemów z produktem należy się skontaktować z naszym zespołem ds. usług wsparcia Technical Support.

Świat:	www.netiq.com/support/contactinfo.asp
Ameryka Północna i Południowa:	1-713-418-5555
Europa, Bliski Wschód i Afryka:	+353 (0) 91-782 677
Adres e-mail:	support@netiq.com
Witryna WWW:	www.netiq.com/support

Kontakt ze wsparciem ds. dokumentacji

Naszym celem jest dostarczanie dokumentacji, która spełnia potrzeby użytkowników. W razie propozycji ulepszeń należy kliknąć opcję **Add Comment** (Dodaj komentarz) u dołu dowolnej strony zawierającej wersję HTML dokumentacji opublikowanej w witrynie www.netiq.com/documentation. Można też wysłać wiadomość e-mail na adres Documentation-Feedback@netiq.com. Cenimy opinie naszych Klientów, dlatego z niecierpliwością czekamy na komentarze.

Kontakt ze wspólnotą użytkowników w trybie online

Qmunity — wspólnota firmy NetIQ w trybie online — to sieć współpracy łącząca użytkowników oraz ekspertów firmy NetIQ. Dzięki dostępowi do aktualniejszych informacji, przydatnych łączy do zasobów pomocy oraz ekspertów firmy NetIQ wspólnota Qmunity pomaga opanować wiedzę niezbędną do pełnego wykorzystania potencjału poczynionych inwestycji IT. Więcej informacji można znaleźć w witrynie http://community.netiq.com.

1 Co to jest Identity Console?

Identity Console to nowoczesna internetowa konsola administracyjna, która zapewnia wirtualny, bezpieczny i zindywidualizowany dostęp do narzędzi administracji sieciowej z dowolnego miejsca przez Internet i przeglądarkę internetową. Identity Console znacznie ułatwia decentralizację zadań administracyjnych.

Funkcje Identity Console

Identity Console zapewnia następujące funkcje:

- Administrowanie obiektami, użytkownikami, schematem, partycjami, replikami, prawami itp. usługi eDirectory
- Zarządzanie programami obsługi i zestawami programów obsługi Identity Manager
- Wyświetlanie statystyki wydajności programu obsługi i zarządzanie nią
- Inspekcja obiektów, wyświetlanie przepływu danych programu obsługi, zarządzanie uwierzytelnieniami, zleceniami pracy itp.
- Zarządzanie stanem synchronizacji haseł i ustawieniami dla programów obsługi
- Zarządzanie założeniami haseł i metodami logowania
- Zarządzanie certyfikatami
- Administrowanie różnymi zasobami sieciowymi
- Ulepszone środki bezpieczeństwa zapewniające ochronę danych
- Ulepszona skalowalność umożliwiająca zarządzanie większymi obiektami eDirectory
- Bezpieczne logowanie do portalu Identity Console za pośrednictwem jednego dostawcy jednokrotnego logowania
- Utworzony z wykorzystaniem najnowszej w branży technologii interfejsu użytkownika
- Łatwość instalacji i konfiguracji za pośrednictwem kontenerów dockera

2 Jak uzyskać dostęp do Identity Console?

Oprogramowanie Identity Console, wraz z całym zestawem swych funkcji, jest dostępne z dowolnej obsługiwanej przeglądarki internetowej. Dostęp do Identity Console można też uzyskać za pomocą przeglądarki internetowej niewymienionej na liście obsługiwanych przeglądarek, ale w przypadku przeglądarek, które nie są oficjalnie obsługiwane, nie można zagwarantować uzyskania pełnej funkcjonalności.

WAŻNE: Informacje na temat obsługiwanych przeglądarek internetowych znajdziesz w *Podręczniku instalacji Identity Console*.

Uzyskiwanie dostępu do Identity Console

Aby uzyskać dostęp do serwerowej wersji Identity Console, wykonaj następujące czynności:

1. W polu adresu URL obsługiwanej przeglądarki Web wprowadź następujący adres.

   Bezpieczne logowanie: `https://<adres-ip-serwera/nazwa_hosta>:<port>/identityconsole/`

   W przykładach adresem IP w *<adres-ip-serwera>* powinien być IPv4. Domyślny port to 9000.
2. Zaloguj się za pomocą nazwy wyróżniającej użytkownika i hasła.
3. Podaj adres IP lub DNS drzewa eDirectory z bezpiecznym portem LDAP lub bez niego.

UWAGA

- Odświeżenie dowolnej karty w oprogramowaniu Identity Console spowoduje wylogowanie użytkownika ze względów bezpieczeństwa.
- Otwarcie powielonej karty oprogramowania Identity Console w przeglądarce spowoduje wylogowanie użytkownika ze względów bezpieczeństwa.
- Nazwa wyróżniająca użytkownika powinna być podana w formacie `cn=admin,ou=sa,o=system`.
- Gdy usługa eDirectory jest skonfigurowana z portem innym niż domyślny, należy podać numer portu.

---

3 Poruszanie się po interfejsie Identity Console

W tej części opisano, jak poruszać się po interfejsie internetowym Identity Console.

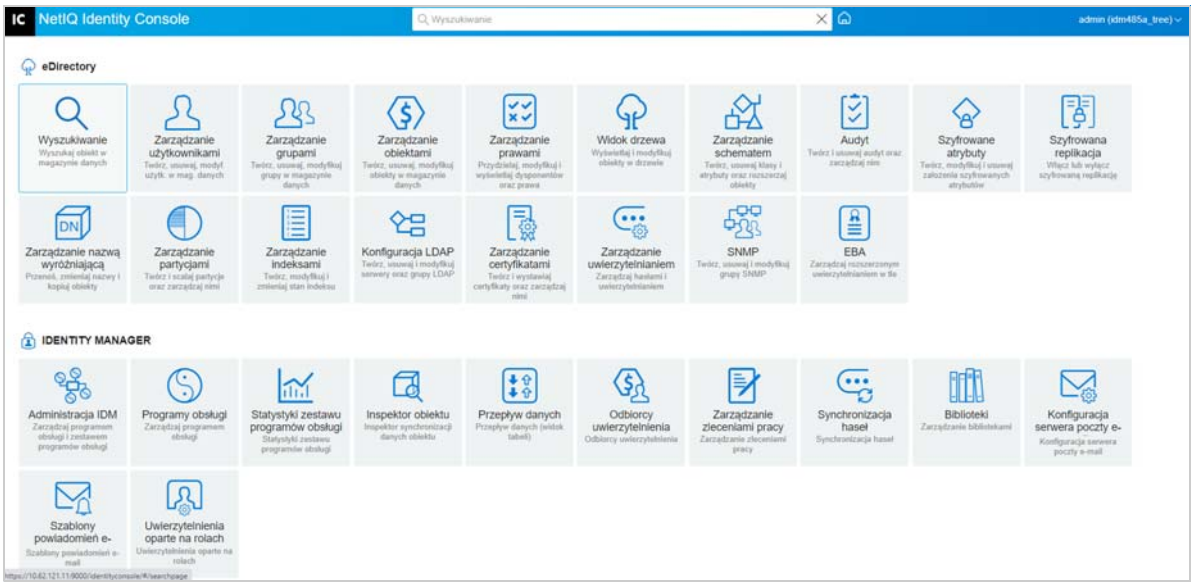
Wyszukaj (podgląd technologii)

Wyszukaj (podgląd technologii) przedstawia wstępny układ funkcji wyszukiwania. W podglądzie tym można określić słowa kluczowe, a pole wyszukiwania określa źródło informacji do przeszukania i wyświetlenia pasujących wyników. Korzystając z tej opcji, można wyszukać zasób i uzyskać do niego łatwy dostęp na każdej stronie aplikacji Identity Console.

Interfejs Identity Console

Interfejs Identity Console składa się z modułów eDirectory i Identity Manager.

Rysunek 3-1 *Interfejs Identity Console*



WAŻNE: Kilka animacji GIF użytych w tym podręczniku działa tylko w dokumentacji online. Jeśli przełączysz się na format PDF, będą widoczne tylko zrzuty ekranu.

Tabela 3-1 *Objaśnienie różnych modułów portalu internetowego Identity Console*

Nazwa modułu	Opis
Wyszukiwanie	Wyszukiwanie obiektu w magazynie danych. Aby uzyskać więcej informacji, zobacz Rozdział 4, „Wykonywanie wyszukiwania”, na stronie 25.
Zarządzanie użytkownikami	Tworzenie, usuwanie i modyfikowanie użytkowników w magazynie danych. Aby uzyskać więcej informacji, zobacz Rozdział 5, „Zarządzanie użytkownikami”, na stronie 29.
Zarządzanie grupami	Tworzenie, usuwanie i modyfikowanie grup w magazynie danych. Aby uzyskać więcej informacji, zobacz Rozdział 6, „Zarządzanie grupami”, na stronie 37.
Zarządzanie obiektami	Tworzenie, usuwanie i modyfikowanie obiektów w magazynie danych. Aby uzyskać więcej informacji, zobacz Rozdział 7, „Zarządzanie obiektami”, na stronie 43.
Zarządzanie prawami	Przypisywanie, modyfikowanie oraz wyświetlanie dysponentów i praw. Aby uzyskać więcej informacji, zobacz Rozdział 8, „Zarządzanie prawami”, na stronie 51.
Widok drzewa	Wyświetlanie i modyfikowanie obiektów w drzewie. Aby uzyskać więcej informacji, zobacz Rozdział 9, „Widok drzewa”, na stronie 55.
Zarządzanie schematem	Tworzenie, usuwanie klas, klas pomocniczych, atrybutów i obiektów rozszerzonych. Aby uzyskać więcej informacji, zobacz Rozdział 10, „Zarządzanie schematem”, na stronie 59.
Audyt	Włączanie, wyłączanie audytu CEF i zarządzanie nim. Aby uzyskać więcej informacji, zobacz Rozdział 11, „Zarządzanie zdarzeniami audytu”, na stronie 67.
Szyfrowane atrybuty	Tworzenie, modyfikowanie, usuwanie i wyświetlanie założeń szyfrowanych atrybutów. Aby uzyskać więcej informacji, zobacz Rozdział 12, „Zarządzanie szyfrowanymi atrybutami”, na stronie 73.
Szyfrowana replikacja	Włączanie, wyłączanie i wyświetlanie szyfrowanej replikacji. Aby uzyskać więcej informacji, zobacz Rozdział 13, „Zarządzanie szyfrowaną replikacją”, na stronie 77.
Zarządzanie nazwą DN	Przenoszenie, zmiana nazw i kopiowanie obiektów. Aby uzyskać więcej informacji, zobacz Rozdział 7, „Zarządzanie obiektami”, na stronie 43.

Nazwa modułu	Opis
Zarządzanie partycjami	Tworzenie, scalanie i przenoszenie partycji oraz replik. Aby uzyskać więcej informacji, zobacz Rozdział 14, „Zarządzanie partycjami i replikami”, na stronie 79.
Zarządzanie indeksami	Tworzenie, modyfikowanie i zmienianie stanu indeksów. Aby uzyskać więcej informacji, zobacz Rozdział 15, „Zarządzanie indeksami”, na stronie 83.
Konfiguracja LDAP	Tworzenie, usuwanie i modyfikowanie obiektów LDAP. Aby uzyskać więcej informacji, zobacz Rozdział 16, „Konfigurowanie obiektów LDAP”, na stronie 87.
Zarządzanie certyfikatami	Tworzenie certyfikatów serwera i certyfikatów ośrodka certyfikacji oraz zarządzanie nimi. Aby uzyskać więcej informacji, zobacz Rozdział 17, „Zarządzanie certyfikatami”, na stronie 91.
Zarządzanie uwierzytelnianiem	Tworzenie metod i sekwencji logowania/do użycia po logowaniu oraz zarządzanie nimi. Przy użyciu tego modułu można również zarządzać założeniami haseł i zestawami odzewu. Aby uzyskać więcej informacji, zobacz Rozdział 18, „Zarządzanie systemem uwierzytelniania”, na stronie 111.
SNMP	Tworzenie, usuwanie i modyfikowanie grup SNMP. Aby uzyskać więcej informacji, zobacz Rozdział 19, „Zarządzanie obiektami grupy SNMP”, na stronie 127.
EBA	Zarządzanie rozszerzonym uwierzytelnianiem w tle. Aby uzyskać więcej informacji, zobacz Rozdział 20, „Zarządzanie rozszerzonym uwierzytelnianiem w tle”, na stronie 131.
Administracja IDM	Zarządzanie programami obsługi i zestawami programów obsługi Identity Manager. Aby uzyskać więcej informacji, zobacz Rozdział 21, „Zarządzanie programami obsługi i zestawami programów obsługi”, na stronie 135. Przy użyciu tego modułu można również zarządzać właściwościami zestawu programów obsługi. Aby uzyskać więcej informacji, zobacz Rozdział 22, „Zarządzanie właściwościami zestawu programów obsługi”, na stronie 143.
Właściwości programu obsługi	Zarządzanie właściwościami różnych programów obsługi. Aby uzyskać więcej informacji, zobacz Rozdział 23, „Zarządzanie właściwościami programów obsługi”, na stronie 157.
Statystyki zestawu programów obsługi	Wyświetlanie statystyki zestawu programów obsługi i zarządzanie nią. Aby uzyskać więcej informacji, zobacz Rozdział 24, „Zarządzanie statystykami zestawu programów obsługi”, na stronie 189.

Nazwa modułu	Opis
Inspektor obiektu	Zarządzanie skojarzeniami obiektu i synchronizacją danych. Aby uzyskać więcej informacji, zobacz Rozdział 25, „Badanie obiektów programu Identity Manager”, na stronie 191.
Przepływ danych	Wyświetlanie przepływu danych programów obsługi i zarządzanie nim. Aby uzyskać więcej informacji, zobacz Rozdział 26, „Zarządzanie przepływem danych”, na stronie 193.
Odbiorcy uwierzytelnienia	Zarządzanie odbiorcami uwierzytelnienia. Aby uzyskać więcej informacji, zobacz Rozdział 27, „Zarządzanie odbiorcami uwierzytelnienia”, na stronie 195.
Zarządzanie zleceniami pracy	Zarządzanie zleceniami pracy. Aby uzyskać więcej informacji, zobacz Rozdział 28, „Zarządzanie zleceniami pracy”, na stronie 197.
Synchronizacja haseł	Zarządzanie synchronizacją i stanem haseł. Aby uzyskać więcej informacji, zobacz Rozdział 29, „Zarządzanie stanem i synchronizacją haseł”, na stronie 201.
Zarządzanie bibliotekami	Zarządzanie bibliotekami. Aby uzyskać więcej informacji, zobacz Rozdział 30, „Zarządzanie bibliotekami”, na stronie 205.
Konfiguracja serwera e-mail	Zarządzanie opcjami serwera e-mail. Aby uzyskać więcej informacji, zobacz Rozdział 31, „Zarządzanie opcjami serwera e-mail”, na stronie 207.
Szablony powiadomień e-mail	Zarządzanie szablonami poczty e-mail. Aby uzyskać więcej informacji, zobacz Rozdział 32, „Zarządzanie szablonami poczty e-mail”, na stronie 209.

Zarządzanie usługą eDirectory przy użyciu Identity Console

W tej sekcji opisano różne zadania, które można wykonywać w celu zarządzania serwerami eDirectory przy użyciu portalu Identity Console.

4 Wykonywanie wyszukiwania

Kafelek Wyszukiwanie umożliwia określenie operacji wyszukiwania do wykonania w drzewie katalogu i wyświetlenie wyników. Ta opcja umożliwia wyszukiwanie różnych obiektów, użytkowników, grup i kilku innych rzeczy. Aby wykonać operację wyszukiwania dla różnych obiektów w magazynie danych, wykonaj następujące czynności:

1. Podaj nazwę obiektu do wyszukania. Aby określić nazwę częściową, należy użyć gwiazdki jako znaku wyrażenia regularnego. Przykłady: `ldap*`, `*cert`, `*server`itp. Jeśli w tym polu użyjesz samej gwiazdki, Identity Console zwróci wszystkie wyniki wyszukiwania na podstawie zawartości pól **Typ** i **Kontekst**.

   UWAGA: Korzystając z przeglądarki kontekstowej, możesz przeglądać całe drzewo eDirectory, podając gwiazdkę (*) w polu wyszukiwania. Można też filtrować obiekty w przeglądarce kontekstowej, korzystając z wyszukiwania z użyciem wyrażenia regularnego. Na przykład `admin*`. To zachowanie przeglądarki kontekstowej jest obsługiwane w różnych modułach portalu Identity Console.

   ---

2. Wybierz typ obiektu do wyszukania w polu **Typ**. Identity Console wyświetli tylko obiekty określonego typu. Domyślnie w tym polu jest wybrany typ **Użytkownik**.

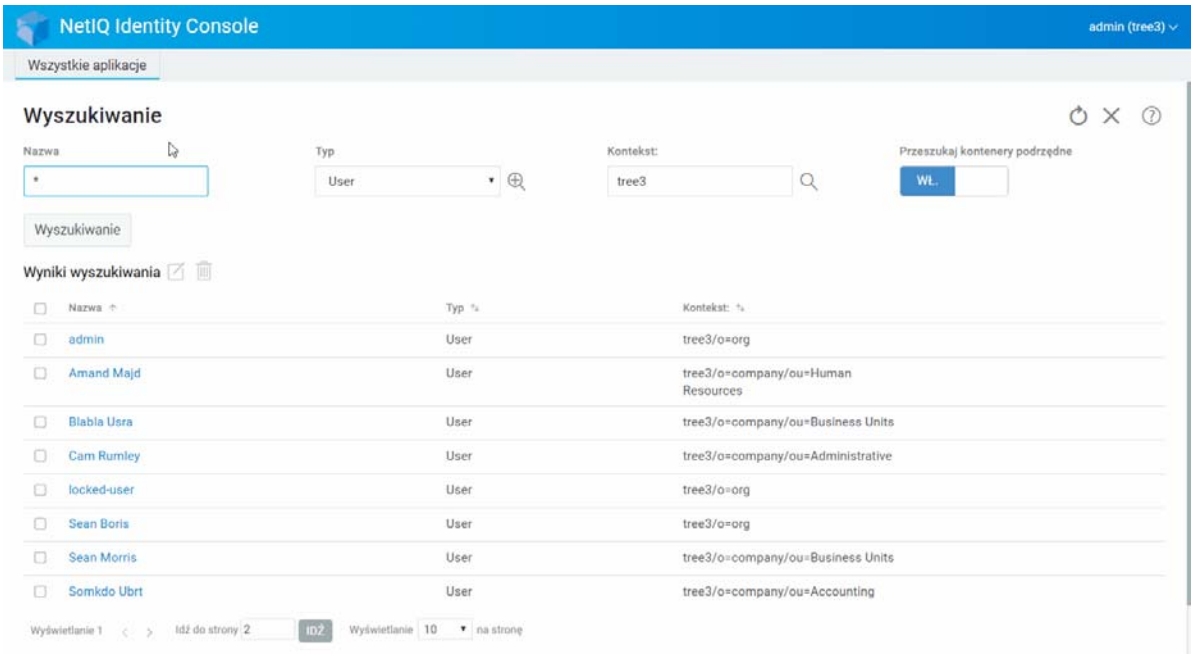
   Kliknij ikonę  , aby zdefiniować dodatkowe ustawienia wyszukiwania na poziomie atrybutu. Aby uzyskać więcej informacji, zobacz „Konfigurowanie wyszukiwania zaawansowanego” na stronie 26.

3. W polu **Kontekst** podaj kontener początkowy dla operacji wyszukiwania.

4. Jeśli wyszukiwanie ma obejmować kontenery podrzędne, wybierz ustawienie **Wł.** dla opcji Przeszukaj kontenery podrzędne.

5. Kliknij przycisk Wyszukiwanie.

Rysunek 4-1 *Wykonywanie operacji wyszukiwania*



Konfigurowanie wyszukiwania zaawansowanego

Opcja Wybór zaawansowany zapewnia bardziej konfigurowalne środowisko wyszukiwania żądanych obiektów w katalogu.

Typ obiektu: Określa wyszukiwaną klasę bazową obiektu. Na przykład: Użytkownik.

Klasy pomocnicze: Kliknij ikonę +, aby określić klasę pomocniczą do uwzględnienia w wyszukiwaniu.

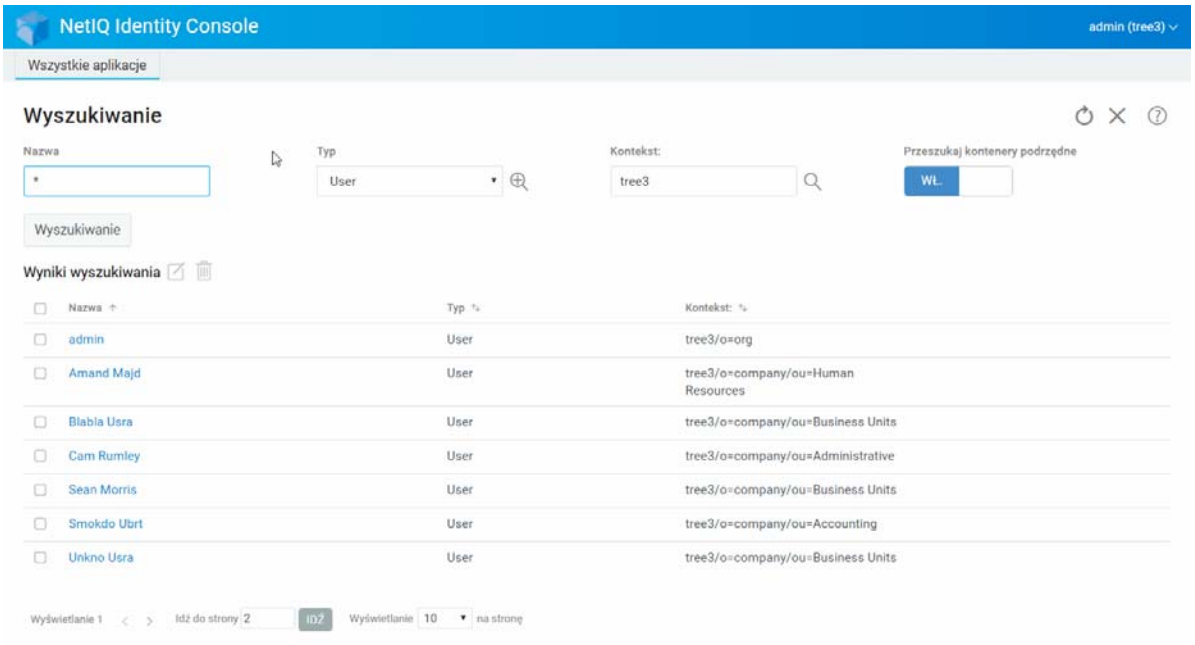
Atrybut: Określa atrybut (właściwość), który ma zostać użyty jako część filtru.

Operator: Określa operator logiczny do zastosowania w filtrze. Dostępne są następujące opcje.

Wartość: Określa wartość atrybutu używaną w charakterze filtru. Aby wskazać część wartości, można użyć gwiazdki (*) jako znaku wyrażenia regularnego. Na przykład: kowal*, *ski i *walsk*.

Ponadto można połączyć wiele filtrów atrybutów w grupę filtrów, używając ikony + Rule w celu dodania drugiego atrybutu do listy. W przypadku używania wielu filtrów atrybutów należy je połączyć za pomocą operatorów logicznych AND lub OR.

Rysunek 4-2 *Konfigurowanie wyszukiwania zaawansowanego*



5 Zarządzanie użytkownikami

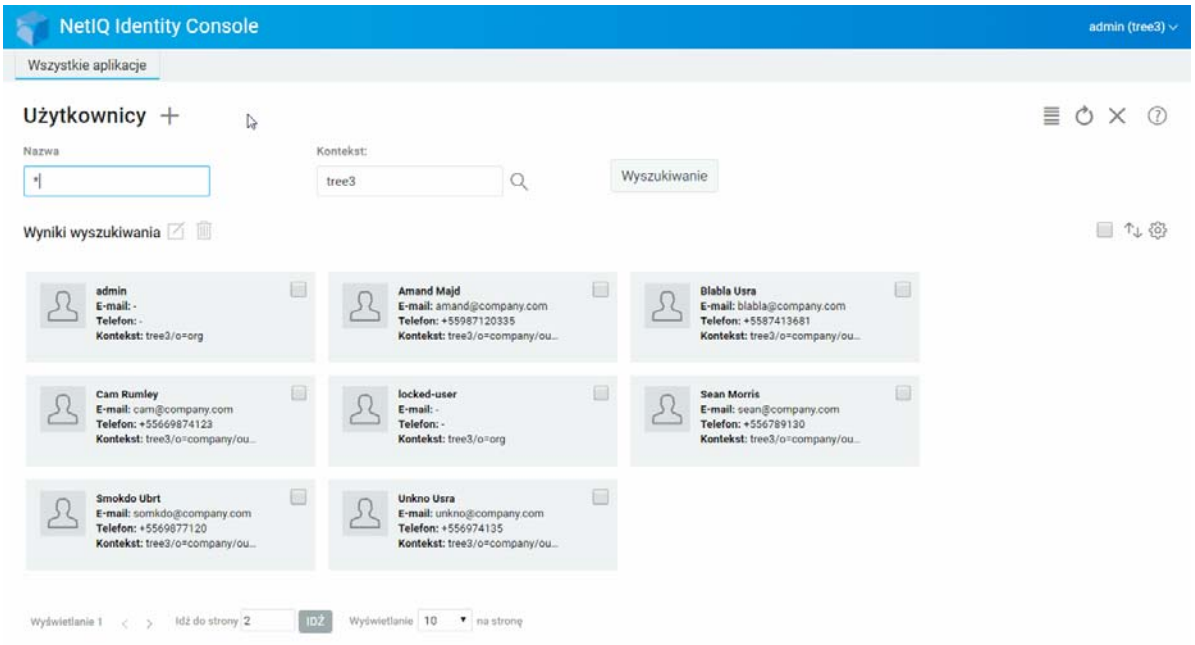
Zarządzanie użytkownikami i ich dostępem do sieci jest głównym celem magazynu danych. Przy użyciu portalu internetowego Identity Console można wykonywać następujące zadania związane z użytkownikami:

Tworzenie użytkownika

Aby utworzyć nowy obiekt użytkownika:

1. Kliknij opcję **Zarządzanie użytkownikami** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz użytkownika podaj co najmniej wymagane informacje związane z użytkownikiem, a następnie kliknij przycisk Utwórz.
   - **Nazwa użytkownika**
   - **Kontekst**
   - **Nazwisko**
   - **Hasło**
4. Zostanie wyświetlone potwierdzenie informujące o utworzeniu obiektu użytkownika.

Rysunek 5-1 *Tworzenie użytkowników*

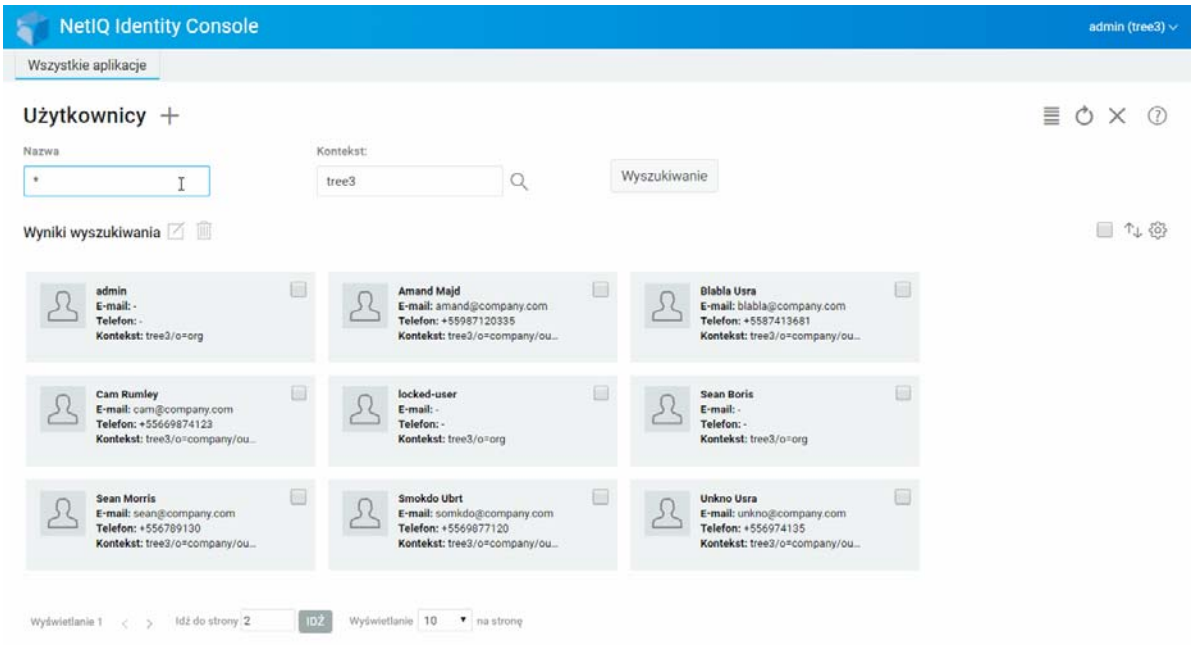


Usuwanie użytkownika

Aby usunąć obiekt użytkownika:

1. Kliknij opcję **Zarządzanie użytkownikami** na stronie docelowej Identity Console.
2. Wpisz nazwę i kontekst obiektu lub znajdź obiekt przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekt użytkownika z listy użytkowników i kliknij ikonę .
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu obiektu użytkownika.

Rysunek 5-2 *Usuwanie użytkownika*

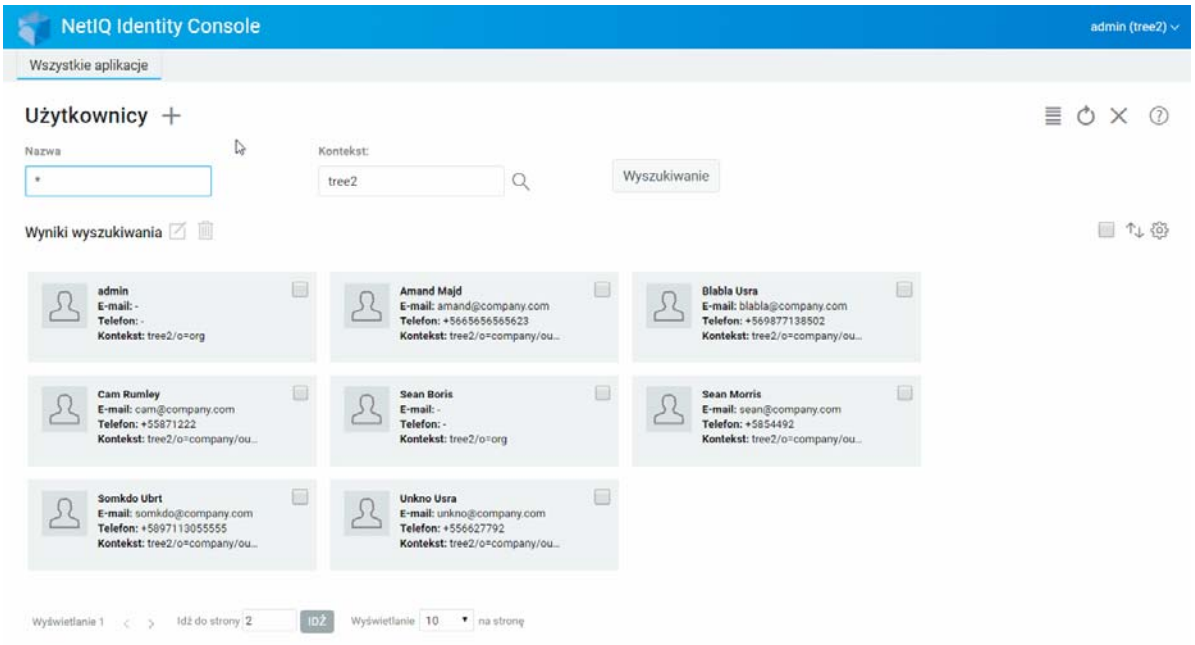


Modyfikowanie użytkowników

Aby zmodyfikować obiekt użytkownika:

1. Kliknij opcję **Zarządzanie użytkownikami** na stronie docelowej Identity Console.
2. Wpisz nazwę i kontekst obiektu lub znajdź obiekt przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekt użytkownika z listy użytkowników i kliknij ikonę .
4. Wprowadź zmiany, a następnie kliknij przycisk Zapisz.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu obiektu użytkownika.

Rysunek 5-3 *Modyfikowanie użytkownika*

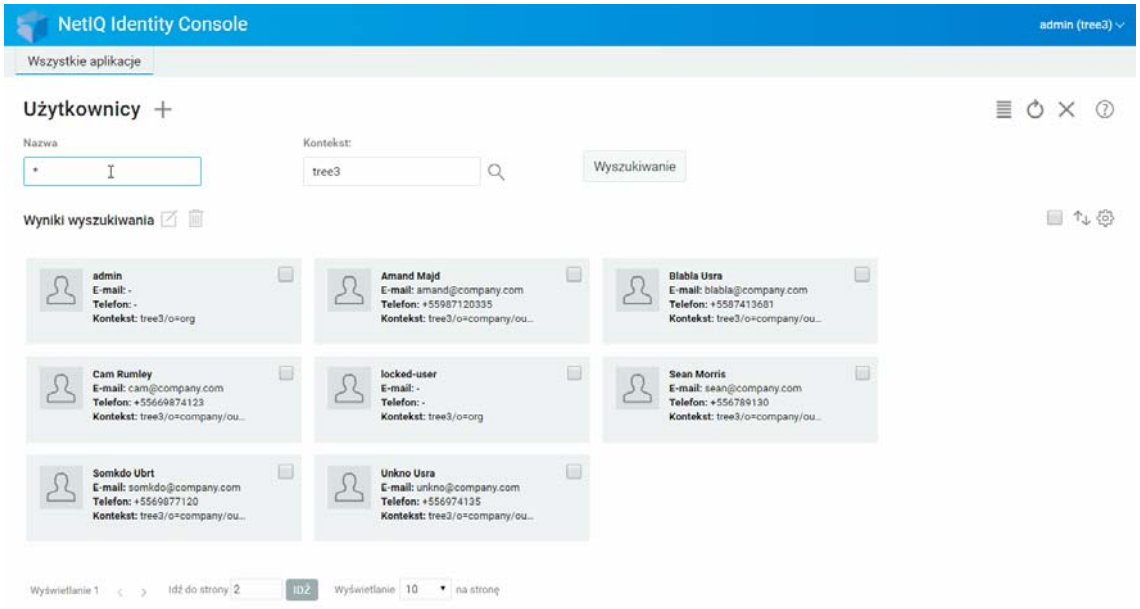


Wyszukiwanie użytkownika

Aby wyszukać obiekt użytkownika:

1. Kliknij opcję **Zarządzanie użytkownikami** na stronie docelowej Identity Console.
2. Użytkownika możesz wyszukiwać na podstawie samej nazwy lub nazwy i kontekstu. Po podaniu wszystkich niezbędnych szczegółów kliknij ikonę Wyszukiwanie.

Rysunek 5-4 *Wyszukiwanie użytkownika*

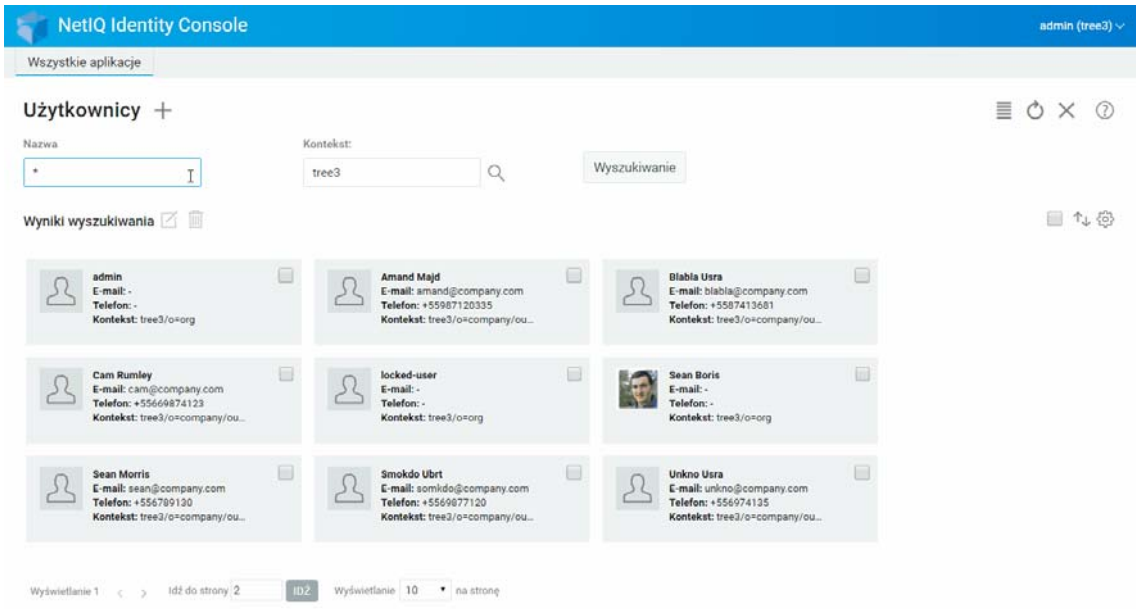


Ustawianie ograniczeń haseł

Funkcja Ograniczenia haseł umożliwia wykonywanie następujących czynności:

- Umożliwia użytkownikom zmianę ich haseł
- Wymuszanie hasła do zalogowania się
- Określanie siły hasła
- Wymuszanie okresowej zmiany hasła
- Określanie daty ważności hasła
- Wymuszanie tworzenia unikatowych haseł
- Określanie okresu dodatkowego logowania w przypadku wygaśnięcia hasła

Rysunek 5-5 *Ograniczenia hasła*

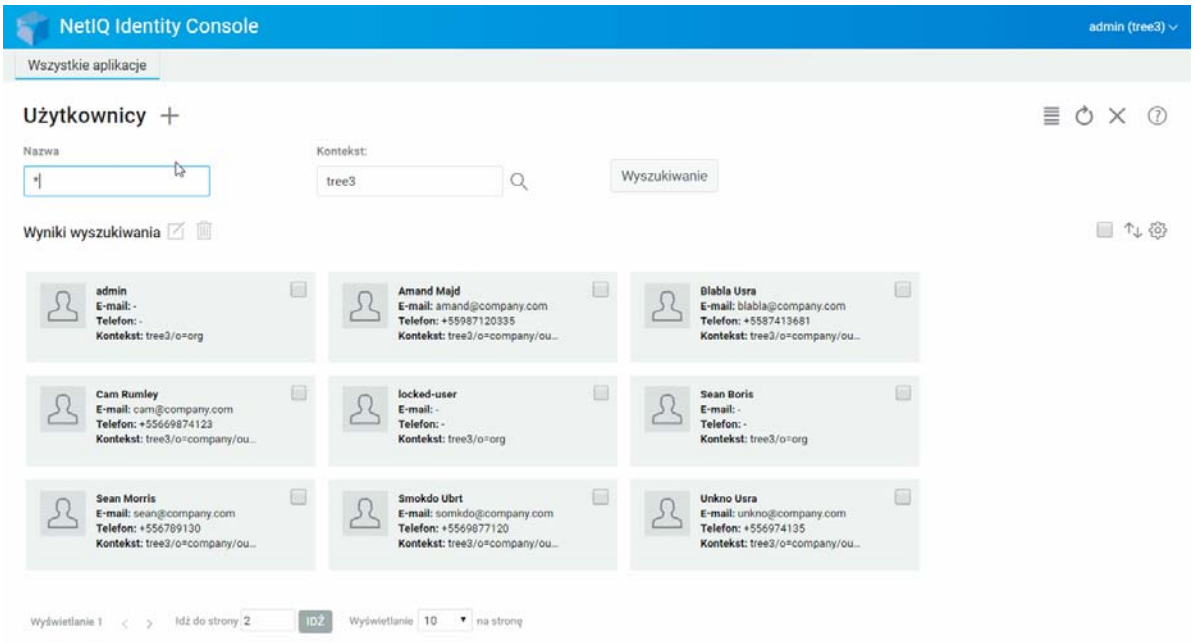


Włączanie i wyłączanie konta użytkownika

Aby wyłączyć konto użytkownika, wykonaj następujące czynności:

1. Wybierz użytkownika, którego konto ma zostać wyłączone, i kliknij ikonę .
2. Kliknij kartę **Ograniczenia** na stronie **Modyfikuj użytkownika**.
3. Rozwiń kartę **Ograniczenia logowania** i zaznacz pole wyboru **Konto wyłączone**.
4. Kliknij ikonę Zapisz.
5. Konto użytkownika jest teraz wyłączone. Aby włączyć wyłączone konto użytkownika, odznacz pole wyboru **Konto wyłączone**.

Rysunek 5-6 *Włączanie i wyłączanie konta użytkownika*

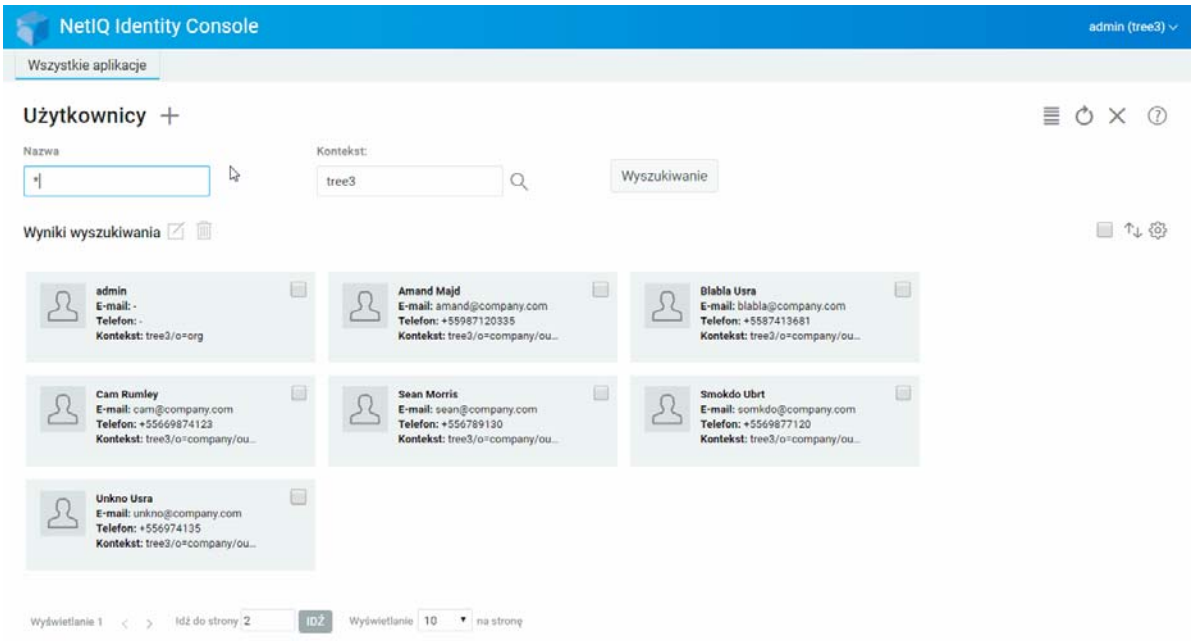


Ustawianie daty wygaśnięcia ważności konta

Aby ustawić datę wygaśnięcia ważności konta dla użytkowników, wykonaj następujące czynności:

1. Wybierz użytkownika, dla którego ma zostać ustawiona data ważności konta, i kliknij ikonę .
2. Kliknij kartę **Ograniczenia** na stronie **Modyfikuj użytkownika**.
3. Rozwiń kartę **Ograniczenia logowania** i zaznacz pole wyboru **Konto ma ograniczoną ważność**, a następnie podaj datę w polu **Data wygaśnięcia**.
4. Kliknij ikonę Zapisz.

Rysunek 5-7 *Ustawianie daty wygaśnięcia ważności konta*

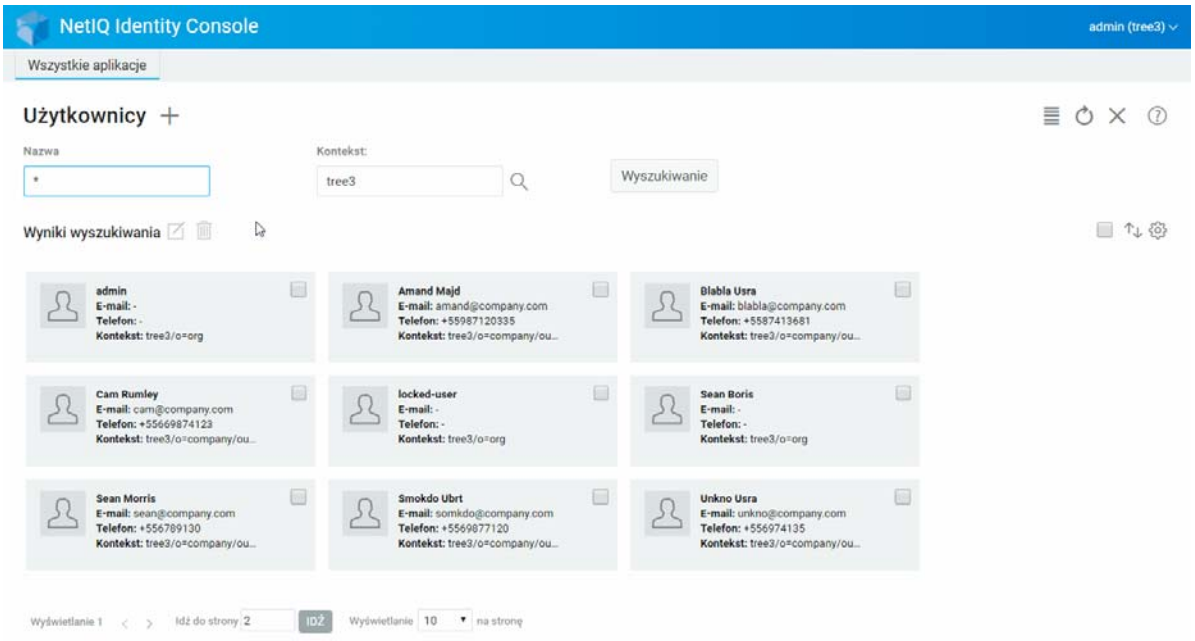


Sprawdzanie i czyszczenie blokady po wykryciu intruza

Portal internetowy Identity Console umożliwia przeglądanie szczegółów blokady po wykryciu intruza dla dowolnego konta użytkownika. Aby wyświetlić szczegóły blokady po wykryciu intruza:

1. Wybierz użytkownika, dla którego mają zostać sprawdzone szczegóły blokady po wykryciu intruza, i kliknij ikonę .
2. Kliknij kartę **Ograniczenia** na stronie **Modyfikuj użytkownika**.
3. Rozwiń kartę **Blokada po wykryciu intruza** i przejrzyj szczegóły blokady.
4. Teraz wybierz kartę **Wyczyść blokadę** i kliknij przycisk Wyczyść blokadę.
5. Kliknij przycisk Zapisz.

Rysunek 5-8 *Sprawdzanie i czyszczenie blokady po wykryciu intruza*



6 Zarządzanie grupami

Grupy zawierają zwykle pewną liczbę członków. Użytkownik, który utworzył grupę, automatycznie staje się jej właścicielem. Za pomocą funkcji Zarządzanie grupami można wykonywać następujące operacje:

- „Tworzenie grupy” na stronie 37
- „Usuwanie grup” na stronie 38
- „Modyfikowanie grup” na stronie 39
- „Dodawanie lub modyfikowanie członków grupy” na stronie 40
- „Wyszukiwanie grup” na stronie 41

Więcej informacji o używaniu i konfigurowaniu obiektów grup zawiera dokument *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Podręcznik administracji NetIQ eDirectory 9.2).

Tworzenie grupy

Aby utworzyć grupę:

1. Kliknij opcję **Zarządzanie grupami** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz grupę wprowadź następujące szczegóły:
   - Podaj nazwę grupy
   - Podaj kontekst

   Zaznacz pole wyboru **Grupa dynamiczna**, aby nowa grupa była grupą dynamiczną o klasie `dynamicGroup`. W przeciwnym razie grupa zostanie utworzona jako grupa statyczna.

   Wybierz opcję **Grupa zagnieżdżona**, aby nowa grupa stała się grupą zagnieżdżoną — została utworzona z klasą pomocniczą `nestedGroupAux`.

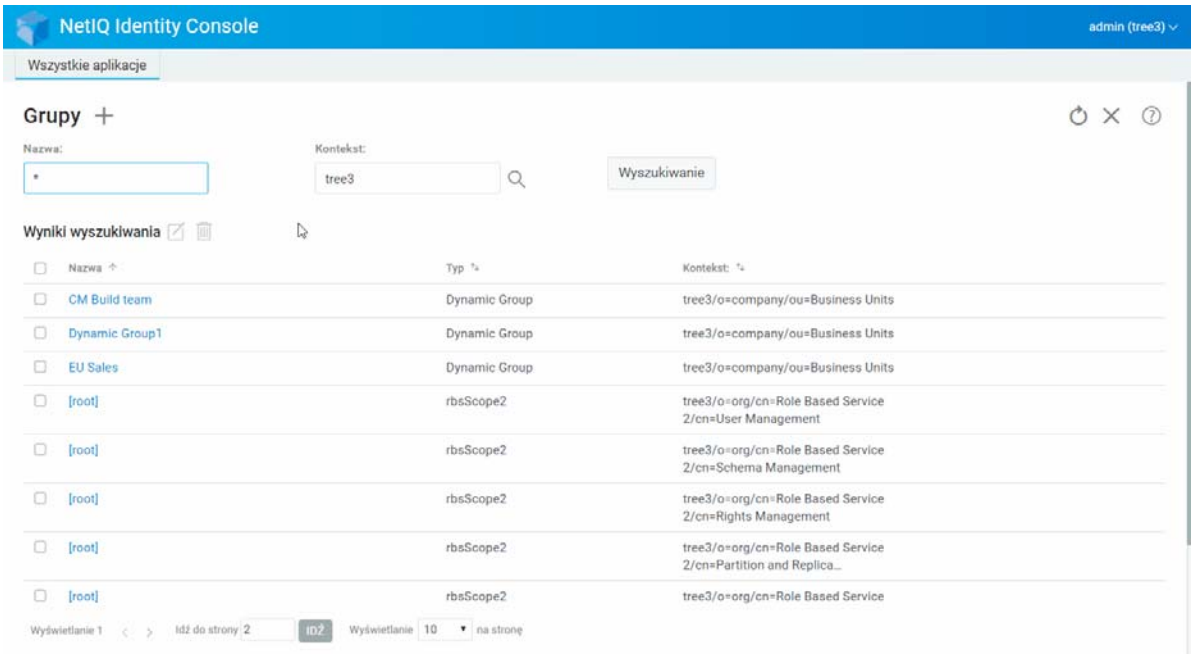
   UWAGA: Grupę statyczną można przekonwertować na grupę dynamiczną lub zagnieżdżoną, używając procedury opisanej w części Modyfikowanie obiektów. Rozszerza to przynależność wybranego obiektu grupy odpowiednio do klasy `dynamicGroupAux` lub `nestedGroupAux`.

   Grupa może być albo zagnieżdżona, albo dynamiczna. Nie można utworzyć grupy, która jest jednocześnie zagnieżdżona i dynamiczna.

   ---

4. Po podaniu wszystkich niezbędnych szczegółów kliknij przycisk Utwórz.
5. Zostanie wyświetlone potwierdzenie informujące o utworzeniu grupy.

Rysunek 6-1 *Tworzenie grupy*

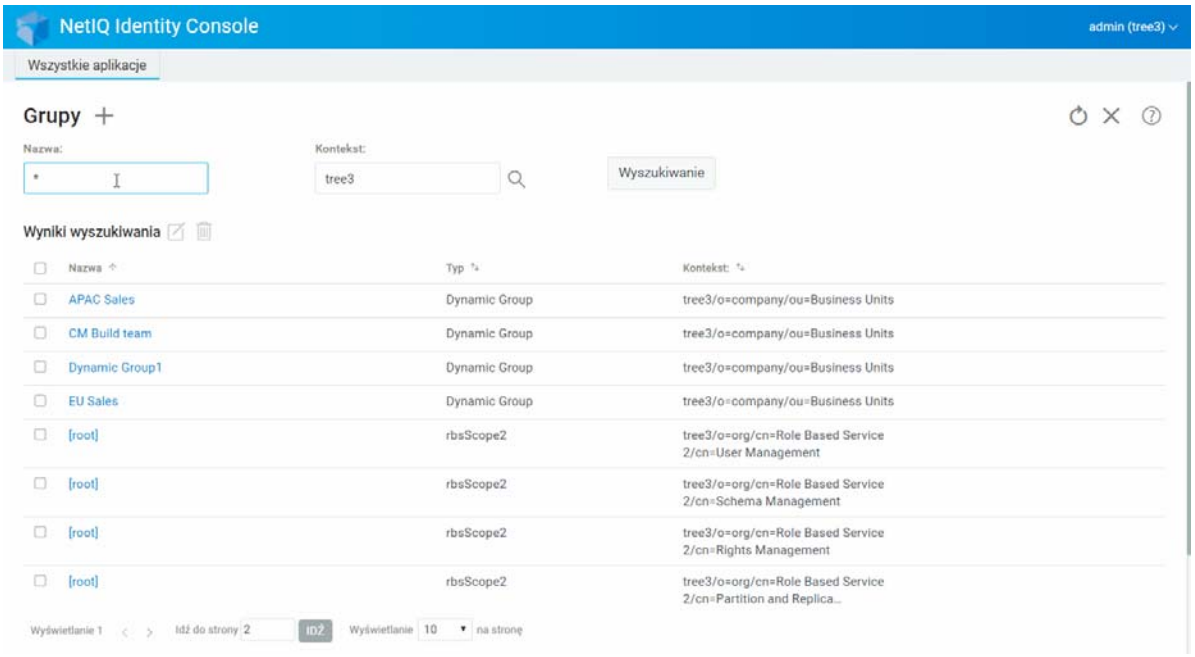


Usuwanie grup

Aby usunąć grupy:

1. Kliknij opcję **Zarządzanie grupami** na stronie docelowej Identity Console.
2. Podaj nazwę i kontekst grupy lub znajdź atrybut przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Zaznacz grupę, która ma zostać usunięta, i kliknij ikonę .
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu grupy.

Rysunek 6-2 *Usuwanie grup*

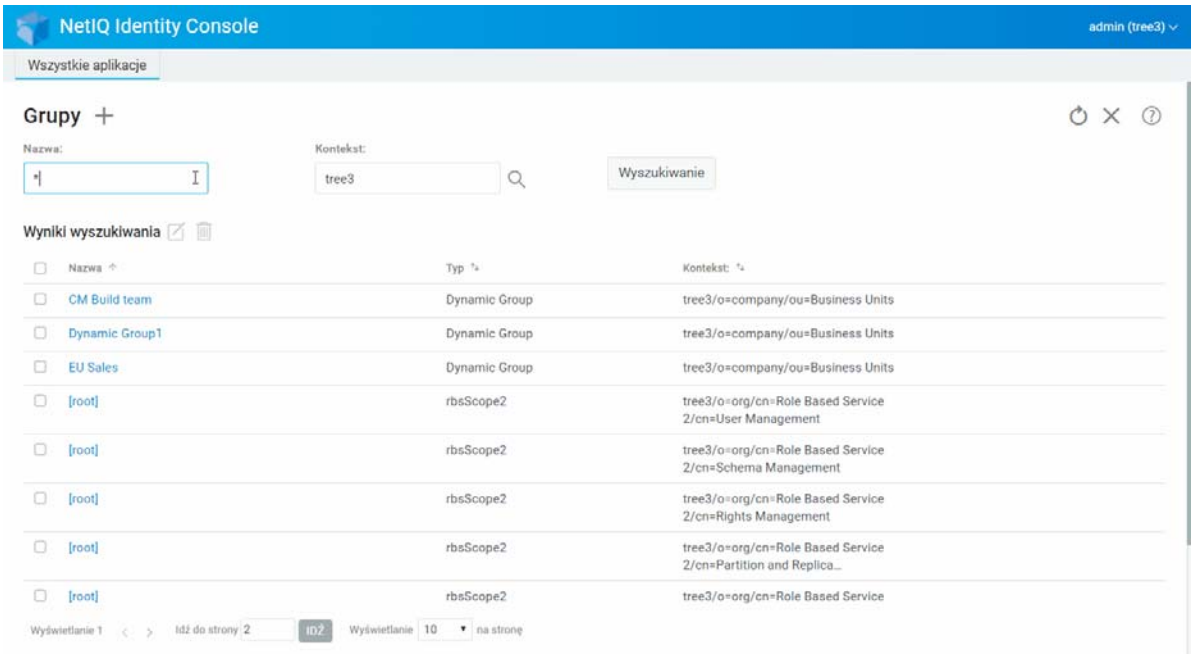


Modyfikowanie grup

Aby zmodyfikować grupy:

1. Kliknij opcję **Zarządzanie grupami** na stronie docelowej Identity Console.
2. Wpisz nazwę i kontekst grupy, a następnie kliknij przycisk Wyszukiwanie.
3. Zaznacz grupę, która ma zostać zmodyfikowana, i kliknij ikonę .
4. Wprowadź zmiany, a następnie kliknij przycisk Zapisz.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu grupy.

Rysunek 6-3 *Modyfikowanie grup*

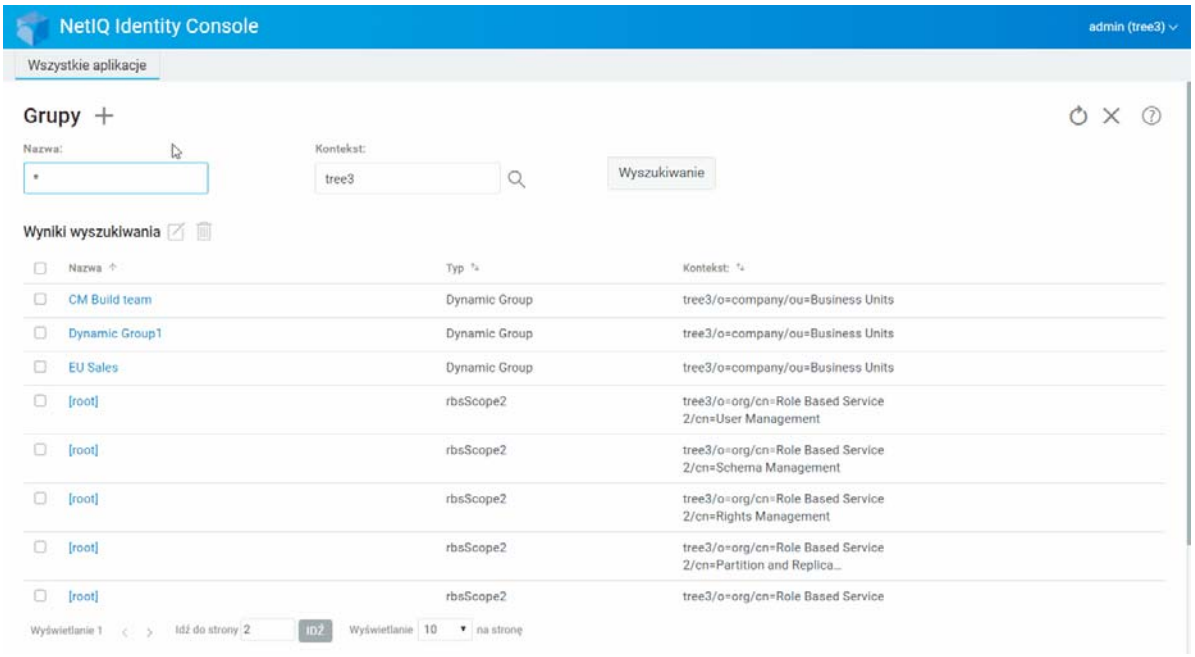


Dodawanie lub modyfikowanie członków grupy

Aby dodać lub zmodyfikować członków grupy:

1. Kliknij opcję **Zarządzanie grupami** na stronie docelowej Identity Console.
2. Wpisz nazwę i kontekst grupy, a następnie kliknij przycisk Wyszukiwanie.
3. Zaznacz grupę i kliknij ikonę .
4. Kliknij kartę **Członkowie** na stronie **Modyfikuj grupę**.
5. Użyj ikony , aby dodać nowego członka do grupy. Jeśli chcesz usunąć członków z grupy, kliknij ikonę .
6. Po wprowadzeniu zmian kliknij przycisk Zapisz.
7. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu grupy.

Rysunek 6-4 *Dodawanie lub modyfikowanie członków grupy*

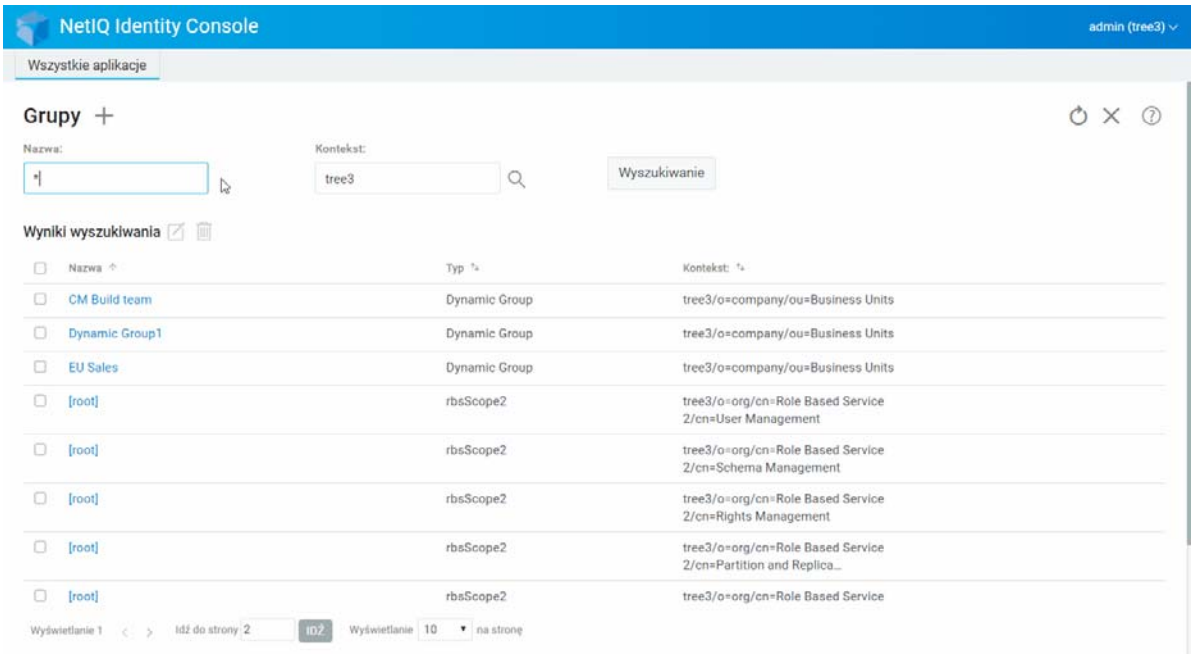


Wyszukiwanie grup

Aby wyszukać grupy:

1. Kliknij opcję **Zarządzanie grupami** na stronie docelowej Identity Console.
2. Grupę możesz wyszukiwać na podstawie samej nazwy lub nazwy i kontekstu.
3. Po podaniu wszystkich niezbędnych szczegółów kliknij ikonę Wyszukiwanie.

Rysunek 6-5 *Wyszukiwanie grup*



7 Zarządzanie obiektami

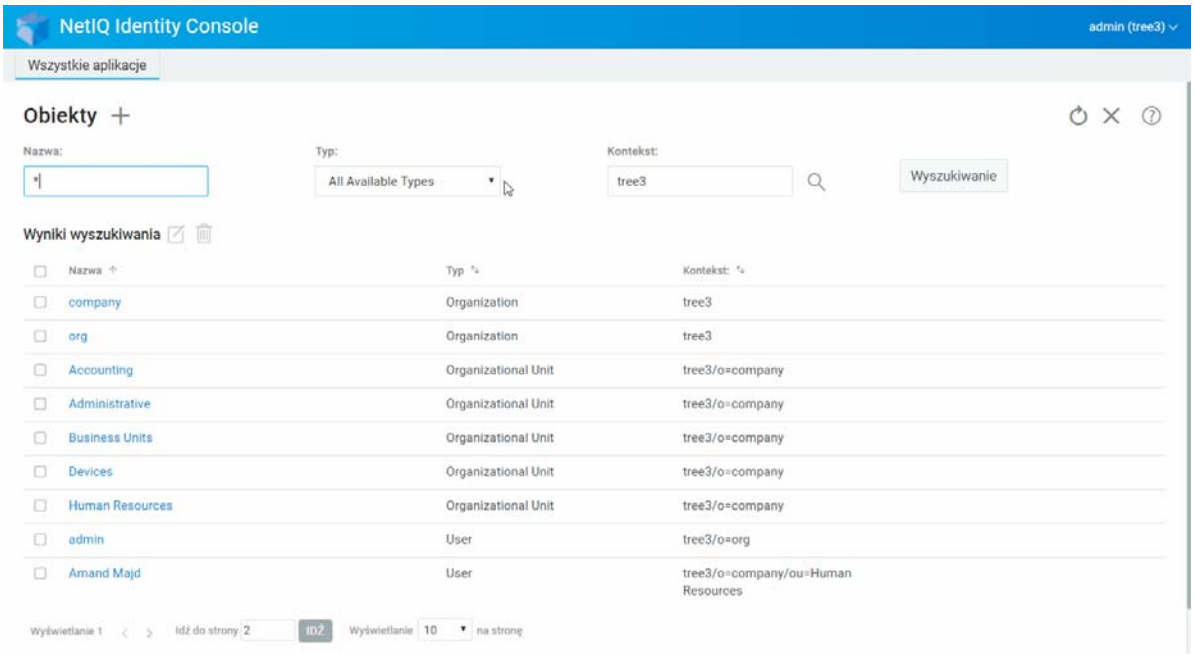
Identity Console umożliwia zarządzanie różnymi obiektami w magazynie danych. Za pomocą tego modułu można tworzyć, modyfikować, usuwać i wyszukiwać obiekty.

Tworzenie obiektu

Aby utworzyć nowy obiekt:

1. Kliknij opcję **Zarządzanie obiektami** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz obiekt wprowadź następujące szczegóły:
   - Podaj nazwę obiektu
   - Podaj typ
   - Podaj kontekst
4. Po podaniu wszystkich wymaganych szczegółów kliknij kolejno opcje **Dalej** > **Utwórz**.
5. Zostanie wyświetlone potwierdzenie informujące o utworzeniu obiektu.

Rysunek 7-1 *Tworzenie obiektu*

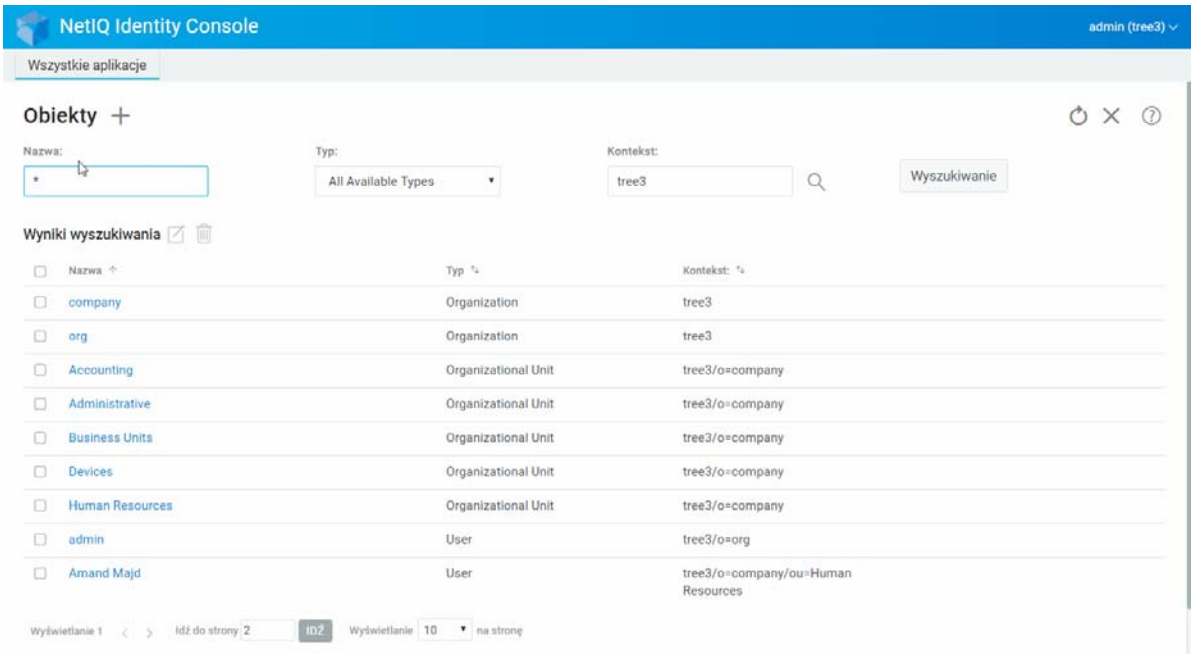


Usuwanie obiektów

Aby usunąć obiekty:

1. Kliknij opcję **Zarządzanie obiektami** na stronie docelowej Identity Console.
2. Podaj nazwę, typ i kontekst obiektu lub znajdź obiekt przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekt z listy wyszukiwania i kliknij ikonę 🗑.
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu obiektu.

Rysunek 7-2 *Usuwanie obiektów*

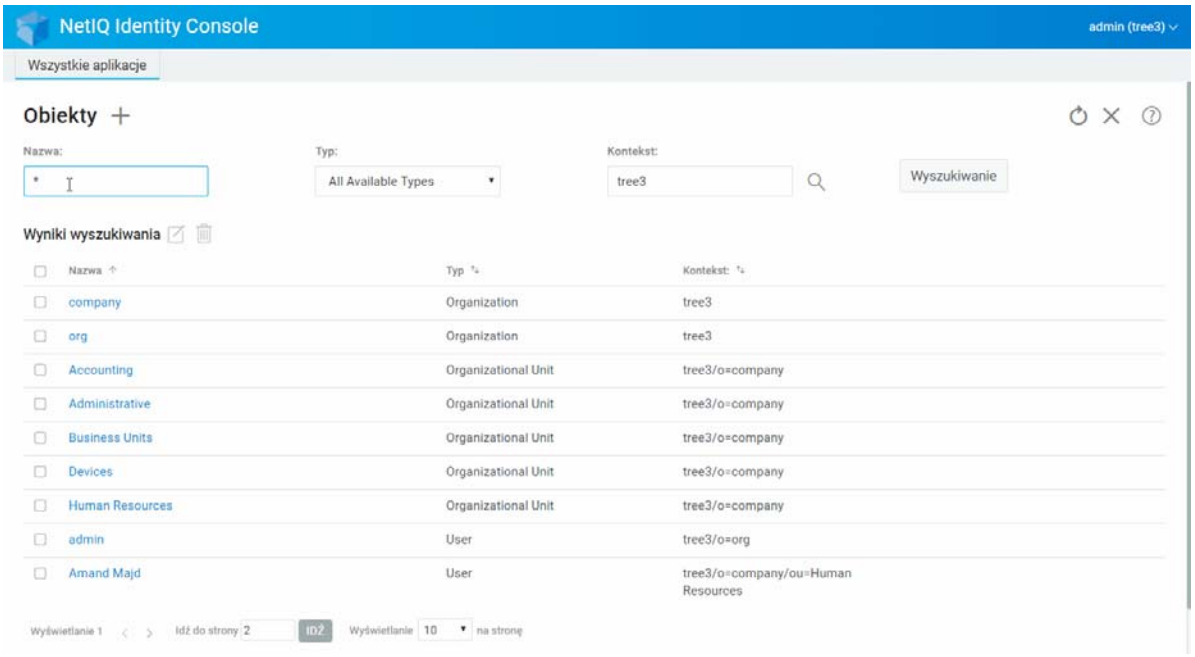


Modyfikowanie obiektów

Aby zmodyfikować obiekty:

1. Kliknij opcję **Zarządzanie obiektami** na stronie docelowej Identity Console.
2. Wpisz nazwę, typ i kontekst obiektu, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekt z listy wyszukiwania i kliknij ikonę .
4. Wprowadź zmiany, a następnie kliknij przycisk Zapisz.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu obiektu.

Rysunek 7-3 *Modyfikowanie obiektów*

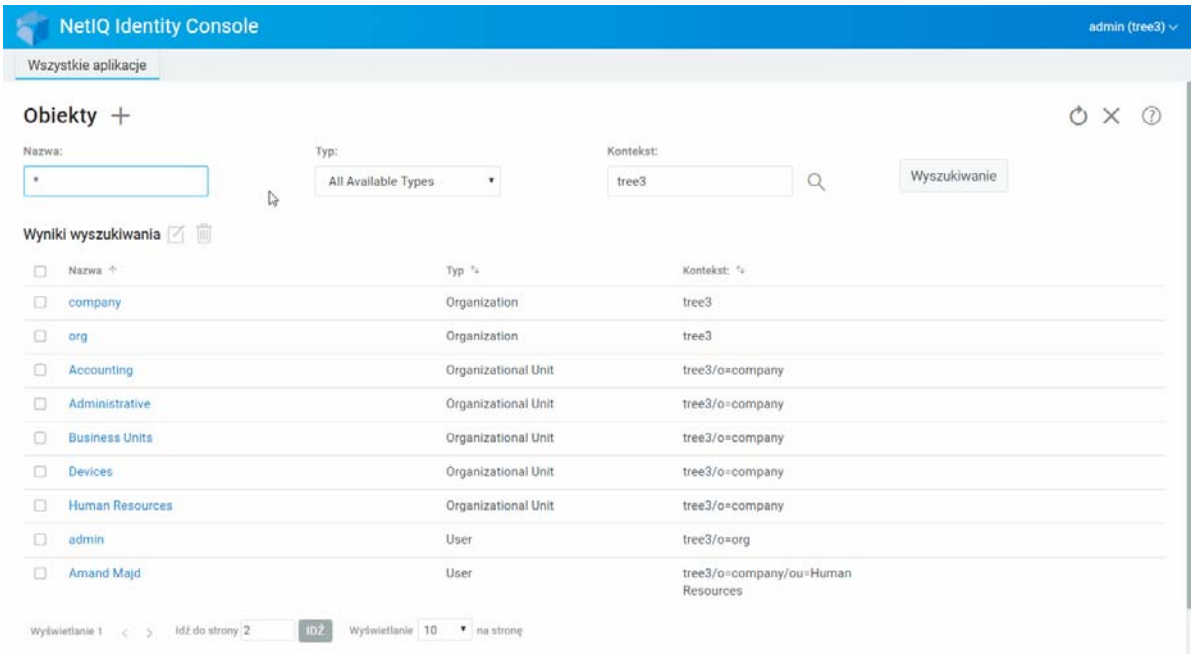


Wyszukiwanie obiektu

Aby wyszukać obiekt:

1. Kliknij opcję **Zarządzanie obiektami** na stronie docelowej Identity Console.
2. Obiekt możesz wyszukiwać na podstawie samej nazwy lub nazwy, typu i kontekstu.
3. Po podaniu wszystkich niezbędnych szczegółów kliknij przycisk Wyszukiwanie.

Rysunek 7-4 *Wyszukiwanie obiektu*



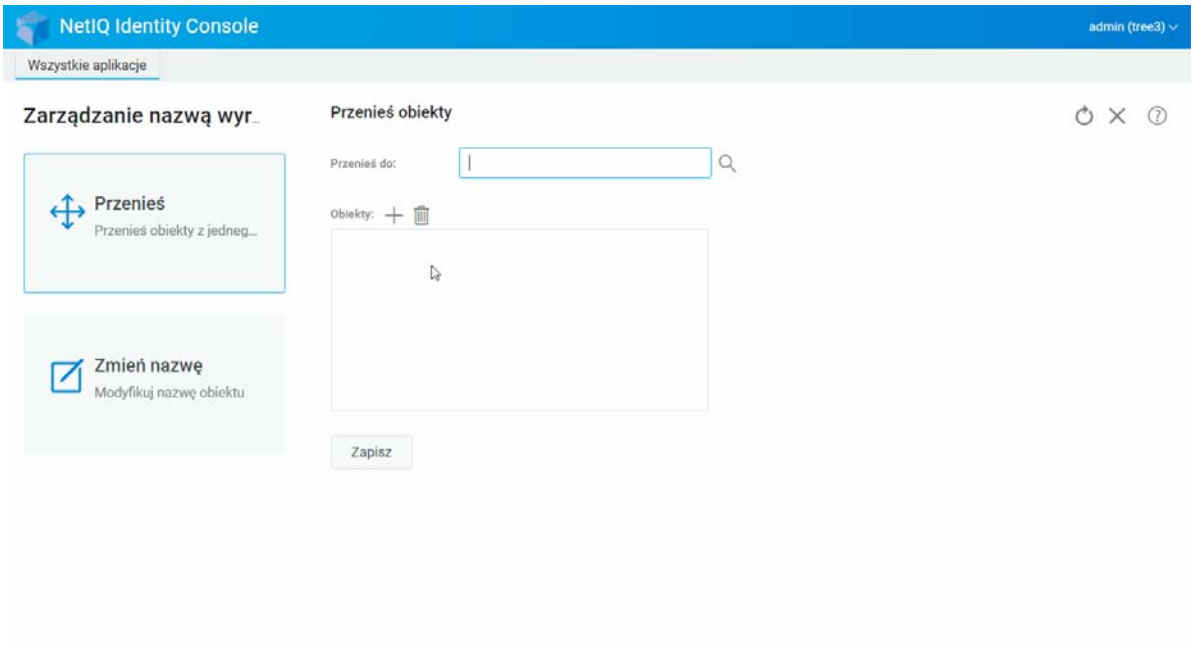
Przenoszenie obiektu

Aby przenieść obiekt:

1. Kliknij opcję **Zarządzanie nazwą wyróżniającą** na stronie docelowej Identity Console.
2. Opcja **Przenieś obiekt** będzie domyślnie zaznaczona.
3. W polu **Przenieś do** wybierz kontener, do którego ma zostać przeniesiony obiekt.
4. Kliknij ikonę +, aby dodać obiekt, który chcesz przenieść do innego kontenera.

   Jeśli chcesz usunąć wybrany obiekt, kliknij ikonę 🗑.
5. Kliknij przycisk Zapisz.
6. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym wykonaniu operacji przeniesienia obiektu.

Rysunek 7-5 *Przenoszenie obiektu*

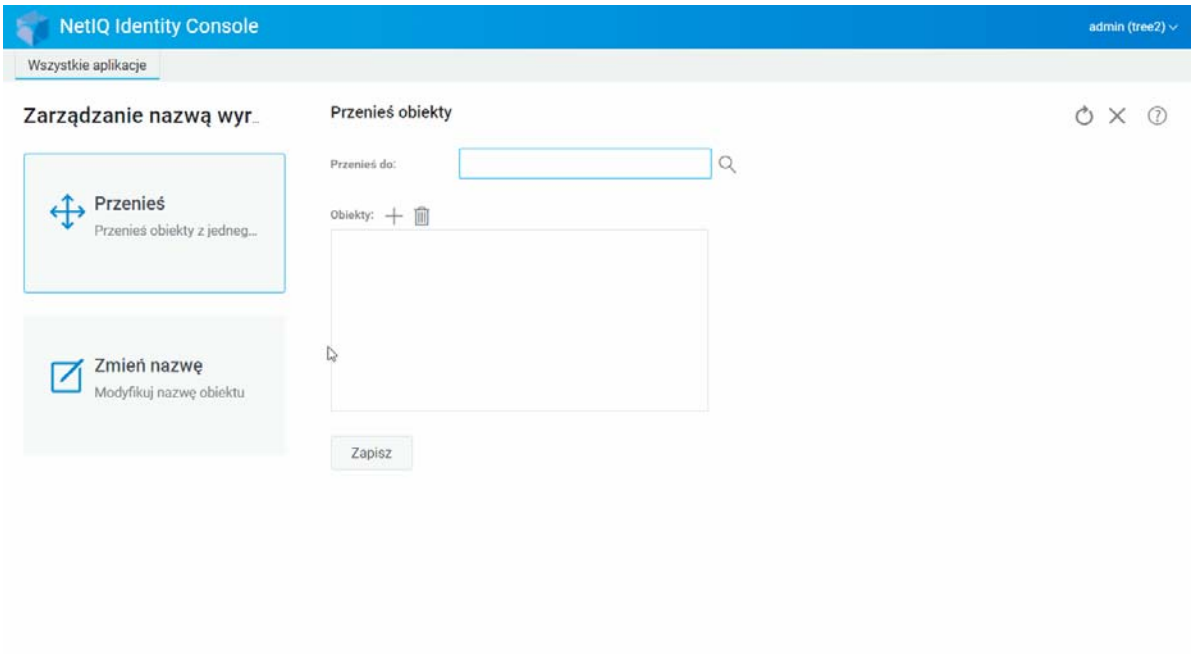


Zmienianie nazwy obiektu

Aby zmienić nazwę obiektu:

1. Kliknij opcję **Zarządzanie nazwą wyróżniającą** na stronie docelowej Identity Console.
2. Wybierz opcję **Zmiana nazwy obiektu**.
3. W polu **Nazwa obiektu** znajdź za pomocą funkcji wyszukiwania obiekt, którego nazwa ma zostać zmieniona.
4. W polu **Nowa nazwa** podaj tylko nową nazwę obiektu. Nie podawaj kontekstu.
5. Aby zapisać starą nazwę, wybierz opcję zapisania tej nazwy.
6. Kliknij przycisk Zapisz.
7. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym wykonaniu operacji zmiany nazwy obiektu.

Rysunek 7-6 *Zmienianie nazwy obiektu*



8 Zarządzanie prawami

Prawa są związane z prawami dysponentów eDirectory i dysponentami. Domyślne prawa przypisywane podczas tworzenia drzewa umożliwiają ogólny dostęp do sieci z zachowaniem zabezpieczeń. Identity Console umożliwia wykonywanie następujących zadań związanych z prawami:

- „Modyfikowanie filtru praw dziedziczonych” na stronie 51
- „Modyfikowanie praw dysponentów” na stronie 52
- „Wyświetlanie praw efektywnych” na stronie 53

Więcej informacji o prawach usługi eDirectory zawiera dokument *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Podręcznik administracji NetIQ eDirectory 9.2).

Modyfikowanie filtru praw dziedziczonych

Usługa eDirectory zawiera mechanizm o nazwie Filtr praw dziedziczonych (IRF), który umożliwia blokowanie dziedziczenia praw dla poszczególnych elementów podrzędnych.

Więcej informacji na temat filtrów praw dziedziczonych zawiera dokument *NetIQ eDirectory 9.2 Administration Guide* (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/bookinfo.html) (Podręcznik administracji NetIQ eDirectory 9.2).

1. Kliknij opcję **Zarządzanie prawami** na stronie docelowej Identity Console.
2. Wybierz opcję **Filtr praw dziedziczonych**.

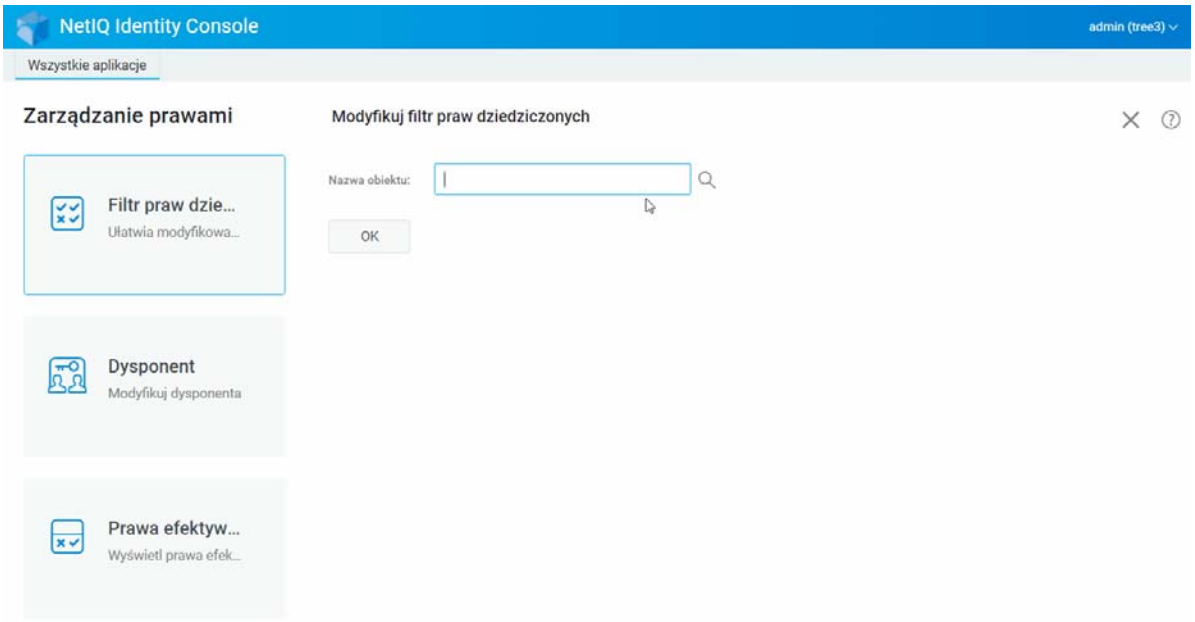
   UWAGA: Opcja Filtr praw dziedziczonych jest wybrana domyślnie.

3. Podaj pełną nazwę obiektu, którego filtr praw dziedziczonych ma zostać zmodyfikowany, lub znajdź obiekt przy użyciu ikony Selektor obiektów, a następnie kliknij przycisk **OK**.

   Zostanie wyświetlona lista filtrów praw dziedziczonych, które zostały dotychczas ustawione dla tego obiektu.
4. W obszarze **Właściwości** zmień zgodnie z potrzebami listę filtrów praw dziedziczonych, a następnie kliknij przycisk **Zastosuj**.

   Do edytowania listy filtrów niezbędne jest posiadanie praw nadzorcy lub kontroli dostępu do właściwości ACL obiektu. Można ustawić filtry blokujące uprawnienia dziedziczone do obiektu jako całości albo do wszystkich lub wybranych właściwości obiektu.

Rysunek 8-1 *Modyfikowanie filtru praw dziedziczonych*



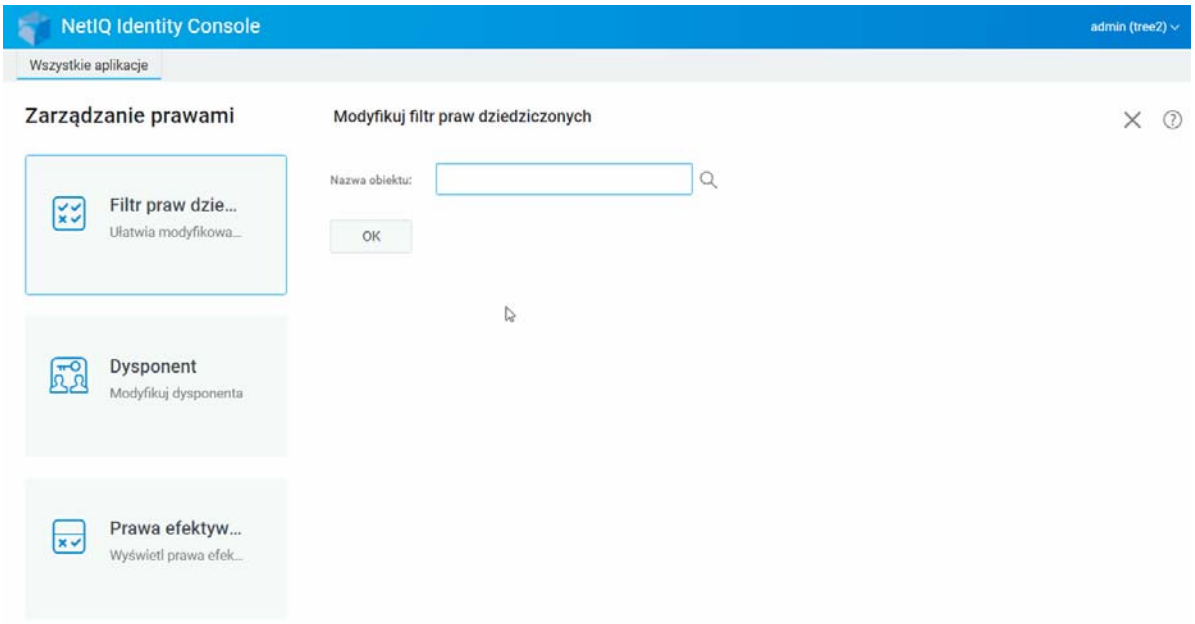
Modyfikowanie praw dysponentów

Dysponent to obiekt, któremu przyznano bezpośrednie prawa do innego obiektu w drzewie katalogu. Aby zmodyfikować listę dysponentów danego obiektu:

1. Kliknij opcję **Zarządzanie prawami** na stronie docelowej Identity Console.
2. Wybierz opcję **Dysponent**.
3. Podaj nazwę obiektu, którego lista dysponentów ma zostać wyświetlona, lub znajdź obiekt przy użyciu ikony Selektor obiektów, a następnie kliknij przycisk **OK**.

   Spowoduje to otwarcie listy dysponentów przypisanych aktualnie do obiektu.
4. Zmodyfikuj listę dysponentów zgodnie z potrzebami, a następnie kliknij przycisk **OK**.
   - Aby dodać dysponenta, kliknij ikonę +.
   - Aby usunąć dysponenta, zaznacz odpowiadające mu pole wyboru i kliknij ikonę .
   - Aby zmodyfikować przypisanie praw dysponenta, wybierz łącze **Przydzielone prawa** dla tego dysponenta.

Rysunek 8-2 *Modyfikowanie praw dysponentów*



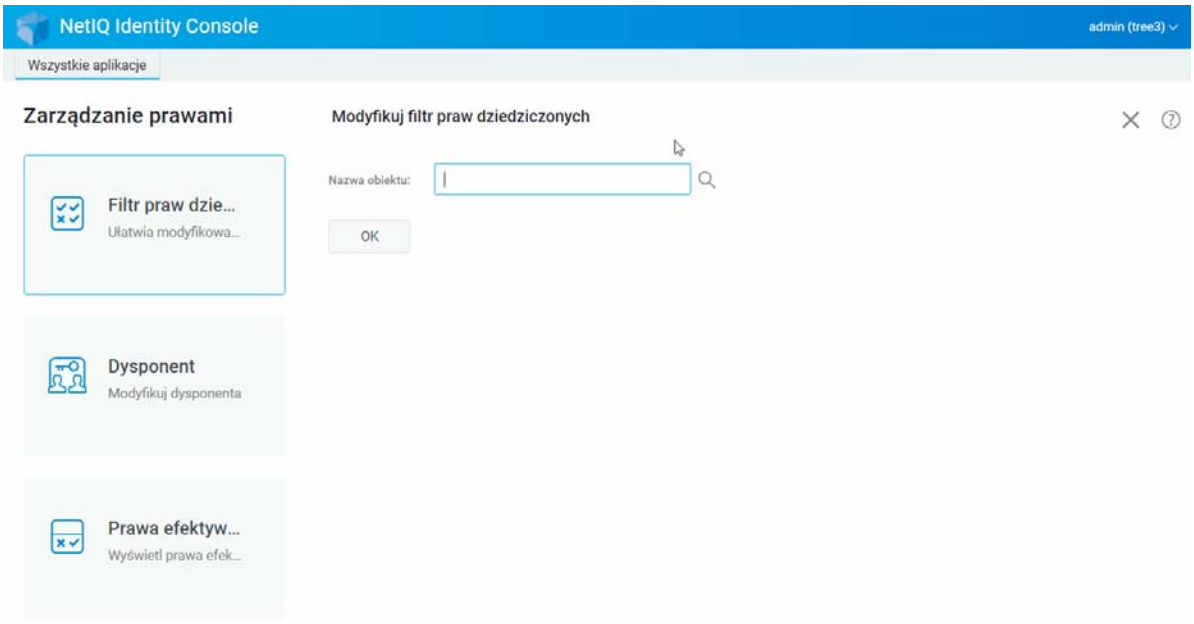
Wyświetlanie praw efektywnych

Prawa efektywne to kombinacja praw bezpośrednich i praw dziedziczonych, jakie ma obiekt w dowolnym punkcie drzewa katalogu. Aby wyświetlić efektywne prawa obiektu do innego obiektu:

1. Kliknij opcję **Zarządzanie prawami** na stronie docelowej Identity Console.
2. Wybierz opcję **Prawa efektywne**.
3. Podaj nazwę dysponenta, którego prawa mają zostać wyświetlone, lub znajdź dysponenta przy użyciu ikony Selektor obiektów, a następnie kliknij przycisk **OK**.
4. W polu Nazwa obiektu podaj nazwę obiektu, dla którego mają zostać wyświetlone prawa efektywne dysponenta.

   Usługa eDirectory obliczy prawa efektywne i wyświetli je w polu **Prawa efektywne**.

Rysunek 8-3 *Wyświetlanie praw efektywnych*



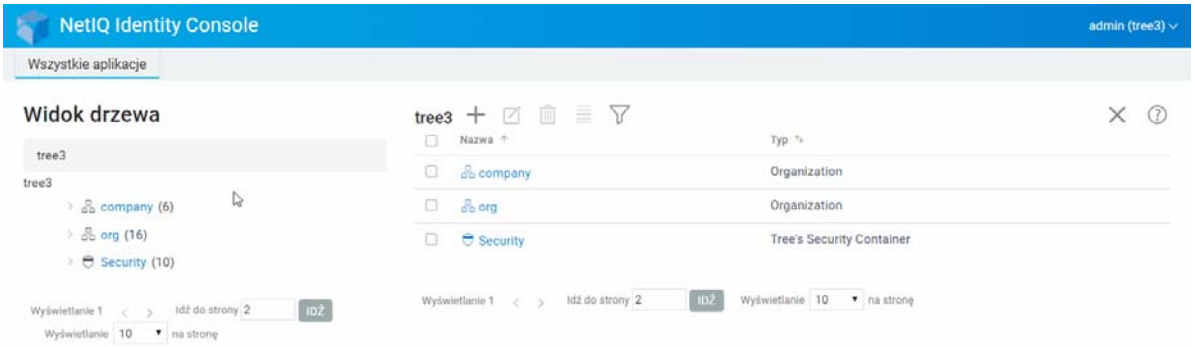
9 Widok drzewa

Widok drzewa umożliwia przeglądanie drzewa katalogów oraz tworzenie, usuwanie lub modyfikowanie różnych obiektów w tym drzewie. Widok drzewa ma ramkę nawigacyjną i ramkę zawartości.

Ramka nawigacyjna widoku drzewa

W ramce nawigacyjnej widoku drzewa jest wyświetlana struktura katalogów. W ramce nawigacyjnej są wyświetlane obiekty kontenerów, w tym obiekty wolumenów (systemu plików). Wszystkie opcje wyświetlane w ramce nawigacyjnej można klikać, co pomaga przeglądać strukturę katalogów. Domyślnie w ramce nawigacyjnej jest wyświetlane do 10 obiektów podrzędnych dla każdego kontenera, ale ustawienie to można zmienić w panelu ramki nawigacyjnej w widoku drzewa.

Rysunek 9-1 *Ramka nawigacyjna w widoku drzewa*



Ramka zawartości widoku drzewa

Wybranie jednego z obiektów kontenerów w ramce nawigacyjnej powoduje wyświetlenie wszystkich obiektów zawartych w tym kontenerze w ramce zawartości. Ramka zawartości to miejsce wyświetlania i modyfikowania obiektów katalogu. Zawiera ona nagłówek, z którego można wybierać dostępne czynności:

Pasek tytułu: Na pasku tytułu ramki zawartości jest wyświetlana nazwa obecnie wybranego obiektu kontenera.

Nagłówek listy obiektów: Nagłówek listy obiektów zapewnia dostęp do następujących elementów:

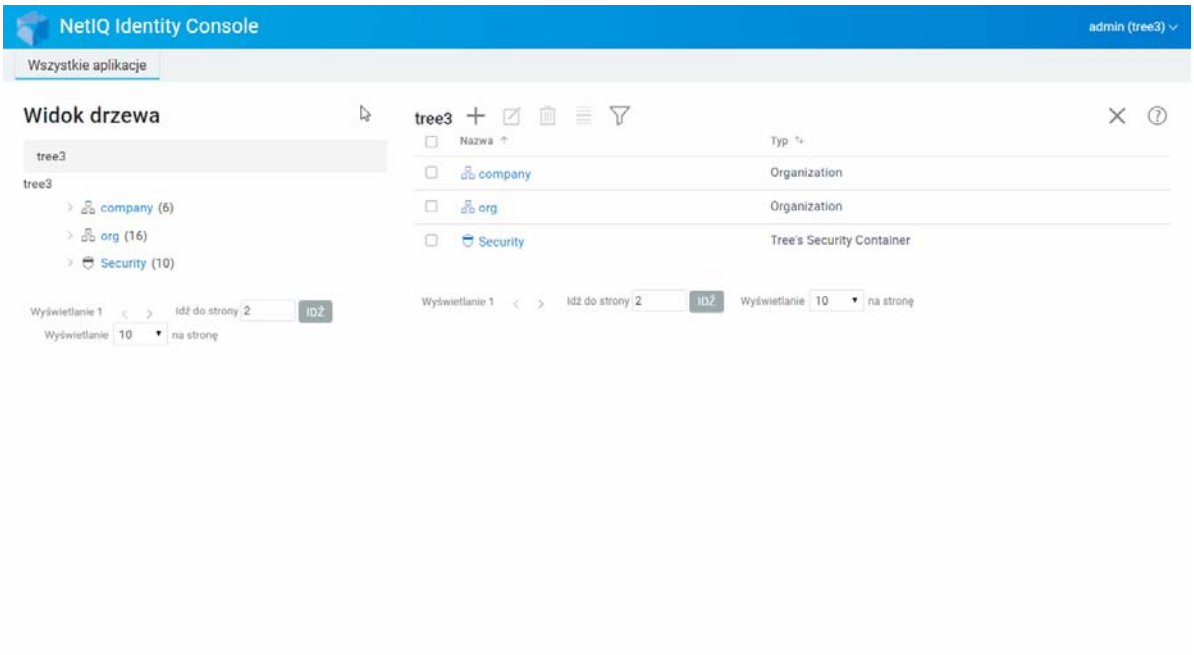
- **Dodaj:** Kliknij ikonę  , aby dodać nowy obiekt.
- **Modyfikuj:** Wybierz obiekt i kliknij ikonę  w celu zmodyfikowania go. Zostanie otwarta książka właściwości dla zaznaczonych obiektów, umożliwiając zmodyfikowanie ich atrybutów. Nie można modyfikować kilku obiektów razem.
- **Usuń:** Wybierz obiekt i kliknij ikonę  w celu usunięcia wybranych obiektów. Nie można usuwać kilka obiektów razem. Nie można usuwać obiektów niebędących liściem.
- **Czynności:** Wybierz obiekt i kliknij ikonę  , aby utworzyć menu rozwijane obsługiwanych zadań dla wybranych obiektów. Aby wykonać zadanie, należy je wybrać z menu rozwijanego, a następnie podać wymagane informacje.
- **Liczba obiektów**: Widok drzewa wyświetla u dołu strony liczbę obiektów na bieżącej stronie. Domyślnie w ramce zawartości jest wyświetlane do 20 obiektów podrzędnych dla każdego kontenera, ale ustawienie to można zmienić.
- **Zaznacz wszystko**: pole wyboru w nagłówku pełni funkcję pola wyboru „zaznacz wszystko” dla bieżącej strony obiektów.
- **Sortuj**: Sortować można kolumny **Nazwa** i **Typ**. Klikanie dowolnego z tych elementów powoduje przełączanie sortowania obiektów między rosnącą a malejącą kolejnością alfabetyczną.
- **Filtr wyszukiwania:** kliknij ikonę  , aby uruchomić okno podręczne filtru. Przy użyciu tej opcji można utworzyć filtr ograniczający obiekty wyświetlane na liście obiektów. Obiekty można filtrować według typów i nazw, zgodnie z potrzebami.

  Wybranie opcji  powoduje otwarcie okna dialogowego Filtr zaawansowany, w którym można utworzyć filtr, używając niemal dowolnego atrybutu obiektu. Aby uzyskać więcej informacji, zobacz „Konfigurowanie wyszukiwania zaawansowanego” na stronie 26.

Aby wykonać czynność na obiekcie, zaznacz odpowiadające mu pole wyboru, a następnie wybierz odpowiednią ikonę czynności  z nagłówka listy obiektów. Aby wykonać czynność na przeglądanym obecnie kontenerze, wybierz obiekt Poziom bieżący. Przy użyciu tej opcji można wykonywać następujące czynności:

- „Modyfikowanie filtru praw dziedziczonych” na stronie 51
- „Modyfikowanie praw dysponentów” na stronie 52
- „Rozszerzanie obiektu” na stronie 64
- „Zmienianie nazwy obiektu” na stronie 48
- Ustaw hasło
- „Wyświetlanie praw efektywnych” na stronie 53

Rysunek 9-2 *Ramka zawartości w widoku drzewa*



10 Zarządzanie schematem

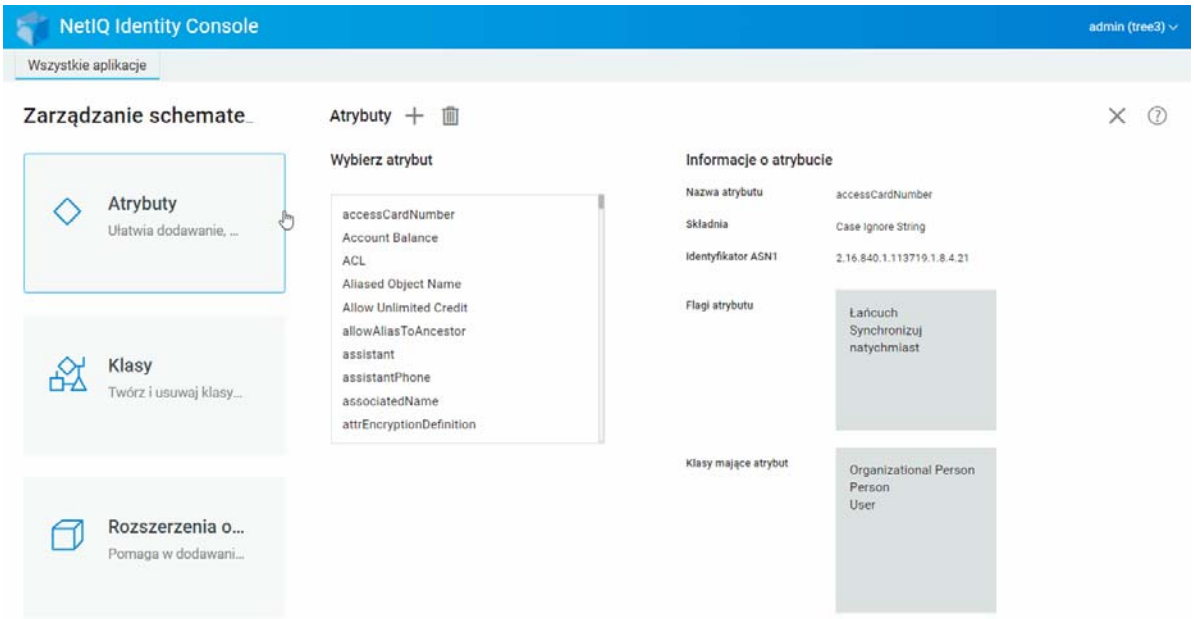
Schemat katalogu definiuje typy obiektów, które można tworzyć w danym drzewie (takie jak Użytkownicy, Drukarki, Grupy itp.) i określa, które informacje są wymagane, a które opcjonalne w chwili tworzenia obiektu. Identity Console umożliwia wykonywanie następujących zadań związanych ze schematem:

Tworzenie atrybutu

Istnieje możliwość definiowania niestandardowych typów atrybutów i dodawania ich jako atrybutów opcjonalnych do istniejących klas obiektów. Nie można jednak dodawać atrybutów obowiązkowych do istniejących klas. Aby utworzyć atrybut:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz atrybut wprowadź następujące szczegóły:
   - Nazwa atrybutu
   - Identyfikator ASN1 (opcjonalnie)
   - Składnia
   - Flagi atrybutu
4. Po podaniu wszystkich wymaganych szczegółów kliknij przycisk Utwórz.
5. Zostanie wyświetlone potwierdzenie informujące o utworzeniu atrybutu.

Rysunek 10-1 *Tworzenie atrybutu*



Tworzenie klasy

Przy użyciu opcji **Zarządzanie schematem** można definiować własne klasy. Następnie można rozszerzać poszczególne obiekty, dodając właściwości zdefiniowane w klasach. Aby utworzyć klasę:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Klasy**.
2. Kliknij ikonę +.
3. Na stronie Utwórz atrybut wprowadź następujące szczegóły:
   - Nazwa klasy
   - Identyfikator ASN1 (opcjonalnie)
   - Flagi klasy: wybierz jedną z następujących flag klasy:
     - **Klasa efektywna:** Tę flagę można ustawić w przypadku tworzenia klasy efektywnej, która może służyć do tworzenia obiektów.
     - **Klasa nieefektywna:** Służy jako wypełniacz dla grupy atrybutów. Klasa nieefektywna nie może być wykorzystywana do tworzenia obiektów, ale można ją określić jako klasę, po której inne klasy będą mogły dziedziczyć atrybuty. Na przykład klasa Osoba jest klasą nieefektywną, która przechowuje atrybuty dziedziczone przez klasę Użytkownik.
     - **Klasa pomocnicza:** Zbiór atrybutów, które mogą dotyczyć tylko poszczególnych obiektów, a nie całych klas.
     - **Klasa kontenera:** Tę flagę należy ustawić w przypadku, gdy dana klasa ma być klasą kontenera. Jeśli zostanie ona użyta do tworzenia obiektów, obiekty te staną się obiektami kontenerów (takimi jak OU). Nie należy ustawiać tej flagi dla klasy obiektów liści.

UWAGA: Jeśli wybierzesz opcję Klasa efektywna lub Klasa nieefektywna, musisz też podać wartości dla klasy nadrzędnej. Jeśli wybierzesz opcję Klasa pomocnicza, klasa nadrzędna będzie opcjonalna.

4 Po podaniu wszystkich wymaganych szczegółów kliknij przycisk **Dalej**.

5 Na następnym ekranie wybierz atrybuty opcjonalne, obowiązkowe i nazewnictwa, a następnie kliknij przycisk **OK**.

6 Zostanie wyświetlone potwierdzenie informujące o utworzeniu klasy.

Przypisywanie atrybutów do klasy

Istnieje możliwość dodawania atrybutów opcjonalnych do istniejących klas, jeśli zmieni się struktura informacji używanych przez organizację, a także w czasie przygotowania do łączenia drzew. Aby dodać atrybut do istniejącej klasy:

UWAGA: Atrybuty obowiązkowe można definiować tylko w trakcie procesu tworzenia klasy. Atrybut obowiązkowy to taki, którego wartość musi zostać określona podczas tworzenia obiektu.

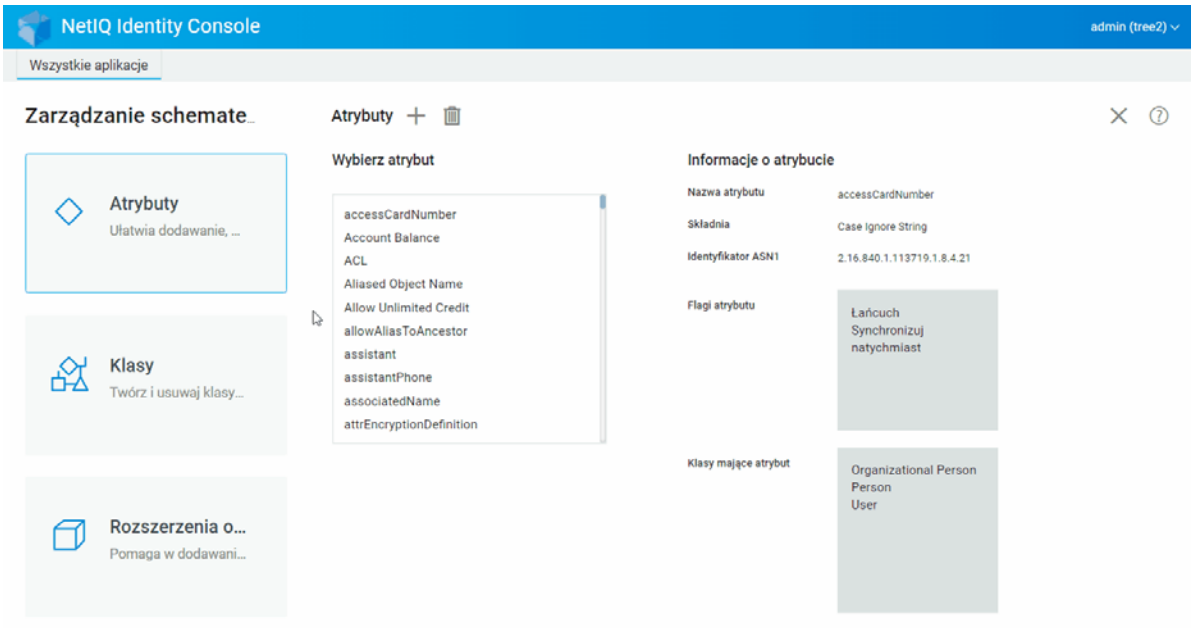
1 Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Klasy**.

2 Kliknij dowolną klasę na liście **Wybierz klasę**.

3 Z prawej strony ekranu zostaną wyświetlone odpowiednie informacje o klasie.

4 Kliknij przycisk + obok opcji**Atrybuty**, wybierz atrybuty do dodania, a następnie wybierz kolejno opcje **Dodaj** > **Zapisz**.

Rysunek 10-2 *Przypisywanie atrybutów do klasy*

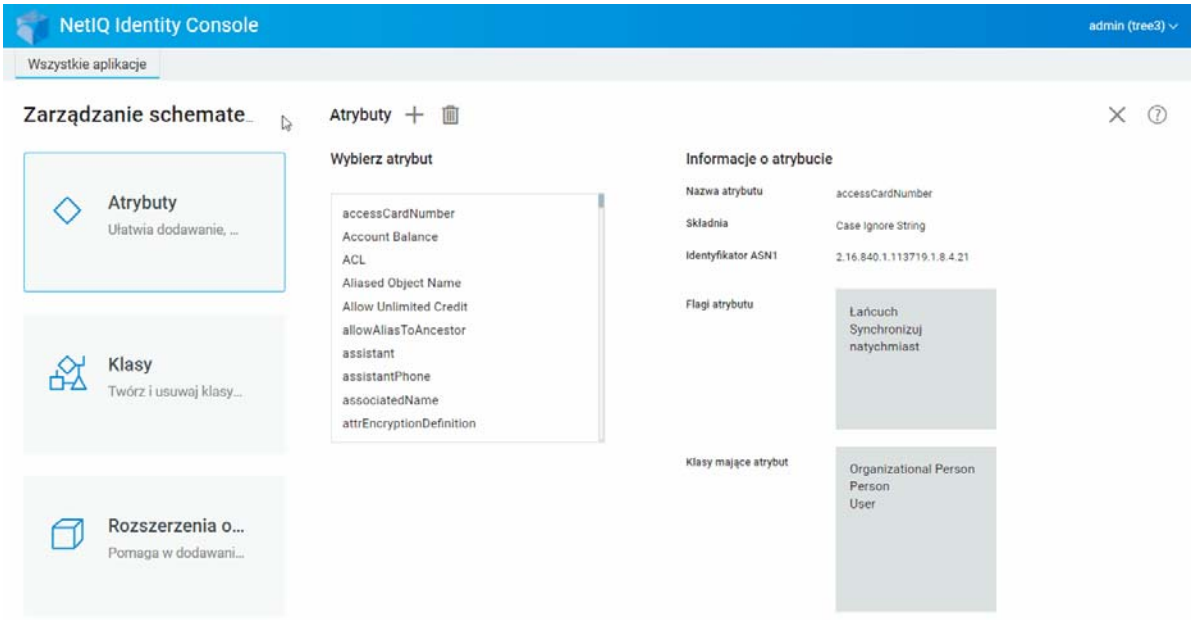


Wyświetlanie informacji dotyczących atrybutów

Istnieje możliwość wyświetlenia szczegółów strukturalnych dotyczących atrybutu, takich jak składnia, flagi i klasy używające atrybutu. Aby wyświetlić informacje dotyczące atrybutu:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Atrybuty**.
2. Kliknij dowolny atrybut na liście **Wybierz atrybut**.
3. Z prawej strony ekranu zostaną wyświetlone odpowiednie informacje o atrybucie.

Rysunek 10-3 *Wyświetlanie informacji dotyczących atrybutów*



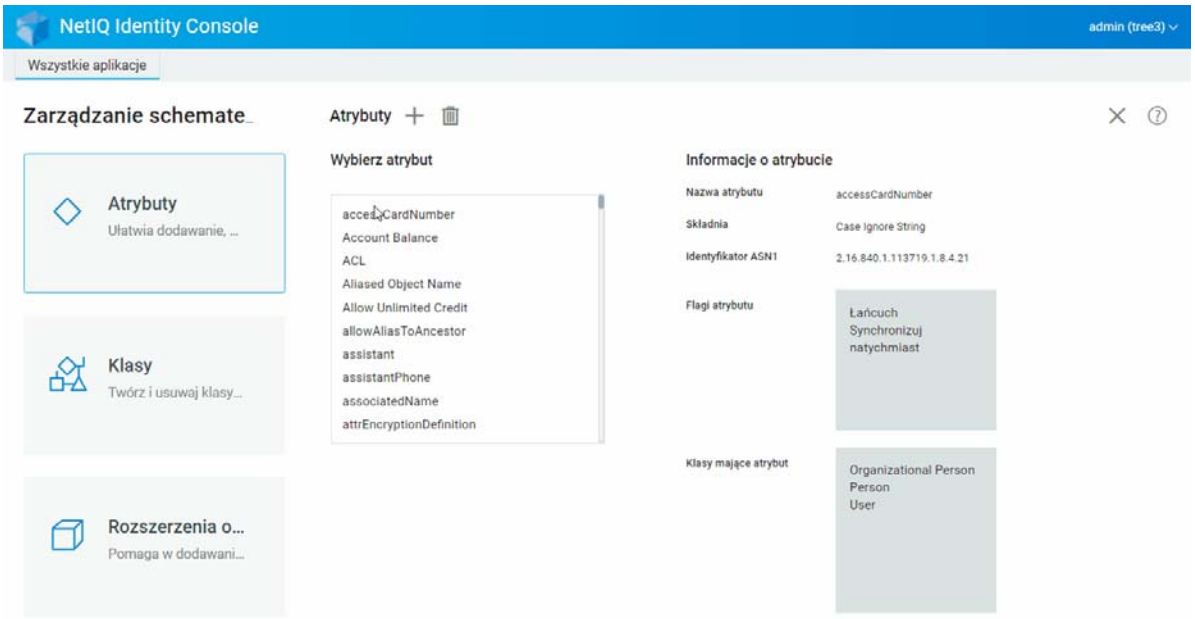
Usuwanie atrybutu

Możliwe jest usuwanie nieużywanych atrybutów, które nie należą do podstawowego schematu drzewa eDirectory. Może to być pomocne po scaleniu dwóch drzew katalogu lub jeśli atrybut stał się z czasem przestarzały. Aby usunąć atrybut:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Atrybuty**.
2. Na liście **Wybierz atrybut** wybierz atrybut, który chcesz usunąć, a następnie kliknij ikonę .

   UWAGA: Ikona będzie aktywna tylko po wybraniu atrybutu, który można usunąć.
3. Kliknij przycisk **OK**, aby potwierdzić usunięcie.

Rysunek 10-4 *Usuwanie atrybutu*



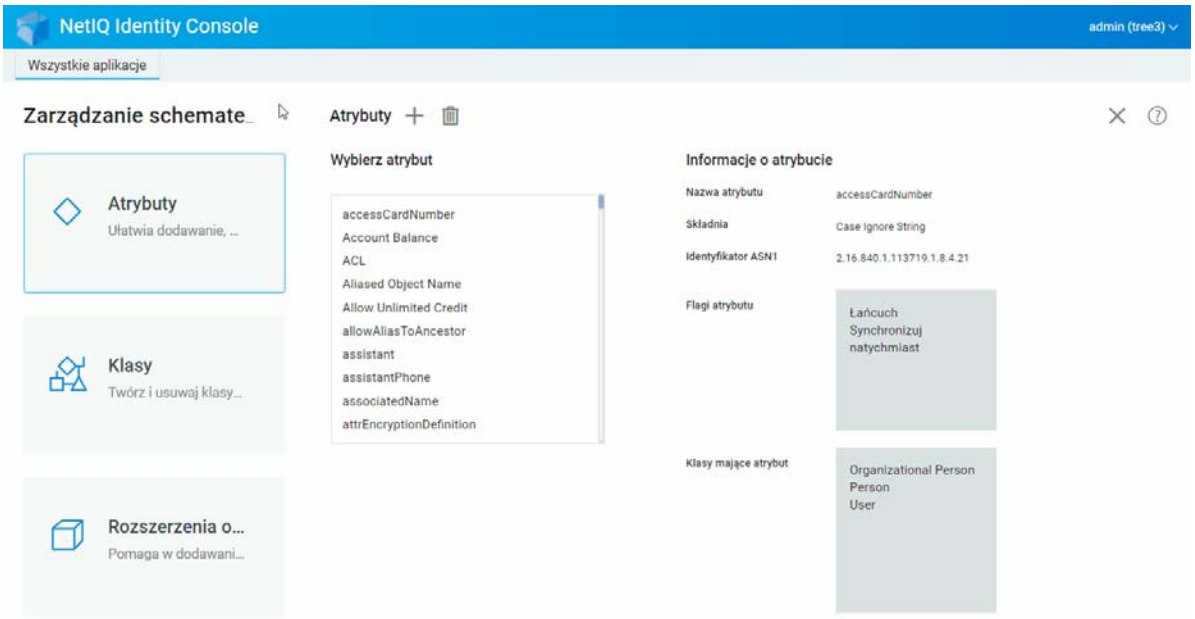
Usuwanie klasy

Możliwe jest usuwanie nieużywanych klas, które nie należą do podstawowego schematu drzewa eDirectory. Identity Console nie zezwala na usuwanie klas aktualnie używanych w lokalnie replikowanych partycjach. Aby usunąć klasę:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Klasy**.
2. Na liście **Wybierz klasę** wybierz klasę, którą chcesz usunąć, a następnie kliknij ikonę .

   UWAGA: Ikona będzie aktywna tylko po wybraniu klasy, którą można usunąć.
3. Kliknij przycisk **OK**, aby potwierdzić usunięcie.

Rysunek 10-5 *Usuwanie klasy*



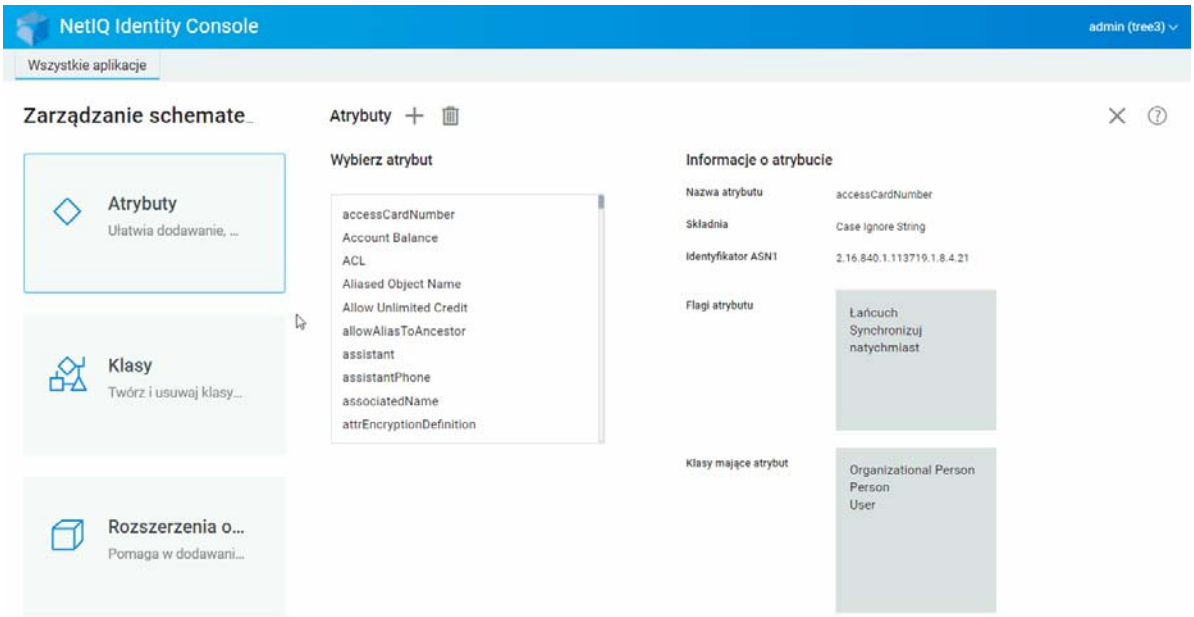
Rozszerzanie obiektu

Wykonaj następujące czynności, aby rozszerzyć obiekt:

1. Kliknij opcję **Zarządzanie schematem** na stronie docelowej Identity Console i wybierz opcję **Rozszerzenie obiektu**.
2. Podaj nazwę obiektu, który ma zostać rozszerzony, lub wybierz go za pomocą selektora obiektów, a następnie kliknij ikonę .
3. Kliknij ikonę i wybierz klasę pomocniczą, a następnie kliknij przycisk **OK**.

   UWAGA: Jeśli do wybranej klasy pomocniczej jest dołączony atrybut obowiązkowy, pojawi się monit o wprowadzenie wymaganych wartości w oknie podręcznym **Atrybuty obowiązkowe**.
4. Pojawi się komunikat potwierdzający dodanie klasy pomocniczej do obiektu.
5. Aby usunąć istniejącą klasę pomocniczą z obiektu, wybierz klasę i kliknij ikonę .

Rysunek 10-6 *Rozszerzanie obiektu*



11 Zarządzanie zdarzeniami audytu

W tym rozdziale wyjaśniono, jak zarządzać różnymi zdarzeniami audytu za pomocą Identity Console. Przy użyciu tej funkcji można włączać i wyłączać zdarzenia audytu dla serwera NCP.

Konfigurowanie zdarzeń audytu CEF

1. Zaloguj się do Identity Console za pomocą nazwy użytkownika i hasła.
2. Wybierz opcję **Audyt**.
3. Wybierz serwer NCP, który chcesz monitorować, a następnie kliknij przycisk **OK**.

   UWAGA: Po włączeniu po raz pierwszy zdarzeń CEF dla dowolnego serwera NCP domyślnie będzie zaznaczonych kilka zdarzeń.

4. Skonfiguruj zdarzenia audytu CEF:
   - **Konfiguracja zdarzeń:** Włącz lub wyłącz następujące zdarzenia w zależności od audytu wymaganego w danym środowisku:

UWAGA: Poszczególne kategorie zdarzeń w sekcji konfiguracji zdarzeń będą domyślnie zwinięte. Każdą kategorię można rozwinąć w celu wybrania poszczególnych zdarzeń.

Opcje	Opis
Zdarzenia zabezpieczeń	Wybierz zdarzenia zabezpieczeń, które chcesz zapisywać w dzienniku. W dzienniku można zapisywać zdarzenia dodawania lub usuwania członków, wykrycia intruza, zmiany hasła, uwierzytelniania użytkowników itd.
Zdarzenia obiektów	Wybierz zdarzenia obiektów, które chcesz zapisywać w dzienniku. W dzienniku można zapisywać zdarzenia tworzenia, usuwania, zmiany nazwy, przenoszenia i wyszukiwania obiektów.
Zdarzenia atrybutów	Wybierz zdarzenia atrybutów, które chcesz zapisywać w dzienniku. W dzienniku można zapisywać zdarzenia odczytu i usuwania atrybutów oraz dodawania, usuwania i porównywania wartości atrybutów.
Zdarzenia LDAP	Wybierz zdarzenia LDAP, które chcesz zapisywać w dzienniku.

- **Ustawienia zaawansowane:** Używając ustawień zaawansowanych, można wykonywać następujące czynności.
  - **Globalne:** Można wybrać lub wyczyścić ustawienia globalne dla powielonych wpisów.
    - **Nie wysyłaj zdarzeń replikowanych:** Wybierz tę opcję, aby przestać otrzymywać zdarzenia powielone z powodu replikacji z innych serwerów.
  - **Zapisz w dzienniku wartości zdarzeń:** Zdarzenia są zapisywane w pliku dziennika. Wartości zdarzeń o rozmiarze przekraczającym 768 bajtów są traktowane jako „duże wartości”. W dzienniku można zapisywać zdarzenia o dowolnym rozmiarze.
    - **Zapisz w dzienniku duże wartości:** Zaznacz tę opcję, aby rejestrować zdarzenia o rozmiarze przekraczającym 768 bajtów.
    - **Zapisz w dzienniku wartości atrybutów:** Zaznacz tę opcję, aby wyświetlić wartości atrybutów. Dotyczy ona jedynie zdarzeń **Dodanie wartości** i **Usunięcie wartości**.
    - **Zapisz w dzienniku wartości szyfrowanych atrybutów:** Zaznacz tę opcję, aby wyświetlić wartości szyfrowanych atrybutów. Dotyczy ona jedynie zdarzeń **Dodanie wartości** i **Usunięcie wartości**.

    UWAGA: Jeśli rozmiar zdarzenia przekracza 768 bajtów, wartość zdarzenia zostaje przycięta i zapisana w pliku dziennika.

Omówienie typów zdarzeń CEF

Format CEF można skonfigurować do zapisywania w dzienniku zdarzeń w następujących kategoriach:

- Zabezpieczenia
- Obiekty

- Atrybuty
- LDAP

Można przeprowadzać audyt następującego domyślnego zestawu typów zdarzeń:

Kategoria	Typ zdarzenia
Zabezpieczenia	◆ Zmiana listy kontroli dostępu ◆ Dodanie członka ◆ Usunięcie członka ◆ Wykryto intruza ◆ Logowanie wyłączone ◆ Logowanie włączone ◆ Zalogowanie ◆ Zmiana równoważności zabezpieczeń ◆ Konfiguracja audytu ◆ Zmiana hasła ◆ Odblokowanie konta ◆ Wylogowanie ◆ Połączenie ◆ Personifikacja ◆ Uwierzytelnienie ◆ Weryfikacja hasła ◆ Zmiana konfiguracji logowania ◆ Zapytanie o poświadczenia
Obiekty	◆ Utworzenie obiektu ◆ Usunięcie obiektu ◆ Zmiana nazwy obiektu ◆ Przeniesienie obiektu ◆ Odczyt agenta DSA ◆ Wyszukiwanie
Atrybuty	◆ Odczyt atrybutu ◆ Usunięcie atrybutu ◆ Dodanie wartości ◆ Usunięcie wartości ◆ Porównanie wartości atrybutu

Kategoria	Typ zdarzenia
LDAP	◆ Powiązanie LDAP ◆ Odpowiedź powiązania LDAP ◆ Odwiązanie LDAP ◆ Połączenie LDAP ◆ Wyszukiwanie LDAP ◆ Odpowiedź wyszukiwania LDAP ◆ Odpowiedź wyszukiwania wpisu LDAP ◆ Dodanie LDAP ◆ Odpowiedź dodania LDAP ◆ Porównanie LDAP ◆ Odpowiedź porównania LDAP ◆ Modyfikacja LDAP ◆ Odpowiedź modyfikacji LDAP ◆ Usunięcie LDAP ◆ Odpowiedź usunięcia LDAP ◆ Modyfikacja w pełni kwalifikowanej nazwy LDAP ◆ Odpowiedź modyfikacji w pełni kwalifikowanej nazwy LDAP ◆ Porzucenie LDAP ◆ Rozszerzona operacja LDAP ◆ Rozszerzona operacja systemu LDAP ◆ Odpowiedź rozszerzonej operacji LDAP ◆ Modyfikacja konfiguracji serwera LDAP ◆ Nieznana operacja LDAP ◆ Modyfikacja hasła LDAP

Konfigurowanie filtrowania audytu CEF

Używając filtrów i powiadomień o zdarzeniach, format CEF może raportować wystąpienie bądź niewystąpienie określonego typu zdarzenia. Można też filtrować zdarzenia pod kątem co najmniej jednej klasy obiektów lub atrybutu, w zależności od typu zdarzenia. CEF ocenia wszystkie wygenerowane zdarzenia na podstawie skonfigurowanych filtrów na serwerze eDirectory i zapisuje w dzienniku tylko te zdarzenia, które odpowiadają filtrom.

Ta sekcja zawiera informacje potrzebne do skonfigurowania filtrów i powiadomień systemowych.

- „Filtrowanie zdarzeń eDirectory za pomocą filtru wykluczeń” na stronie 71
- „Filtrowanie zdarzeń obiektów CEF” na stronie 71
- „Filtrowanie zdarzeń atrybutów CEF” na stronie 72

Filtrowanie zdarzeń eDirectory za pomocą filtru wykluczeń

Kliknij łącze **Filtr wykluczeń**, aby skonfigurować filtrowanie dla tych klas obiektów oraz atrybutów, dla których nie mają być generowane zdarzenia. Możesz wybrać klasy obiektów i atrybuty.

Aby skonfigurować filtrowanie dla niepożądanych zdarzeń eDirectory:

1. Na stronie domowej Identity Console wybierz opcję **Audyt**.
2. Wybierz serwer NCP, który chcesz monitorować, a następnie kliknij przycisk **OK**.
3. Teraz przejdź do obszaru **Ustawienia zaawansowane** i kliknij opcję **Filtr wykluczeń** pod nagłówkiem **Filtry**.

   Zostanie wyświetlone okno Filtrowanie wykluczeń CEF.
4. Na liście **Dostępne klasy obiektów** zaznacz klasy obiektów, dla których nie mają być zbierane zdarzenia, a następnie kliknij strzałkę w prawo, aby przenieść je na listę **Wybrane klasy obiektów**.
5. Na liście **Dostępne atrybuty** zaznacz dowolną liczbę atrybutów. Zaznacz atrybut, a następnie kliknij strzałkę w prawo w celu dodania go do listy wybranych atrybutów.
6. Kliknij przycisk **OK**.

Na podstawie skonfigurowanego filtru moduł audytu CEF przestanie generować zdarzenia dla wszystkich wybranych klas obiektów i atrybutów.

Filtrowanie zdarzeń obiektów CEF

Filtrowanie można skonfigurować dla obiektów, tak aby wyszukiwać określone zdarzenie lub zdarzenia. Na przykład jeśli chcesz otrzymywać powiadomienie, gdy ktoś utworzy konto użytkownika w usłudze eDirectory, możesz utworzyć filtr, wybierając klasę Obiekt użytkownika, aby zapisywać w dzienniku zdarzenia utworzenia nowego obiektu użytkownika.

Aby skonfigurować filtrowanie kont, kliknij łącze Zdarzenia obiektów, zaznacz klasę, a następnie kliknij przycisk **OK** w celu zamknięcia aplikacji.

Aby skonfigurować filtry dla zdarzeń zarządzania kontem:

1. Na stronie domowej Identity Console wybierz opcję **Audyt**.
2. Wybierz serwer NCP, który chcesz monitorować, a następnie kliknij przycisk **OK**.
3. Teraz przejdź do obszaru **Ustawienia zaawansowane** i kliknij opcję **Zdarzenia obiektów** pod nagłówkiem **Filtry**.

   Zostanie wyświetlone okno Filtrowanie obiektów CEF.
4. Na liście **Dostępne klasy obiektów** zaznacz dowolną klasę obiektów, kliknij strzałkę w prawo, aby przenieść klasę obiektów na listę **Wybrane klasy obiektów**, a następnie kliknij przycisk **OK**.

Na podstawie skonfigurowanego filtru moduł audytu CEF sprawdza wszystkie wygenerowane zdarzenia dla wybranych klas obiektów i zapisuje te zdarzenia w dzienniku.

Filtrowanie zdarzeń atrybutów CEF

Kliknij łącze **Zdarzenia atrybutów**, aby skonfigurować filtrowanie dla zdarzeń atrybutów. Na przykład jeśli chcesz otrzymywać powiadomienie, gdy ktoś doda nową wartość atrybutu w usłudze eDirectory, możesz utworzyć filtr powodujący zapisywanie w dzienniku zdarzeń dodania nowej wartości.

Aby skonfigurować filtrowanie dla zdarzeń atrybutów:

1. Na stronie domowej Identity Console wybierz opcję **Audyt**.
2. Wybierz serwer NCP, który chcesz monitorować, a następnie kliknij przycisk **OK**.
3. Teraz przejdź do obszaru **Ustawienia zaawansowane** i kliknij opcję **Zdarzenia atrybutów** pod nagłówkiem **Filtry**.

   Zostanie wyświetlone okno **Filtrowanie konfiguracji atrybutów**.
4. Na liście **Dostępne klasy obiektów** zaznacz klasy obiektów, dla których mają być zbierane zdarzenia, a następnie kliknij strzałkę w prawo, aby przenieść je na listę **Wybrane klasy obiektów**.
5. Na liście **Dostępne atrybuty** zaznacz dowolną liczbę atrybutów dla wybranych klas obiektów. Zaznacz atrybut, a następnie kliknij strzałkę w prawo w celu dodania go do listy wybranych atrybutów.

   UWAGA: Wybranie klasy obiektów spowoduje wybranie wszystkich zdarzeń atrybutów dla wszystkich atrybutów w tej klasie obiektów. W takim przypadku otrzymasz wszystkie zdarzenia atrybutów dla wszystkich atrybutów w wybranej klasie obiektów.

   ---
6. Kliknij przycisk **OK**.

Na podstawie skonfigurowanego filtru moduł audytu CEF sprawdza wszystkie wygenerowane zdarzenia dla wybranych klas obiektów oraz atrybutów i zapisuje te zdarzenia w dzienniku.

12 Zarządzanie szyfrowanymi atrybutami

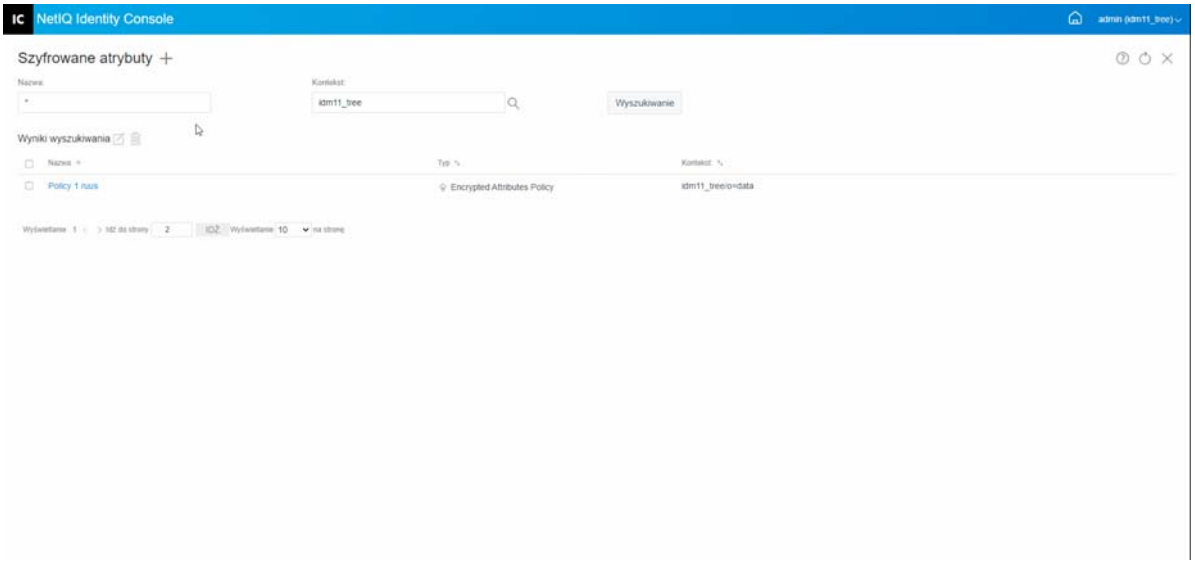
Identity Console ma możliwość bezpiecznego odczytywania szyfrowanych atrybutów z serwera eDirectory. Przy użyciu Identity Console można tworzyć, modyfikować lub usuwać kilka założeń dla tych szyfrowanych atrybutów.

Tworzenie założeń dla szyfrowanych atrybutów

Aby utworzyć nowe założenia atrybutów:

1. Kliknij opcję **Szyfrowane atrybuty** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz założenia szyfrowanych atrybutów wprowadź następujące szczegóły:
   - Podaj nazwę założeń
   - Wprowadź lub wybierz kontekst
   - Wybierz serwer NCP
   - Wybierz atrybuty
4. Po podaniu wszystkich wymaganych szczegółów kliknij przycisk **Zakończ**.
5. Zostanie wyświetlone potwierdzenie informujące o utworzeniu założeń.

Rysunek 12-1 *Tworzenie założeń szyfrowanych atrybutów*

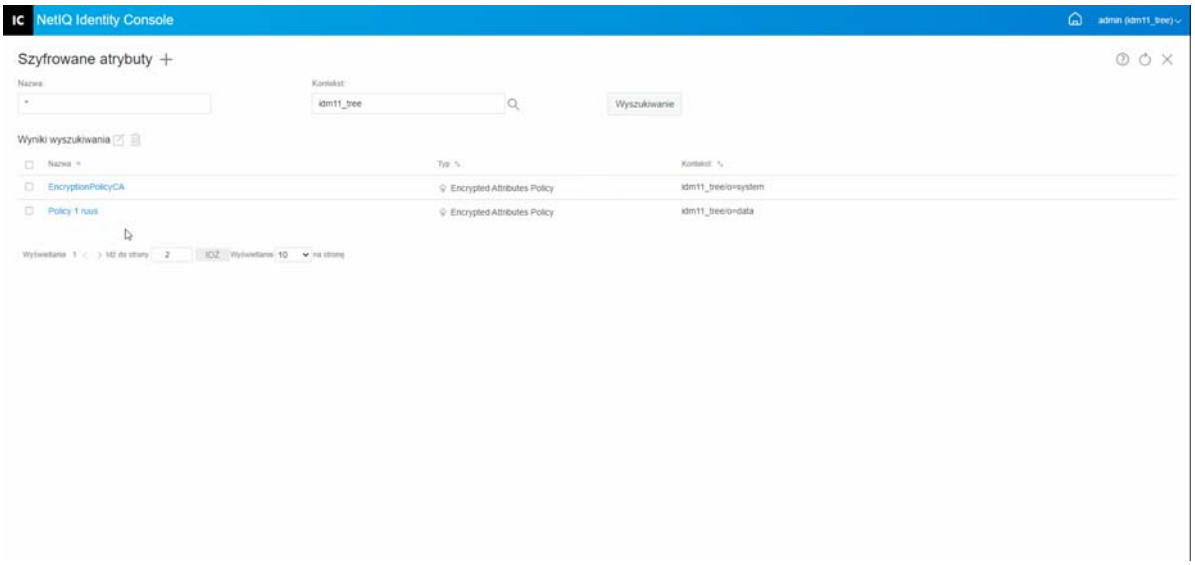


Usuwanie założeń szyfrowanych atrybutów

Aby usunąć założenia szyfrowanych atrybutów:

1. Kliknij opcję **Szyfrowane atrybuty** na stronie docelowej Identity Console.
2. Podaj nazwę i kontekst atrybutu lub znajdź atrybut przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz atrybuty z listy i kliknij ikonę.
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu założeń.

Rysunek 12-2 *Usuwanie założeń szyfrowanych atrybutów*

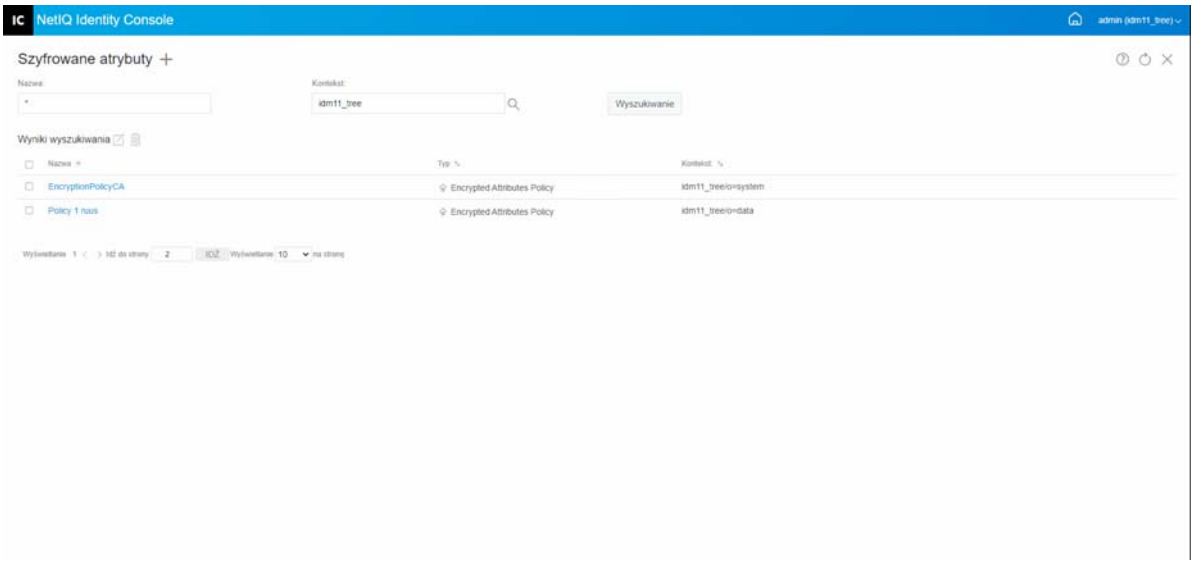


Modyfikowanie założeń szyfrowanych atrybutów

Aby zmodyfikować założenia szyfrowanych atrybutów:

1. Kliknij opcję **Szyfrowane atrybuty** na stronie docelowej Identity Console.
2. Wpisz nazwę i kontekst obiektu, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz atrybut z listy obiektów i kliknij ikonę.
4. Wprowadź zmiany, a następnie kliknij przycisk Zapisz.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu założeń.

Rysunek 12-3 *Modyfikowanie założeń szyfrowanych atrybutów*



13 Zarządzanie szyfrowaną replikacją

Aby włączyć szyfrowaną replikację, należy skonfigurować partycję dla szyfrowanej replikacji. Ustawienia konfiguracji są przechowywane w głównym obiekcie partycji. Szyfrowaną replikację można włączyć tylko na poziomie partycji. Włączenie szyfrowanej replikacji na poziomie partycji powoduje szyfrowanie wszystkich replikacji między replikami udostępniającymi tę partycję. Jeśli na przykład partycja P1 ma repliki R1, R2, R3 i R4, można zaszyfrować replikację między wszystkimi replikami.

- „Włączanie szyfrowanej replikacji dla partycji” na stronie 77

Włączanie szyfrowanej replikacji dla partycji

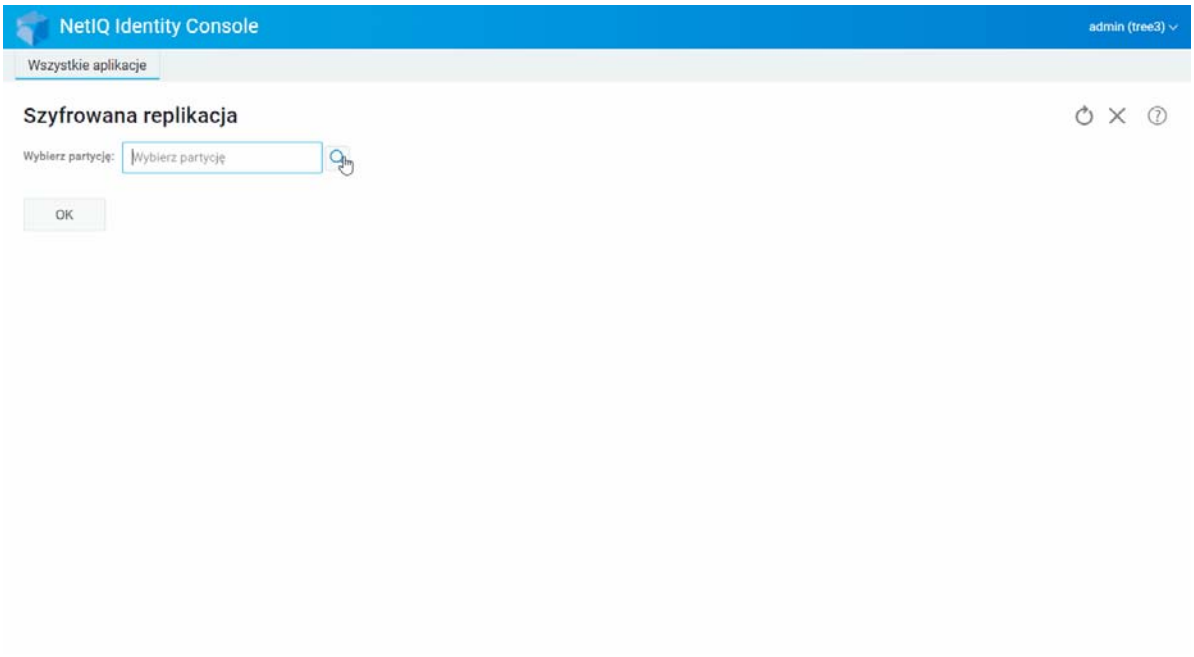
Aby włączyć szyfrowaną replikację dla partycji:

UWAGA: Aby można było włączyć szyfrowaną replikację dla partycji, wszystkie serwery udostępniające tę partycję muszą być serwerami eDirectory 9.2 lub nowszymi.

---

1. Kliknij opcję **Szyfrowana replikacja** na stronie docelowej Identity Console.
2. Określ lub wyszukaj za pomocą funkcji przeglądania partycję, dla której chcesz włączyć szyfrowaną replikację.
3. Zaznacz opcję **Włącz szyfrowaną replikację**. Jeśli wyłączasz szyfrowaną replikację dla partycji, odznacz tę opcję.
4. Kliknij przycisk **Zakończ**.
5. Zostanie wyświetlone potwierdzenie informujące o włączeniu szyfrowanej replikacji.

Rysunek 13-1 *Włączanie szyfrowanej replikacji dla partycji*



14 Zarządzanie partycjami i replikami

Operacje na partycjach i replikach umożliwiają zarządzanie fizyczną strukturą usługi eDirectory oraz jej dystrybucją na serwerach katalogowych.

Partycje są logicznymi obszarami drzewa eDirectory. Na przykład po wybraniu jednostki organizacyjnej i utworzeniu jej jako nowej partycji, jednostka ta, wraz ze wszystkimi swymi obiektami podrzędnymi, zostanie oddzielona od partycji nadrzędnej. Wybrana jednostka stanie się obiektem głównym nowej partycji. Repliki nowej partycji będą znajdować się na tych samych serwerach co repliki partycji nadrzędnej, a obiekty nowej partycji będą należeć do obiektu głównego nowej partycji.

Przy użyciu modułu Partycja można wykonywać następujące zadania:

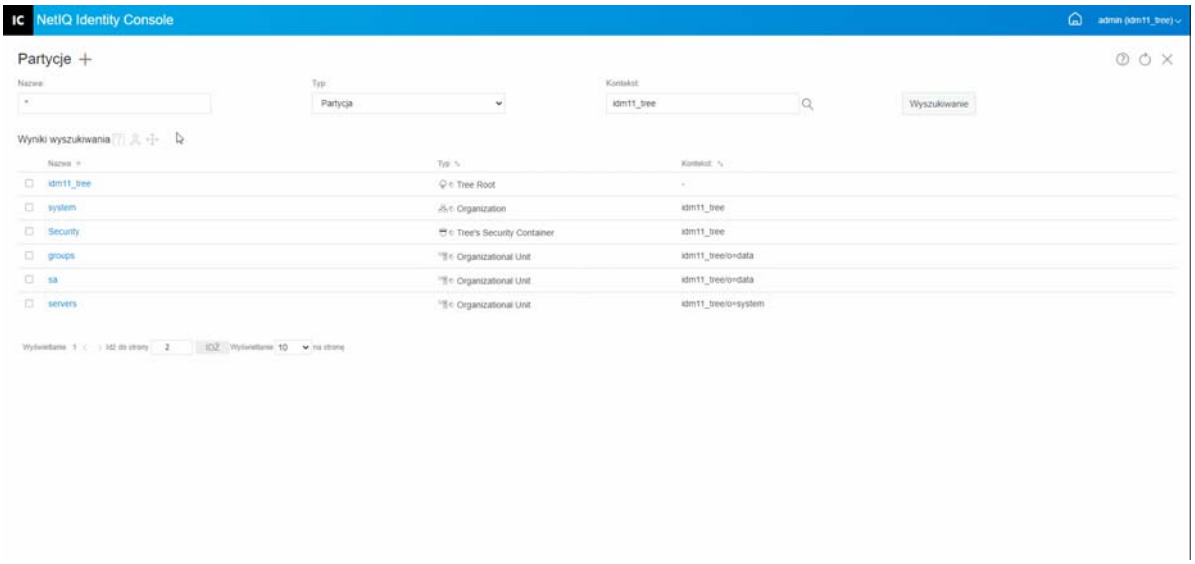
- „Tworzenie partycji” na stronie 79
- „Scalanie partycji” na stronie 80
- „Modyfikowanie partycji” na stronie 81
- „Przenoszenie partycji” na stronie 81

Tworzenie partycji

Aby utworzyć nową partycję:

1. Kliknij opcję **Zarządzanie partycjami** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz partycję określ kontener, który ma zostać obiektem głównym nowej partycji, lub znajdź kontener przy użyciu ikony Selektor obiektów, a następnie kliknij przycisk **Utwórz**.
4. Zostanie wyświetlone potwierdzenie informujące o utworzeniu partycji.

Rysunek 14-1 *Tworzenie nowej partycji*

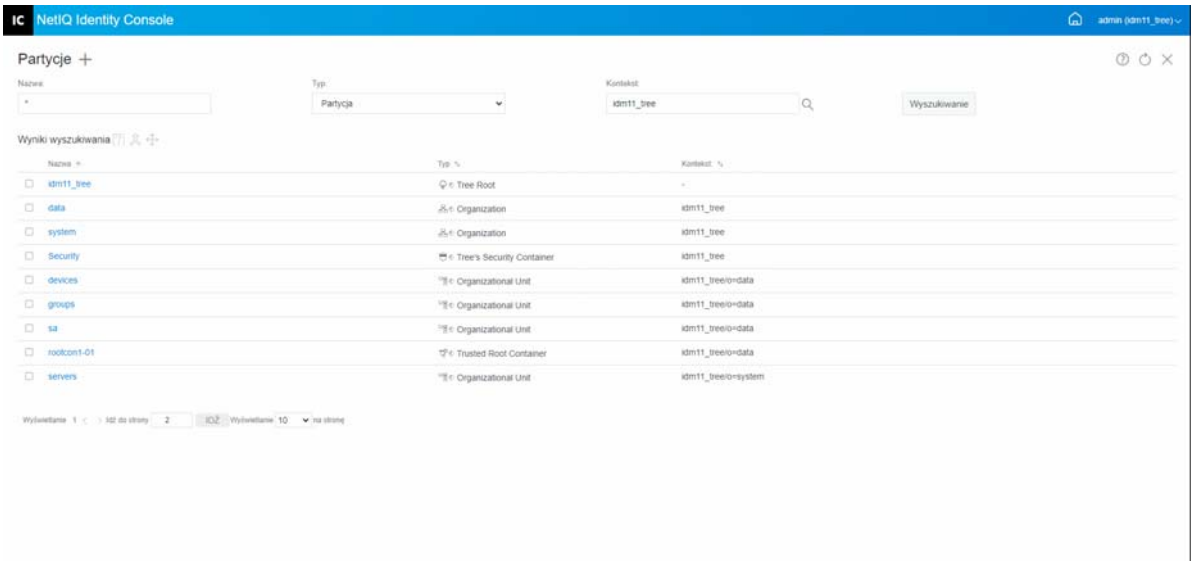


Scalanie partycji

Aby scalić partycję z jej partycją nadrzędną:

1. Kliknij opcję **Zarządzanie partycjami** na stronie docelowej Identity Console.
2. Podaj nazwę, typ i kontekst partycji lub znajdź partycję przy użyciu funkcji wyszukiwania, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz partycję z listy wyszukiwania, kliknij ikonę , a następnie kliknij przycisk **OK**.
4. Zostanie wyświetlone potwierdzenie informujące o scaleniu partycji.

Rysunek 14-2 *Scalanie partycji*



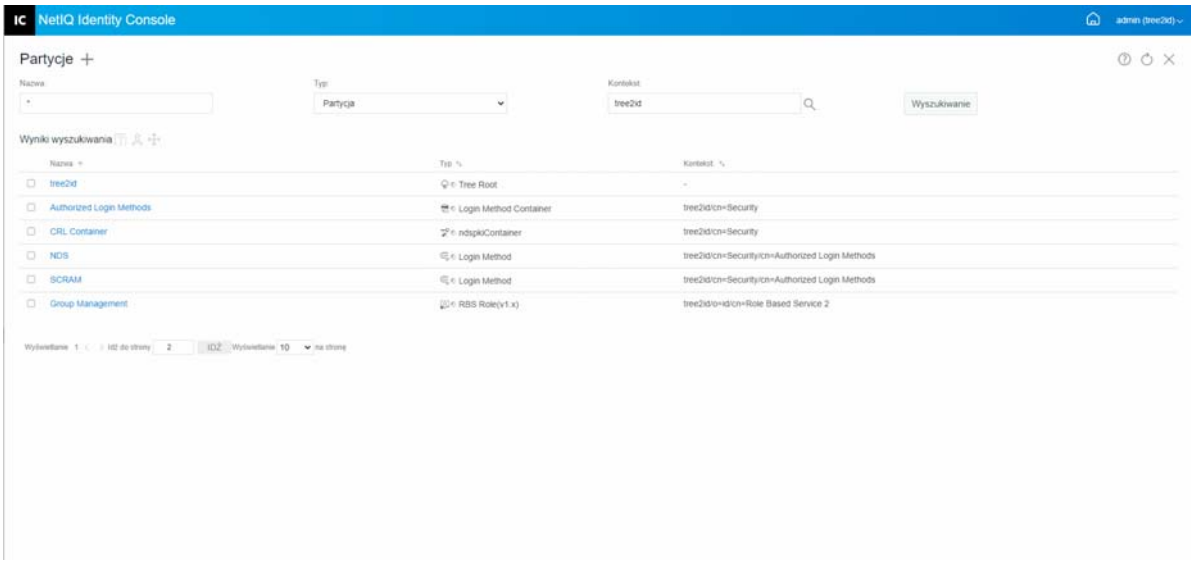
Modyfikowanie partycji

Aby zmodyfikować partycje:

1. Kliknij opcję **Zarządzanie partycjami** na stronie docelowej Identity Console.
2. Wpisz nazwę, typ i kontekst partycji, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz partycję z listy wyszukiwania i kliknij ikonę .
4. Kliknij opcję **Edytuj** w obszarze **Filtr**, aby zmienić filtry repliki oraz jej odpowiednie klasy i atrybuty, a następnie kliknij przycisk **OK**.

   W przypadku wybrania opcji **Serwer** w polu **Typ** zostanie wyświetlona lista wszystkich serwerów. Kliknięcie serwera spowoduje wyświetlenie listy wszystkich partycji na tym serwerze.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu partycji.

Rysunek 14-3 *Modyfikowanie partycji*



Przenoszenie partycji

Przenoszenie partycji pozwala przenieść drzewo podrzędne w drzewie katalogu. Operacja ta nosi też nazwę obcięcia i szczepienia. Można przenosić tylko te partycje, które nie mają partycji podrzędnych. Jeśli istnieją partycje podrzędne, to przed wykonaniem operacji przeniesienia należy je najpierw połączyć.

Po przeniesieniu partycji drzewo eDirectory zmienia wszystkie odwołania do głównego obiektu tej partycji. Nazwa zwykła obiektu pozostaje niezmieniona, ale zmienia się pełna nazwa kontenera (i wszystkich jego elementów podrzędnych).

UWAGA: Przenosząc partycję, należy przestrzegać reguł przynależności drzewa eDirectory. Na przykład nie można przenieść jednostki organizacyjnej bezpośrednio do katalogu głównego drzewa katalogu, ponieważ reguły zawartości katalogu głównego zezwalają jedynie na obiekty typu Umiejscowienie, Kraj lub Organizacja, ale nie typu Jednostka organizacyjna.

Aby przenieść partycję:

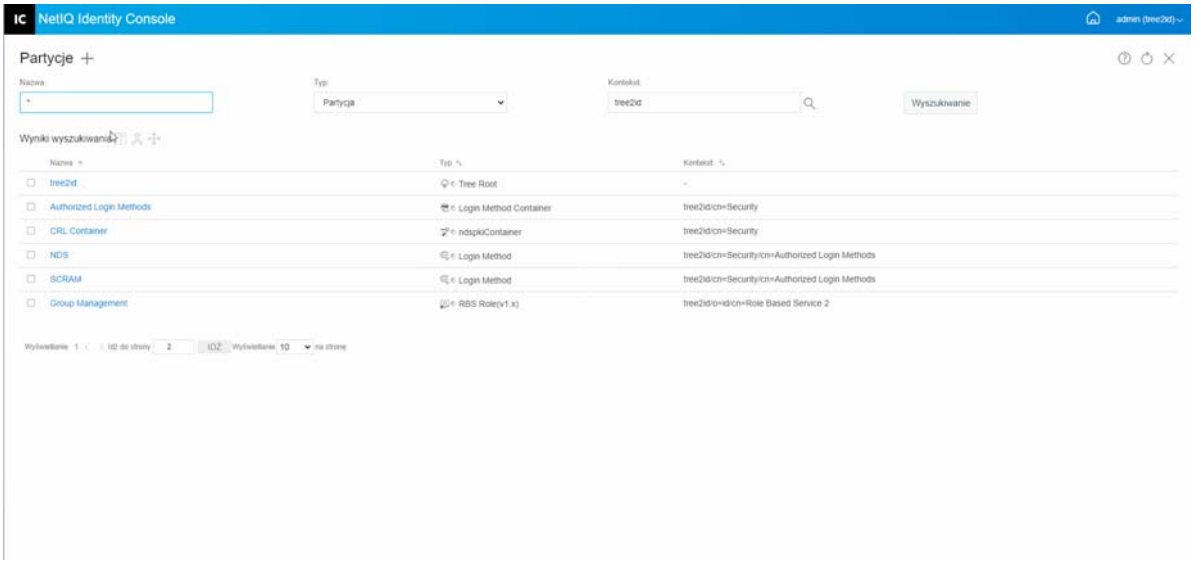
1. Kliknij opcję **Zarządzanie partycjami** na stronie docelowej Identity Console.
2. Wpisz nazwę, typ i kontekst partycji, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz partycję z listy wyszukiwania i kliknij ikonę .
4. Wybierz obiekt kontenera docelowego, do którego chcesz przenieść określoną partycję, a następnie kliknij przycisk **OK**.

UWAGA: Opcja **Utwórz alias w miejscu przeniesionej partycji** umożliwia utworzenie wskaźnika do nowej lokalizacji partycji. Dzięki temu wszystkie operacje odnoszące się do starej lokalizacji będą w dalszym ciągu funkcjonowały aż do ich aktualizacji w celu uwzględnienia nowego położenia. Użytkownicy będą mogli nadal logować się do sieci i znajdować obiekty w pierwotnym położeniu katalogu.

---

5. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym wykonaniu operacji przeniesienia partycji.

Rysunek 14-4 *Przenoszenie partycji*



15 Zarządzanie indeksami

Index Manager to atrybut obiektu Serwer umożliwiający zarządzanie indeksami baz danych. Indeksy te są używane przez usługę eDirectory i w znacznym stopniu poprawiają szybkość zapytań.

Usługa eDirectory jest dostarczana z zestawem indeksów zapewniających podstawową funkcjonalność zapytań. Te indeksy domyślne są przeznaczone dla poniższych atrybutów.

Przy użyciu modułu Indeks można wykonywać następujące zadania:

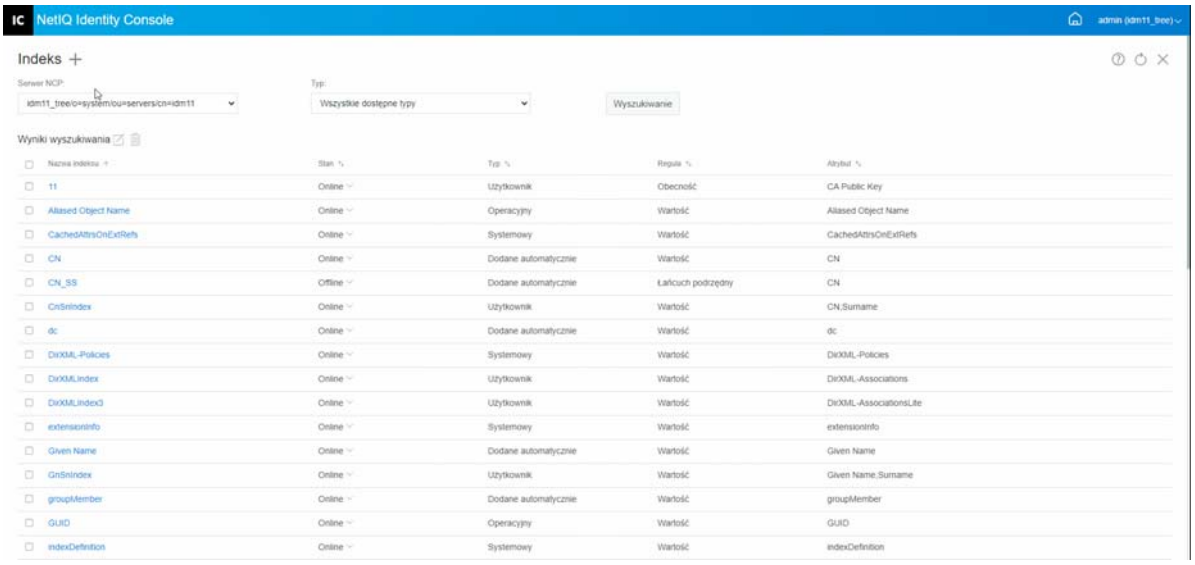
- „Tworzenie indeksu” na stronie 83
- „Usuwanie indeksu” na stronie 84
- „Kopiowanie indeksu” na stronie 85
- „Zmienianie stanu indeksu” na stronie 85

Tworzenie indeksu

Aby utworzyć nowy indeks:

1. Kliknij opcję **Zarządzanie indeksami** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Wprowadź nazwę indeksu.
4. Wybierz serwery z listy dostępnych serwerów NCP.
5. Wybierz wymagane atrybuty.
6. Wybierz regułę indeksu:
   - 6a **Łańcuch podrzędny:** Ta opcja pozwala dopasować podzbiór znaków, które występują w łańcuchu wartości atrybutu. Na przykład użycie zapytania do wyszukania nazwiska, w którym występuje łańcuch podrzędny „ski”, spowodowałoby zwrócenie takich wyników, jak: Skibiński, Kowalski czy Kwaskiewicz. Utworzenie indeksu z regułą Łańcuch podrzędny oraz jego obsługa wymaga użycia największej ilości zasobów.
   - 6b **Obecność:** Wymagana jest sama obecność atrybutu, a nie jego konkretne wartości. Indeks obecności zostałby użyty w zapytaniu służącym do wyszukania wszystkich pozycji z atrybutem Skrypt logowania.
   - 6c **Wartość:** Ta opcja pozwala dopasować całą wartość lub pierwszą część wartości atrybutu. Reguła z dopasowaniem wartości mogłaby zostać na przykład użyta do wyszukania pozycji, w których w polu Nazwisko występuje wartość „Marecki”, oraz pozycji, w których tekst tego pola rozpoczyna się od łańcucha „Mar”.
7. Kliknij przycisk Utwórz.
8. Zostanie wyświetlone potwierdzenie informujące o utworzeniu indeksu.

Rysunek 15-1 *Tworzenie nowego indeksu*

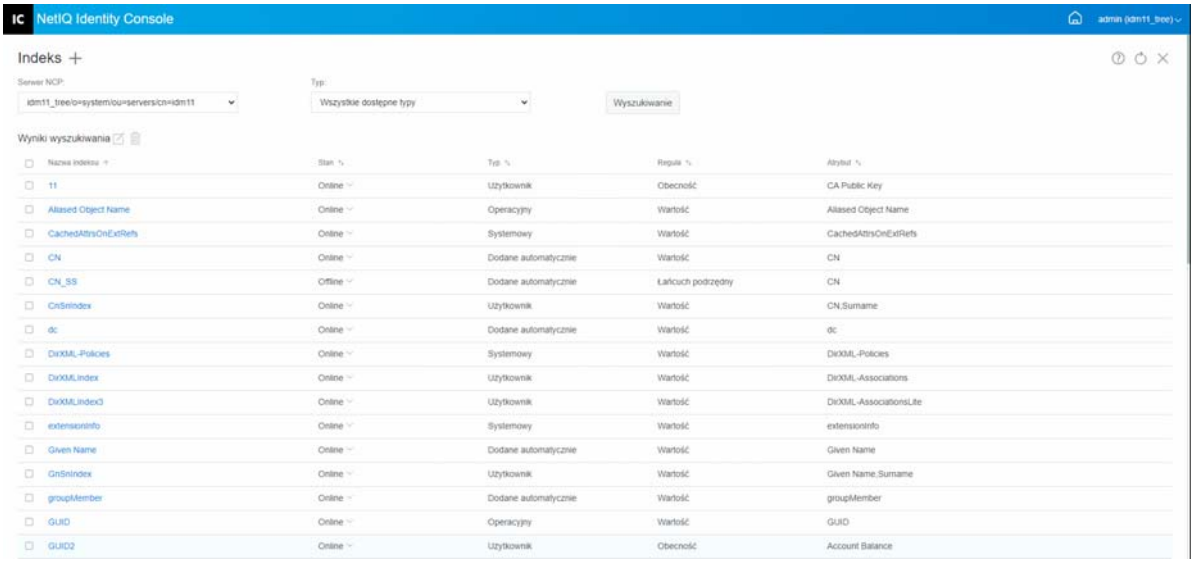


Usuwanie indeksu

Aby usunąć indeks:

1. Kliknij opcję **Zarządzanie indeksami** na stronie docelowej Identity Console.
2. Wybierz serwer NCP i typ indeksu, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz indeks z listy wyszukiwania i kliknij ikonę 🗑.
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu indeksu.

Rysunek 15-2 *Usuwanie indeksu*



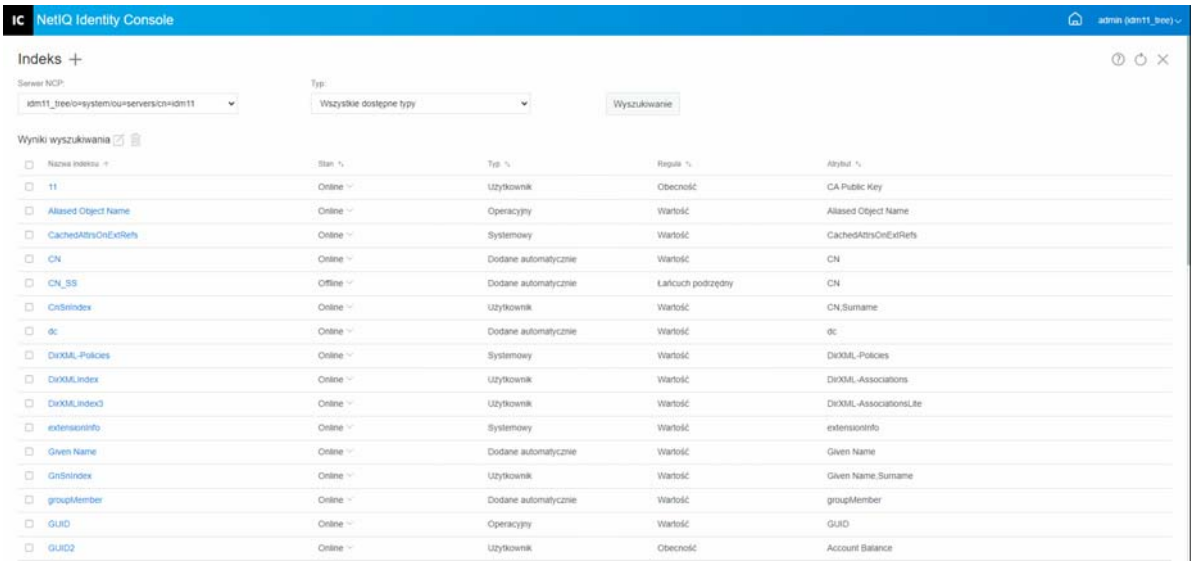
Kopiowanie indeksu

Jeśli określony indeks okazał się przydatny na jednym serwerze i widać potrzebę zastosowania go na innym, można skopiować definicję indeksu z jednego serwera na inny. Przeglądając dane predykatów, można również natrafić na przypadek odwrotny: indeks zaspokajający potrzeby kilku serwerów przestał być użyteczny na jednym z nich. W takim przypadku można usunąć indeks z pojedynczego serwera, który już z niego nie korzysta.

Aby skopiować indeks:

1. Kliknij opcję **Zarządzanie indeksami** na stronie docelowej Identity Console.
2. Wybierz serwer NCP i typ indeksu, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz indeks z listy wyszukiwania i kliknij ikonę .
4. Wybierz serwery NCP, na które chcesz skopiować indeks, i kliknij przycisk Zapisz.
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu indeksu.

Rysunek 15-3 *Kopiowanie indeksu*



Zmienianie stanu indeksu

W godzinach szczytu może być konieczne dostrojenie wydajności przez tymczasowe przeniesienie indeksów w tryb offline. Na przykład w celu przyspieszenia ładowania masowego można zawiesić wszystkie indeksy zdefiniowane przez użytkownika. Ze względu na to, że każda operacja dodania lub

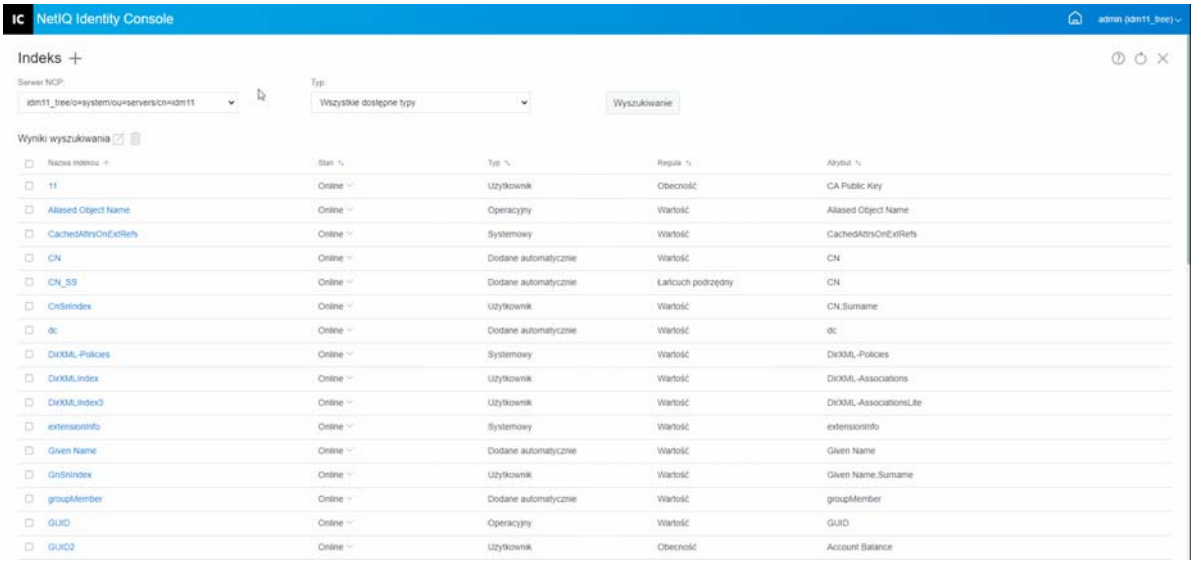
zmodyfikowania obiektu wymaga zaktualizowania zdefiniowanych indeksów, utrzymywanie aktywności wszystkich indeksów może spowodować spowolnienie masowego ładowania danych. Po zakończeniu ładowania masowego indeksy można z powrotem przełączyć w tryb online.

Aby przełączyć indeks w tryb offline:

1. Kliknij opcję **Zarządzanie indeksami** na stronie docelowej Identity Console.
2. Wybierz serwer NCP i typ indeksu, a następnie kliknij przycisk Wyszukiwanie.
3. Na liście indeksów kliknij listę rozwijaną **Stan**. Indeks może mieć jeden z następujących stanów:
   - **Online:** Aktualnie uruchomiony.
   - **Offline:** Wstrzymany. Indeks można uruchomić ponownie.

UWAGA: Stanu indeksów typu Systemowy i Operacyjny nie można zmieniać. Tego rodzaju indeksów nie można również usuwać.

Rysunek 15-4 *Przełączanie indeksu w tryb offline*



16 Konfigurowanie obiektów LDAP

Instalacja usługi eDirectory powoduje utworzenie obiektu serwera LDAP i obiektu grupy LDAP. Domyślna konfiguracja usług LDAP znajduje się w katalogu tych dwóch obiektów. Domyślną konfigurację można zmienić przy użyciu zadania Zarządzanie LDAP w portalu Identity Console.

Obiekt serwera LDAP reprezentuje dane konfiguracji specyficzne dla serwera. Jednak obiekt grupy LDAP zawiera informacje o konfiguracji, które można wygodnie udostępniać wielu serwerom LDAP. Ten obiekt zawiera wspólne dane konfiguracji i reprezentuje grupę serwerów LDAP. Serwery mają wspólne dane.

Z jednym obiektem grupy LDAP można skojarzyć wiele obiektów serwerów LDAP. Wszystkie skojarzone serwery LDAP otrzymują wówczas specyficzną dla siebie konfigurację od swojego obiektu serwera LDAP, natomiast informacje wspólne lub udostępnione — od obiektu grupy LDAP.

Przy użyciu modułu LDAP można wykonywać następujące zadania:

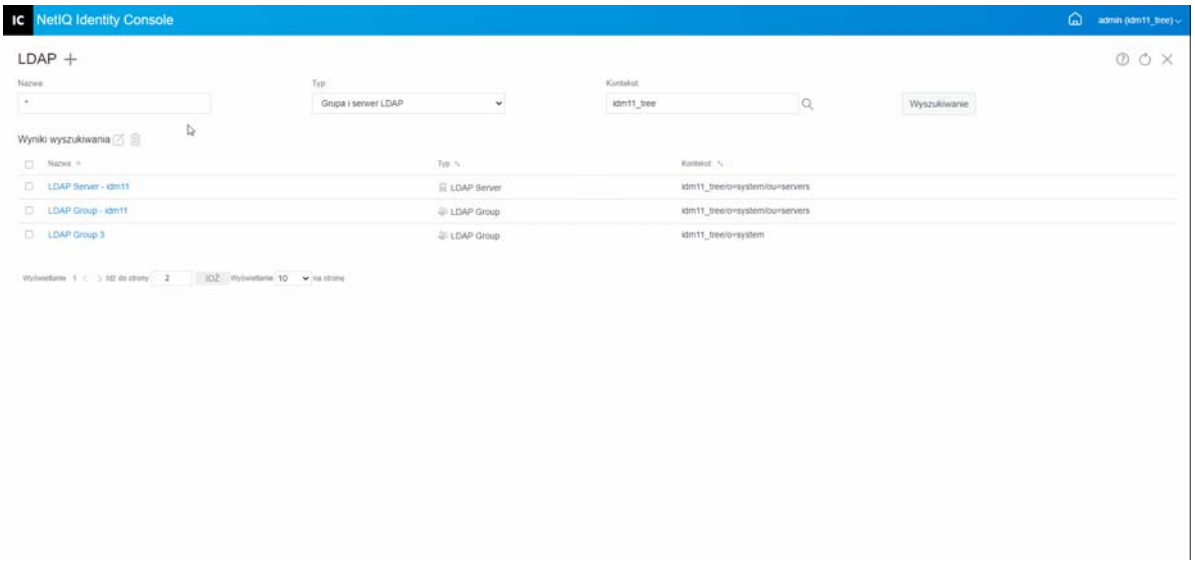
- „Tworzenie obiektów LDAP” na stronie 87
- „Usuwanie obiektów LDAP” na stronie 88
- „Modyfikowanie obiektów LDAP” na stronie 89

Tworzenie obiektów LDAP

Aby utworzyć nowy obiekt LDAP:

1. Kliknij opcję **Konfiguracja LDAP** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie Utwórz obiekt LDAP określ nazwę, typ i kontekst lub znajdź go za pomocą ikony Kontekst wyszukiwania, a następnie kliknij przycisk **Utwórz**.
4. Zostanie wyświetlone potwierdzenie informujące o utworzeniu obiektu LDAP.

Rysunek 16-1 *Tworzenie nowego obiektu LDAP*

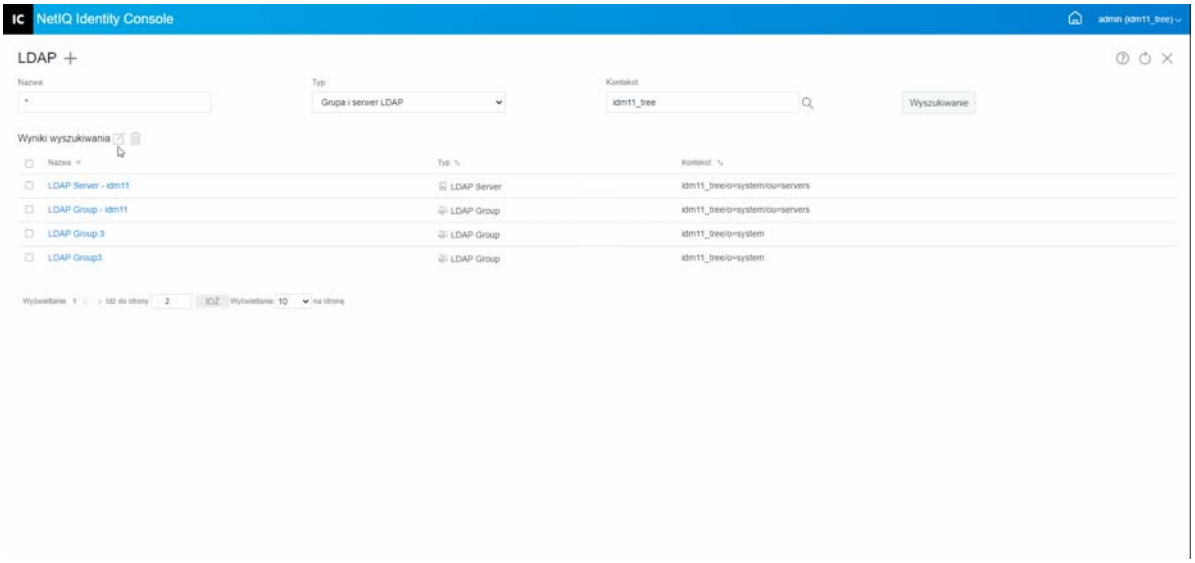


Usuwanie obiektów LDAP

Aby usunąć obiekty LDAP:

1. Kliknij opcję **Konfiguracja LDAP** na stronie docelowej Identity Console.
2. Określ nazwę, typ i kontekst obiektu LDAP, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekty LDAP z listy wyszukiwania i kliknij ikonę 🗑.
4. Zostanie wyświetlone potwierdzenie informujące o usunięciu obiektów LDAP.

Rysunek 16-2 *Usuwanie obiektów LDAP*

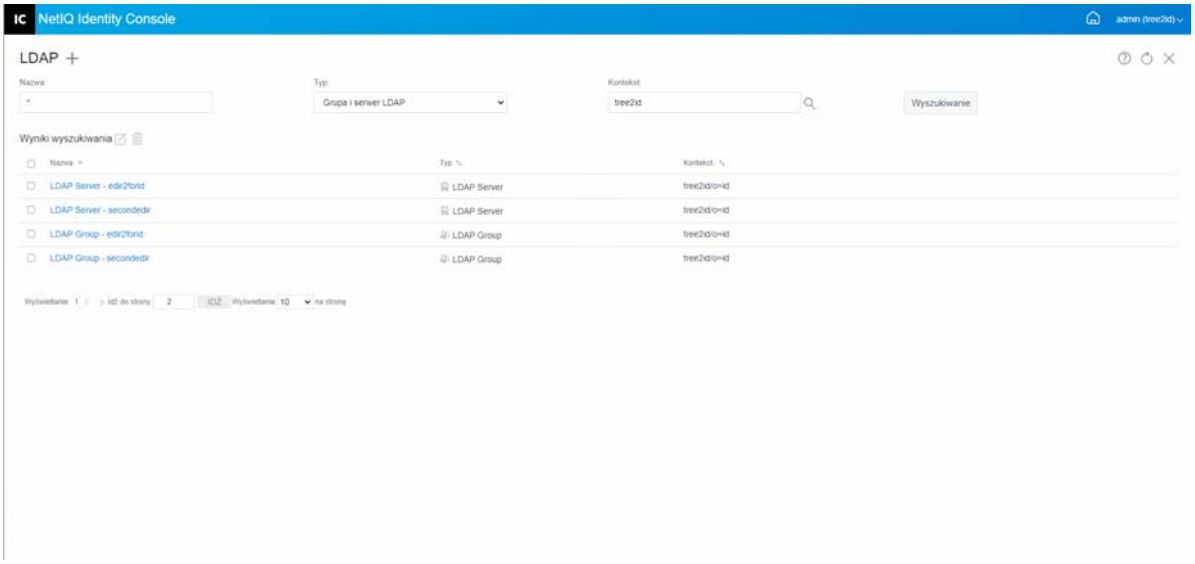


Modyfikowanie obiektów LDAP

Aby zmodyfikować obiekty LDAP:

1. Kliknij opcję **Konfiguracja LDAP** na stronie docelowej Identity Console.
2. Wpisz nazwę, typ i kontekst obiektu LDAP, a następnie kliknij przycisk Wyszukiwanie.
3. Wybierz obiekt LDAP z listy wyszukiwania i kliknij ikonę .
4. Zmodyfikuj odpowiednio do potrzeb atrybuty i informacje dotyczące określonego obiektu LDAP, a następnie kliknij przycisk Zapisz. Aby uzyskać więcej informacji na temat atrybutów obiektów LDAP, zobacz Configuring LDAP Server and LDAP Group Objects on Linux (Konfigurowanie serwera LDAP i obiektów grupy LDAP w systemie Linux) w dokumencie *NetIQ eDirectory Administration Guide* (NetIQ eDirectory — podręcznik administracji).
5. Zostanie wyświetlone potwierdzenie informujące o zmodyfikowaniu obiektu LDAP.

Rysunek 16-3 *Modyfikowanie obiektów LDAP*



17 Zarządzanie certyfikatami

NetIQ Certificate Server jest instalowany automatycznie razem z usługą eDirectory. Certificate Server świadczy usługi kryptograficzne kluczy publicznych, które w sposób rodzimy są zintegrowane z usługą eDirectory i które umożliwiają tworzenie oraz wystawianie certyfikatów użytkownika i serwera, a także zarządzanie nimi. Usługi te umożliwiają ochronę poufnych transmisji danych w publicznych kanałach komunikacyjnych, takich jak Internet.

UWAGA: Aby korzystać z modułu Zarządzanie certyfikatami z portalem Identity Console, musisz uaktualnić serwer eDirectory do wersji 9.2.4 HF2.

Identity Console umożliwia wykonywanie następujących zadań zarządzania certyfikatami:

Zarządzanie ośrodkiem certyfikacji

Domyślnie w ramach procesu instalacji NetIQ Certificate Server jest tworzony wewnętrzny ośrodek certyfikacji (CA). Użytkownik musi określić jego nazwę. Kliknięcie przycisku Zakończ powoduje utworzenie wewnętrznego ośrodka certyfikacji z parametrami domyślnymi i umieszczenie go w kontenerze Zabezpieczenia. Aby uzyskać większą kontrolę nad tworzeniem wewnętrznego ośrodka certyfikacji, można utworzyć go ręcznie w portalu Identity Console. Po usunięciu wewnętrznego ośrodka certyfikacji należy utworzyć go ponownie.

Przy użyciu modułu Ośrodek certyfikacji można wykonywać następujące zadania:

Tworzenie obiektu wewnętrznego ośrodka certyfikacji

Aby utworzyć obiekt wewnętrznego ośrodka certyfikacji, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.
2. Jeśli nie istnieje żaden obiekt wewnętrznego ośrodka certyfikacji, zostanie otwarte okno dialogowe Create an Organizational Certificate Authority Object (Utwórz obiekt wewnętrznego ośrodka certyfikacji) i odpowiedni kreator, który utworzy ten obiekt. Wykonaj instrukcje w celu utworzenia obiektu.

   UWAGA: Należy się upewnić, że określona w tym miejscu ścieżka pliku CRL jest zgodna ze ścieżką instalacji usługi eDirectory.

   ---

3. Po zakończeniu tworzenia ośrodka certyfikacji zalecamy utworzenie kopii zapasowej pary kluczy publiczny/prywatny ośrodka certyfikacji i zachowanie jej w bezpiecznym miejscu. Aby uzyskać więcej informacji, zobacz „Tworzenie kopii zapasowej certyfikatów wewnętrznego ośrodka certyfikacji” na stronie 92.

Tworzenie kopii zapasowej certyfikatów wewnętrznego ośrodka certyfikacji

Zalecamy utworzenie kopii zapasowej certyfikatów i klucza prywatnego wewnętrznego ośrodka certyfikacji na wypadek nieodwracalnej awarii serwera hosta wewnętrznego ośrodka certyfikacji. W przypadku wystąpienia awarii plik kopii zapasowej umożliwia przywrócenie wewnętrznego ośrodka certyfikacji na dowolnym serwerze w drzewie.

UWAGA: Możliwość utworzenia kopii zapasowej wewnętrznego ośrodka certyfikacji jest dostępna tylko w przypadku wewnętrznych ośrodków certyfikacji utworzonych za pomocą produktu Certificate Server w wersji co najmniej 9.0. We wcześniejszych wersjach produktu Certificate Server klucz prywatny wewnętrznego ośrodka certyfikacji był tworzony w sposób uniemożliwiający jego eksportowanie.

Plik kopii zapasowej zawiera klucz prywatny, certyfikat samopodpisany, certyfikat klucza publicznego i kilka innych certyfikatów niezbędnych do działania ośrodka certyfikacji. Informacje te są zachowywane w formacie PKCS #12 (nazywanym także PFX).

Kopię zapasową wewnętrznego ośrodka certyfikacji należy utworzyć, gdy działa on prawidłowo.

Aby utworzyć kopię zapasową wewnętrznego ośrodka certyfikacji, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.
2. Kliknij kartę **Certyfikaty**.
3. Wybierz opcję **Self Signed Certificate** (Certyfikat samopodpisany) lub **Public Key Certificate** (Certyfikat klucza publicznego). Oba certyfikaty są zapisywane w pliku w trakcie operacji tworzenia kopii zapasowej. Zalecamy wybranie opcji Certyfikat samopodpisany oddzielnie dla certyfikatów RSA i ECDSA.
4. Kliknij ikonę .

5 Wybierz eksportowanie klucza prywatnego, określ hasło składające się z co najmniej 6 znaków alfanumerycznych do użytku podczas szyfrowania pliku PFX, wybierz format eksportowania PKCS12, a następnie kliknij przycisk **OK**.

6 Zaszyfrowany plik kopii zapasowej zostanie zapisany w określonej lokalizacji. Teraz jest on gotowy do przechowywania w bezpiecznym miejscu na wypadek sytuacji awaryjnej.

Przywracanie wewnętrznego ośrodka certyfikacji

Jeśli obiekt wewnętrznego ośrodka certyfikacji został usunięty lub uszkodzony albo jeśli serwer hosta wewnętrznego ośrodka certyfikacji uległ nieodwracalnej awarii, wewnętrzny ośrodek certyfikacji można przywrócić do pełnego działania, używając pliku kopii zapasowej utworzonego w sposób opisany w sekcji „Tworzenie kopii zapasowej certyfikatów wewnętrznego ośrodka certyfikacji” na stronie 92.

Aby przywrócić wewnętrzny ośrodek certyfikacji, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.

2 Kliknij ikonę ↑↓ u góry ekranu (obok opcji **Zarządzanie ośrodkami certyfikacji**), aby usunąć istniejący wewnętrzny ośrodek certyfikacji.

3 Zostanie wyświetlony monit o skonfigurowanie nowego wewnętrznego ośrodka certyfikacji. Spowoduje to otwarcie okna dialogowego „Utwórz obiekt wewnętrznego ośrodka certyfikacji” i odpowiedniego kreatora, który utworzy obiekt.

4 W oknie dialogowym tworzenia określ serwer, na którym powinien być hostowany wewnętrzny ośrodek certyfikacji, i nadaj nazwę obiektowi wewnętrznego ośrodka certyfikacji.

5 Wybierz opcję **Importuj**.

6 Wybierz zarówno certyfikat RSA, jak i ECDSA. Certificate Server wymaga, aby oba certyfikaty miały tę samą nazwę podmiotu. Jednak Certificate Server nie obsługuje importowania zewnętrznych samopodpisanych certyfikatów ośrodka certyfikacji. Umożliwia natomiast importowanie podrzędnych certyfikatów ośrodka certyfikacji.

7 Na kolejnych ekranach znajdź i wybierz nazwę pliku dla certyfikatów RSA i ECDSA.

8 Wprowadź hasło służące do szyfrowania pliku po utworzeniu kopii zapasowej i kliknij przycisk **OK**.

9 Certyfikaty i klucz prywatny wewnętrznego ośrodka certyfikacji zostały przywrócone i ośrodek certyfikacji jest w pełni funkcjonalny. Plik można teraz ponownie zachować do użytku w przyszłości.

Zatwierdzanie certyfikatów wewnętrznego ośrodka certyfikacji

Jeśli istnieją podejrzenia, że wystąpił problem z certyfikatem lub certyfikat stracił ważność, można go łatwo zatwierdzić przy użyciu Identity Console. Można zatwierdzić dowolny certyfikat w drzewie eDirectory, w tym również certyfikaty wystawione przez zewnętrzne ośrodki certyfikacji.

Proces zatwierdzania certyfikatu obejmuje kilka testów danych w certyfikacie, a także danych w łańcuchu certyfikatów. Łańcuch certyfikatów składa się z głównego certyfikatu ośrodka certyfikacji oraz, opcjonalnie, certyfikatów co najmniej jednego pośredniego ośrodka certyfikacji.

Aby zatwierdzić certyfikat:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.
2. Kliknij kartę **Certyfikaty**.
3. Wybierz opcję **Certyfikat samopodpisany** lub **Certyfikat klucza publicznego**.
4. Kliknij ikonę , aby zatwierdzić wybrane certyfikaty ośrodka certyfikacji.

Zastępowanie wewnętrznych certyfikatów ośrodka certyfikacji

Jeśli z jakiegoś powodu certyfikaty staną się uszkodzone lub nieważne albo jeśli chcesz tylko zastąpić istniejące certyfikaty, wykonaj następujące czynności:

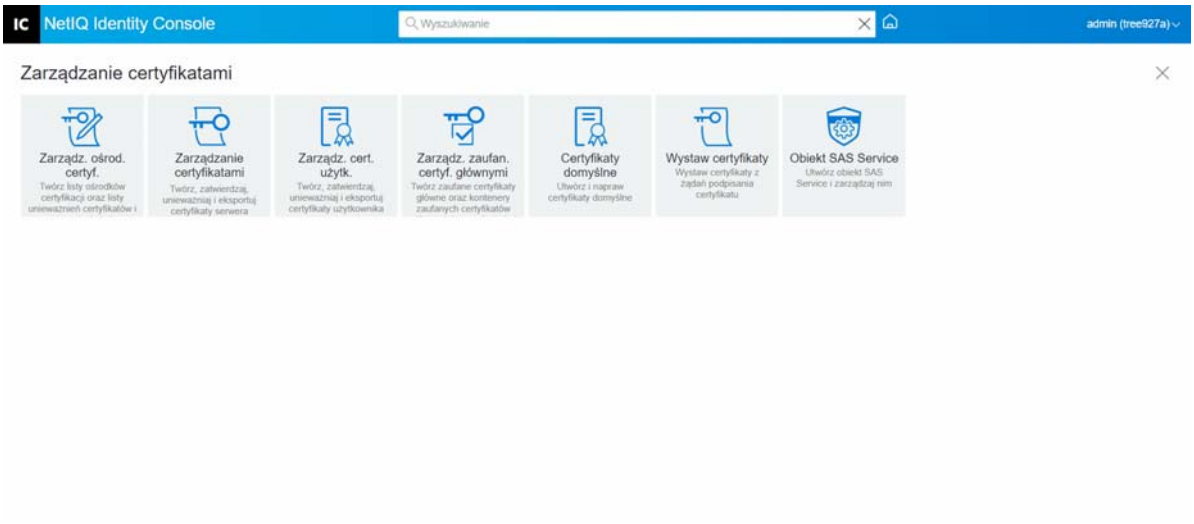
1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.
2. Kliknij kartę **Certyfikaty**.
3. Wybierz opcję **Certyfikat samopodpisany** lub **Certyfikat klucza publicznego**.
4. Kliknij ikonę , aby zastąpić wybrany certyfikat ośrodka certyfikacji.
5. Zaimportuj certyfikat ośrodka certyfikacji w formacie `PFX` lub `P12` i określ hasło do szyfrowania klucza prywatnego.
6. Kliknij przycisk **OK**.

Unieważnianie wewnętrznych certyfikatów ośrodka certyfikacji

Aby unieważnić certyfikat:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. ośrod. certyf.** na stronie docelowej Identity Console.
2. Kliknij kartę **Certyfikaty**.
3. Wybierz opcję **Certyfikat samopodpisany** lub **Certyfikat klucza publicznego**.
4. Kliknij ikonę .
5. Przeczytaj ze zrozumieniem informacje o ryzyku związanym z unieważnianiem certyfikatów serwera.
6. Z listy rozwijanej wybierz prawidłową przyczynę unieważnienia, wybierz datę utraty ważności i dodaj wszystkie pozostałe komentarze.
7. Kliknij przycisk **OK**, aby zakończyć unieważnianie.

Rysunek 17-1 *Zarządzanie ośrodkiem certyfikacji*



Zarządzanie certyfikatami serwera

Przy użyciu modułu Zarządzanie certyfikatami serwera administrator może wykonywać następujące zadania:

- „Tworzenie obiektów certyfikatu serwera” na stronie 95
- „Eksportowanie obiektów certyfikatu serwera” na stronie 96
- „Zatwierdzanie obiektów certyfikatu serwera” na stronie 96
- „Zastępowanie obiektu certyfikatu serwera” na stronie 96
- „Unieważnianie obiektów certyfikatu serwera” na stronie 97
- „Usuwanie obiektów certyfikatu serwera” na stronie 97

Tworzenie obiektów certyfikatu serwera

Aby utworzyć obiekt certyfikatu serwera, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie **Utwórz certyfikat serwera** określ **nazwę skróconą**, serwer i wybierz dowolną z następujących opcji:
   - **Standardowe (parametry domyślne):** Umożliwia utworzenie domyślnego obiektu certyfikatu serwera typu RSA lub ECDSA.
   - **Niestandardowe (parametry są określane przez użytkownika):** Umożliwia określenie niestandardowych parametrów obiektu certyfikatu serwera.
   - **Import (Umożliwia pobranie kluczy i certyfikatów z pliku PKCS12):** Umożliwia zaimportowanie pliku `PKCS12` w formacie `PFX` lub `P12`.

4 Po określeniu parametrów kliknij przycisk **Dalej**, aby przejrzeć podsumowanie certyfikatu.

5 Na ekranie **Podsumowanie** kliknij przycisk **OK**, aby utworzyć obiekt certyfikatu serwera.

Eksportowanie obiektów certyfikatu serwera

Aby wyeksportować obiekty certyfikatu serwera, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.

2 Wybierz odpowiedni serwer z listy rozwijanej.

3 Wybierz odpowiedni certyfikat serwera z listy i kliknij ikonę .

4 Na następnym ekranie zaznacz pole wyboru opcji **Eksportuj klucz prywatny** i określ hasło do ochrony klucza prywatnego. Potwierdź hasło i wybierz format eksportu.

UWAGA: Certyfikaty serwera można eksportować tylko w formacie `PKCS12`.

---

5 Kliknij przycisk **OK**, aby wyeksportować obiekt certyfikatu serwera.

Zatwierdzanie obiektów certyfikatu serwera

Aby zatwierdzić obiekt certyfikatu serwera, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.

2 Wybierz odpowiedni serwer z listy rozwijanej.

3 Wybierz odpowiedni certyfikat serwera z listy i kliknij ikonę .

4 Zostanie wyświetlone potwierdzenie informujące o pomyślnym zatwierdzeniu obiektu certyfikatu serwera.

Zastępowanie obiektu certyfikatu serwera

Jeśli z jakiegoś powodu certyfikaty serwera staną się uszkodzone lub nieważne albo jeśli chcesz tylko zastąpić istniejące certyfikaty domyślne, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.

2 Wybierz odpowiedni serwer z listy rozwijanej.

3 Wybierz odpowiedni certyfikat serwera z listy i kliknij ikonę .

4 Przeczytaj ze zrozumieniem informacje o ryzyku związanym z zastępowaniem certyfikatów serwera i kliknij przycisk **OK**.

5 Na następnym ekranie znajdź i wybierz nowy certyfikat serwera w formacie `PFX` lub `P12`, a następnie określ hasło.

6 Kliknij przycisk **OK**, aby zastąpić certyfikat serwera.

Unieważnianie obiektów certyfikatu serwera

Aby unieważnić obiekt certyfikatu serwera, wykonaj następujące czynności:

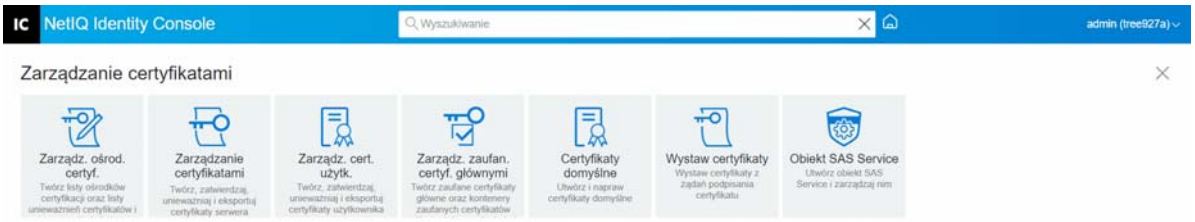
1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat serwera z listy i kliknij ikonę ⊘.
4. Przeczytaj ze zrozumieniem informacje o ryzyku związanym z unieważnianiem certyfikatów serwera i kliknij przycisk **OK**.
5. Na następnym ekranie wybierz prawidłową przyczynę unieważnienia z listy rozwijanej, wybierz datę utraty ważności i dodaj wszystkie pozostałe komentarze.
6. Kliknij przycisk **OK**, aby zakończyć unieważnianie.

Usuwanie obiektów certyfikatu serwera

Aby usunąć obiekty certyfikatu serwera, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządzanie certyfikatami serwera** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat serwera z listy i kliknij ikonę 🗑.
4. Na następnym ekranie kliknij przycisk **OK**.
5. Zostanie wyświetlone potwierdzenie informujące o pomyślnym usunięciu obiektu certyfikatu serwera.

Rysunek 17-2 *Zarządzanie certyfikatami serwera*



Zarządzanie certyfikatami użytkownika

Przy użyciu modułu Zarządzanie certyfikatami użytkownika można wykonywać następujące zadania:

Tworzenie obiektów certyfikatu użytkownika

Aby utworzyć obiekt certyfikatu użytkownika, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. cert. użytk.** na stronie docelowej Identity Console.
2. Kliknij ikonę +.
3. Na stronie **Utwórz certyfikat użytkownika** określ **nazwę skróconą**, serwer i wybierz dowolną z następujących opcji:
   - **Standardowe (parametry domyślne):** Umożliwia utworzenie domyślnego obiektu certyfikatu użytkownika typu RSA lub ECDSA.
   - **Niestandardowe (parametry są określane przez użytkownika):** Umożliwia określenie niestandardowych parametrów obiektu certyfikatu użytkownika.
   - **Importuj:** Umożliwia zaimportowanie pliku certyfikatu w formacie `CERT` lub `PKCS12`.
4. Po określeniu parametrów kliknij przycisk **Dalej**, aby przejrzeć podsumowanie certyfikatu.
5. Na ekranie **Podsumowanie** kliknij przycisk **OK**, aby utworzyć obiekt certyfikatu użytkownika.

Eksportowanie obiektów certyfikatu użytkownika

Aby wyeksportować obiekty certyfikatu użytkownika, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. cert. użytk.** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat użytkownika z listy i kliknij ikonę  .
4. Na następnym ekranie zaznacz pole wyboru opcji **Eksportuj klucz prywatny** i określ hasło do ochrony klucza prywatnego. Potwierdź hasło i wybierz format eksportu.

   UWAGA: Certyfikaty użytkownika można eksportować tylko w formacie `PKCS12`.
5. Kliknij przycisk **OK**, aby wyeksportować obiekt certyfikatu użytkownika.

Zatwierdzanie obiektów certyfikatu użytkownika

Aby zatwierdzić obiekt certyfikatu użytkownika, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. cert. użytk.** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat użytkownika z listy i kliknij ikonę .
4. Zostanie wyświetlone potwierdzenie informujące o pomyślnym zatwierdzeniu obiektu certyfikatu użytkownika.

Unieważnianie obiektów certyfikatu użytkownika

Aby unieważnić obiekt certyfikatu użytkownika, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. cert. użytk.** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat użytkownika z listy i kliknij ikonę .
4. Przeczytaj ze zrozumieniem informacje o ryzyku związanym z unieważnianiem certyfikatów użytkownika.
5. Z listy rozwijanej wybierz prawidłową przyczynę unieważnienia, wybierz datę utraty ważności i dodaj wszystkie pozostałe komentarze.
6. Kliknij przycisk **OK**, aby zakończyć unieważnianie.

Usuwanie obiektów certyfikatu użytkownika

Aby usunąć obiekty certyfikatu użytkownika, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. cert. użytk.** na stronie docelowej Identity Console.
2. Wybierz odpowiedni serwer z listy rozwijanej.
3. Wybierz odpowiedni certyfikat użytkownika z listy i kliknij ikonę .
4. Na następnym ekranie kliknij przycisk **OK**.
5. Zostanie wyświetlone potwierdzenie informujące o pomyślnym usunięciu obiektu certyfikatu użytkownika.

Rysunek 17-3 *Zarządzanie certyfikatami użytkownika*

Zarządzanie zaufanym certyfikatem głównym i kontenerami

Zaufany certyfikat główny stanowi podstawę relacji zaufania w kryptografii klucza publicznego. Zaufane certyfikaty główne służą do zatwierdzania certyfikatów podpisanych przez inne ośrodki certyfikacji. Zaufane certyfikaty główne umożliwiają włączenie zabezpieczeń dla protokołu SSL, bezpiecznej poczty e-mail i uwierzytelniania opartego na certyfikatach.

Przy użyciu modułu Zarządzanie zaufanymi certyfikatami głównymi można wykonywać następujące zadania:

- „Tworzenie kontenera zaufanego certyfikatu głównego” na stronie 100
- „Tworzenie obiektu zaufanego certyfikatu głównego” na stronie 101
- „Eksportowanie obiektów zaufanego certyfikatu głównego” na stronie 101
- „Zatwierdzanie obiektów zaufanego certyfikatu głównego” na stronie 102
- „Usuwanie obiektów zaufanego certyfikatu głównego” na stronie 102
- „Usuwanie kontenerów zaufanego certyfikatu głównego” na stronie 102

Tworzenie kontenera zaufanego certyfikatu głównego

Aby utworzyć kontener zaufanego certyfikatu głównego, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone.
2. Kliknij ikonę +, aby utworzyć nowy kontener zaufanego certyfikatu głównego.
3. Określ nazwę kontenera zaufanego certyfikatu głównego.

4 Za pomocą selektora obiektów znajdź odpowiedni kontener.

5 Kliknij przycisk **OK**.

6 Zostanie wyświetlone potwierdzenie informujące o pomyślnym utworzeniu kontenera zaufanego certyfikatu głównego.

Tworzenie obiektu zaufanego certyfikatu głównego

Aby utworzyć obiekt zaufanego certyfikatu głównego, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone. Zaznacz pole wyboru **Zaufany certyfikat główny**.

2 Kliknij ikonę +, aby utworzyć nowy obiekt zaufanego certyfikatu głównego.

3 Określ nazwę obiektu zaufanego certyfikatu głównego.

4 Z listy rozwijanej wybierz odpowiedni kontener zaufanego certyfikatu głównego.

5 Znajdź i wybierz odpowiedni plik certyfikatu w formacie `DER` lub `B64`.

UWAGA: W obiekcie zaufanego certyfikatu głównego można przechowywać certyfikaty dowolnego typu (certyfikaty ośrodka certyfikacji, certyfikaty pośredniego ośrodka certyfikacji lub certyfikaty użytkownika).

---

6 Kliknij przycisk **OK**.

7 Zostanie wyświetlone potwierdzenie informujące o pomyślnym utworzeniu obiektu zaufanego certyfikatu głównego.

Eksportowanie obiektów zaufanego certyfikatu głównego

Aby wyeksportować obiekty zaufanego certyfikatu głównego, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone. Zaznacz pole wyboru **Zaufany certyfikat główny**.

2 Wybierz odpowiedni zaufany certyfikat główny z listy i kliknij ikonę .

3 Na następnym ekranie zaznacz pole wyboru opcji **Eksportuj klucz prywatny** i określ hasło do ochrony klucza prywatnego. Potwierdź hasło i wybierz format eksportu.

UWAGA: Zaufane certyfikaty główne można eksportować tylko w formacie `DER` lub `BASE64`.

---

4 Kliknij przycisk **OK**, aby wyeksportować obiekt zaufanego certyfikatu głównego.

Zatwierdzanie obiektów zaufanego certyfikatu głównego

Aby zatwierdzić obiekty zaufanego certyfikatu głównego, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone. Zaznacz pole wyboru **Zaufany certyfikat główny**.
2. Wybierz odpowiedni zaufany certyfikat główny z listy i kliknij ikonę .
3. Zostanie wyświetlone potwierdzenie informujące o pomyślnym zatwierdzeniu obiektu zaufanego certyfikatu głównego.

Usuwanie obiektów zaufanego certyfikatu głównego

Aby usunąć obiekty zaufanego certyfikatu głównego, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone. Zaznacz pole wyboru **Zaufany certyfikat główny**.
2. Wybierz odpowiedni zaufany certyfikat główny z listy i kliknij ikonę .
3. Na ekranie ostrzeżenia kliknij przycisk **OK**.
4. Zostanie wyświetlone potwierdzenie informujące o pomyślnym usunięciu obiektu zaufanego certyfikatu głównego.

Usuwanie kontenerów zaufanego certyfikatu głównego

Aby usunąć kontener zaufanego certyfikatu głównego, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Zarządz. zaufan. certyf. głównymi** na stronie docelowej Identity Console. Pole wyboru **Kontener zaufanego certyfikatu głównego** będzie domyślnie zaznaczone.
2. Wybierz odpowiedni kontener zaufanego certyfikatu głównego z listy i kliknij ikonę .
3. Na ekranie ostrzeżenia kliknij przycisk **OK**.
4. Zostanie wyświetlone potwierdzenie informujące o pomyślnym usunięciu kontenera zaufanego certyfikatu głównego.

Rysunek 17-4 *Zarządzanie kontenerami zaufanego certyfikatu głównego*

Tworzenie domyślnych obiektów certyfikatu serwera

Instalacja modułu Certificate Server powoduje utworzenie domyślnych obiektów certyfikatu serwera.

- SSL CertificateDNS — *nazwa_serwera*
- Certyfikat dla każdego adresu IP skonfigurowanego na serwerze (IPAG*xxx.xxx.xxx.xxx* — *nazwa_serwera*)
- Certyfikat dla każdej nazwy DNS skonfigurowanej na serwerze (DNSAG*www.example.com* — *nazwa_serwera*)

UWAGA: Usługa eDirectory nie tworzy automatycznie certyfikatu SSL CertificateIP. SSL Certificate DNS zawiera listę wszystkich adresów IP wymienionych w obszarze Nazwa alternatywna podmiotu. Próby tworzenia lub naprawiania certyfikatów domyślnych przy użyciu portalu Identity Console domyślnie nie powodują utworzenia ani naprawienia certyfikatu SSL CertificateIP. Jednak w interfejsie dodatku typu plug-in znajduje się pole wyboru, które można zaznaczyć, aby zastąpić zachowanie domyślne i wymusić utworzenie/naprawienie certyfikatu SSL CertificateIP.

Jeśli wewnętrzny ośrodek certyfikacji ma certyfikat ECDSA, usługa eDirectory w wersji 9.0 lub nowszej automatycznie tworzy certyfikaty ECDSA.

Jeśli z jakiegoś powodu te certyfikaty staną się uszkodzone lub nieważne albo jeśli chcesz tylko zastąpić istniejące certyfikaty domyślne, możesz użyć kreatora tworzenia domyślnych certyfikatów serwera, zgodnie z opisem w poniższej procedurze:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Certyfikaty domyślne** na stronie docelowej Identity Console.
2. Wybierz serwery, dla których chcesz utworzyć certyfikaty domyślne, a następnie kliknij przycisk **Dalej**.

3 Wybierz opcję Tak, jeśli chcesz zastąpić istniejące domyślne certyfikaty serwera, lub opcję Nie, jeśli chcesz zastąpić istniejące domyślne certyfikaty serwera tylko w przypadku, gdy są one nieważne.

4 (Dotyczy tylko pojedynczego serwera) Jeśli chcesz użyć istniejącego adresu DNS, wybierz tę opcję. Jeśli chcesz użyć innego adresu DNS, wybierz tę opcję i określ nowy adres DNS.

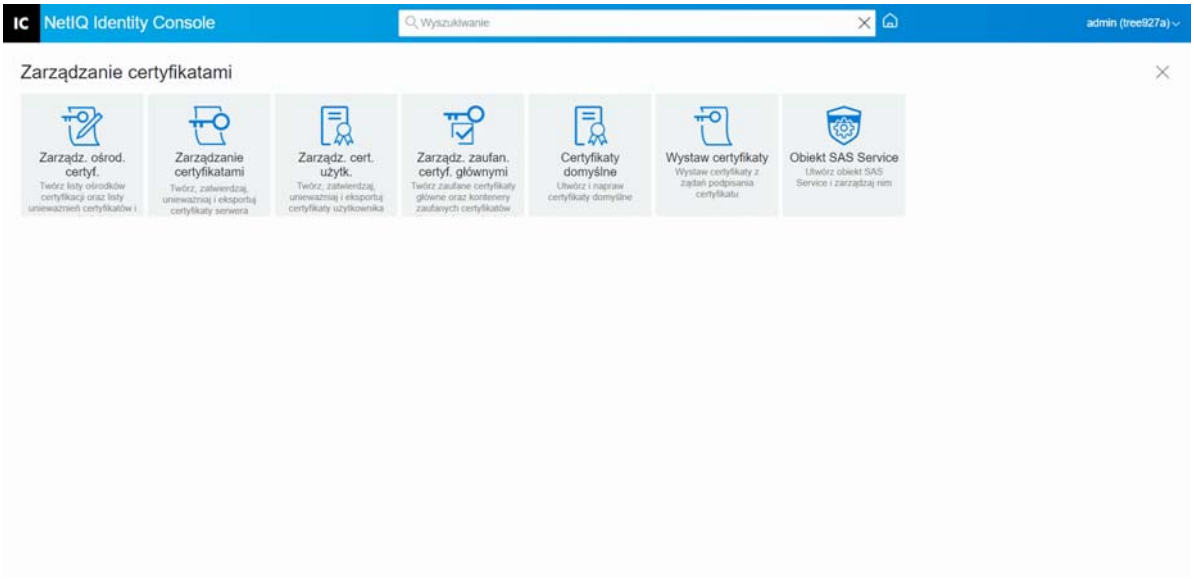
5 (Dotyczy tylko pojedynczego serwera) Jeśli chcesz użyć istniejącego domyślnego adresu IP, wybierz tę opcję. Jeśli chcesz użyć innego adresu IP, wybierz tę opcję i określ nowy adres IP.

6 Kliknij przycisk **Dalej**.

7 Przejrzyj stronę podsumowania, a następnie kliknij przycisk **Zakończ**.

Jeśli potrzebna jest większa kontrola nad tworzeniem obiektu certyfikatu serwera, można utworzyć go ręcznie. Aby uzyskać więcej informacji, zobacz „Tworzenie obiektów certyfikatu serwera” na stronie 95.

Rysunek 17-5 *Tworzenie domyślnych obiektów certyfikatu serwera*



Wystawianie certyfikatu klucza publicznego

Wewnętrzny ośrodek certyfikacji działa w taki sam sposób jak zewnętrzny. Oznacza to, że ma możliwość wystawiania certyfikatów z żądań podpisania certyfikatu (CSR). Używając wewnętrznego ośrodka certyfikacji, można wystawiać certyfikaty, gdy użytkownik wysyła żądanie podpisania certyfikatu. Użytkownik żądający certyfikatu może następnie zaimportować wystawiony certyfikat bezpośrednio do aplikacji z włączoną obsługą kryptografii.

To zadanie umożliwia generowanie certyfikatów dla aplikacji obsługujących kryptografię, które nie rozpoznają obiektów certyfikatu serwera.

Aby wystawić certyfikat, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie certyfikatami** > **Wystaw certyfikaty** na stronie docelowej Identity Console.

2 Znajdź i wybierz plik CSR.

3 W obszarze Specyfikacje użycia klucza wybierz właściwy typ klucza i odpowiadający mu sposób wykorzystania klucza. Te opcje umożliwiają wybranie typu klucza. Z każdym typem klucza są skojarzone wstępnie zdefiniowane wartości użycia klucza:

3a **Nieokreślone:** Ta opcja jest zaznaczona domyślnie i nie aktywuje żadnego sposobu wykorzystania klucza w certyfikacie.

3b **Ośrodek certyfikacji:** Ta opcja aktywuje dwa sposoby wykorzystania klucza — podpisywanie certyfikatu i podpisywanie listy CRL.

3c **Szyfrowanie:** Ta opcja aktywuje wykorzystanie klucza w celu szyfrowania kluczy.

3d **Podpis:** Ta opcja aktywuje wykorzystanie klucza w roli podpisu elektronicznego.

3e **SSL lub TLS:** Ta opcja konfiguruje klucz tak, aby można go było używać w transakcjach SSL lub TLS.

3f **Niestandardowy:** Ta opcja umożliwia ręczne wybranie dowolnej lub wszystkich opcji użycia klucza.

3g **Ustaw rozszerzenie użycia klucza jako krytyczne:** Rozszerzenie użycia klucza można oznaczyć jako krytyczne w przypadku każdego typu klucza z wyjątkiem typu Nieokreślone. Każde rozszerzenie krytyczne musi być zrozumiałe dla oprogramowania odbierającego, aby certyfikat mógł zostać użyty w jakimkolwiek celu. Z tego względu zaznaczenie rozszerzenia jako krytycznego wiąże się z pewnym ryzykiem, ponieważ nie wszystkie aplikacje mogą korzystać z tego certyfikatu. Jednak dla dobrze znanych rozszerzeń, takich jak użycie klucza, ryzyko to jest minimalne. Ogólnie rzecz biorąc, jeśli określone jest użycie klucza, to rozszerzenie powinno być ustawione jako krytyczne.

4 Można określić zakodowanie rozszerzenia **Użycie klucza rozszerzonego** w certyfikacie. Aby aktywować tę funkcję, należy wybrać opcję **Włącz użycie klucza rozszerzonego**:

4a **Serwer:** Ta opcja aktywuje użycie klucza rozszerzonego Uwierzytelnianie serwera.

4b **Użytkownik:** Ta opcja aktywuje użycie klucza rozszerzonego Uwierzytelnianie użytkownika i Ochrona poczty e-mail.

4c **Niestandardowy:** Ta opcja umożliwia wybór dowolnej lub wszystkich opcji użycia klucza rozszerzonego.

4d **Dowolny:** Umożliwia użycie klucza w dowolnym rozszerzonym użyciu klucza.

4e **Ustaw rozszerzenie rozszerzonego użycia klucza jako krytyczne:** Każde rozszerzenie krytyczne musi być zrozumiałe dla oprogramowania odbierającego, aby certyfikat mógł zostać użyty w jakimkolwiek celu. Z tego względu zaznaczenie rozszerzenia jako krytycznego wiąże się z pewnym ryzykiem, ponieważ nie wszystkie aplikacje mogą korzystać z tego certyfikatu. Ponieważ wiele aplikacji nie obsługuje rozszerzenia zaawansowanego użycia klucza, oznaczenie tego rozszerzenia jako krytycznego wiąże się ze znacznym ryzykiem braku akceptacji certyfikatu przez daną aplikację. Z tego względu ustawianie go jako krytycznego powinno mieć miejsce tylko w razie konieczności.

5 Wybierz odpowiednie **ograniczenia podstawowe**:

5a Typ certyfikatu:

5a1 Nieokreślone: Tę opcję należy wybrać, jeśli do certyfikatu nie ma zostać dodane rozszerzenie ograniczenia podstawowego.

5a2 Ośrodek certyfikacji: Tę opcję należy wybrać, aby dodać do certyfikatu rozszerzenie ograniczenia podstawowego ośrodka certyfikacji. Jeśli certyfikat jest przeznaczony dla ośrodka certyfikacji, wybór tej opcji jest konieczny.

5a3 Jednostka końcowa: Tę opcję należy wybrać, aby dodać do certyfikatu rozszerzenie ograniczenia podstawowego określające, że jest to certyfikat jednostki końcowej (podmiot nie jest ośrodkiem certyfikacji). Uwaga: jeśli certyfikat jest typu Jednostka końcowa, długość ścieżki powinna zostać ustawiona na wartość Nieokreślone.

5b Długość ścieżki:

5b1 Nieokreślone: Tę opcję należy wybrać, jeśli liczba poziomów podrzędnych ośrodków certyfikacji, które można utworzyć poniżej danego ośrodka certyfikacji, nie ma być określana.

UWAGA: Jeśli certyfikat jest typu Jednostka końcowa, długość ścieżki powinna zostać ustawiona na wartość Nieokreślone.

5b2 Określona: Tę opcję należy wybrać, jeśli określona ma zostać liczba poziomów podrzędnych ośrodków certyfikacji, które można utworzyć poniżej tego ośrodka certyfikacji. Klikając strzałkę w górę i strzałkę w dół, można określić długość tej ścieżki.

UWAGA: Jeśli tworzony certyfikat jest podrzędnym ośrodkiem certyfikacji, długość ścieżki musi być spójna z ustawieniami nadrzędnego ośrodka certyfikacji. Jeśli na przykład długość ścieżki w nadrzędnym ośrodku certyfikacji została ustawiona na wartość 3, to w podrzędnym ośrodku certyfikacji długość ścieżki musi mieć wartość 2 lub mniejszą. Jeśli nadrzędny ośrodek certyfikacji nie ma określonej długości ścieżki, podrzędny ośrodek może również nie mieć określonej długości ścieżki lub też mieć dowolną żądaną długość ścieżki.

5c Ustaw rozszerzenie ograniczeń podstawowych jako krytyczne: Zwykle rozszerzenie ograniczeń podstawowych musi być ustawione jako krytyczne dla certyfikatów ośrodków certyfikacji. Każde rozszerzenie krytyczne musi być zrozumiałe dla oprogramowania odbierającego, aby certyfikat mógł zostać użyty w jakimkolwiek celu. Z tego względu zaznaczenie rozszerzenia jako krytycznego wiąże się z pewnym ryzykiem, ponieważ nie wszystkie aplikacje mogą korzystać z tego certyfikatu. Jednak dla dobrze znanych rozszerzeń, takich jak ograniczenia podstawowe, ryzyko to jest minimalne.

6 Określ następujące parametry certyfikatu:

6a Nazwa podmiotu: W tym polu jest wyświetlana wpisana w pełnej formie nazwa drzewa eDirectory.

6b Nazwa podmiotu: W tym polu jest wyświetlana wpisana w pełnej formie nazwa drzewa eDirectory.

6c Okres ważności: Korzystając z listy rozwijanej, należy określić okres, w którym certyfikat będzie ważny. Zakres może wahać się od sześciu miesięcy aż do terminu w roku 2036 (jest to maksymalna wartość wynikająca z zastosowania liczb 32-bitowych do zapisu czasu). Po

wybraniu opcji Określ daty można utworzyć niestandardowy okres ważności, edytując pola Data efektywna i Data wygaśnięcia. Najpóźniejsza wybrana data musi przypadać w okresie ważności ośrodka certyfikacji.

6c1 **Data efektywna:** Umożliwia wyświetlanie lub edycję daty i godziny określających moment, w którym certyfikat nabierze ważności.

6c2 **Data wygaśnięcia:** Umożliwia wyświetlanie lub edycję daty i godziny wygaśnięcia ważności certyfikatu.

6d **Rozszerzenia niestandardowe:** Ta funkcja umożliwia serwerowi certyfikatów obsługiwanie dowolnych standardowych lub niestandardowych rozszerzeń, które można dołączać podczas tworzenia certyfikatu. Rozszerzenia należy wcześniej utworzyć i zapisać w pliku (jedno rozszerzenie w jednym pliku). Wszystkie rozszerzenia muszą być zakodowane w standardzie ASN.1 zgodnie z definicją w sekcji 4.2 dokumentu IETF RFC 2459/3280.

Aby dołączyć jedno lub więcej rozszerzeń niestandardowych do tworzonego certyfikatu, należy kliknąć przycisk Nowy, a następnie odszukać plik zawierający rozszerzenie niestandardowe i dodać go do certyfikatu. Powtarzając ten proces, można dodać kolejne rozszerzenia.

Aby usunąć plik rozszerzeń niestandardowych, należy go zaznaczyć, a następnie kliknąć ikonę  .

7 Wybierz odpowiedni format certyfikatu spośród następujących opcji:

7a **Plik w formacie binarnym DER:** Ta opcja umożliwia zapisanie lub wyeksportowanie certyfikatu do pliku wyświetlanego w polu Nazwa pliku. Domyślnie plik ten jest zapisywany z rozszerzeniem `DER` w katalogu głównym dysku C: stacji roboczej Identity Console z systemem Windows i w katalogu domowym użytkownika stacji roboczej Identity Console z systemem Linux.

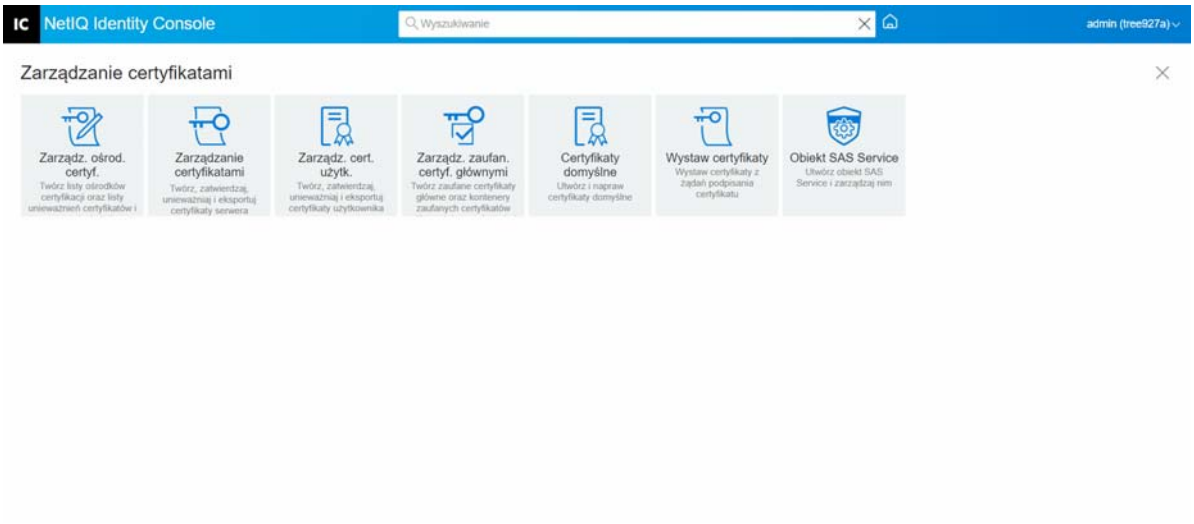
7b **Plik w formacie Base64:** Ta opcja umożliwia zapisanie pliku CSR lub wyeksportowanie certyfikatu do pliku wyświetlanego w polu Nazwa pliku. Domyślnie plik ten jest zapisywany z rozszerzeniem B64 w katalogu głównym dysku C: stacji roboczej Identity Console z systemem Windows i w katalogu domowym użytkownika stacji roboczej Identity Console z systemem Linux.

7c **Plik w formacie CER:** Ta opcja umożliwia zapisanie pliku CSR lub wyeksportowanie certyfikatu do pliku wyświetlanego w polu Nazwa pliku. Domyślnie plik ten jest zapisywany z rozszerzeniem CER w katalogu głównym dysku C: stacji roboczej Identity Console z systemem Windows i w katalogu domowym użytkownika stacji roboczej Identity Console z systemem Linux.

8 Przejrzyj podsumowanie certyfikatu na następnym ekranie i kliknij przycisk **OK**.

9 Zostanie wyświetlone potwierdzenie informujące o pomyślnym wystawieniu certyfikatu.

Rysunek 17-6 *Wystawianie certyfikatu klucza publicznego*



Zarządzanie obiektem usługi SAS Service

Obiekt usługi SAS Service zapewnia komunikację między serwerem a jego certyfikatami. Jeśli serwer zostanie usunięty z drzewa eDirectory, należy również usunąć skojarzony z tym serwerem obiekt usługi SAS Service. Jeśli serwer ma zostać umieszczony z powrotem w drzewie, należy dla tego serwera utworzyć nowy obiekt usługi SAS Service. W przeciwnym razie nie będzie można tworzyć nowych certyfikatów serwera.

Obiekt usługi SAS Service jest tworzony automatycznie w ramach kontroli stanu serwera. Nie należy tworzyć go ręcznie.

Nowy obiekt usługi SAS Service zostanie utworzony pod warunkiem, że w kontenerze, w którym znajduje się obiekt serwera, nie znajduje się żaden poprawnie nazwany obiekt usługi SAS Service. Na przykład dla serwera o nazwie WAKE zostanie utworzony obiekt usługi SAS Service o nazwie SAS Service — WAKE. Narzędzie dodaje wskaźniki DS z obiektu serwera do obiektu SAS, a z obiektu SAS do obiektu serwera, ponadto ustawia prawidłowe wpisy ACL w obiekcie usługi SAS Service.

Jeśli obiekt usługi SAS Service już istnieje i ma poprawną nazwę, nie można utworzyć nowego obiektu. Stary obiekt usługi SAS Service może zawierać uszkodzone wskaźniki DS lub nie zawierać ich wcale, a wpisy ACL mogą być nieprawidłowe. W takim przypadku można usunąć uszkodzony obiekt usługi SAS Service i za pomocą portalu Identity Console utworzyć nowy.

Tworzenie lub usuwanie obiektu usługi SAS Service

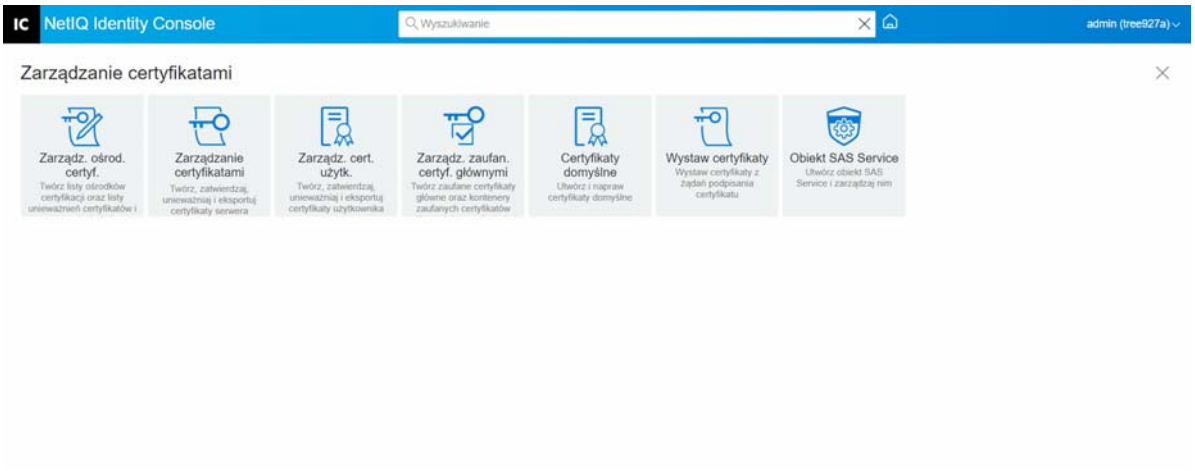
Aby utworzyć lub usunąć obiekt usługi SAS Service, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie certyfikatami** > **Obiekt SAS Service** na stronie docelowej Identity Console.
2. Jeśli dla istniejącego serwera nie utworzono obiektu usługi SAS Service, kliknij ikonę +, aby utworzyć nowy.
3. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym utworzeniu obiektu usługi SAS Service.

4 Aby usunąć obiekt usługi SAS Service, kliknij ikonę .

5 Na ekranie potwierdzenia kliknij przycisk **OK**, aby pomyślnie usunąć obiekt usługi SAS Service.

Rysunek 17-7 *Zarządzanie obiektami usługi SAS Service*



18 Zarządzanie systemem uwierzytelniania

Przy użyciu modułu Uwierzytelnianie można wykonywać następujące zadania:

Zarządzanie metodami i sekwencjami logowania i do użycia po logowaniu

NMAS obejmuje obsługę kilku metod logowania i do użycia po logowaniu od NetIQ oraz innych deweloperów uwierzytelniania. Niektóre metody wymagają dodatkowego sprzętu i oprogramowania. Użytkownik powinien się upewnić, że ma cały niezbędny sprzęt i oprogramowanie dla metod, których będzie używał.

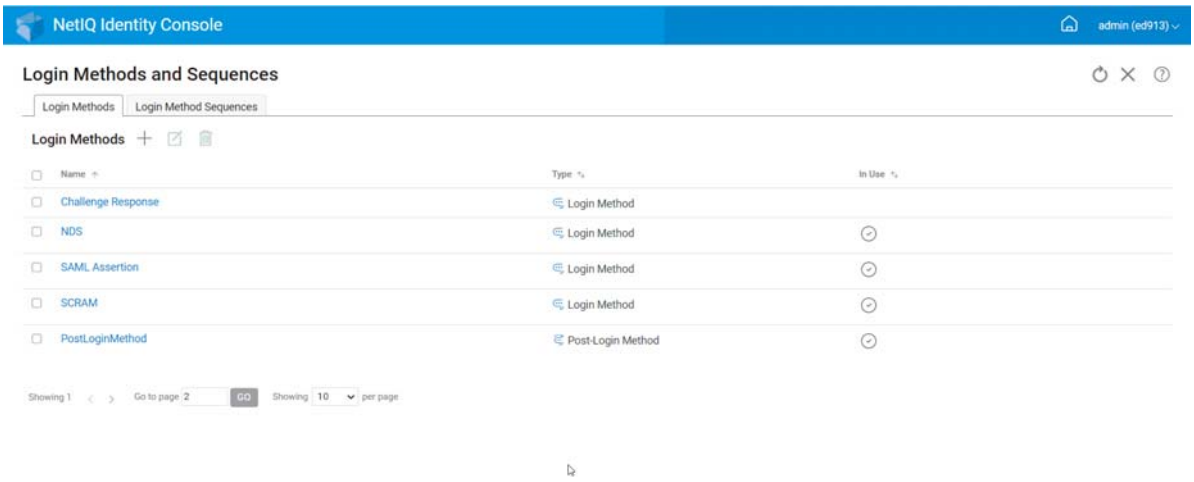
W tej sekcji opisano sposób instalowania, ustawiania oraz konfigurowania metod i sekwencji logowania/do użycia po logowaniu dla NMAS.

Instalowanie metody logowania lub metody do użycia po logowaniu

Aby zainstalować metodę logowania, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby zainstalować nową metodę logowania.
3. Znajdź i wybierz plik (ZIP) metody logowania, który chcesz zainstalować, a następnie kliknij przycisk **Dalej**.
4. Wykonaj instrukcje kreatora instalacji, aby ukończyć proces instalowania metody logowania.

Rysunek 18-1 *Instalowanie nowej metody logowania*

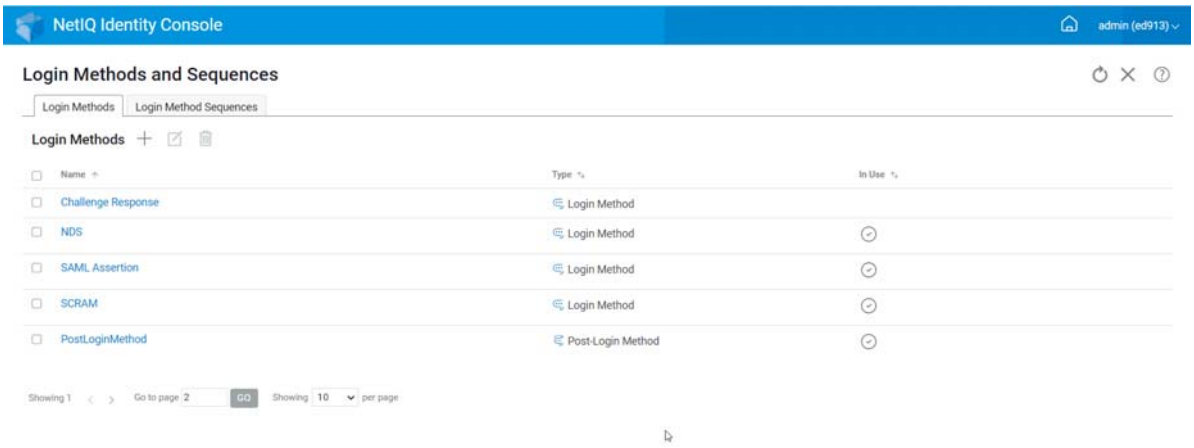


Aktualizowanie istniejącej metody logowania lub metody do użycia po logowaniu

Aby zaktualizować istniejącą metodę logowania, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz z listy metodę logowania, którą chcesz zaktualizować, i kliknij ikonę ☑.
3. Znajdź i wybierz plik (ZIP) metody logowania, którą chcesz zaktualizować, a następnie kliknij przycisk **Dalej**.
4. Wykonaj instrukcje kreatora aktualizacji, aby ukończyć aktualizowanie metody logowania.

Rysunek 18-2 *Aktualizowanie istniejącej metody logowania*

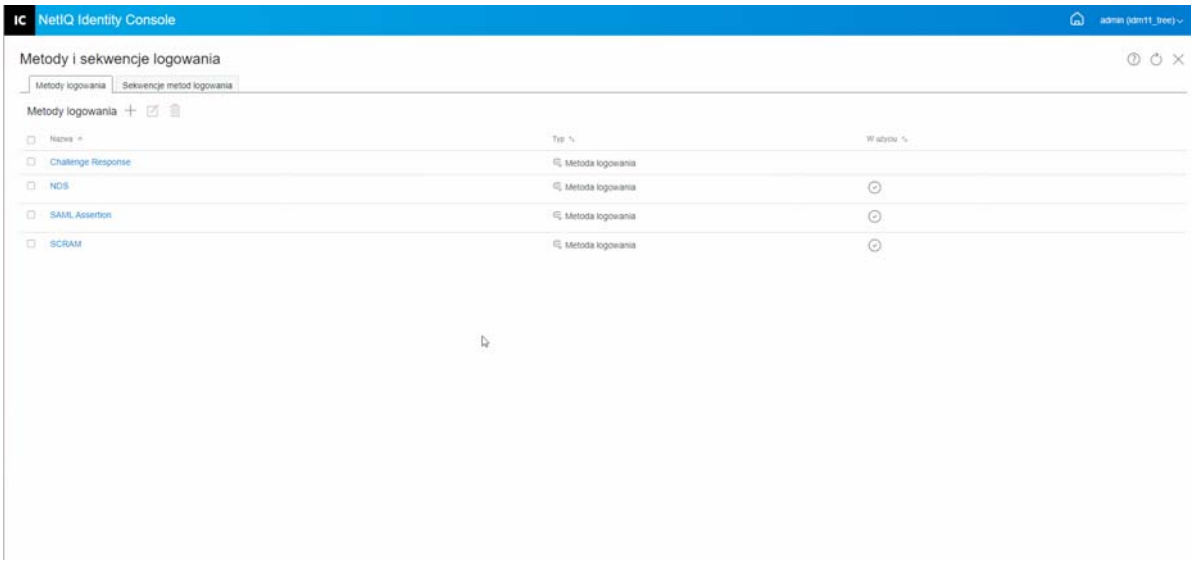


Odinstalowywanie metod logowania lub metod do użycia po logowaniu

Aby odinstalować metody logowania lub metody do użycia po logowaniu, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz z listy metody logowania, które chcesz odinstalować, i kliknij ikonę 🗑.
3. Na następnym ekranie kliknij przycisk **OK**.
4. Zostanie wyświetlony komunikat potwierdzenia informujący o odinstalowaniu metod logowania.

Rysunek 18-3 *Odinstalowywanie metody logowania*



Tworzenie nowej sekwencji metod logowania

Gdy w środowisku są utworzone różne metody logowania, można zadecydować, w jakiej kolejności powinny być używane. Aby utworzyć nową sekwencję metod logowania, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz kartę **Sekwencje metod logowania**.
3. Kliknij ikonę +, aby utworzyć nową sekwencję metod logowania.
4. Określ **nazwę** i wybierz **typ sekwencji**.
5. Z listy dostępnych metod logowania i metod do użycia po logowaniu wybierz te, które są wymagane.

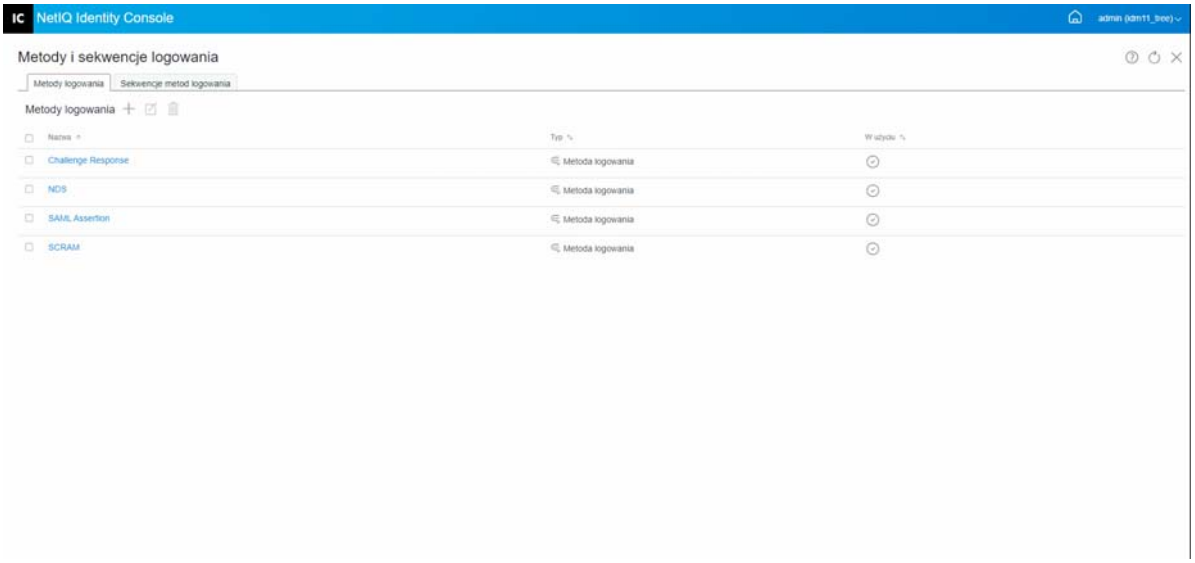
UWAGA: Kolejność metod logowania można określić, klikając strzałki w górę i w dół widoczne na obiektach metod logowania.

---

6 Kliknij przycisk **Utwórz**.

7 Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym utworzeniu nowej sekwencji metod logowania.

Rysunek 18-4 *Tworzenie sekwencji metod logowania*



Modyfikowanie sekwencji metod logowania

Aby zmodyfikować istniejącą sekwencję metod logowania, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.

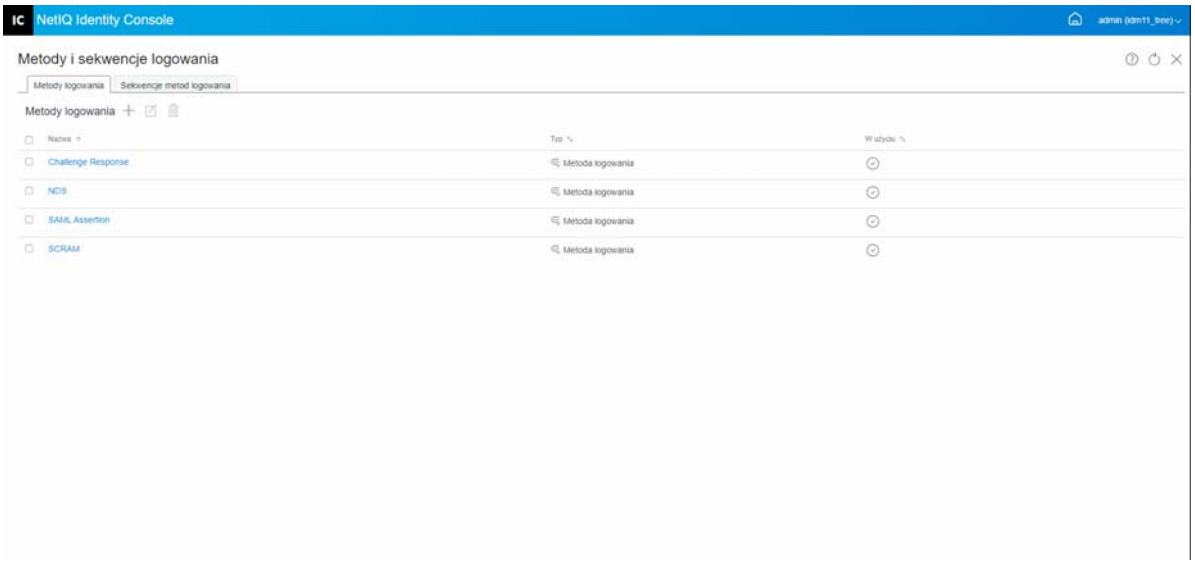
2 Wybierz kartę **Sekwencje metod logowania**.

3 Kliknij ikonę ☑, aby zmodyfikować istniejącą sekwencję metod logowania.

4 Wprowadź niezbędne zmiany na stronie **Modyfikuj sekwencję metod logowania** i kliknij przycisk **Zapisz**.

5 Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym zmodyfikowaniu sekwencji metod logowania.

Rysunek 18-5 *Modyfikowanie sekwencji metod logowania*

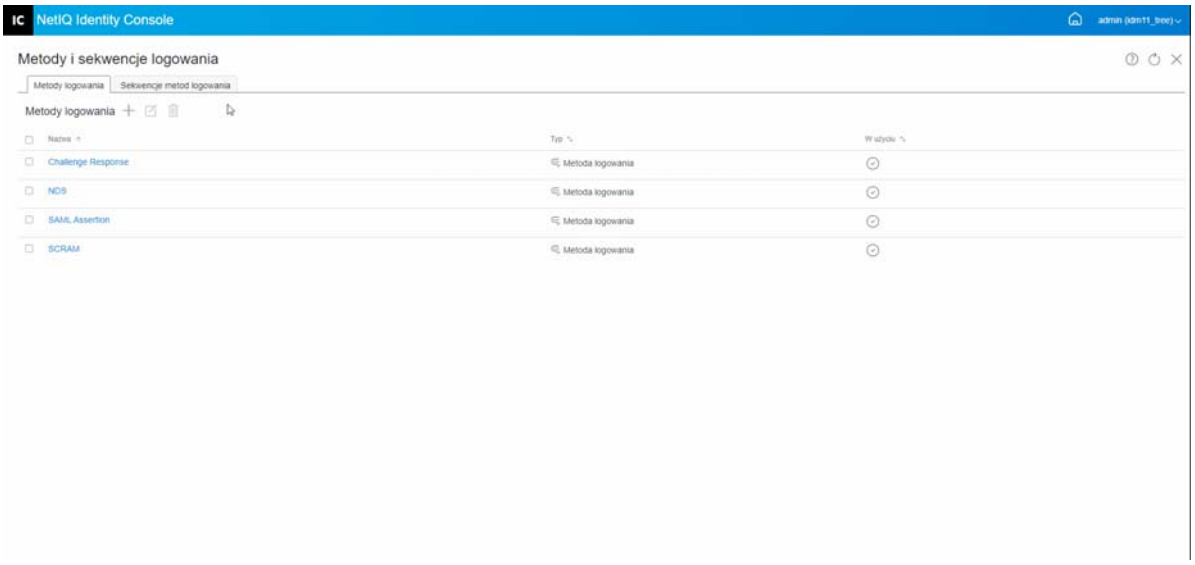


Autoryzowanie i cofanie autoryzacji sekwencji metod logowania

Sekwencja metod logowania powinna być autoryzowana i ustawiona jako domyślna, aby można było skojarzyć ją z użytkownikami, kontenerami i partycjami. Aby autoryzować sekwencję metod logowania, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz kartę **Sekwencje metod logowania**.
3. Wybierz odpowiednią sekwencję metod logowania z listy i kliknij ikonę ⓥ.
4. Aby wycofać autoryzację sekwencji metod logowania, wybierz ją i kliknij ikonę ⓧ.
5. Sekwencję metod logowania możesz również autoryzować i cofać jej autoryzację za pomocą menu rozwijanego w kolumnie **Autoryzowane** na liście Sekwencje metod logowania.

Rysunek 18-6 *Autoryzowanie i cofanie autoryzacji sekwencji metod logowania*

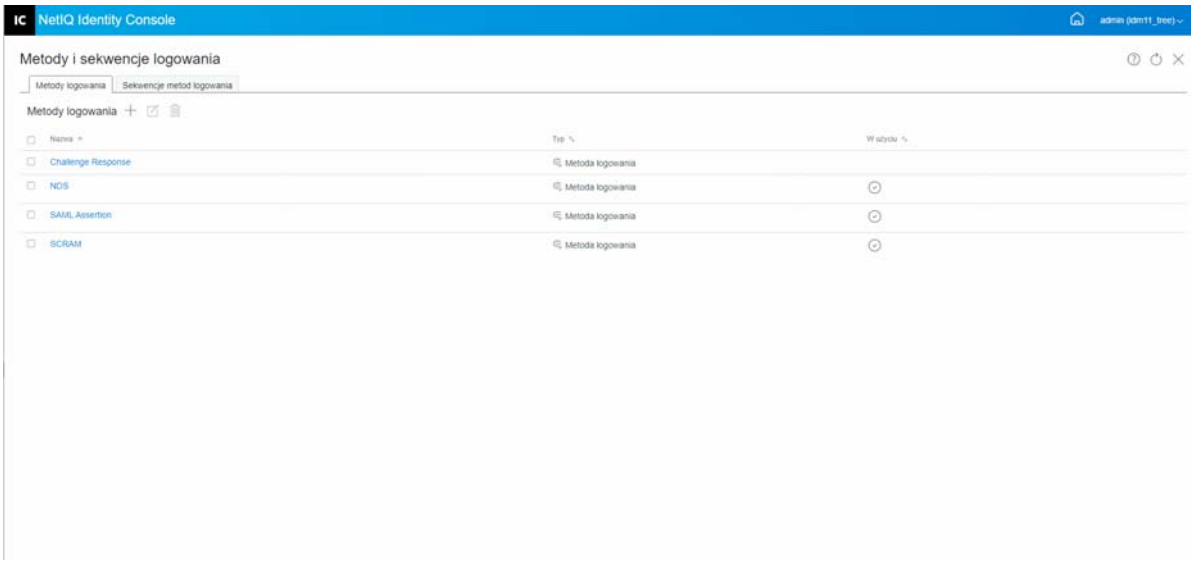


Ustawianie domyślnej sekwencji metod logowania

Aby ustawić domyślną sekwencję metod logowania, dzięki której użytkownicy nie będą musieli określać jej podczas logowania:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz kartę **Sekwencje metod logowania**.
3. Włącz ikonę , aby ustawić autoryzowaną sekwencję metod logowania jako domyślną.

Rysunek 18-7 *Ustawianie domyślnej sekwencji metod logowania*

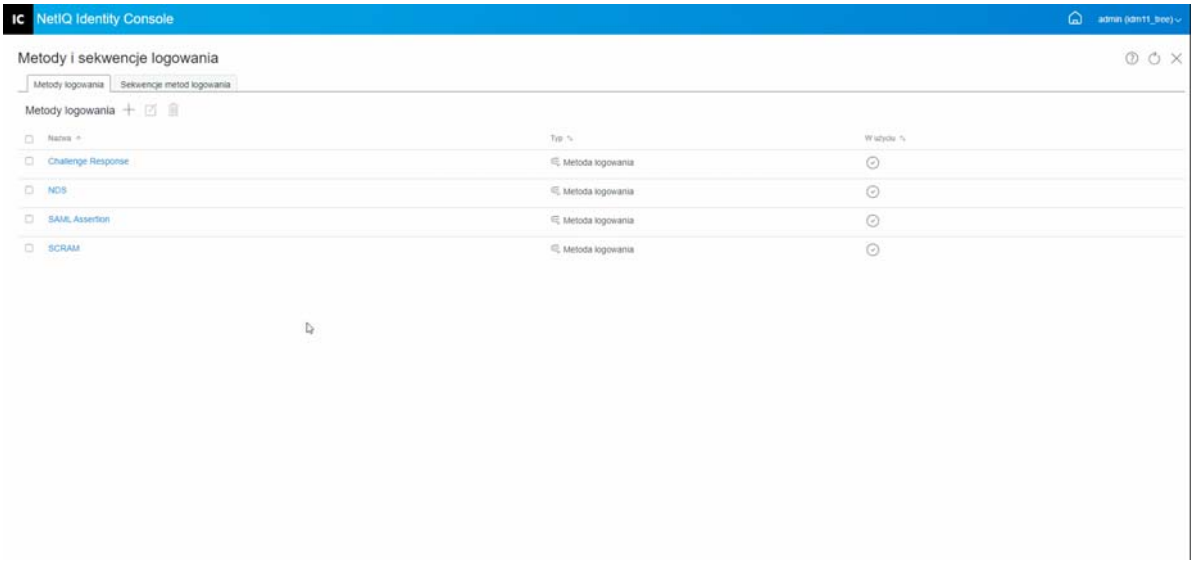


Usuwanie sekwencji metod logowania

Aby usunąć sekwencję metod logowania:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Metody i sekwencje logowania** na stronie docelowej Identity Console.
2. Wybierz kartę **Sekwencje metod logowania**.
3. Wybierz odpowiednią sekwencję metod logowania z listy i kliknij ikonę .
4. Na następnym ekranie potwierdzenia kliknij przycisk **OK**.

Rysunek 18-8 *Usuwanie sekwencji metod logowania*



Zarządzanie założeniami haseł

Założenia haseł to kolekcja zdefiniowanych przez administratora reguł, które określają kryteria tworzenia i zamieniania haseł użytkowników końcowych. NMAS umożliwia wymuszanie założeń haseł przypisywanych do użytkowników w usłudze eDirectory. Założenia haseł mogą również obejmować samoobsługową funkcję Zapomniane hasło, która pozwala ograniczyć liczbę połączeń ze stanowiskiem pomocy technicznej w sprawie zapomnianych haseł. Inną samoobsługową funkcją jest Zresetowanie hasła. Pozwala ona użytkownikom zmieniać ich hasła zgodnie z regułami określonymi przez administratora w założeniach haseł. Użytkownicy mogą uzyskać dostęp do tych funkcji za pośrednictwem aplikacji Identity Manager User Application lub Identity Console.

Przy użyciu modułu Założenia haseł można wykonywać następujące zadania:

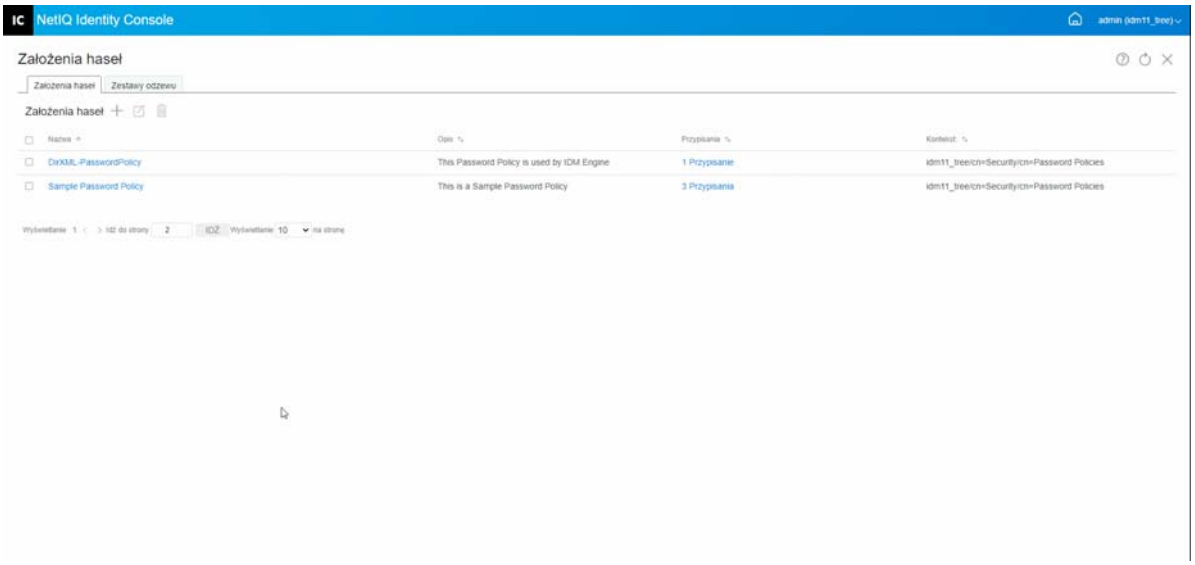
- „Tworzenie założeń haseł za pomocą ustawień domyślnych” na stronie 118
- „Tworzenie założeń haseł za pomocą ustawień niestandardowych” na stronie 118
- „Modyfikowanie założeń haseł” na stronie 121
- „Usuwanie założeń haseł” na stronie 122

Tworzenie założeń haseł za pomocą ustawień domyślnych

Aby utworzyć nowe założenia haseł, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby utworzyć nowe założenia haseł.
3. Na następnym ekranie określ nazwę, kontekst, opis i komunikat dotyczący zmiany hasła.
4. Jeśli chcesz utworzyć założenia haseł za pomocą ustawień domyślnych, zaznacz pole wyboru **Utwórz nowe założenia haseł na podstawie ustawień domyślnych** i kliknij przycisk **Dalej**, aby wyświetlić stronę **Podsumowanie**.
5. Zweryfikuj szczegóły na stronie **Podsumowanie** i kliknij przycisk **Utwórz**.
6. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym utworzeniu założeń haseł.

Rysunek 18-9 *Tworzenie założeń haseł za pomocą ustawień domyślnych*



Tworzenie założeń haseł za pomocą ustawień niestandardowych

Aby utworzyć założenia haseł za pomocą ustawień niestandardowych, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby utworzyć nowe założenia haseł.
3. Na następnym ekranie określ nazwę, kontekst, opis i komunikat dotyczący zmiany hasła.
4. Jeśli chcesz utworzyć założenia haseł za pomocą ustawień niestandardowych, kliknij przycisk **Dalej**.

5 Na stronie **Konfiguracja** wykonaj następujące działania:

5a Włącz hasło uniwersalne: Włączenie hasła uniwersalnego dla założeń umożliwia korzystanie z opcji udostępnianych przez funkcję Założenia haseł. Jednak warunkiem włączenia hasła uniwersalnego dla założeń jest spełnienie wymagań wstępnych dla hasła uniwersalnego w danym środowisku.

5b Włącz zaawansowane reguły hasła: Ta opcja włącza reguły haseł dostępne na karcie Zaawansowane reguły hasła. Reguły te zwiększają bezpieczeństwo środowiska, ponieważ zapewniają użytkownikowi kontrolę nad kryteriami, na przykład czasem obowiązywania hasła i zawartością hasła, taką jak kombinacja liter, cyfr, wielkich lub małych liter i znaków specjalnych. Można również wykluczyć hasła, które nie wydają się bezpieczne, takie jak nazwa firmy.

5c Synchronizacja haseł: Te opcje określają sposób synchronizacji hasła uniwersalnego w usłudze eDirectory z hasłami innego typu w bezpiecznych magazynach tożsamości. Synchronizacja haseł zawiera następujące opcje:

5c1 Usuń hasło NDS podczas ustawiania hasła: Jeżeli ta opcja zostanie zaznaczona, hasło NDS zostanie wyłączone po ustawieniu hasła uniwersalnego. Użytkownicy nie będą mogli korzystać ze starszych metod lub narzędzi, które logują się bezpośrednio za pomocą hasła NDS, zamiast komunikować się z usługami NMAS. Po ustawieniu tej opcji kolejna opcja **Synchronizuj hasło NDS podczas ustawiania hasła** będzie domyślnie wyłączona.

5c2 Synchronizuj hasło NDS podczas ustawiania hasła: Po zaznaczeniu tej opcji ustawienie hasła uniwersalnego w aplikacjach, takich jak Identity Console, powoduje również zmianę hasła NDS.

5c3 Synchronizuj proste hasło podczas ustawiania hasła: Ta opcja zapewnia zgodność z klientami NetIQ i innych firm używającymi prostego hasła i zaopatrywania użytkownika.

5c4 Synchronizuj hasło dystrybucyjne podczas ustawiania hasła: Ta opcja określa, czy za pomocą mechanizmu metakatalogów można odczytać lub ustawić hasło uniwersalne użytkownika w usłudze eDirectory.

5d Pobieranie uniwersalnego hasła: Dostępne są następujące opcje:

5d1 Zezwalaj użytkownikowi na pobieranie hasła: Zezwala agentowi użytkownika na pobieranie hasła. Ta opcja określa, czy samoobsługowa funkcja Zapomniane hasło może odczytać hasło w imieniu użytkownika w celu wysłania go do tego użytkownika pocztą e-mail. Jeśli ta opcja nie jest zaznaczona, odpowiednia funkcja jest wygaszona na karcie Zapomniane hasło w założeniach haseł.

5d2 Zezwalaj administratorowi na pobieranie haseł: To pole należy zaznaczyć, jeśli istnieje określona usługa, która go potrzebuje. W Identity Manager nie występuje potrzeba, aby administratorzy pobierali hasła. Jednak niektóre usługi innych firm mogą korzystać z tej opcji.

5d3 Zezwalaj następującym obiektom na pobieranie haseł: Klikając ikonę +, wybierz odpowiedniego użytkownika, który powinien pobierać hasło.

5e Uwierzytelnianie:

5e1 Weryfikuj, czy istniejące hasła są zgodne z założeniami haseł (weryfikacja następuje podczas logowania): Ta opcja jest użyteczna w przypadku wdrażania nowych założeń haseł lub zmieniania zaawansowanych reguł hasła dla istniejących założeń. Pozwala ona zapewnić zgodność istniejących haseł z nowymi lub zmienionymi regułami.

Zaznaczenie tej opcji powoduje, że podczas logowania hasła użytkowników są analizowane w celu zapewnienia zgodności z zaawansowanymi regułami hasła w nowych lub zmienionych założeniach haseł. Jeśli istniejące hasło okaże się niezgodne, użytkownik będzie musiał je zmienić.

Po zakończeniu kliknij przycisk **Dalej**.

6 **Zaawansowane reguły hasła** zwiększają bezpieczeństwo środowiska, zapewniając kontrolę nad szczegółami hasła, takimi jak czas obowiązywania hasła, częstotliwość zmiany hasła i zawartość hasła.

Znaki specjalne to znaki, które nie są cyframi (0–9) ani literami alfabetu.

Na stronie Zaawansowane reguły hasła wykonaj następujące działania:

6a Używając składni Microsoft Complexity Policy (przed systemem Microsoft Windows Server 2008), Microsoft Server 2008 Password Policy lub Novell, możesz zarządzać ustawieniami składni.

6b W kreatorze określ wymagane opcje Zmiana hasła, Czas obowiązywania hasła, Długość i skład hasła oraz Wykluczenia haseł, a następnie kliknij przycisk **Dalej**.

7 Włączając samoobsługową funkcję **Zapomniane hasło** z myślą o użytkownikach, którzy zapomnieli hasła, można zredukować koszty związane z prowadzeniem centrum pomocy technicznej. Te samoobsługowe funkcje są udostępniane użytkownikom za pośrednictwem portalu Identity Console. Na stronie Zapomniane hasło wykonaj następujące działania:

UWAGA: Włączając funkcję Zapomniane hasło, trzeba również określić, czy w celu udzielenia użytkownikowi pomocy przy logowaniu wymagany będzie zestaw odzewu.

7a **Zestawy odzewu:** W przypadku korzystania z zestawów odzewu użytkownicy nie mogą używać samoobsługowej funkcji Zapomniane hasło, dopóki nie odpowiedzą na pytania zestawu odzewu. Aby upewnić się, że użytkownicy są proszeni o wprowadzenie tych informacji za pośrednictwem portalu Identity Console, wybierz opcję **Wymagaj zestawu odzewu**.

7b **Działanie:** Opcje dostępne na tej karcie umożliwiają użytkownikowi resetowanie hasła przy użyciu zestawów odzewu i hasła uniwersalnego, wysyłanie bieżącego hasła lub podpowiedzi do hasła pocztą e-mail oraz wyświetlanie opcji podpowiedzi do hasła.

7c **Uwierzytelnienie:** Zaznacz pole wyboru **Wymuś na użytkowniku skonfigurowanie pytania o odzew i/lub podpowiedzi podczas uwierzytelniania**, aby zagwarantować, że użytkownicy otrzymają monit o określenie zestawów odzewu lub podpowiedzi do hasła.

Po zakończeniu kliknij przycisk **Dalej**.

8 Założenia nie są obowiązujące, dopóki nie zostaną przypisane do co najmniej jednego obiektu. W celu uproszczenia procesu administrowania zalecamy przypisywanie założeń możliwie jak najwyżej w drzewie. Założenia haseł można przypisać do następujących obiektów:

8a **Obiekt Założenia logowania:** Zalecamy utworzenie domyślnych założeń haseł dla wszystkich użytkowników w drzewie i przypisanie ich do obiektu Założenia logowania, który znajduje się w kontenerze Zabezpieczenia.

8b **Kontener będący katalogiem głównym partycji:** Przypisanie założeń do kontenera, który jest katalogiem głównym partycji, powoduje, że wszyscy użytkownicy w tej partycji, w tym również użytkownicy w kontenerach podrzędnych, dziedziczą przypisanie założeń.

8c **Kontener niebędący katalogiem głównym partycji:** Przypisanie założeń do kontenera, który nie jest katalogiem głównym partycji, powoduje, że przypisanie założeń jest dziedziczone tylko przez użytkowników znajdujących się w tym konkretnym kontenerze. Użytkownicy przechowywani w kontenerach podrzędnych nie dziedziczą założeń.

Aby zastosować założenia do wszystkich użytkowników poniżej kontenera, który nie jest katalogiem głównym partycji, należy przypisać je do każdego kontenera podrzędnego osobno.

8d **Użytkownik:** Możesz przypisać założenia do co najmniej jednego użytkownika.

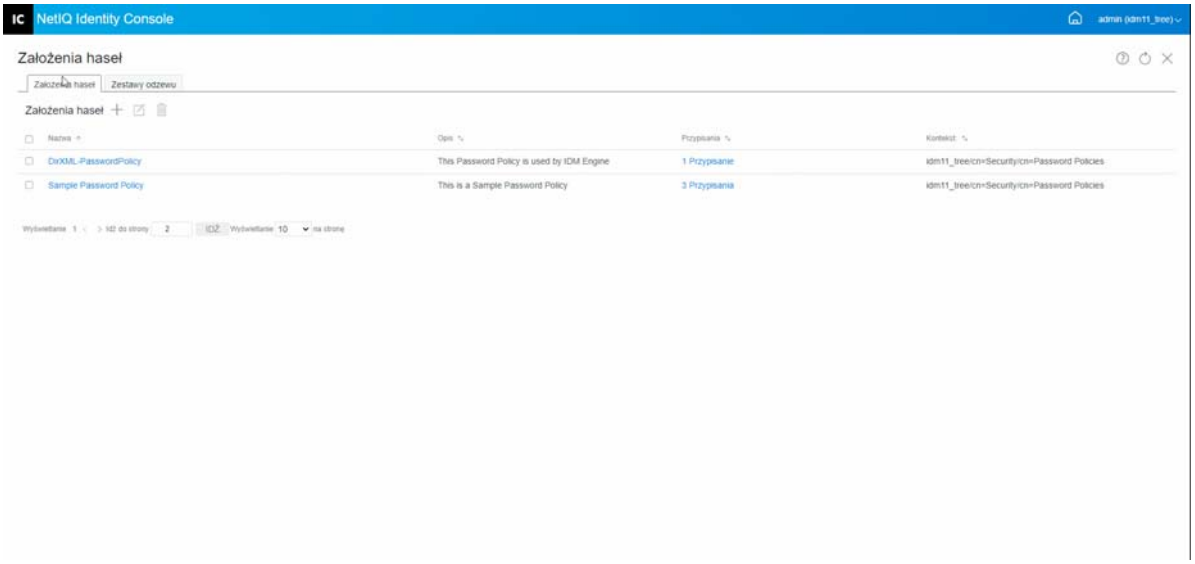
Aby przypisać założenia, kliknij ikonę +. Następnie znajdź i wybierz odpowiedni obiekt do przypisania założeń haseł.

Jeśli chcesz usunąć skojarzenie założeń, wybierz założenia z listy i kliknij ikonę 🗑.

9 Zweryfikuj szczegóły na stronie **Podsumowanie** i kliknij przycisk **Utwórz**.

10 Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym utworzeniu założeń haseł.

Rysunek 18-10 *Tworzenie założeń haseł za pomocą ustawień niestandardowych*



Modyfikowanie założeń haseł

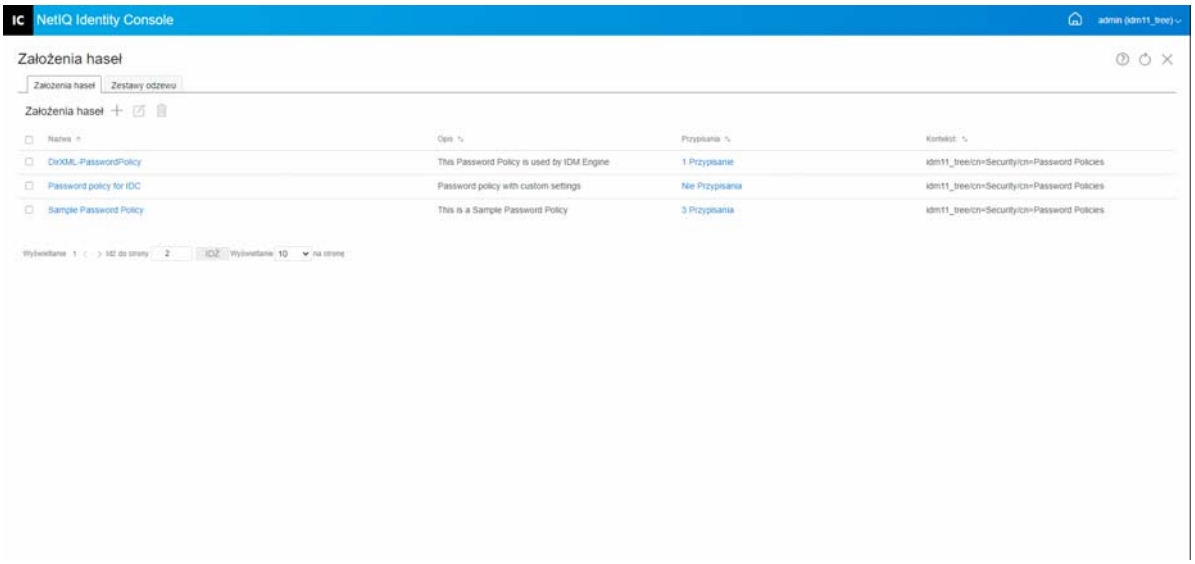
Aby zmodyfikować istniejące założenia haseł, wykonaj następujące czynności:

1 Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** na stronie docelowej Identity Console.

2 Wybierz odpowiednie założenia haseł z listy i kliknij ikonę ☑.

3 Wprowadź niezbędne zmiany na stronie **Modyfikuj założenia haseł** i kliknij przycisk **Zapisz**.

Rysunek 18-11 *Modyfikowanie założeń haseł*

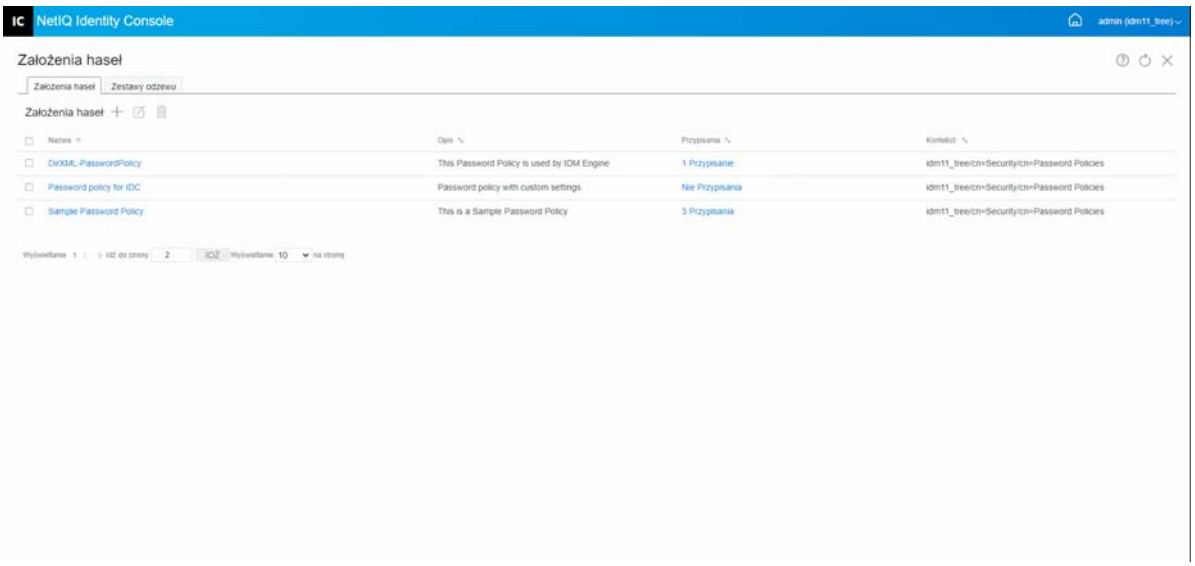


Usuwanie założeń haseł

Aby usunąć założenia haseł, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** na stronie docelowej Identity Console.
2. Wybierz odpowiednie założenia haseł z listy i kliknij ikonę .
3. Na następnym ekranie ostrzeżenia kliknij przycisk **OK**.
4. Zostanie wyświetlony komunikat potwierdzenia informujący o usunięciu założeń haseł.

Rysunek 18-12 *Usuwanie założeń haseł*



Zarządzanie zestawami odzewu

Zestaw odzewu to co najmniej jedno pytanie, na które musi odpowiedzieć użytkownik, aby potwierdzić swoją tożsamość. Zestaw odzewu jest częścią samoobsługowej funkcji Hasło.

W przypadku wystąpienia problemu z zapamiętaniem hasła lub jego użyciem użytkownik może skorzystać z samoobsługowej funkcji Hasło, zamiast dzwonić na stanowisko pomocy technicznej. Zestaw odzewu umożliwia użytkownikowi potwierdzenie jego tożsamości, a następnie otrzymanie podpowiedzi lub hasła w wiadomości e-mail, lub zresetowanie hasła przy użyciu przeglądarki internetowej.

Użytkownikom można pozwolić na tworzenie własnych pytań i odpowiadanie na nie lub wymagać od nich odpowiedzi na już utworzone pytania.

Na stronie Zestawy odzewu można wyszukiwać już istniejące zestawy, utworzyć nowy zestaw odzewu lub edytować istniejące zestawy.

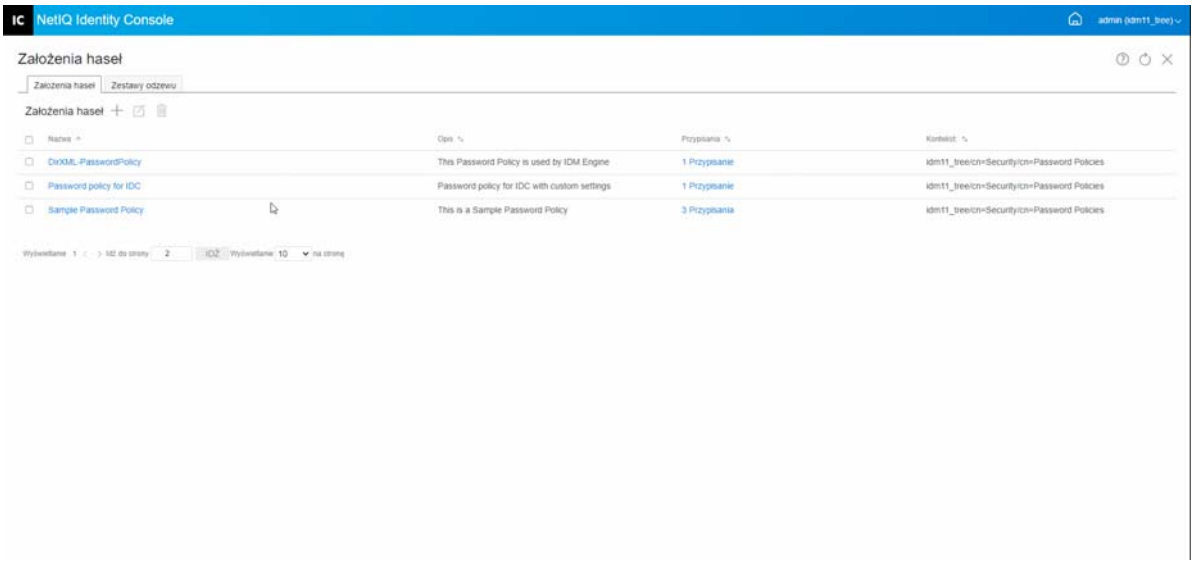
- „Tworzenie nowego zestawu odzewu” na stronie 123
- „Modyfikowanie zestawu odzewu” na stronie 124
- „Usuwanie zestawów odzewu” na stronie 125

Tworzenie nowego zestawu odzewu

Aby utworzyć nowy zestaw odzewu, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** > **Zestawy odzewu** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby utworzyć nowy zestaw odzewu.
3. Określ nazwę obiektu Zestaw odzewu i wybierz kontener lub kontener podrzędny, w którym powinien zostać utworzony zestaw odzewu.
4. Utwórz nowy zestaw pytań, które należy zadać w celu odzyskania hasła użytkownika. Możesz również wybrać pytania z istniejącego zestawu losowych pytań.
5. Ustaw liczbę pytań do zadania i kliknij przycisk **Utwórz**.
6. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym utworzeniu zestawu odzewu.

Rysunek 18-13 *Tworzenie zestawu odzewu*

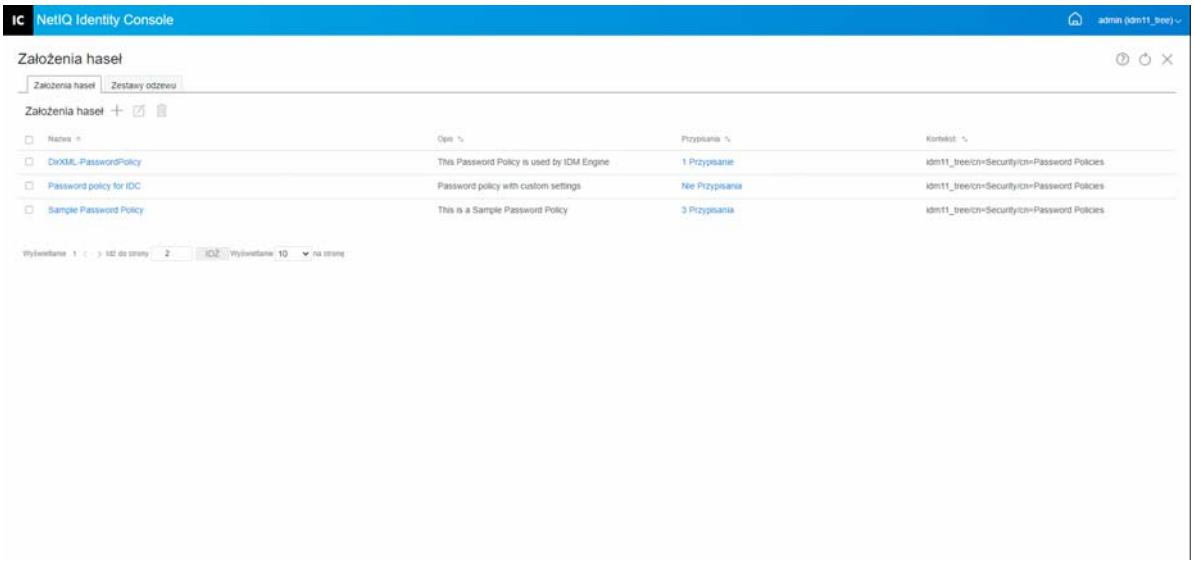


Modyfikowanie zestawu odzewu

Aby zmodyfikować istniejący zestaw odzewu, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** > **Zestawy odzewu** na stronie docelowej Identity Console.
2. Wybierz odpowiedni zestaw odzewu z listy i kliknij ikonę ☑.
3. Wprowadź niezbędne zmiany na stronie Modyfikuj zestaw odzewu i kliknij przycisk **Zapisz**.
4. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym zmodyfikowaniu zestawu odzewu.

Rysunek 18-14 *Modyfikowanie zestawu odzewu*

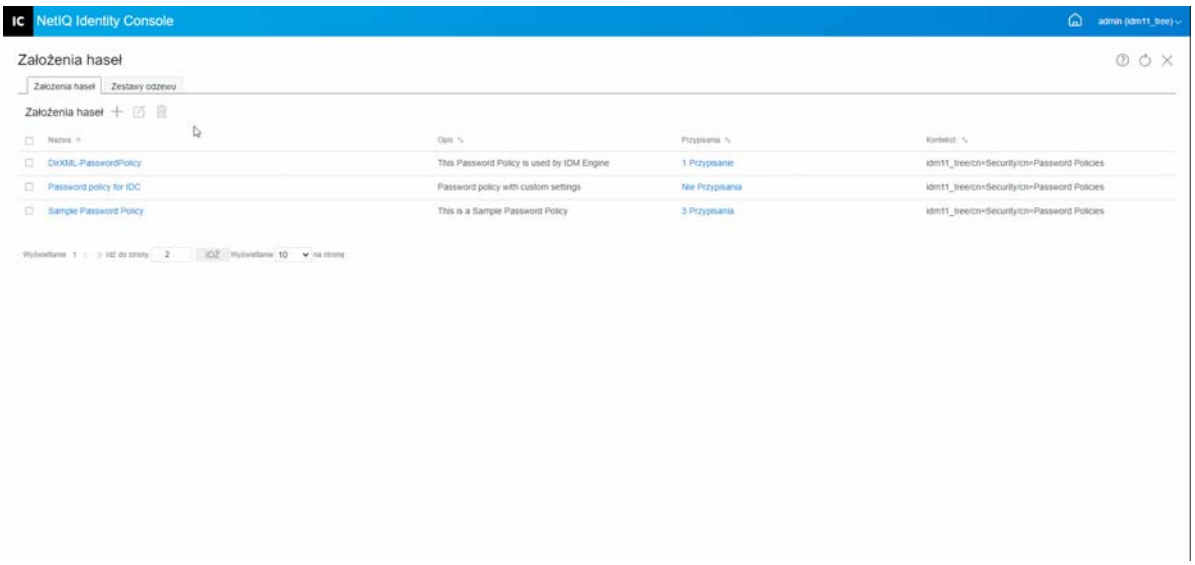


Usuwanie zestawów odzewu

Aby usunąć zestawy odzewu, wykonaj następujące czynności:

1. Kliknij opcje **Zarządzanie uwierzytelnianiem** > **Założenia haseł** > **Zestawy odzewu** na stronie docelowej Identity Console.
2. Wybierz wymagany zestaw odzewu z listy i kliknij ikonę .
3. Na ekranie potwierdzenia kliknij przycisk **OK**.
4. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym usunięciu zestawu odzewu.

Rysunek 18-15 *Usuwanie zestawu odzewu*



19 Zarządzanie obiektami grupy SNMP

Protokół SNMP (Simple Network Management Protocol) to standardowy protokół działania i utrzymania dla Internetu do wymiany informacji dotyczących zarządzania między aplikacjami konsoli administracyjnej i zarządzanymi urządzeniami.

Przy użyciu modułu SNMP można wykonywać następujące zadania:

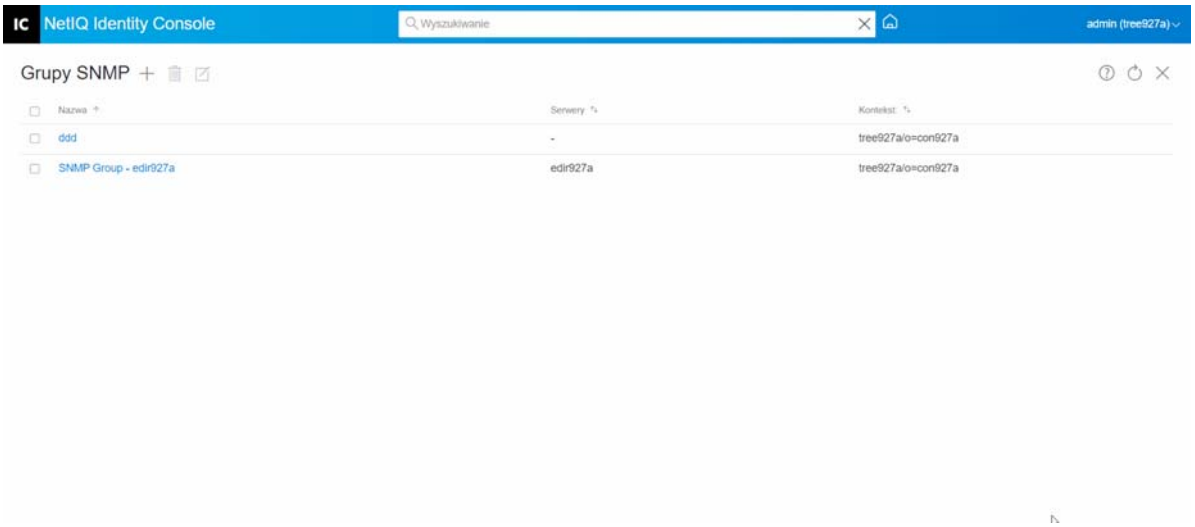
- „Tworzenie obiektów grupy SNMP” na stronie 127
- „Modyfikowanie obiektów grupy SNMP” na stronie 128
- „Usuwanie obiektów grupy SNMP” na stronie 128

Tworzenie obiektów grupy SNMP

Aby utworzyć obiekty grupy SNMP, wykonaj następujące czynności:

1. Kliknij moduł **SNMP** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby utworzyć nowy obiekt grupy SNMP.
3. Określ nazwę i wybierz kontekst w celu utworzenia nowego obiektu grupy SNMP.
4. Kliknij przycisk **Utwórz**.
5. Na ekranie zostanie wyświetlony komunikat potwierdzający pomyślne utworzenie obiektu grupy SNMP.

Rysunek 19-1 *Tworzenie obiektów grupy SNMP*

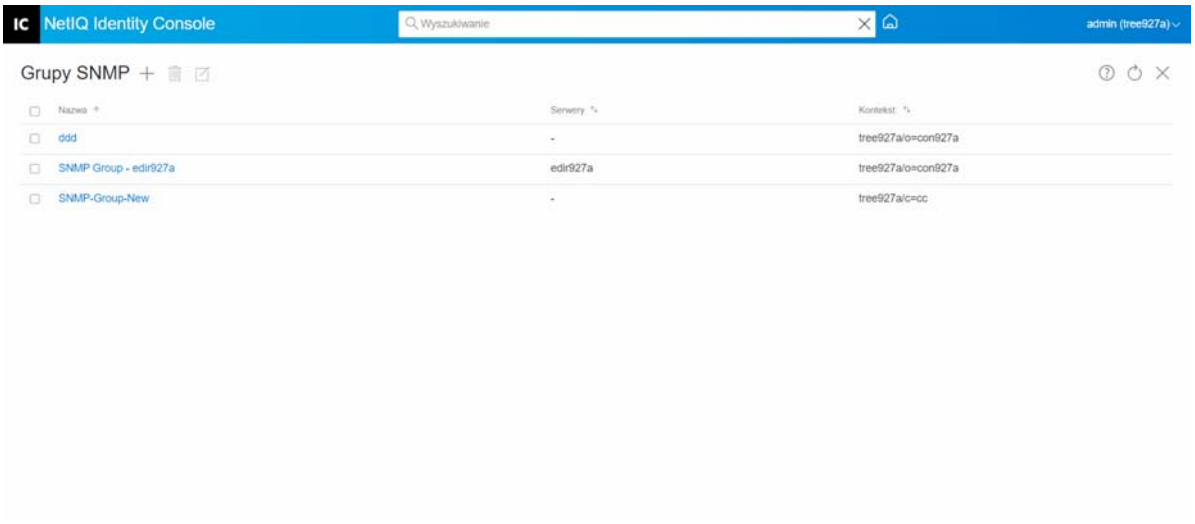


Modyfikowanie obiektów grupy SNMP

Aby zmodyfikować obiekty grupy SNMP, wykonaj następujące czynności:

1. Kliknij moduł **SNMP** na stronie docelowej Identity Console.
2. Wybierz obiekt grupy SNMP, który chcesz zmodyfikować, i kliknij ikonę .
3. Na stronie **Ogólne**/**Pułapki** zmodyfikuj parametry, które da się konfigurować.
4. Po zakończeniu kliknij przycisk **Zapisz**.
5. Na ekranie zostanie wyświetlony komunikat potwierdzający pomyślne zmodyfikowanie obiektu grupy SNMP.

Rysunek 19-2 *Modyfikowanie obiektów grupy SNMP*

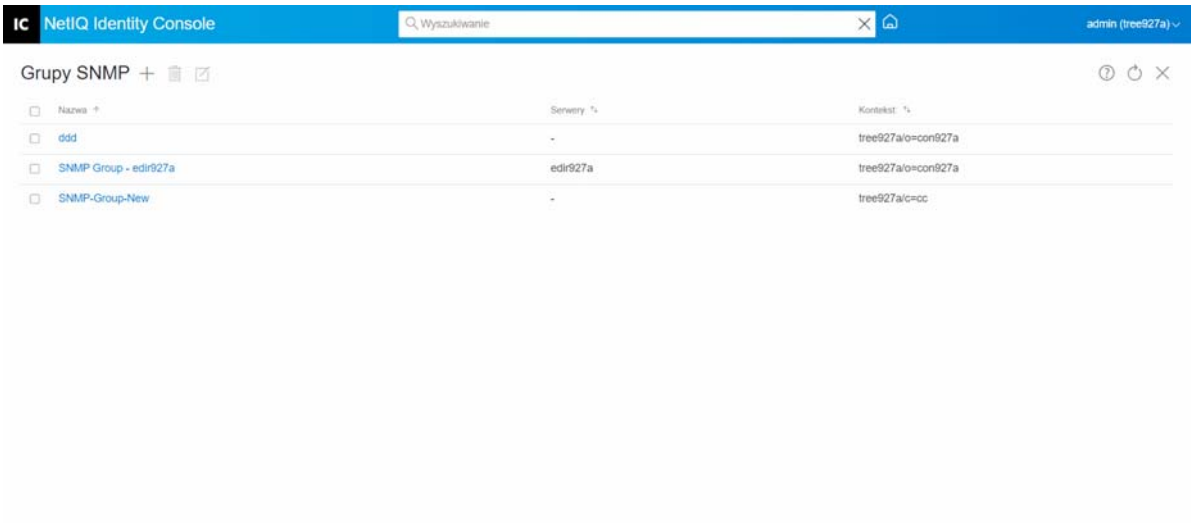


Usuwanie obiektów grupy SNMP

Aby usunąć obiekty grupy SNMP, wykonaj następujące czynności:

1. Kliknij moduł **SNMP** na stronie docelowej Identity Console.
2. Wybierz obiekt grupy SNMP, który chcesz zmodyfikować, i kliknij ikonę .
3. Na następnym ekranie kliknij przycisk **OK**.
4. Na ekranie zostanie wyświetlony komunikat potwierdzający pomyślne usunięcie obiektu grupy SNMP.

Rysunek 19-3 *Usuwanie obiektów grupy SNMP*



20 Zarządzanie rozszerzonym uwierzytelnianiem w tle

Aby można było uzyskać dostęp do usługi eDirectory z poziomu dodatku typu plug-in EBA do Identity Console, w drzewie musi się znajdować serwer z obsługą uwierzytelniania EBA z prawidłowym plikiem eba.p12. Aby uzyskać więcej informacji na temat włączania uwierzytelniania EBA w drzewie eDirectory, zobacz Enabling EBA on an eDirectory Tree (Włączanie uwierzytelniania EBA w drzewie eDirectory) w dokumencie *NetIQ eDirectory Administration Guide* (Podręcznik administracji NetIQ eDirectory).

UWAGA: Aby korzystać modułu EBA z portalem Identity Console, musisz uaktualnić serwer eDirectory do wersji 9.2.4 HF2.

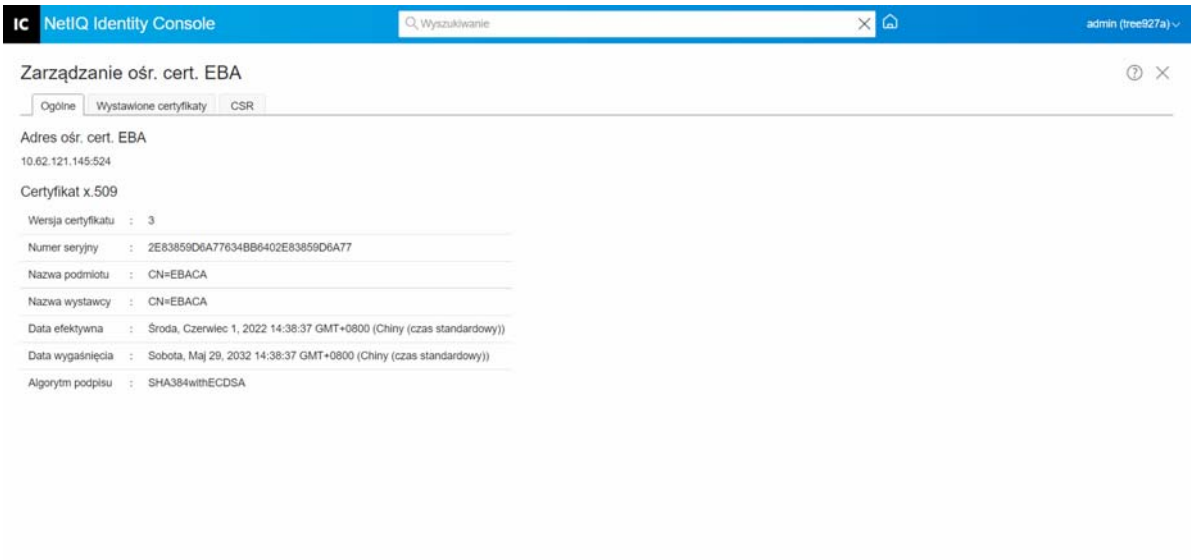
Aby otworzyć stronę zarządzania ośrodkiem certyfikacji EBA, zaloguj się do portalu Identity Console i kliknij moduł **EBA**.

Strona zarządzania ośrodkiem certyfikacji EBA zawiera następujące karty służące do zarządzania różnymi aspektami ośrodka certyfikacji EBA:

- **Ogólne:** Wyświetla adres IP urzędu EBA CA i jego certyfikat.
- **Wystawione certyfikaty:** Wyświetla certyfikaty NCP CA wraz z ich adresem IP i portem.

  Aby unieważnić certyfikat, zaznacz certyfikat i kliknij przycisk ⊘. Tej opcji należy używać tylko w skrajnych sytuacjach, ponieważ serwer będący właścicielem certyfikatu ośrodka certyfikacji NCP przestanie działać, gdy jego certyfikat zostanie unieważniony. Zwykle unieważnienie certyfikatu staje się konieczne w przypadku naruszenia bezpieczeństwa serwera.
- **CSR:** Zawiera listę żądań podpisania certyfikatu oczekujących na zatwierdzenie przez administratora. Aby zatwierdzić żądanie podpisania certyfikatu, wybierz certyfikat z listy i kliknij przycisk **Zatwierdź**.

Rysunek 20-1 *Zarządzanie rozszerzonym uwierzytelnianiem w tle*



II Zarządzanie programem Identity Manager przy użyciu Identity Console

W tej sekcji opisano różne zadania, które można wykonywać w celu zarządzania serwerami Identity Manager przy użyciu programu Identity Console.

21 Zarządzanie programami obsługi i zestawami programów obsługi

Zestaw programów obsługi to kontener, w którym znajdują się programy obsługi Identity Manager. W danym momencie na serwerze może być aktywny tylko jeden zestaw programów obsługi. W związku z tym wszystkie aktywne programy obsługi muszą być zgrupowane w tym samym zestawie programów obsługi. Zestaw programów obsługi można utworzyć przy użyciu narzędzia Designer. Aby uzyskać więcej informacji, zobacz Configuring Driver Sets (Konfigurowanie zestawów programów obsługi) w dokumencie *NetIQ Designer for Identity Manager Administration Guide* (NetIQ Designer for Identity Manager — podręcznik administracji).

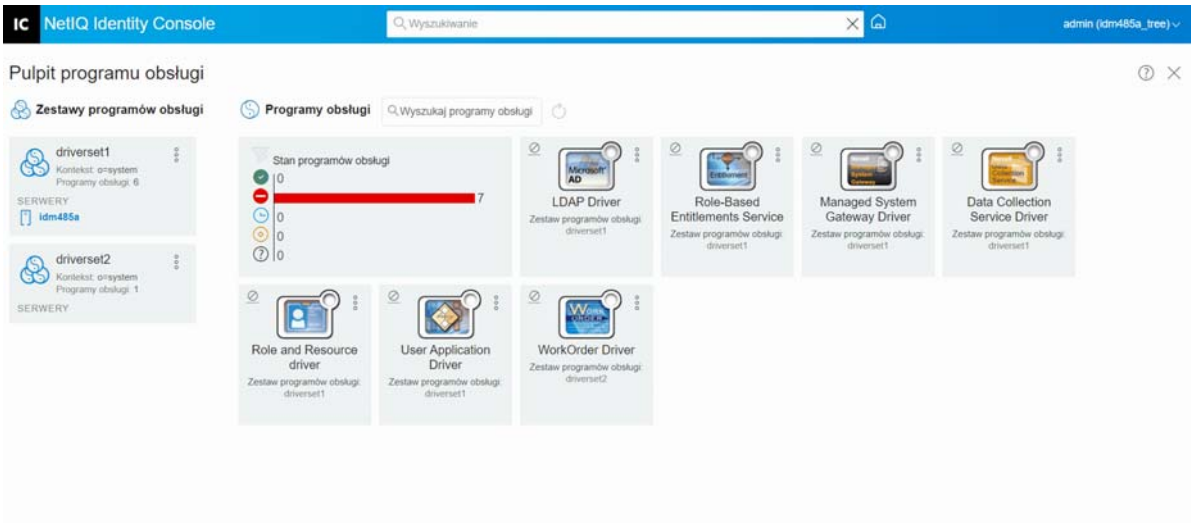
Dodawanie lub usuwanie serwerów

W danym momencie zestaw programów obsługi może być skojarzony z jednym serwerem lub kilkoma serwerami. Jednak w zależności od wymagań można skojarzyć inny obiekt zestawu programów obsługi z dostępnym serwerem.

Aby dodać nowy serwer, kliknij ikonę na określonym obiekcie zestawu programów obsługi > wybierz opcję **Dodaj serwery** i wybierz właściwy serwer z przeglądarki kontekstowej.

Aby usunąć istniejący serwer, wybierz opcję **Usuń serwer**.

Rysunek 21-1 *Dodawanie serwera do zestawu programów obsługi*



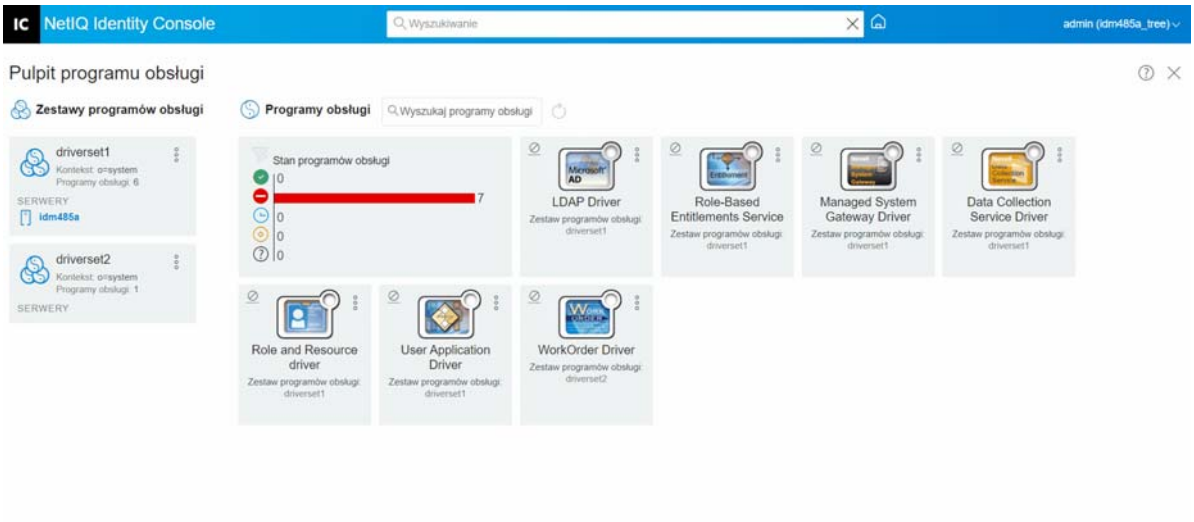
Aktywowanie zestawów programów obsługi przy użyciu klucza aktywacji produktu

Przed użyciem jakiegokolwiek zestawu i znajdujących się w nim programów obsługi należy aktywować go za pomocą kodu aktywacji otrzymanego pocztą e-mail. Po zakupieniu licencji użytkownik otrzyma klucz aktywacji od NetIQ. Aby aktywować zestaw programów obsługi za pomocą klucza aktywacji, wykonaj następujące czynności:

1. Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.
2. Kliknij ikonę Działania w polu określonego zestawu programów obsługi, który chcesz aktywować, i kliknij opcję **Instalacja aktywacji**.

   Po zastosowaniu aktywacji każda karta zestawu programów obsługi na kafelku Administracja IDM wyświetla informacje o aktywacji dla wszystkich serwerów powiązanych z tym zestawem programów obsługi. Informacje te pomagają określić, kiedy aktywacja wygaśnie.
3. Jeśli plik aktywacji został pobrany na komputer, zaznacz pole wyboru **Wybierz plik zawierający poświadczenia**.
4. Znajdź i wybierz plik aktywacji, a następnie kliknij przycisk **Prześlij**.
5. Zestaw programów obsługi możesz również aktywować przy użyciu treści pliku aktywacji. Zaznacz pole wyboru **Wprowadź poświadczenia**.
   - **5a** Otwórz plik poświadczenia aktywacji produktu, a następnie skopiuj jego treść do schowka.
   - **5b** Kopiując treść, nie dodawaj żadnych dodatkowych wierszy ani spacji. Skopiuj treść od pierwszego myślnika (-) poświadczenia (----BEGIN PRODUCT ACTIVATION CREDENTIAL) do ostatniego myślnika (-) poświadczenia (END PRODUCT ACTIVATION CREDENTIAL-----) i kliknij przycisk **Zakończ**.
6. Zostanie wyświetlony komunikat potwierdzenia informujący o pomyślnym aktywowaniu zestawu programów obsługi.

Rysunek 21-2 *Aktywowanie zestawów programów obsługi*

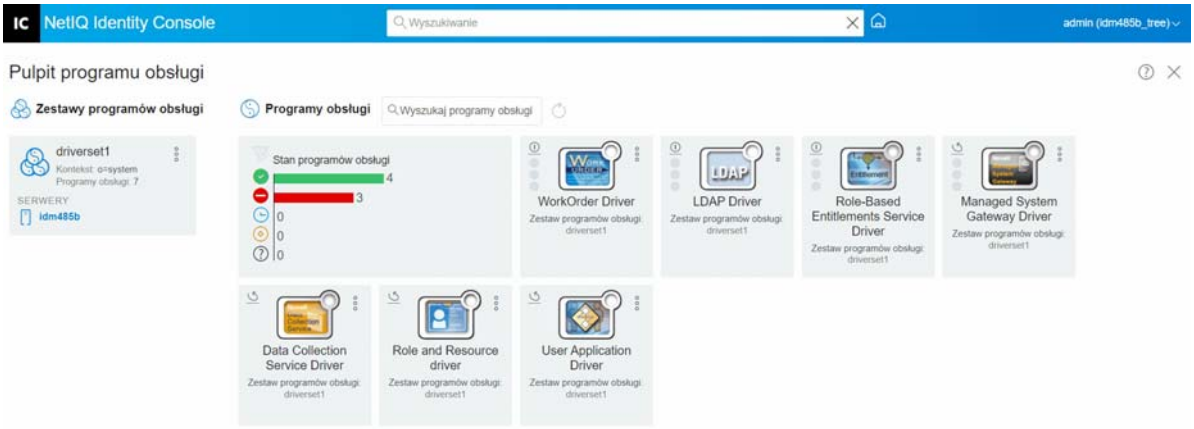


Wyświetlanie informacji o aktywacji zestawów programów obsługi

Po aktywowaniu zestawu programów obsługi należy zweryfikować, czy został on pomyślnie aktywowany. Aby przeprowadzić weryfikację, wykonaj następujące czynności:

1. Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.
2. Kliknij ikonę Działania na określonym obiekcie zestawu programów obsługi, którego informacje o aktywacji chcesz zweryfikować, i kliknij opcję **Informacje o aktywacji**.
3. Na komputerze zostanie wyświetlone okno informacji związanych z aktywacją. Na tej stronie można zweryfikować szczegóły aktywacji określonego zestawu programów obsługi.

Rysunek 21-3 *Wyświetlanie informacji o aktywacji zestawów programów obsługi*

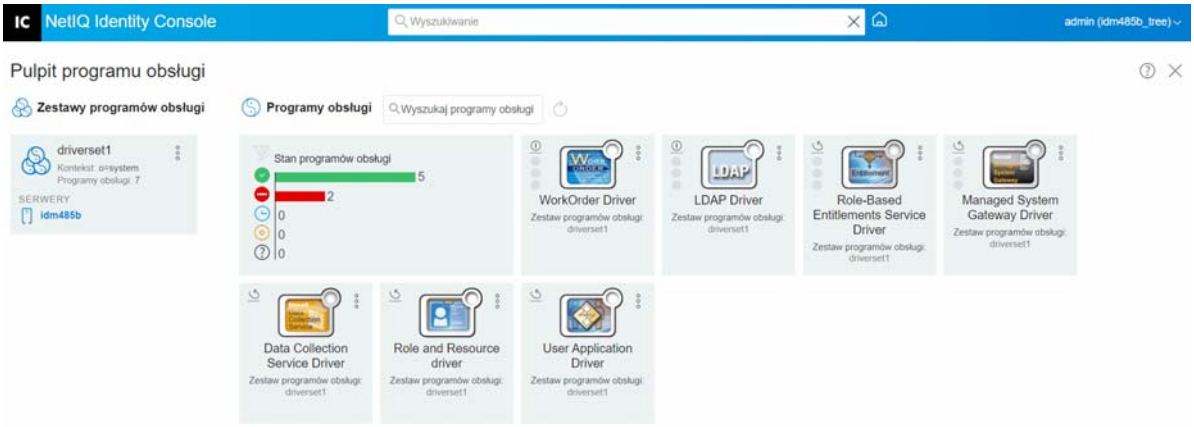


Uruchamianie i zatrzymywanie programów obsługi

Program obsługi po utworzeniu jest domyślnie zatrzymany. Aby zaczął działać, należy go uruchomić. Identity Manager to system oparty na zdarzeniach, dlatego uruchomiony program obsługi pozostaje w stanie bezczynności do czasu wystąpienia zdarzenia. W celu uruchomienia/zatrzymania programów obsługi należy wykonać poniższe czynności.

1. Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.
2. Kliknij określony obiekt zestawu programów obsługi po prawej stronie ekranu komputera, aby wyświetlić wszystkie skojarzone z nim programy obsługi.
3. Kliknij ikonę Działania na określonym programie obsługi i wybierz polecenie **Uruchomienie programu obsługi**.
4. Aby zatrzymać obiekt programu obsługi, kliknij ikonę Działania na określonym programie obsługi i wybierz polecenie **Zatrzymaj program obsługi**.
5. (Opcjonalnie) Wszystkie programy obsługi znajdujące się w tym samym zestawie programów obsługi możesz uruchamiać i zatrzymywać jednocześnie. Kliknij ikonę Działania na obiekcie zestawu programów obsługi i wybierz polecenie **Uruchom wszystkie programy obsługi** lub **Zatrzymaj wszystkie programy obsługi**.

Rysunek 21-4 *Uruchamianie i zatrzymywanie programów obsługi*

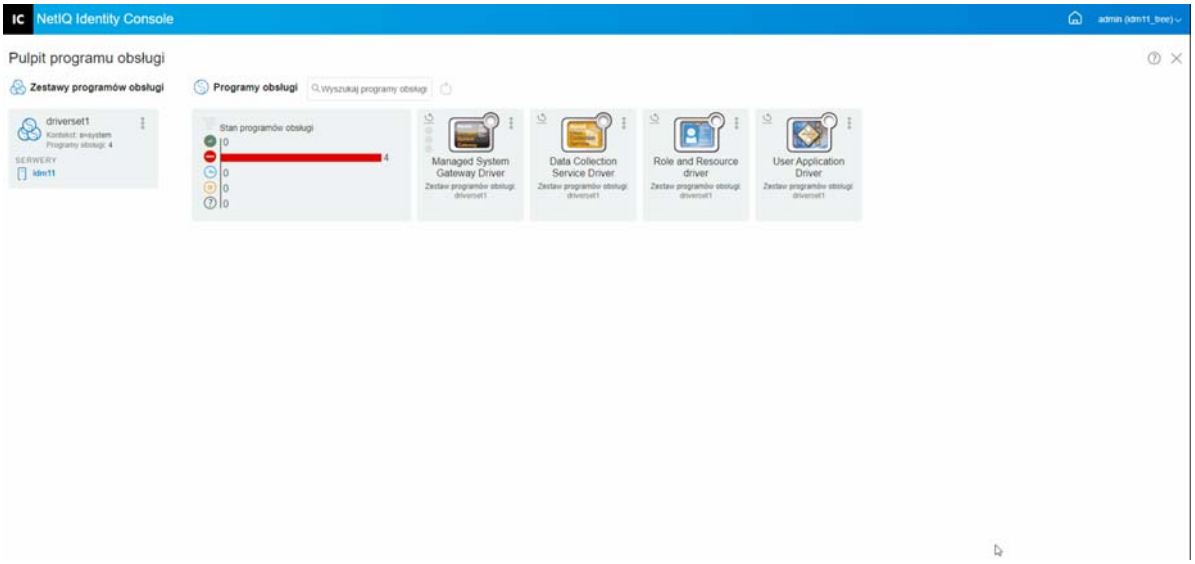


Wyszukiwanie programów obsługi

Identity Console udostępnia opcję wyszukania określonego programu obsługi na serwerze. Aby wyszukać program obsługi, wykonaj następujące czynności:

1. Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.
2. Określ nazwę programu obsługi w polu **Wyszukaj**. Określony obiekt programu obsługi zostanie wyświetlony na ekranie komputera. Możesz też odświeżyć listę programów obsługi, klikając ikonę .

Rysunek 21-5 *Wyszukiwanie programów obsługi*



Filtrowanie programów obsługi i zestawów programów obsługi

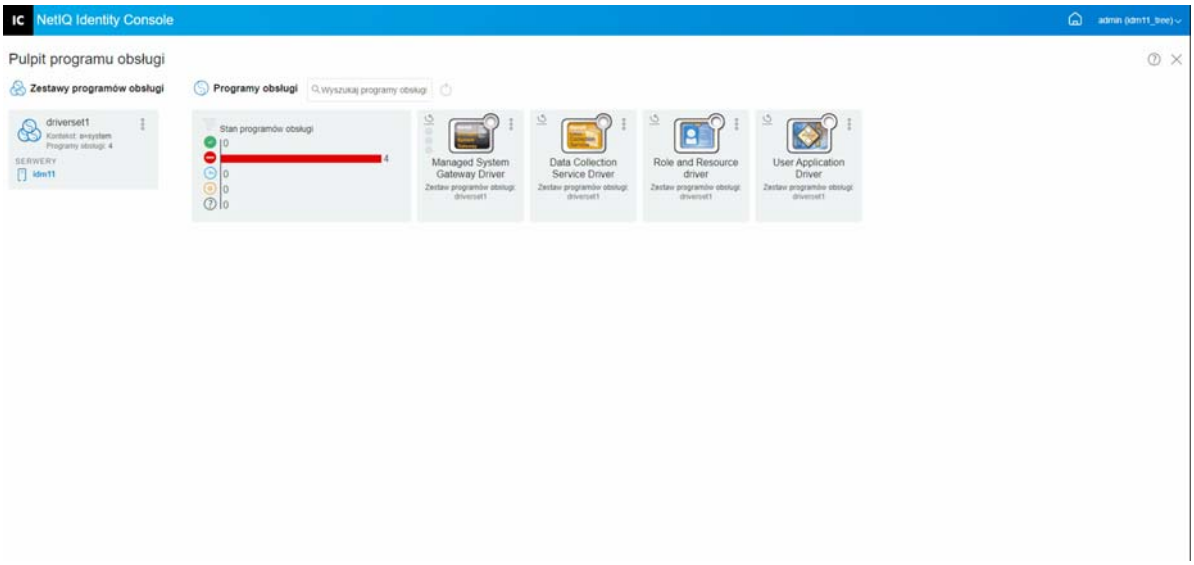
Programy obsługi można filtrować na podstawie ich stanu na stronie **IDM Administration** (Administracja IDM). Aby odfiltrować programy obsługi:

1. Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.
2. Na kafelku **Drivers' Status** (Stan programów obsługi) kliknij następujące ikony, aby odfiltrować programy obsługi na podstawie ich stanu:
   - Kliknij ikonę , aby odfiltrować wszystkie uruchomione programy obsługi na serwerze.
   - Kliknij ikonę , aby odfiltrować wszystkie zatrzymane programy obsługi na serwerze.
   - Kliknij ikonę , aby odfiltrować wszystkie programy obsługi, które są uruchamiane.
   - Kliknij ikonę , aby odfiltrować wszystkie programy obsługi, które są zatrzymywane.
   - Kliknij ikonę , aby odfiltrować programy obsługi, z którymi nie jest skojarzony żaden stan. Gdy z zestawem programów obsługi nie jest skojarzony żaden serwer, znajdujące się w tym zestawie programy obsługi wyświetlają stan **Nieznane**.

Aby wyczyścić dowolny filtr zastosowany względem programów obsługi, kliknij ikonę widoczną na kafelku **Stan programów obsługi**.

3 Zestawy programów obsługi można również filtrować przy użyciu portalu Identity Console. Domyślnie w portalu Identity Console są wyświetlane wszystkie programy obsługi skojarzone ze wszystkimi zestawami programów obsługi na serwerze. Jeśli chcesz wyświetlić programy obsługi z określonego zestawu programów obsługi, musisz wybrać odpowiedni zestaw programów obsługi z listy znajdującej się po lewej stronie portalu Identity Console. Aby wyczyścić wybór zestawu programów obsługi, kliknij ponownie wybrany zestaw.

Rysunek 21-6 *Filtrowanie programów obsługi i zestawów programów obsługi*



Usuwanie zestawu programów obsługi

Aby usunąć program obsługi, wykonaj następujące czynności:

1 Kliknij kartę **Administracja IDM** na ekranie domowym Identity Console.

2 Kliknij przycisk działań na zestawie programów obsługi, który chcesz usunąć.

3 Wybierz opcję **Usuń**.

Działania programu obsługi

Po kliknięciu ikony działań na tytule pojedynczego programu obsługi są obsługiwane następujące działania:

- **Uruchom program obsługi**: umożliwia uruchomienie programu obsługi
- **Zatrzymaj program obsługi**: umożliwia zatrzymanie programu obsługi

- **Uruchom ponownie program obsługi**: umożliwia ponowne uruchomienie zatrzymanego programu obsługi
- **Usuń program obsługi**: umożliwia usunięcie programu obsługi
- **Statystyka**: umożliwia wyświetlenie statystyki wydajności programu obsługi
- **Kopiuj dane**: umożliwia skopiowanie danych programu obsługi z jednego serwera na inny. Ta opcja jest dostępna tylko w środowiskach z wieloma serwerami.

22 Zarządzanie właściwościami zestawu programów obsługi

W tej sekcji znajdują się informacje na temat właściwości, które są wspólne dla wszystkich zestawów programów obsługi. Należą do nich wszystkie właściwości (Nazwane hasło, Poziom dziennika, Inspektor zestawu programów obsługi itd.).

Ta sekcja jest podzielona na następujące kategorie:

Konfigurowanie zestawów programów obsługi

Aby zmodyfikować konfigurację zestawu programów obsługi, wykonaj następujące czynności:

1. Kliknij opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi**.
2. Domyślnie zostanie wyświetlona strona **Konfiguracja zestawu programów obsługi**. Opcje konfiguracji zestawu programów obsługi są podzielone na następujące kategorie:

Nazwane hasło

Identity Manager umożliwia bezpieczne przechowywanie wielu haseł dla zestawu programów obsługi. Ta funkcja nosi nazwę nazwanych haseł. Dostęp do poszczególnych haseł uzyskuje się za pomocą klucza lub nazwy.

Nazwane hasła można dodać do zestawu programów obsługi lub do pojedynczych programów obsługi. Nazwane hasła zestawu programów obsługi są dostępne dla wszystkich programów obsługi w tym zestawie.

Aby użyć nazwanego hasła w założeniach programu obsługi, należy odwołać się do niego za pomocą nazwy hasła, a nie rzeczywistego hasła. Hasło do programu obsługi jest wysyłane przez mechanizm Identity Manager. Metody przechowywania i pobierania nazwanych haseł, która została opisana w tej sekcji, można użyć z dowolnym programem obsługi, bez konieczności wprowadzania zmian w podkładce programu obsługi.

Dostęp do nazwanego hasła można uzyskać, wybierając opcję **Administracja IDM** > **klikając menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Nazwane hasło** na stronie **Konfiguracja zestawu programów obsługi**.

Aby dodać nowe nazwane hasło, kliknij ikonę +. Aby usunąć istniejące nazwane hasło, wybierz odpowiednie hasło i kliknij ikonę .

Globalne wartości konfiguracyjne

Wyświetla uporządkowaną listę obiektów konfiguracji globalnej. Obiekty zawierają definicje globalnych wartości konfiguracyjnych (GCV) rozszerzenia, które Identity Manager ładuje podczas uruchamiania programu obsługi. Obiekty konfiguracji globalnej można dodawać i usuwać. Można również zmieniać kolejność wykonywania obiektów. Kliknij ikonę , aby zapisać globalne wartości konfiguracyjne. Aby odświeżyć listę globalnych wartości konfiguracyjnych, kliknij ikonę .

Konfigurowanie parametrów środowiska Java

Aby skonfigurować parametry środowiska Java, wykonaj następujące czynności:

1. W portalu Identity Console kliknij opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi**.
2. Kliknij opcję **Parametry środowiska Java** w obszarze **Konfiguracja zestawu programów obsługi**, aby wyświetlić stronę właściwości zawierającą parametry środowiska Java.
3. Zmodyfikuj odpowiednio do potrzeb następujące ustawienia:

   Dodatki ścieżki klasy: Określ dodatkowe ścieżki maszyny wirtualnej Java (JVM) w celu wyszukiwania plików pakietów (`JAR`) i klas (`CLASS`). Działanie tego parametru przynosi takie same rezultaty jak użycie polecenia `java -classpath`. Wprowadzając wiele ścieżek klasy, rozdzielaj je średnikiem (;) w przypadku maszyny wirtualnej Java systemu Windows i dwukropkiem (:) w przypadku maszyny wirtualnej systemu UNIX lub Linux.

   Opcje JVM: Określ dodatkowe opcje, które będą używane z maszyną wirtualną Java. Prawidłowe opcje można znaleźć w dokumentacji JVM.

   Odpowiednia zmienna środowiskowa to `DHOST_JVM_OPTIONS`. Określa ona argumenty dla wirtualnej maszyny Java w wersji 1.2. Na przykład:

   ```
   -Xnoagent -Xdebug -Xrunjdwp: transport=dt_socket,server=y, address=8000
   ```

   Poszczególne łańcuchy opcji rozdziela się spacją. Łańcuch opcji zawierający spację musi być ujęty w cudzysłów podwójny.

   Opcja atrybutu zestawu programów obsługi ma pierwszeństwo przed zmienną środowiskową `DHOST_JVM_OPTIONS`. Ta zmienna środowiskowa jest dołączana na końcu opcji atrybutu zestawu programów obsługi.

Początkowy rozmiar sterty: Określ początkowy (minimalny) rozmiar sterty dostępny dla maszyny wirtualnej Java. Zwiększenie początkowego rozmiaru sterty może skrócić czas uruchamiania i poprawić przepustowość. Użyj wartości liczbowej i litery G, M lub K. Jeśli nie zostanie określona litera rozmiaru, rozmiar domyślnie będzie podawany w bajtach. Działanie tego parametru przynosi takie same rezultaty jak użycie polecenia `java -Xms`.

Odpowiednia zmienna środowiskowa to `DHOST_JVM_INITIAL_HEAP`. Określa ona początkowy rozmiar sterty JVM w dziesiętnej liczbie bajtów. Ma pierwszeństwo przed opcją atrybutu zestawu programów obsługi.

Informacje na temat domyślnego początkowego rozmiaru sterty JVM można znaleźć w dokumentacji JVM.

Maks. rozmiar sterty: Określ maksymalny rozmiar sterty dostępny dla maszyny wirtualnej Java. Użyj wartości liczbowej i litery G, M lub K. Jeśli nie zostanie określona litera rozmiaru, rozmiar domyślnie będzie podawany w bajtach. Działanie tego parametru przynosi takie same rezultaty jak użycie polecenia `java -Xmx`.

Odpowiednia zmienna środowiskowa to `DHOST_JVM_MAX_HEAP`. Określa ona maksymalny rozmiar sterty JVM w dziesiętnej liczbie bajtów. Ma pierwszeństwo przed opcją atrybutu zestawu programów obsługi.

Informacje na temat domyślnego maksymalnego rozmiaru sterty JVM można znaleźć w dokumentacji JVM.

4 Kliknij ikonę , aby zapisać zmiany.

5 Uruchom ponownie bezpieczny magazyn tożsamości, aby zastosować zmiany.

Zarządzanie listą atrybutów z wartościami

Aby dodać atrybuty do listy atrybutów z wartościami dla określonego zestawu programów obsługi, wykonaj następujące czynności:

1 W portalu Identity Console wybierz moduł **Zarządzanie obiektami**.

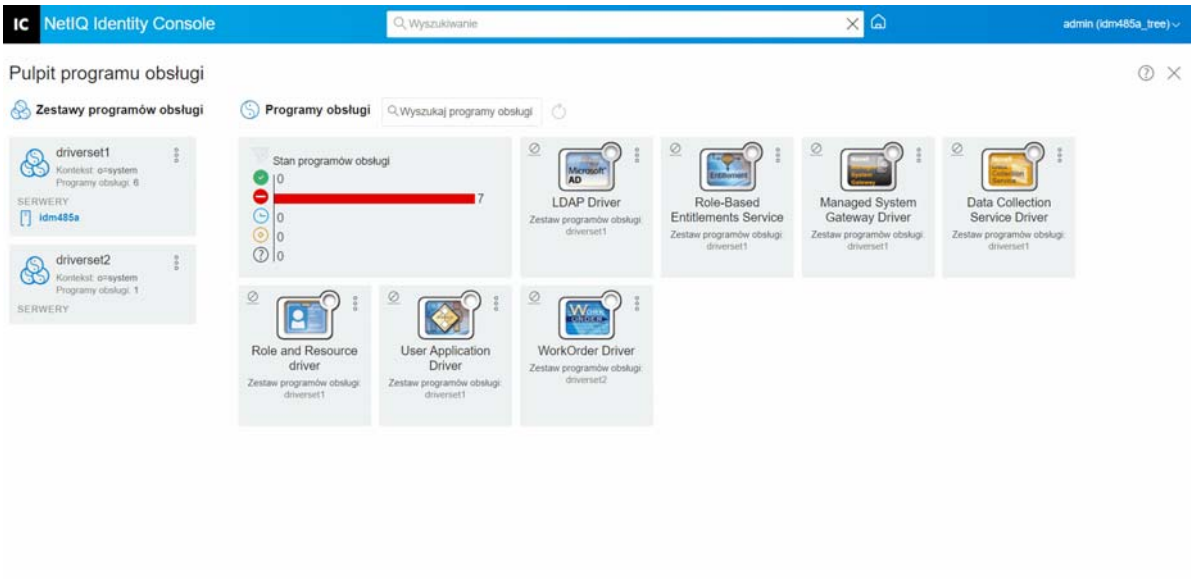
2 Z listy rozwijanej wybierz typ **DirXML-DriverSet** i kliknij przycisk Wyszukaj.

3 Kliknij odpowiedni zestaw programów obsługi na liście.

4 Aby dodać atrybuty bez wartości do listy atrybutów z wartościami, kliknij ikonę obok pozycji **Atrybuty z wartościami** i wybierz właściwe atrybuty bez wartości z listy.

5 Po zakończeniu kliknij przycisk **OK**.

Rysunek 22-1 *Zarządzanie parametrami konfiguracji zestawu programów obsługi*



Zarządzanie zadaniami dla zestawów programów obsługi

Opcja Zadania w portalu Identity Console umożliwia planowanie zdarzeń dla wszystkich programów obsługi znajdujących się w odpowiednim zestawie programów obsługi.

Strona Zadania zawiera nazwę zadania, stan zadania (włączone lub wyłączone), zaplanowany czas uruchomienia i opis zadania. Kliknij nazwę zadania, aby wyświetlić stronę Zadania. Kliknij ikonę włączenia/wyłączenia w kolumnie Włączono, aby włączyć lub wyłączyć zadanie. Kliknij opis zadania, aby wyświetlić pełne informacje o zadaniu.

Dostęp do strony Zadania uzyskuje się, wybierając opcję **Administracja IDM** > **klikając menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > kartę **Zaawansowane** na stronie głównej Identity Console. Na karcie Zadania znajduje się tabela zawierająca istniejące obiekty zadań wybranego programu obsługi, który jest wyświetlany pod w pełni kwalifikowaną nazwą we wpisie Program obsługi.

Na stronie Zadania można wykonać następujące zadania:

- **Utwórz zadanie**: kliknij ikonę +, aby utworzyć nowe zadanie.

  W oknie podręcznym **Nowe zadanie** wykonaj następujące czynności w celu utworzenia nowego zadania:

  1. Podaj nazwę zadania.
  2. Wybierz typ zadania.
  3. Kliknij ikonę ∨ i z dostępnej listy serwerów wybierz serwer, na którym zadanie ma być uruchamiane. W przeciwnym razie określ nazwę serwera, a następnie wybierz serwer.
  4. Kliknij przycisk **Utwórz**.
- **Uruchom wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ▷.

- **Zatrzymaj wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę .
- **Włącz wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę .
- **Wyłącz wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę .
- **Uzyskaj stan**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę .
- **Usuń wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę .

Kliknij zadanie, aby uzyskać dostęp do strony **Job Property** (Właściwość zadania). Na stronie tej możesz skonfigurować sposób uruchamiania zadania.

Ogólne: przedstawia nazwę klasy Java dla zadania. Na tej stronie możesz włączyć lub wyłączyć zadanie, usunąć zadanie po jego wykonaniu, wybrać serwer lub serwery, na których zadanie ma być uruchamiane, określić serwer poczty e-mail oraz nadać zadaniu inną nazwę i opis.

Plan: umożliwia ustawienie czasu uruchamiania zadania. Podaj wartość w polu Uruchom zadanie o, aby ustawić godzinę, i określ, czy zadanie ma być uruchamiane codziennie, co tydzień, co miesiąc czy co rok. Możesz też dostosować czas uruchamiania zadania lub włączyć przełącznik, aby uruchamiać zadanie ręcznie.

Zakres: umożliwia określenie obiektów, których dotyczy to zadanie. Obiekt może być kontenerem, grupą dynamiczną, grupą lub obiektem typu liść. Kliknij przycisk Dodaj, aby wybrać obiekt, którego ma dotyczyć to zadanie. Możesz użyć przycisku Przeglądaj, aby wybrać obiekt, a następnie kliknij przycisk OK. Aby usunąć obiekt z listy zakresu, wybierz obiekt zakresu, klikając pole po lewej stronie obiektu DN, a następnie kliknij przycisk Usuń.

Po dodaniu obiektu wybierz go, aby wyświetlić więcej opcji. Jeśli wybierzesz obiekt grupy, masz możliwość zastosowania zadania do członków grupy lub tylko do grupy. Jeśli wybierzesz obiekt kontenera, masz możliwość zastosowania zadania do wszystkich elementów potomnych w tym kontenerze, do wszystkich elementów podrzędnych w kontenerze lub tylko do kontenera.

Parametry: umożliwia dodanie dodatkowych parametrów do zadania oraz podgląd parametrów w aktualnej konfiguracji. Parametry te zmieniają się w zależności od wybranego rodzaju zadania.

Wyniki: umożliwia określenie, co chcesz zrobić z wynikami zadania. Strona Wyniki jest podzielona na dwie części: Wynik pośredni i Wynik końcowy, przy czym dozwolone są następujące wyniki: Powodzenie, Ostrzeżenie, Błąd i Przerwano. Na prawo od kolumny Wyniki znajduje się kolumna Działanie. Kliknięcie kolumny Działanie pozwala ustawić sposób powiadamiania o każdym wyniku. Działania obejmują wysłanie wyniku audytu lub wysłanie wiadomości e-mail po zakończeniu wyniku. Jeśli nie wybierzesz opcji, nie zostanie podjęte żadne działanie dla wyniku.

Na karcie **Śledzenie** można skonfigurować śledzenie dla określonego programu obsługi. Aby uzyskać więcej informacji, zobacz „Konfigurowanie poziomu śledzenia” na stronie 177.

Zarządzanie bibliotekami określonego zestawu programów obsługi

W obiektach bibliotek są przechowywane liczne założenia i inne zasoby współdzielone przez programy obsługi. Obiekt biblioteki można utworzyć w obiekcie zestawu programów obsługi lub w dowolnym kontenerze usługi eDirectory. W drzewie usługi eDirectory może istnieć wiele bibliotek. Programy obsługi mogą odwoływać się do dowolnej biblioteki w drzewie, dopóki na serwerze z uruchomionym programem obsługi jest przechowywana replika do odczytu/zapisu lub replika główna obiektu biblioteki.

Arkusze stylów, założenia, reguły i inne obiekty zasobów mogą być przechowywane w bibliotece i używane przez programy obsługi.

Przy użyciu modułu Zarządzanie bibliotekami można wykonywać następujące zadania:

- „Wyświetlanie i usuwanie istniejącej biblioteki” na stronie 148
- „Wyświetlanie i usuwanie obiektów z biblioteki” na stronie 148

Wyświetlanie i usuwanie istniejącej biblioteki

Aby wyświetlić i usunąć istniejącą bibliotekę, wykonaj następujące czynności:

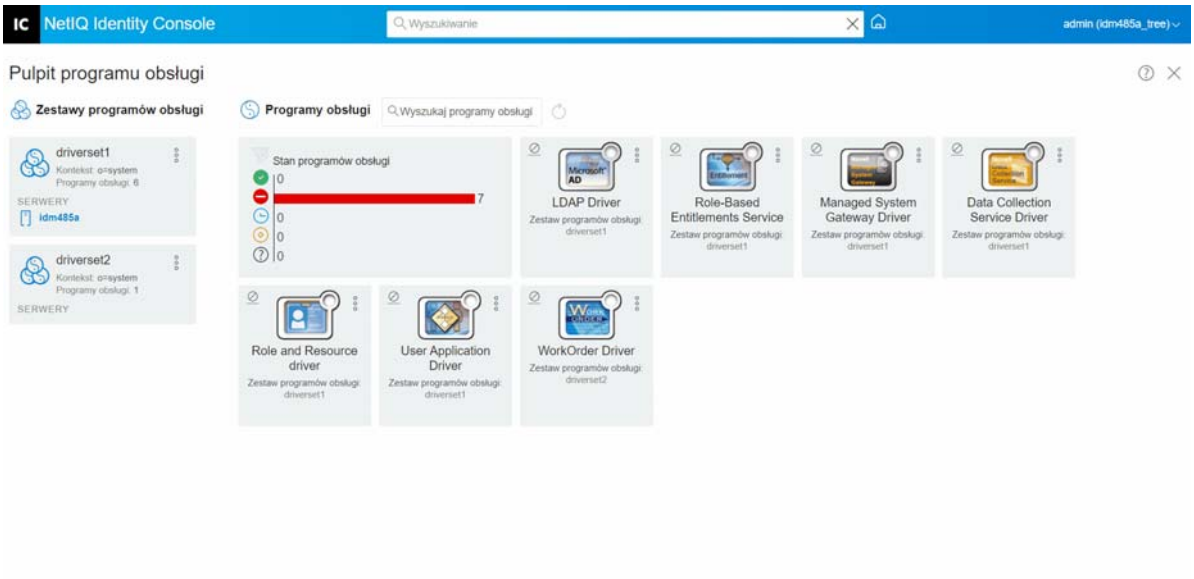
1. W portalu Identity Console wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Zaawansowane** > **Biblioteki**.
2. Wybierz odpowiednią bibliotekę z listy.
3. Kliknij ikonę  . Kliknij przycisk **OK**, aby potwierdzić.

Wyświetlanie i usuwanie obiektów z biblioteki

Istnieje możliwość wyświetlania i usuwania założeń oraz tabel mapowania z obiektów bibliotek. Aby usunąć obiekty, wykonaj następujące czynności:

1. W portalu Identity Console wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Zaawansowane** > **Biblioteki**.
2. Kliknij odpowiednią bibliotekę na liście.
3. Aby usunąć założenia, wybierz kartę **Założenia**.
4. Wybierz odpowiednie założenia z listy i kliknij ikonę  .
5. Aby usunąć tabele mapowania, wybierz kartę **Tabele mapowania**.
6. Wybierz odpowiednią tabelę mapowania z listy i kliknij ikonę  .
7. Kliknij przycisk **OK**, aby potwierdzić.

Rysunek 22-2 *Zarządzanie zadaniami i bibliotekami dla zestawów programów obsługi*



Konfigurowanie poziomów dziennika i śledzenia zestawów programów obsługi

Aby skonfigurować zapis w dzienniku i śledzenie dla zestawów programów obsługi, wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > kartę **Konfiguracja zapisu w dzienniku i śledzenia** na stronie głównej Identity Console. Ta sekcja jest podzielona na następujące kategorie:

- „Konfigurowanie poziomu dziennika” na stronie 149
- „Konfigurowanie poziomu śledzenia” na stronie 150
- „Śledzenie skryptu DirXML” na stronie 151

Konfigurowanie poziomu dziennika

Każdy zestaw programów obsługi ma pole poziomu dziennika — można w nim zdefiniować poziom błędów, które powinny być śledzone. Wskazany w tym miejscu poziom określa, jakie komunikaty są dostępne w dziennikach. Domyślnie poziom dziennika jest ustawiony na śledzenie komunikatów o błędach. (Obejmuje to również komunikaty o błędach krytycznych). W celu śledzenia dodatkowych typów komunikatów należy zmienić poziom dziennika. Aby skonfigurować poziom dziennika, wybierz Identity Console, wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Konfiguracja zapisu w dzienniku i śledzenia** > **Poziom dziennika**. W poniższej tabeli opisano ustawienia poziomu dziennika:

Opcja	Opis
Wyłącz zapis dziennika dla dzienników zestawu programów obsługi, subskrybenta i wydawcy	Wyłącza wszystkie zapisy dziennika dla wszystkich programów obsługi w obiekcie zestawu programów obsługi, kanale subskrybenta i kanale wydawcy.

Opcja	Opis
Maksymalna liczba pozycji w dzienniku (50–500)	Liczba pozycji w dzienniku. Wartość domyślna to 50.
Poziom dziennika	Dostępne do wyboru są następujące poziomy dziennika: ◆ **Zapisuj w dzienniku błędy**: w dzienniku są zapisywane tylko błędy. ◆ Zapisuj w dzienniku błędy i ostrzeżenia: w dzienniku są zapisywane błędy i ostrzeżenia. ◆ **Zapisuj w dzienniku określone zdarzenia**: w dzienniku są zapisywane wybrane zdarzenia. Wybranie tej opcji powoduje włączenie następującej listy zdarzeń: ◆ **Zdarzenia mechanizmu metakatalogów** ◆ **Zdarzenia stanu** ◆ **Zdarzenia operacji** ◆ **Zdarzenia transformacji** ◆ **Zdarzenia zaopatrywania poświadczeń** ◆ **Aktualizuj tylko czas ostatniego zapisu dziennika**: powoduje aktualizację czasu ostatniego zapisu dziennika. ◆ **Zapis dziennika wyłączony**: powoduje wyłączenie zapisu dziennika dla programu obsługi.

Konfigurowanie poziomu śledzenia

Dla określonego zestawu programów obsługi można skonfigurować śledzenie. W zależności od poziomu śledzenia określonego dla zestawu programów obsługi śledzenie wyświetla zdarzenia związane z programami obsługi podczas ich przetwarzania przez mechanizm. Poziom śledzenia programu obsługi ma wpływ tylko na program obsługi lub zestaw programów obsługi, w którym ustawiono śledzenie. W przypadku korzystania ze zdalnego modułu ładującego plik śledzenia zdalnego modułu ładującego jest ustawiany bezpośrednio w tym module i zawiera tylko śledzenie podkładki programu obsługi.

Aby skonfigurować śledzenie zestawu programów obsługi, wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Konfiguracja zapisu w dzienniku i śledzenia** > kartę **Śledzenie**. W poniższej tabeli opisano ustawienia śledzenia:

Parametr	Program obsługi
Poziom śledzenia	Wraz ze zwiększaniem poziomu śledzenia programu obsługi rośnie ilość informacji wyświetlanych przez funkcję Śledzenie. Pierwszy poziom śledzenia pokazuje błędy, ale nie ich przyczynę. Aby wyświetlać informacje o synchronizacji haseł, należy ustawić piąty poziom śledzenia. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.

Parametr	Program obsługi
Poziom śledzenia XSL	Śledzenie wyświetla zdarzenia XSL. Ten poziom śledzenia należy ustawiać tylko w przypadku rozwiązywania problemów z arkuszami stylów XSL. Aby nie wyświetlać informacji XSL, należy ustawić poziom na zero.
Port debugowania Java	Umożliwia deweloperom dołączanie debugera Java. Po dołączeniu debugera Java należy uruchomić ponownie bezpieczny magazyn tożsamości.
Plik śledzenia	Umożliwia określenie nazwy pliku i lokalizacji, w której są zapisywane informacje Identity Manager dotyczące wybranego programu obsługi. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.
Kodowanie pliku śledzenia	Plik śledzenia używa domyślnego kodowania systemu. W razie potrzeby można określić inne kodowanie. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.
Limit rozmiaru pliku śledzenia	Umożliwia ustawienie limitu dla pliku śledzenia Java. Jeśli zostanie ustawiony nieograniczony rozmiar pliku, plik będzie rósł, dopóki nie zabraknie miejsca na dysku. **UWAGA:** Określenie limitu rozmiaru pliku powoduje, że plik śledzenia jest dzielony na mniejsze pliki. Identity Manager automatycznie dzieli maksymalny rozmiar pliku przez dziesięć i tworzy oddzielne pliki. Połączony rozmiar tych plików jest równy maksymalnemu rozmiarowi pliku śledzenia. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.

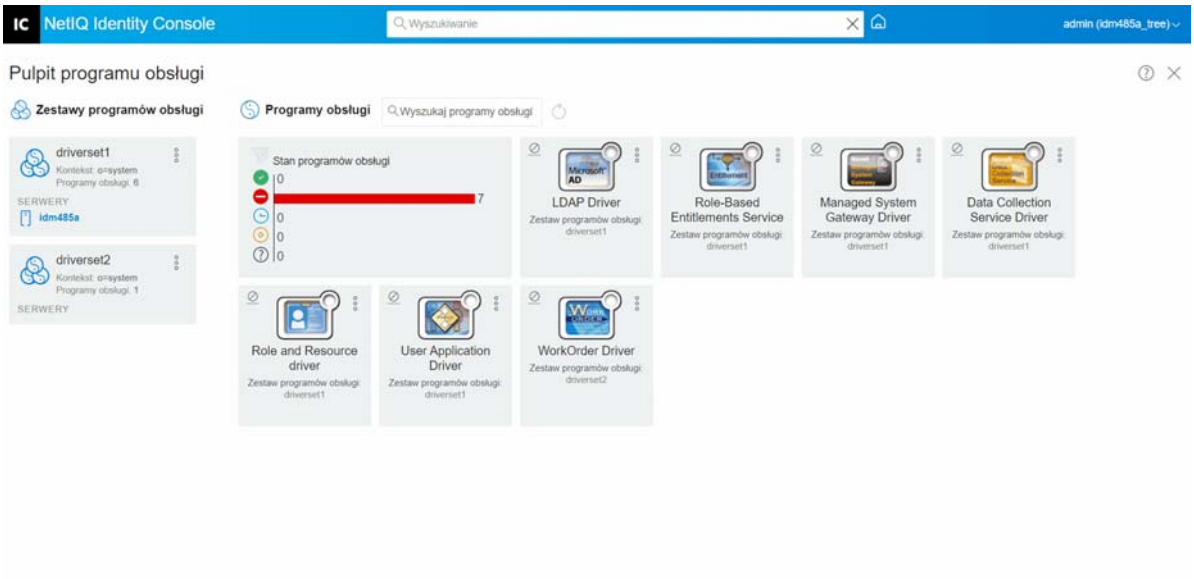
Śledzenie skryptu DirXML

Opcja Śledzenie skryptu DirXML umożliwia wybranie poziomu śledzenia dla zestawu programów obsługi. Wybrana opcja jest stosowana do wszystkich założeń w zestawie programów obsługi. Do wyboru są dostępne następujące opcje śledzenia skryptu DirXML:

- Śledzenie wszystkich skryptów DirXML włączone
- Śledzenie wszystkich skryptów DirXML wyłączone
- Śledzenie reguły skryptu DirXML włączone
- Śledzenie reguły skryptu DirXML wyłączone

Kliknij ikonę  , aby zapisać zmiany.

Rysunek 22-3 *Zarządzanie poziomami dziennika i śledzenia zestawów programów obsługi*



Zarządzanie inspektorem i statystykami zestawu programów obsługi

Inspektor zestawu programów obsługi umożliwia wyświetlanie szczegółowych informacji o obiektach skojarzonych z zestawem programów obsługi. Ta sekcja jest podzielona na następujące kategorie:

- „Wyświetlanie statystyki zestawu programów obsługi” na stronie 152
- „Wyświetlanie informacji o wersjach” na stronie 153
- „Wyświetlanie statystyki skojarzeń” na stronie 154

Wyświetlanie statystyki zestawu programów obsługi

W portalu Identity Console można wyświetlić różne statystyki dotyczące pojedynczego programu obsługi lub całego zestawu programów obsługi. Należą do nich takie statystyki jak: rozmiar pliku pamięci podręcznej, rozmiar nieprzetworzonych transakcji w pliku pamięci podręcznej, najstarsze i najnowsze transakcje oraz całkowita liczba nieprzetworzonych transakcji według kategorii (dodawanie, usuwanie, modyfikowanie itd.). Aby wyświetlić statystyki dotyczące zestawu programów obsługi:

1. W portalu Identity Console wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Inspektor i statystyka** > **Statystyka**.
2. Wybierz odpowiedni serwer z listy rozwijanej.

   Zostanie wyświetlona strona, na której można przejrzeć statystyki dotyczące wszystkich programów obsługi zawartych w zestawie programów obsługi.

   - Aby odświeżyć statystyki, kliknij ikonę .

- Aby zamknąć statystyki dotyczące programu obsługi, kliknij przycisk  w prawym górnym rogu okna statystyk programu obsługi.
- Aby otworzyć statystyki dotyczące wszystkich programów obsługi, kliknij opcje **Działania** > **Pokaż wszystko**.
- Aby zwinąć listę nieprzetworzonych transakcji programu obsługi, kliknij przycisk znajdujący się nad listą. Aby zwinąć listę nieprzetworzonych transakcji wszystkich programów obsługi, kliknij opcje **Działania** > **Zwiń wszystkie transakcje**.
- Aby rozwinąć listę transakcji, kliknij przycisk  . Aby rozwinąć listę nieprzetworzonych transakcji wszystkich programów obsługi, kliknij opcje **Działania** > **Rozwiń wszystkie transakcje**.
- Aby zamknąć pulpit statystyki wyłączonych programów obsługi, kliknij opcję **Działania**, a następnie wybierz opcję **Ukryj wyłączone programy obsługi**.

Wyświetlanie informacji o wersjach

Mechanizm Identity Manager, podkładki programów obsługi i pliki konfiguracji programów obsługi mają oddzielne numery wersji. Opcja Wykrywanie wersji w programie Identity Manager ułatwia znajdowanie wersji mechanizmu Identity Manager i wersji podkładek programów obsługi. Pliki konfiguracji programów obsługi mają własną konwencję nazewnictwa. Aby wyświetlić informacje o wersjach:

1. W portalu Identity Console wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Inspektor i statystyka** > **Wykrywanie wersji**.
2. Wyświetl ekran najwyższego poziomu informacji o wersji:
   - Drzewo usługi eDirectory, w którym jest uwierzytelniony użytkownik

     ---

     UWAGA: W środowisku Identity Manager usługa eDirectory jest nazywana bezpiecznym magazynem tożsamości.

   - Wybrany zestaw programów obsługi
   - Serwery skojarzone z zestawem programów obsługi

     Jeśli zestaw programów obsługi jest skojarzony z co najmniej dwoma serwerami, można wyświetlić informacje środowiska Identity Manager dotyczące każdego z nich.
   - Programy obsługi
3. Kliknij ikonę Wyświetl  , aby wyświetlić tekstową reprezentację informacji zawartych w widoku najwyższego poziomu.
4. Kliknij przycisk  Eksportuj, aby wyeksportować tekst i zapisać go w pliku na dysku lokalnym lub sieciowym.

Wyświetlanie statystyki skojarzeń

Przy użyciu funkcji Statystyka skojarzeń w programie Identity Manager można znajdować szczegóły skojarzeń tożsamości zarządzanych przez program Identity Manager. Identity Manager używa statystyki skojarzeń, aby uzyskać liczbę skojarzeń programów obsługi Identity Manager.

W celu uzyskania aktywnych, nieaktywnych i zarządzanych przez system obiektów programu obsługi należy uruchomić zadanie statystyki skojarzeń. Zadanie statystyki skojarzeń można zaplanować jako wykonywane codziennie, co tydzień, co miesiąc lub co roku. Domyślnie zaplanowane jest uruchamianie zadania co tydzień.

Na pulpicie Statystyka skojarzeń są wyświetlane szczegóły skojarzeń. Szczegóły można również przeglądać po wyeksportowaniu skojarzeń do pliku.

UWAGA

- Liczba skojarzeń dotyczących programów obsługi jest podawana dla każdego serwera osobno. Jeśli obiekt jest skojarzony z więcej niż jednym programem obsługi, liczba skojarzeń jest obliczana dla każdego programu obsługi oddzielnie.
- Jeśli liczba skojarzeń przekracza 200 000, zalecamy ustawienie maksymalnego rozmiaru sterty dla zestawu programów obsługi na co najmniej 2 GB. Aby uzyskać informacje na temat ustawiania rozmiaru sterty, zobacz „Konfigurowanie parametrów środowiska Java” na stronie 144.

Aby wyświetlić statystykę skojarzeń:

1. W portalu Identity Console wybierz opcję **Administracja IDM** > **kliknij menu kontekstowe (trzy kropki) odpowiedniego zestawu programów obsługi** > **Właściwości zestawu programów obsługi** > **Inspektor i statystyka** > **Statystyka skojarzeń**.
2. Wybierz serwer, dla którego chcesz uruchomić statystykę skojarzeń.
3. Liczba skojarzeń przedstawia obliczony wcześniej wynik.

   Identity Console wyświetla liczbę skojarzeń aktywnych, nieaktywnych i zarządzanych przez system obiektów dotyczących wszystkich programów obsługi skojarzonych z zestawem programów obsługi.

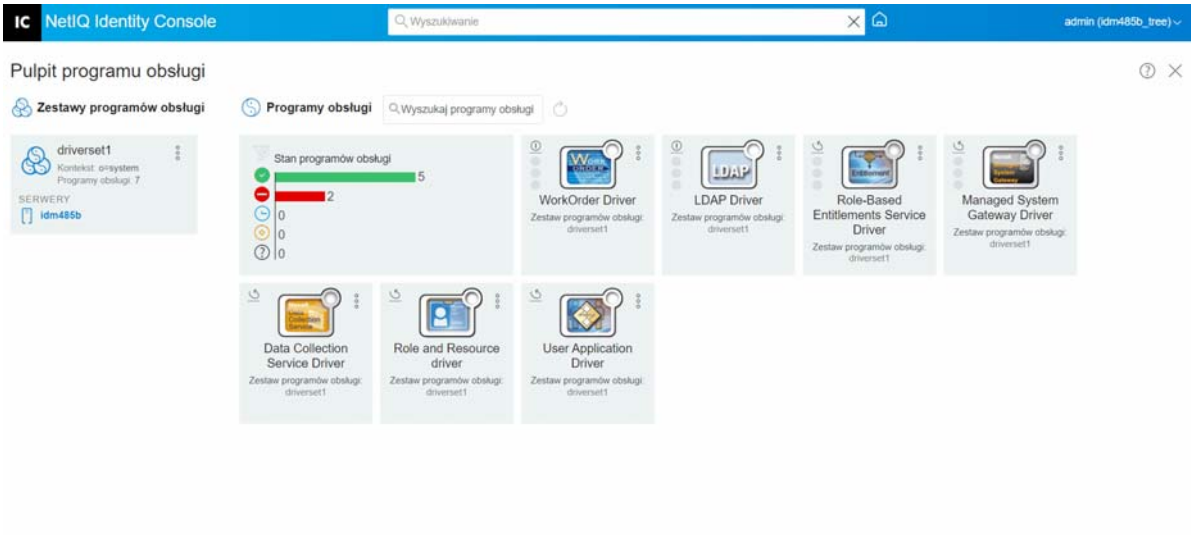
   Identity Console traktuje grupy i jednostki organizacyjne jak obiekty zarządzane przez system. Identity Console uznaje obiekt za nieaktywny, gdy atrybut `Logowanie wyłączone` w obiekcie jest prawdziwy, a obiekt nie został zmodyfikowany w ciągu ostatnich 120 dni. Wszystkie pozostałe obiekty są uważane za aktywne obiekty zarządzane.
4. Kliknij ikonę , aby uzyskać zaktualizowane wyniki.

   Gdy program obsługi jest wyłączony na serwerze, Identity Console nie wyświetla go na pulpicie.
5. Kliknij ikonę , aby wyeksportować szczegóły systemu i szczegóły dotyczące liczby skojarzeń programów obsługi skojarzonych z serwerem.
6. Aby wyeksportować obiekty skojarzone z określonym programem obsługi, kliknij ikonę obok wymaganych obiektów i zapisz plik.

UWAGA: W przypadku programów obsługi Fan-Out eksportowane są tylko unikatowe obiekty. Jeśli obiekt jest skojarzony z wieloma wystąpieniami programu obsługi Fan-Out, Identity Console wyświetla na pulpicie wszystkie liczby skojarzeń. Jednak w przypadku wybrania opcji eksportowania obiektów do pliku, Identity Console eksportuje tylko unikatowe obiekty.

7 Kliknij opcję **Działania** i wybierz wymaganą opcję, aby uporządkować pulpit liczby skojarzeń.

Rysunek 22-4 *Zarządzanie statystykami zestawu programów obsługi*



23 Zarządzanie właściwościami programów obsługi

W tej sekcji znajdują się informacje na temat właściwości, które są wspólne dla wszystkich programów obsługi. Należą do nich wszystkie właściwości (Nazwane hasło, Wartości kontroli mechanizmu, Poziom dziennika itd.).

Wyświetlana jest informacja o aktywacji dla programu obsługi, która przypomina o czynności, jaką należy wykonać w celu aktywowania wygasłego programu obsługi.

Aby zmodyfikować konfigurację programu obsługi, wykonaj następujące czynności:

1. Kliknij kartę **Programy obsługi** na ekranie domowym Identity Console.
2. Kliknij kafelek odpowiedniego programu obsługi, aby wyświetlić stronę konfiguracji programu obsługi.

   Domyślnie zostanie wyświetlona strona **Parametry połączenia**. Opcje konfiguracji programu obsługi są podzielone na następujące kategorie:

Parametry połączenia

Parametry połączenia sterują sposobem uruchamiania programu obsługi — lokalnie lub zdalnie.

- **Java:** Przy użyciu tej opcji można określić nazwę klasy Java, której wystąpienie jest tworzone dla składnika podkładki programu obsługi. Ta klasa może znajdować się w katalogu klas jako plik klasy lub w katalogu `lib` jako plik `JAR`. Tę opcję należy wybrać, aby uruchomić program obsługi lokalnie. Należy również określić opcje Hasło obiektu programu obsługi i Limit pamięci podręcznej programu obsługi. Nowe hasło można ustawić, klikając łącze **Ustaw hasło**.

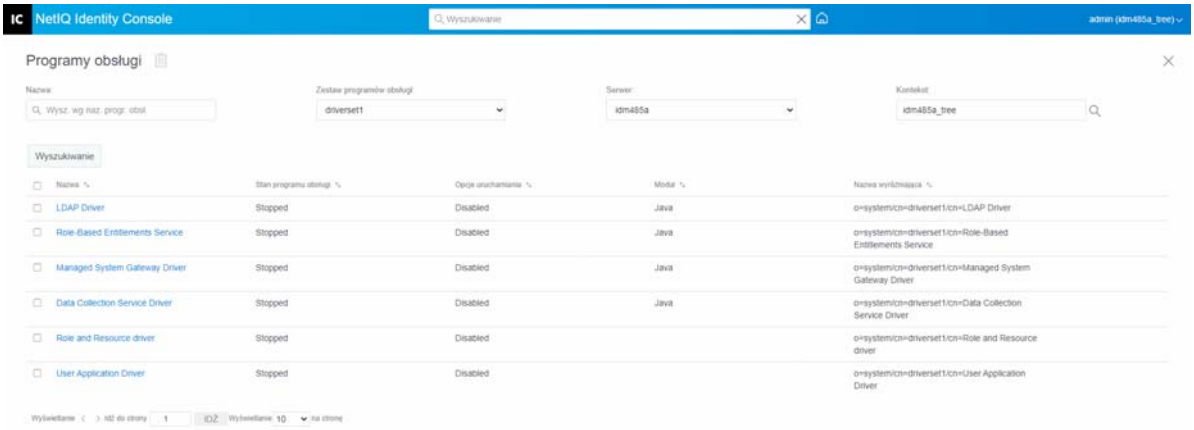
  Na przykład `com.microfocus.nds.dirxml.driver.scim.SCIMDriverShim`
- **Rodzimy:** Ta opcja służy do określania nazwy biblioteki `DLL`, która jest tworzona w rodzimym (na przykład C++) języku programu obsługi. Należy również określić opcje Hasło obiektu programu obsługi i Limit pamięci podręcznej programu obsługi. Nowe hasło można ustawić, klikając łącze **Ustaw hasło**.

  Na przykład `addriver.dll`

- **Połącz ze zdalnym modułem ładującym:** Ta opcja jest używana, gdy program obsługi łączy się zdalnie z połączonym systemem. Po wybraniu tej opcji należy określić następujące opcje podrzędne:
  - **Parametry połączenia zdalnego modułu ładującego**: Zawiera szczegółowe informacje na temat środowiska zdalnego modułu ładującego, takie jak Nazwa hosta, Port połączenia itd.
  - **Hasło zdalnego modułu ładującego**: Hasło dla zdalnego modułu ładującego.
  - **Hasło obiektu programu obsługi**: Określa hasło dla obiektu programu obsługi. Jeśli używany jest zdalny program ładujący, na tej stronie należy wprowadzić hasło. Zdalny moduł ładujący uwierzytelnia się tym hasłem w zdalnej podkładce programu obsługi.
- **Uwierzytelnianie**: Parametry Uwierzytelnianie służą do uwierzytelniania serwerów mechanizmu Identity Manager i zdalnego modułu ładującego. Należy określić następujące parametry:
  - **Identyfikator uwierzytelniania**: Należy określić identyfikator aplikacji użytkownika. Ten identyfikator służy do przekazywania informacji o subskrypcji z bezpiecznego magazynu tożsamości do aplikacji.
  - **Kontekst uwierzytelniania**: Należy określić adres IP lub nazwę serwera, z którym powinna komunikować się podkładka aplikacji.
  - **Hasło aplikacji**: Opcja umożliwiająca ustawienie hasła uwierzytelniania aplikacji.

Po zakończeniu należy kliknąć ikonę , aby zapisać konfigurację.

Rysunek 23-1 *Zarządzanie parametrami połączenia*



Konfiguracja programu obsługi

Sekcja konfiguracji programu obsługi umożliwia skonfigurowanie parametrów specyficznych dla programu obsługi, wartości kontroli mechanizmu, globalnych wartości konfiguracyjnych itd. Zmieniając parametry programu obsługi, dostosowuje się jego zachowanie do danego środowiska sieciowego. Ta sekcja jest podzielona na następujące kategorie:

Parametry programu obsługi

Parametry programu obsługi są podzielone na Ustawienia programu obsługi, Ustawienia subskrybenta i Ustawienia wydawcy. Ustawienie te zostaną wypełnione na podstawie konfiguracji programu obsługi. Więcej informacji na temat parametrów programu obsługi można znaleźć w przewodniku dotyczącym określonego programu obsługi w dokumentacji programów obsługi Identity Manager.

Po zakończeniu możesz zapisać parametry, klikając ikonę  . Aby ustawić domyślne wartości parametrów, kliknij ikonę  . W celu zmodyfikowania konfiguracji programu obsługi przy użyciu pliku XML kliknij ikonę  .

Globalne wartości konfiguracyjne

Wyświetla uporządkowaną listę obiektów konfiguracji globalnej. Obiekty zawierają definicje globalnych wartości konfiguracyjnych (GCV) rozszerzenia, które Identity Manager ładuje w czasie uruchamiania programu obsługi. Obiekty na karcie **Globalne wartości konfiguracyjne** można przeglądać lub modyfikować przy użyciu edytora XML. Kliknij ikonę  , aby zapisać globalne wartości konfiguracyjne. Aby odświeżyć listę globalnych wartości konfiguracyjnych, kliknij ikonę  . Aby usunąć globalne wartości konfiguracyjne, wybierz odpowiedni obiekt GCV i kliknij ikonę  .

Wartości kontroli mechanizmu

Wartości kontroli mechanizmu to sposób zmiany określonych zachowań domyślnych mechanizmu Identity Manager. Dostęp do wartości można uzyskać tylko w przypadku, gdy serwer jest skojarzony z obiektem Zestaw programów obsługi.

Opcja	Opis
Subscriber channel retry interval in seconds (Interwał ponawiania prób kanału subskrybenta w sekundach)	Interwał ponawiania prób kanału subskrybenta kontroluje, jak często mechanizm Identity Manager ponawia próby przetworzenia buforowanej transakcji, gdy obiekt subskrybenta podkładki aplikacji zwraca stan ponawiania próby.
Qualified form for DN-syntax attribute values (Format kwalifikowany wartości atrybutów składni w pełni kwalifikowanej nazwy)	Kwalifikowana specyfikacja wartości atrybutów składni w pełni kwalifikowanej nazwy kontroluje, czy wartości atrybutów składni w pełni kwalifikowanej nazwy są prezentowane w formacie niekwalifikowanym z ukośnikiem, czy w formacie kwalifikowanym z ukośnikiem. Ustawienie Prawda oznacza, że wartości są prezentowane w formacie kwalifikowanym.
Qualified form from rename events (Format kwalifikowany ze zdarzeń zmiany nazwy)	Format kwalifikowany dla zdarzeń zmiany nazwy kontroluje, czy fragment new-name zdarzeń zmiany nazwy pochodzących z bezpiecznego magazynu tożsamości jest prezentowany w kanale subskrybenta z kwalifikatorami typu. Na przykład CN=. Ustawienie Prawda oznacza, że nazwy są prezentowane w formacie kwalifikowanym.
Maximum eDirectory replication wait time in seconds (Maksymalny czas oczekiwania na replikację eDirectory w sekundach)	To ustawienie kontroluje maksymalny czas, przez który mechanizm Identity Manager oczekuje na replikację określonej zmiany między repliką lokalną a repliką zdalną. Ma to wpływ tylko na operacje, w których mechanizm Identity Manager musi skontaktować się ze zdalnym serwerem eDirectory w tym samym drzewie, aby wykonać operację, i przed ukończeniem operacji musi zaczekać na replikację pewnych zmian na serwerze zdalnym lub z serwera zdalnego (na przykład obiekt jest przenoszony, gdy na serwerze Identity Manager nie ma repliki głównej przenoszonego obiektu; operacje dotyczące praw systemu plików dla użytkowników utworzonych z szablonu).
Use non-compliant backwards-compatible mode for XSLT (Używaj niezgodnego trybu zgodności wstecznej dla procesora XSLT)	Ten element sterujący ustawia procesor XSLT używany przez mechanizm Identity Manager w tryb zgodności wstecznej. Tryb zgodności wstecznej powoduje, że procesor XSLT używa co najmniej jednego zachowania, które nie jest zgodne ze standardami XPath 1.0 i XSLT 1.0. Robi się tak w celu uzyskania zgodności wstecznej z istniejącymi arkuszami stylów DirXML, które zależą od niestandardowych zachowań. Na przykład zachowanie operatora XPath “!=”, gdy jednym operandem jest node-set, a drugim — inny niż node-set, jest nieprawidłowe w wersjach DirXML do Identity Manager 2.0 włącznie. To zachowanie zostało skorygowane, jednak skorygowane zachowanie jest domyślnie wyłączane przez ten element sterujący w celu uzyskania zgodności wstecznej z istniejącymi arkuszami stylów DirXML.
Maximum application objects to migrate at once (Maksymalna liczba obiektów aplikacji do jednoczesnej migracji)	Ten element sterujący służy do ograniczania liczby obiektów aplikacji, których żąda mechanizm Identity Manager z aplikacji podczas pojedynczego zapytania wykonywanego w ramach operacji migracji obiektów z aplikacji. Jeśli podczas operacji migracji z aplikacji występują błędy java.lang.OutOfMemoryError, należy ustawić liczbę mniejszą niż domyślna. Wartością domyślną jest 50. **UWAGA:** Ten element sterujący nie ogranicza liczby obiektów aplikacji, które można migrować, a jedynie ogranicza rozmiar partii.

Opcja	Opis
Set creatorsName on objects created in Identity Vault (Ustaw atrybut creatorsName w obiektach utworzonych w bezpiecznym magazynie tożsamości)	Ten element sterujący jest używany przez mechanizm Identity Manager do ustalania, czy atrybut creatorsName powinien być ustawiony na w pełni kwalifikowaną nazwę tego programu obsługi we wszystkich obiektach utworzonych w bezpiecznym magazynie tożsamości przez ten program obsługi. Ustawienie atrybutu creatorsName umożliwia łatwe identyfikowanie obiektów utworzonych przez ten program obsługi, ale wiąże się również ze spadkiem wydajności. Jeśli ta opcja nie jest ustawiona, atrybut creatorsName przyjmuje domyślnie w pełni kwalifikowaną nazwę obiektu serwera NCP, na którym jest hostowany program obsługi.
Write pending associations (Zapisuj oczekujące skojarzenia)	Ten element sterujący określa, czy mechanizm Identity Manager zapisuje oczekujące skojarzenie na obiekcie podczas przetwarzania kanału subskrybenta. Zapisywanie oczekującego skojarzenia przynosi niewielkie korzyści lub nie przynosi żadnych, ale wiąże się z obniżeniem wydajności. Niemniej jednak można włączyć tę opcję w celu zapewnienia zgodności wstecznej.
Use password event values (Użyj wartości zdarzenia dotyczącego hasła)	Ten element sterujący ustala źródło wartości zgłaszanej w przypadku atrybutu nspmDistributionPassword dla zdarzeń dodawania i modyfikowania kanału subskrybenta. Ustawienie elementu sterującego na Fałsz oznacza, że bieżąca wartość atrybutu nspmDistributionPassword jest uzyskiwana i zgłaszana jako wartość zdarzenia atrybutu. Oznacza to, że dostępna jest tylko wartość bieżącego hasła. Jest to zachowanie domyślne. Ustawienie elementu sterującego na Prawda oznacza, że wartość zarejestrowana ze zdarzeniem usługi eDirectory jest deszyfrowana i zgłaszana jako wartość zdarzenia atrybutu. Oznacza to, że dostępna jest zarówno wartość starego hasła (jeśli istnieje), jak i wartość hasła zastępczego w czasie zdarzenia. Przydaje się to do synchronizowania haseł w pewnych aplikacjach, które wymagają starego hasła do ustawienia nowego hasła.
Retry Out of Band events (Ponawiaj próby zdarzeń poza pasmem)	Ten element sterujący określa, czy zdarzenia synchronizacji poza pasmem powinny być ponawiane w przypadku otrzymania stanu **retry** (ponowienie próby) dla zdarzenia synchronizacji poza pasmem. Jeśli element sterujący ma ustawienie Fałsz, próby synchronizacji poza pasmem nie są ponawiane. Jeśli ustawieniem jest Prawda, próby synchronizacji poza pasmem są ponawiane aż do skutku.
Use Rhino ECMAScript engine (Użyj mechanizmu ECMAScript Rhino)	Określa, czy mechanizm Identity Manager używa mechanizmu ECMAScript Rhino. Jako domyślny mechanizm ECMAScript jest używany Rhino. Ten element sterujący domyślnie ma ustawienie **Prawda**. W przypadku ustawienia go na **Fałsz** mechanizm używa skryptu Nashorm.

Opcja	Opis
Enable Subscriber Service Channel (Włącz kanał usług subskrybenta)	Określa, czy mechanizm Identity Manager przetwarza zapytania poza pasmem w kanale usług subskrybenta programu obsługi. Niektóre z typowych przykładów tych zapytań to odświeżanie mapy kodów, zbieranie danych i zapytania wyzwalane z dxcmd. Gdy ten element sterujący jest ustawiony na Prawda, kanał przetwarza te zapytania oddzielnie, nie przerywając zwykłego przetwarzania zdarzeń. Obecnie ten element sterujący jest dostępny tylko do użytku z programem obsługi JDBC Fan-Out (domyślnie włączony).
Enable password synchronization status reporting (Włącz raportowanie stanu synchronizacji haseł)	Ten element sterujący określa, czy mechanizm Identity Manager raportuje stan zdarzeń zmiany hasła w kanale subskrybenta. Raportowanie stanu zdarzeń zmiany hasła w kanale subskrybenta umożliwia aplikacjom, takim jak Identity Manager User Application, monitorowanie postępu synchronizacji zmiany hasła, która powinna być zsynchronizowana z połączoną aplikacją.
Combine values from template object with those from add operation (Połącz wartości z obiektu szablonu z wartościami z operacji dodawania)	Ta wartość określa, czy podczas wykonywania operacji dodawania mechanizm Identity Manager łączy podobne wartości z szablonu tworzenia i operacji dodawania. Ustawienie wartości na Prawda powoduje korzystanie z wartości atrybutu o wielu wartościach z szablonu, oprócz wartości tego samego atrybutu, które są określone w operacji dodawania. Ustawienie wartości na Fałsz powoduje ignorowanie wartości z szablonu, jeśli wartości tego samego atrybutu zostały określone w operacji dodawania.
Allow event loopback from publisher to subscriber channel (Zezwalaj na pętlę zwrotną zdarzenia z kanału wydawcy do kanału subskrybenta)	Ta wartość określa, czy mechanizm Identity Manager zezwala na pętlę zwrotną zdarzenia z kanału wydawcy programu obsługi do kanału subskrybenta. Ustawienie wartości Fałsz powoduje, że mechanizm Identity Manager nie zezwala zdarzeniom na stosowanie pętli zwrotnej. Ustawienie wartości Prawda powoduje, że mechanizm Identity Manager zezwala zdarzeniom na stosowanie pętli z kanału wydawcy do kanału subskrybenta.

Opcja	Opis
Revert to calculated membership value behavior (Przywróć zachowanie obliczonej wartości członkostwa)	Ta wartość określa metodę używaną przez mechanizm Identity Manager podczas wykonywania działań odczytywania i wyszukiwania związanych z członkostwem w grupie. Ustawienie tej wartości na Fałsz (ustawienie domyślne) powoduje, że mechanizm Identity Manager podczas odczytywania lub wyszukiwania atrybutów Member (Członek) i Group Member (Członek grupy) obiektów bezpiecznego magazynu tożsamości zwraca tylko wartości statyczne. Wartości statyczne to obiekty, które otrzymały członkostwo w grupie w wyniku bezpośredniego przypisania do grupy, a nie wskutek odziedziczenia przypisania przez grupę zagnieżdżoną. Ustawienie tej wartości na Prawda powoduje, że mechanizm Identity Manager przywraca metodę używaną przed wersją Identity Manager 3.6. W wersjach starszych niż 3.6 wyszukiwanie atrybutów Member (Członek) i Group Member (Członek grupy) przez mechanizm Identity Manager pobierało wszystkie wartości obliczone. Wartości obliczone obejmują obiekty, które 1) mają członkostwo przypisane statycznie lub 2) mają członkostwo przypisane dynamicznie dzięki obliczeniom hierarchii grupy zagnieżdżonej używanym przez usługę eDirectory. Operacja wyszukiwania atrybutu Członek grupy zwraca wszystkie obiekty, które zostały przypisane do grupy bezpośrednio lub które uzyskały członkostwo za pośrednictwem grupy zagnieżdżonej.
Maximum time to wait for driver shutdown in seconds (Maksymalny czas oczekiwania na zamknięcie programu obsługi w sekundach)	To ustawienie kontroluje maksymalny czas oczekiwania przez mechanizm Identity Manager na zamknięcie kanału wydawcy programu obsługi. Jeśli program obsługi nie zostanie zamknięty w określonym przedziale czasu, mechanizm Identity Manager zakończy jego działanie.
Regular Expression escape meta-characters (Pomijane metaznaki wyrażenia regularnego)	Ten element sterujący określa metaznaki, które zostaną pominięte podczas rozwijania zmiennej lokalnej używanej w kontekście wyrażenia regularnego. Wszystkie znaki, które mają być pomijane, należy dodać do wartości tego elementu sterującego w postaci listy rozdzielonej przecinkami. Jeśli metaznak nie jest obecny w wartości elementu sterującego, nie będzie on pomijany podczas rozwijania zmiennej lokalnej zawierającej wyrażenie regularne. Używając tego elementu sterującego, należy zapewnić spełnienie następujących warunków: ◆ Wartość nie jest pozostawiona pusta. Domyślnie jest ona wypełniona znakiem ***$***. Ten znak jest wymagany do rozwijania zmiennej lokalnej. ◆ Wartość powinna być prawidłową listą rozdzieloną przecinkami (,). W przeciwnym razie podczas oceny założeń będą występować błędy. ◆ Aby pomijać wszystkie metaznaki, jako wartość należy określić "\,$,^,.,?,*,+,[,],(,),|". ◆ Jeśli metaznak nie musi być pomijany, należy usunąć go z wartości. ◆ Aby pomijać dowolny metaznak, należy go określić z ukośnikiem odwrotnym (\).

Opcja	Opis
Ignore Entitlement Changes of other drivers (Ignoruj zmiany uwierzytelnienia innych programów obsługi)	Ten element sterujący określa, czy mechanizm Identity Manager ignoruje, czy przetwarza zmiany uwierzytelnienia innych programów obsługi. Wartością domyślną jest Prawda. Oznacza to, że program obsługi automatycznie ignoruje zmiany uwierzytelnienia innych programów obsługi. Jeśli ten element sterujący jest ustawiony na Fałsz, zmiany uwierzytelnienia innych programów obsługi są buforowane i przetwarzane przez ten program obsługi.
Allow Entitlement event loopback from cprs to subscriber channel (Zezwalaj na pętlę zwrotną zdarzenia uwierzytelnienia z cprs do kanału subskrybenta)	Ten element sterujący określa, czy mechanizm Identity Manager zezwala zdarzeniu uwierzytelnienia, które jest generowane przez przypisanie CPRS, na stosowanie pętli zwrotnej do kanału subskrybenta programu obsługi. Wartością domyślną jest Fałsz. Oznacza to, że zdarzenie nie jest umieszczane w pętli zwrotnej do kanału subskrybenta. Jeśli ten element sterujący jest ustawiony na Prawda, zdarzenie przepływa do kanału subskrybenta programu obsługi.

Opcje uruchamiania

Opcje uruchamiania umożliwiają ustawianie stanu programu obsługi podczas uruchamiania serwera Identity Manager.

- **Automatyczne uruchomienie**: Program obsługi uruchamia się przy każdym uruchomieniu serwera Identity Manager.
- **Ręczne**: Program obsługi nie uruchamia się podczas uruchamiania serwera Identity Manager. Należy go uruchomić przy użyciu portalu Identity Console.
- **Wyłączone**: Program obsługi ma plik pamięci podręcznej, w którym są przechowywane wszystkie zdarzenia. Po ustawieniu programu obsługi na Wyłączone ten plik jest usuwany i nie są w nim zachowywane żadne nowe zdarzenia, dopóki stan programu obsługi nie zostanie zmieniony na Ręczne lub Automatyczne uruchomienie.

Po ustawieniu preferowanej opcji uruchamiania kliknij ikonę  , aby zapisać. Aby zresetować opcję uruchamiania, kliknij ikonę .

Nazwane hasło

Identity Manager umożliwia bezpieczne przechowywanie wielu haseł dla programu obsługi. Ta funkcja nosi nazwę nazwanych haseł. Dostęp do poszczególnych haseł uzyskuje się za pomocą klucza lub nazwy.

Nazwane hasła można dodać do zestawu programów obsługi lub do pojedynczych programów obsługi. Nazwane hasła zestawu programów obsługi są dostępne dla wszystkich programów obsługi w tym zestawie. Nazwane hasła pojedynczego programu obsługi są dostępne tylko dla tego programu.

Aby użyć nazwanego hasła w założeniach programu obsługi, należy odwołać się do niego za pomocą nazwy hasła, a nie rzeczywistego hasła. Hasło do programu obsługi jest wysyłane przez mechanizm Identity Manager. Metody przechowywania i pobierania nazwanych haseł, która została opisana w tej sekcji, można użyć z dowolnym programem obsługi, bez konieczności wprowadzania zmian w podkładce programu obsługi.

Aby dodać nowe nazwane hasło, kliknij ikonę . Aby usunąć istniejące nazwane hasło, kliknij ikonę . Aby zapisać listę, kliknij ikonę .

Równoważności zabezpieczeń

Za pośrednictwem strony Równoważności zabezpieczeń można przeglądać lub modyfikować listę obiektów o poziomie zabezpieczeń, któremu równoważny jest poziom zabezpieczeń programu obsługi. W praktyce obiekt posiada wszystkie prawa wyświetlonych obiektów.

Nowy obiekt można dodać do listy równoważności zabezpieczeń, klikając ikonę . W przypadku dodania lub usunięcia obiektu z listy system automatycznie dodaje lub usuwa ten obiekt z właściwości „Zabezpieczenia równoważne bieżącemu obiektowi”, będącej atrybutem tego obiektu. Do listy nie trzeba dodawać dysponenta o statusie [Publiczny] lub kontenerów nadrzędnych tego obiektu, ponieważ domyślnie poziom zabezpieczeń tego obiektu jest równoważny poziomowi określonemu dla tych elementów.

Aby usunąć istniejący obiekt z tej listy, kliknij ikonę . Aby zapisać listę, kliknij ikonę .

Wykluczone obiekty

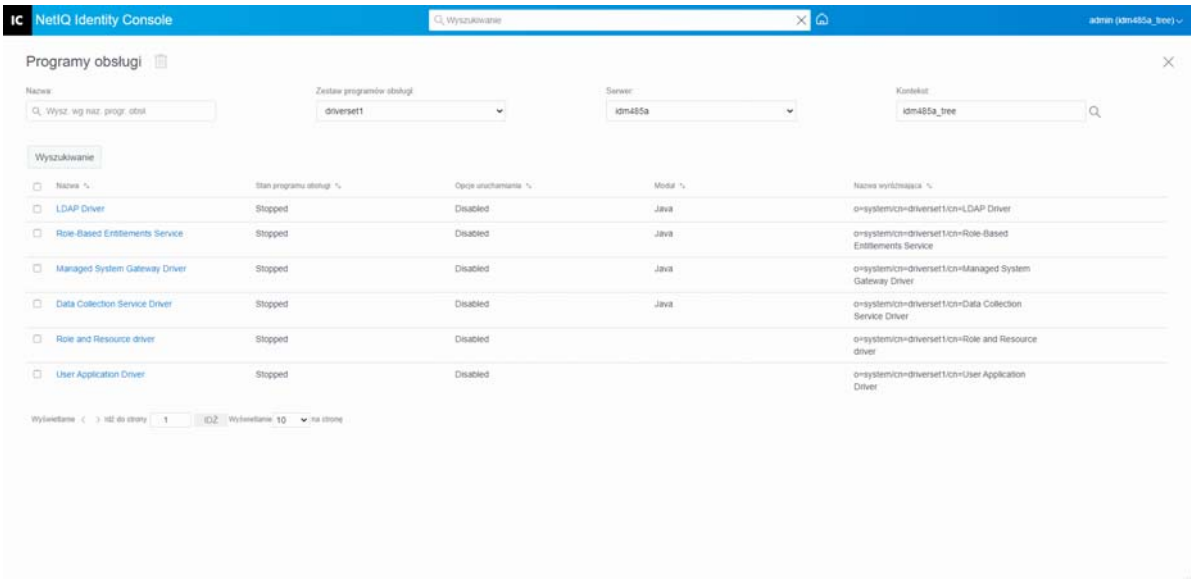
Przy użyciu tej opcji można utworzyć listę obiektów, które nie będą replikowane w aplikacji. Zalecamy dodanie do tej listy wszystkich obiektów reprezentujących role administracyjne (na przykład obiekt Administrator). Nowy obiekt można dodać do tej listy, klikając ikonę . Aby usunąć istniejący obiekt z tej listy, kliknij ikonę . Aby zapisać listę, kliknij ikonę .

Zarządzanie listą atrybutów z wartościami

Aby dodać atrybuty do listy atrybutów z wartościami dla określonego programu obsługi, wykonaj następujące czynności:

1. W portalu Identity Console wybierz moduł **Zarządzanie obiektami**.
2. Z listy rozwijanej wybierz typ **Dir-XML-Driver** i kliknij przycisk Wyszukaj.
3. Kliknij odpowiedni program obsługi na liście wyszukiwania.
4. Aby dodać atrybuty bez wartości do listy atrybutów z wartościami, kliknij ikonę obok pozycji **Atrybuty z wartościami** i wybierz właściwe atrybuty bez wartości z listy.
5. Po zakończeniu kliknij przycisk **OK**.

Rysunek 23-2 *Zarządzanie konfiguracją programów obsługi*



Transformacja i synchronizacja danych

Ta sekcja jest podzielona na następujące kategorie:

- „Widok synchronizacji danych” na stronie 166
- „Filtry klasy i atrybutu” na stronie 169
- „Skrypt ECMA” na stronie 170
- „Wzajemne mapowanie atrybutów” na stronie 170

Widok synchronizacji danych

Strona przeglądu programu obsługi jest podzielona na następujące kategorie:

- „Filtr” na stronie 167
- „Wszystkie założenia” na stronie 167
- „Migruj dane do bezpiecznego magazynu tożsamości” na stronie 167
- „Migracja danych z bezpiecznego magazynu tożsamości” na stronie 168
- „Synchronizowanie obiektów” na stronie 168
- „Śledzenie skryptu DirXML” na stronie 168

Filtr

Filtry istnieją dla programu obsługi i umożliwiają określenie klas i atrybutów, które mogą być wysyłane i odbierane między aplikacją a bezpiecznym magazynem tożsamości. Aby określić konkretną klasę do przekazania do mechanizmu metakatalogów w celu przetwarzania, należy dodać ją do filtru w odpowiednim kanale. Istnieje również możliwość filtrowania obiektów według określonej zdefiniowanej wartości atrybutu.

Aby dodać klasy i atrybuty, które mają być uwzględnione przy synchronizacji, oraz zmodyfikować filtr programu obsługi, kliknij opcję **Filtr** na kanale wydawcy lub subskrybenta.

UWAGA: Graficzna prezentacja przeglądu pokazuje dwa oddzielne obiekty dla filtru programu obsługi na kanale wydawcy i subskrybenta. Mimo że pokazane są dwa obiekty, dla obu kanałów używany jest ten sam filtr.

Wszystkie założenia

Domyślnie jest wyświetlana strona Wszystkie założenia. Istniejące założenia można zaimportować do kontenera, klikając ikonę . Można również usunąć wszelkie założenia, które nie są wymagane. Aby wybrać poziom śledzenia programu obsługi, kliknij ikonę . Założenia można przenosić w górę i w dół listy za pomocą ikon oraz .

UWAGA: Dodawanie i wdrażanie nowych założeń dla programów obsługi nie jest obsługiwane w Identity Console. Do dodawania i wdrażania nowych założeń zalecamy używanie programów iManager i Identity Designer.

Migruj dane do bezpiecznego magazynu tożsamości

Przy użyciu tego zadania można zdefiniować kryteria używane przez Identity Manager w celu migracji obiektów z aplikacji do bezpiecznego magazynu tożsamości. W czasie migracji obiektu mechanizm metakatalogów stosuje do obiektu wszystkie założenia dopasowywania, umieszczania i tworzenia, a także filtr wydawcy. Obiekty są migrowane do bezpiecznego magazynu tożsamości w kolejności określonej na liście klas. Przy użyciu tej opcji można wykonywać następujące zadania:

1. **Dodawanie klasy i atrybutów**: Aby dodać lub usunąć klasy i atrybuty, które mają być poddane migracji, kliknij ikonę . Następnie wybierz klasę i odpowiednie jej atrybuty, które chcesz dodać. Po wybraniu klasy i atrybutów kliknij opcję **Dodaj**, aby zapisać zmiany.
2. **Edytowanie wartości atrybutu**: Aby zmienić wartość atrybutu migracji określoną podczas edytowania listy, kliknij ikonę edycji atrybutu .
3. **Zmienianie kolejności listy klas**: Za pomocą przycisków i zmień kolejność klas na liście. Obiekty są migrowane do bezpiecznego magazynu tożsamości w kolejności określonej na liście klas.
4. **Odświeżanie:** Kliknij ikonę , aby odświeżyć listę.

Migracja danych z bezpiecznego magazynu tożsamości

Na karcie **Eksportuj** można wybrać kontenery lub obiekty, które mają zostać poddane migracji z bezpiecznego magazynu tożsamości do aplikacji. W czasie migracji obiektu mechanizm metakatalogów stosuje do obiektu wszystkie założenia dopasowywania, tworzenia i umieszczania, a także filtr subskrybenta.

Aby przeprowadzić migrację obiektów lub kontenerów z bezpiecznego magazynu tożsamości do innej aplikacji, kliknij ikonę  . Znajdź i wybierz obiekt, który chcesz poddać migracji, a następnie kliknij przycisk **OK**, aby dodać go do listy migracji. Aby usunąć obiekty z listy migracji, kliknij ikonę  .

Po zakończeniu wybierania obiektów do migracji kliknij przycisk  , aby rozpocząć migrację. Na ekranie zostanie wyświetlony postęp migracji. Jeśli chcesz zatrzymać migrację, kliknij przycisk  .

Synchronizowanie obiektów

Operacja synchronizacji szuka obiektów, które zostały zmodyfikowane, i synchronizuje je. Aby rozpocząć synchronizację natychmiast, można wybrać opcję **Sprawdź wszystkie obiekty**. Można również ustawić datę/godzinę rozpoczęcia synchronizacji.

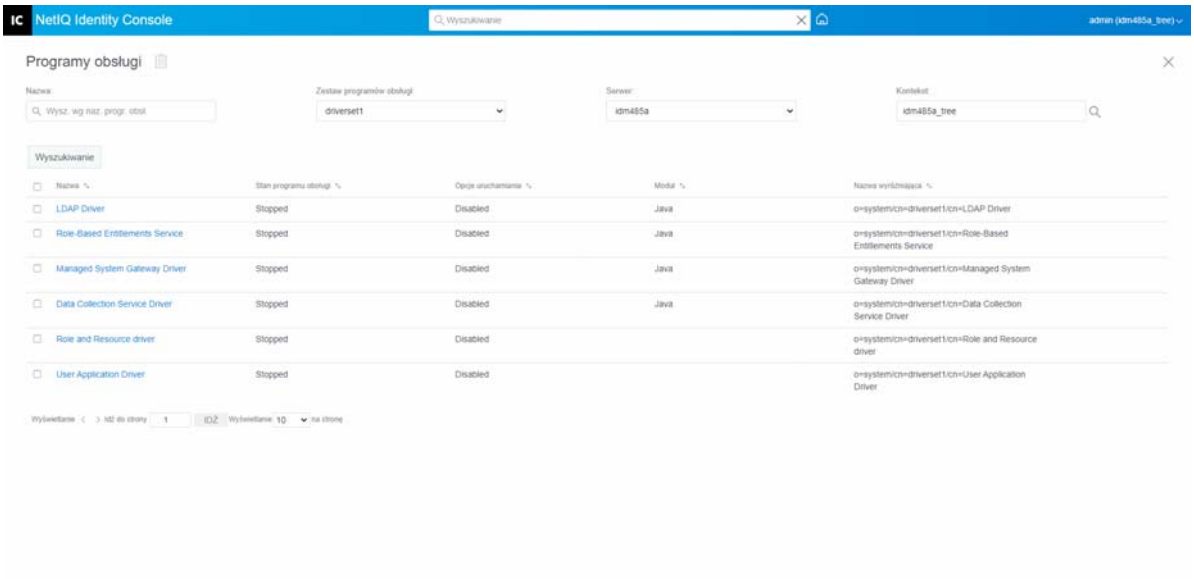
Śledzenie skryptu DirXML

Opcja śledzenia skryptów DirXML umożliwia wybranie poziomu śledzenia dla programu obsługi. Stosuje również ustawienia śledzenia do wszystkich kanałów wydawcy i subskrybenta. Do wyboru są dostępne następujące opcje śledzenia skryptu DirXML:

- Śledzenie wszystkich skryptów DirXML włączone
- Śledzenie wszystkich skryptów DirXML wyłączone
- Śledzenie reguły skryptu DirXML włączone
- Śledzenie reguły skryptu DirXML wyłączone

Kliknij ikonę  , aby zapisać zmiany.

Rysunek 23-3 *Zarządzanie synchronizacją danych programów obsługi*



Filtry klasy i atrybutu

Filtry klasy i atrybutu umożliwiają określenie klas i atrybutów, które mogą być wysyłane i odbierane między aplikacją a bezpiecznym magazynem tożsamości. Aby określić konkretną klasę do przekazania do mechanizmu metakatalogów w celu przetwarzania, należy dodać ją do filtru w odpowiednim kanale. Istnieje również możliwość filtrowania obiektów według określonej zdefiniowanej wartości atrybutu. Przy użyciu tej opcji można wykonywać następujące działania:

- **Ustawienie szablonu**: Ta opcja służy do ustawiania opcji domyślnych dla wszystkich atrybutów dodawanych do filtru. Kliknij ikonę obok etykiety Filtr klasy/atrybutu.
- **Dodanie nowej klasy**: Dodaj nową klasę, klikając ikonę .
- **Dodanie nowego atrybutu**: Dodaj nowy atrybut, klikając ikonę .
- **Kopiuj filtr z**: ta opcja umożliwia skopiowanie filtru z innego programu obsługi. Kliknij ikonę , aby skopiować filtr.
- **Edycja pliku XML**: Przeprowadź edycję ustawień filtru klasy i atrybutu przy użyciu ikony edycji pliku XML .
- **Usunięcie klasy lub atrybutu**: Usuń dowolną klasę lub atrybut, klikając ikonę obok odpowiedniej klasy lub atrybutu.

Dla wartości klasy i atrybutu w kanałach wydawcy i subskrybenta można ustawić następujące opcje:

- Synchronizuj
- Ignoruj
- Powiadom
- Resetuj

Zasada scalania

Jeśli atrybut nie jest synchronizowany w żadnym kanale, scalanie się nie odbywa.

Jeśli atrybut jest synchronizowany tylko w jednym kanale, wszystkie istniejące wartości w lokalizacji docelowej tego kanału są usuwane i zastępowane wartościami z jego lokalizacji źródłowej. Jeśli w lokalizacji źródłowej znajduje się wiele wartości, a lokalizacja docelowa może pomieścić tylko pojedynczą wartość, po stronie docelowej jest używana tylko jedna z wartości.

Jeśli atrybut jest synchronizowany w obu kanałach i obie strony mogą pomieścić tylko pojedyncze wartości, połączona aplikacja pobiera wartości przechowywane w bezpiecznym magazynie tożsamości, chyba że nie ma tam żadnej wartości. W tym scenariuszu bezpieczny magazyn tożsamości uzyskuje wartości z połączonej aplikacji.

Jeśli atrybut jest synchronizowany w obu kanałach i tylko jedna strona może pomieścić wiele wartości, wartość z kanału z pojedynczą wartością jest dodawana do kanału z wieloma wartościami, jeśli jeszcze jej tam nie ma. Jeśli po stronie pojedynczej wartości nie ma żadnej wartości, można wybrać wartość, która zostanie dodana po tej stronie. Dla ustawienia Zasada scalania można wybrać następujące opcje:

- Domyślne
- Bezpieczny magazyn tożsamości
- Aplikacja
- Brak

Kliknij ikonę  , aby zapisać zmiany.

Skrypt ECMA

Wyświetla uporządkowaną listę plików zasobu ECMAScript. Pliki zawierają funkcje rozszerzenia programu obsługi, które Identity Manager ładuje w czasie jego uruchamiania. Można importować dodatkowe pliki, klikając przycisk , usuwać istniejące pliki, klikając przycisk  , lub zmieniać kolejność wykonywanych plików. Można też przenosić skrypty w górę i w dół listy. Aby zapisać listę skryptów ECMA, należy kliknąć ikonę  .

Wzajemne mapowanie atrybutów

Wzajemne mapowania atrybutów umożliwiają tworzenie łączy wstecznych (odwołań) między obiektami oraz zarządzanie nimi. Na przykład obiekt Group (Grupa) zawiera atrybut Members (Członkowie), który odwołuje się do wszystkich obiektów User (Użytkownik) należących do tej grupy. Podobnie każdy obiekt User (Użytkownik) zawiera atrybut Group Membership (Członkostwo w grupie) odwołujący się do obiektów Group (Grupa), których członkiem jest ten użytkownik. Aby mechanizm metakatalogów mógł zachować synchronizację obiektu Group (Grupa) > atrybutu Members (Członkowie) z obiektem User (Użytkownik) > atrybutem Group Membership (Członkostwo

w grupie) dla wszystkich obiektów Group (Grupa) i User (Użytkownik) w bezpiecznym magazynie tożsamości, te atrybuty muszą być połączone. Łącza między atrybutami obiektów noszą nazwę wzajemnych mapowań atrybutów.

Przy użyciu tego modułu można wykonywać następujące działania:

Tworzenie niestandardowych wzajemnych mapowań atrybutów

Ta sekcja dotyczy tylko sytuacji, w której na stronie Wzajemne mapowanie atrybutów jest wyświetlany monit **Program obsługi nie zawiera niestandardowych wzajemnych mapowań atrybutów. Kliknij ikonę „+” powyżej, aby utworzyć podstawowe wzajemne mapowania atrybutów**.

1. Kliknij ikonę +, aby utworzyć nową listę niestandardowych wzajemnych mapowań atrybutów.
2. Zostaną wyświetlone domyślne mapowania atrybutów programu obsługi. Teraz możesz dodawać, modyfikować lub usuwać mapowania.

Dodawanie nowego wzajemnego mapowania atrybutów

Po utworzeniu wzajemnego mapowania atrybutów należy najpierw dodać jeden z atrybutów do listy mapowania wzajemnego.

1. Kliknij ikonę + obok menu rozwijanego Działania.
2. W nowym wpisie atrybutu wybierz żądany atrybut z listy rozwijanej.
3. Określ szczegóły mapowania wzajemnego:
   - 3a **Klasa źródłowa**: Określa nazwę klasy, z którą jest skojarzony atrybut w mapowaniu. Na przykład jeśli na liście mapowania wzajemnego został umieszczony atrybut Group Membership (Członkostwo w grupie), skojarzoną klasą źródłową jest User (Użytkownik).
   - 3b **Klasa docelowa**: Określa nazwę klasy skojarzoną z atrybutem, dla którego ma zostać utworzone mapowanie wzajemne. Na przykład jeśli na liście mapowania wzajemnego został umieszczony atrybut Group Membership (Członkostwo w grupie), skojarzoną klasą docelową jest Group (Grupa).
   - 3c **Atrybut docelowy**: Określa nazwę atrybutu, dla którego ma zostać utworzone mapowanie wzajemne.
4. Jeśli chcesz zamapować atrybut na inny atrybut docelowy, kliknij ikonę + po prawej stronie nazwy atrybutu.

   Na końcu listy atrybutu zostanie dodana nowa sekcja atrybutu. Wybierz klasę źródłową, klasę docelową i atrybut docelowy.

Usuwanie wzajemnego mapowania atrybutów

Aby usunąć wzajemne mapowanie atrybutów:

1. Zaznacz pole wyboru wzajemnego mapowania atrybutów, które chcesz usunąć, przed polem **Klasa źródłowa**.
2. Kliknij ikonę obok listy rozwijanej atrybutu.

Usuwanie atrybutu z listy mapowania wzajemnego

Aby usunąć atrybut z listy mapowania wzajemnego:

1. Wybierz atrybut, który chcesz usunąć, zaznaczając pole wyboru przed atrybutem.
2. Kliknij ikonę obok listy rozwijanej **Działania**.

Zmienianie kolejności mapowanych atrybutów

Mapowania atrybutów są rozstrzygane w wyświetlanej kolejności z góry na dół. Aby zapewnić prawidłową kolejność rozstrzygania mapowanych atrybutów, można przenosić je w górę lub w dół listy. Na ogół najpierw należy wymieniać na liście specyficzne mapowania, a dopiero w dalszej kolejności bardziej ogólne. Na przykład mapowanie atrybutu Member (Członek) na obiekt Group (Grupa) powinno znajdować się na liście przed mapowaniem atrybutu Member (Członek) na dowolne obiekty (opcja <Dowolna klasa>).

Zaznacz pole wyboru przed mapowanym atrybutem, który chcesz przenieść, a następnie kliknij ikonę ↑, aby przenieść atrybut w górę, lub ikonę ↓ w celu przeniesienia go w dół.

Usuwanie niestandardowego wzajemnego mapowania atrybutów

Utworzone przez siebie niestandardowe mapowania atrybutów można usunąć. Powoduje to, że mechanizm metakatalogów używa domyślnych mapowań atrybutów programu obsługi.

Aby usunąć niestandardowe wzajemne mapowanie atrybutów, kliknij ikonę u góry ekranu.

Edytowanie kodu XML atrybutu docelowego

W razie potrzeby można edytować bezpośrednio kod XML atrybutu docelowego. W tym celu kliknij ikonę Edytuj XML na stronie Niestandardowe wzajemne mapowanie atrybutów. Spowoduje to otwarcie podstawowego edytora XML, w którym można zmodyfikować kod XML. Po zakończeniu należy kliknąć przycisk OK lub Anuluj, aby zamknąć edytor XML.

Ustawienia zaawansowane

Ustawienia zaawansowane są podzielone na następujące kategorie:

Zarządzanie uwierzytelnieniami

Na stronie Uwierzytelnienia znajduje się tabela zawierająca wszystkie uwierzytelnienia, które są obecnie zdefiniowane w wybranym programie obsługi (wyświetlane są ich w pełni kwalifikowane nazwy). Na tej stronie są dozwolone następujące działania:

- **Edytowanie w pliku XML**: Aby edytować uwierzytelnienia w pliku XML, wybierz uwierzytelnienie z listy i kliknij ikonę . Następnie zaznacz pole **Włącz edytowanie XML**.
- **Usuwanie**: Aby usunąć uwierzytelnienie, kliknij pole po lewej stronie nazwy uwierzytelnienia, a następnie kliknij ikonę . Zostanie wyświetlony komunikat z informacją o tym, że operacji nie będzie można cofnąć, i z pytaniem, czy na pewno chcesz usunąć wybrane uwierzytelnienie. Kliknij przycisk **OK**, aby usunąć uwierzytelnienie, lub przycisk **Anuluj**, aby zatrzymać operację. Możesz kliknąć kilka pól, aby usunąć kilka uwierzytelnień, lub kliknąć pole po lewej stronie u góry, aby usunąć wszystkie uwierzytelnienia.

Zarządzanie tabelą mapowania obiektów

Tabele mapowania są używane w założeniach Identity Manager do mapowania zestawu wartości na inny zestaw odpowiadających im wartości. Po zainstalowaniu pakietu uwierzytelnień jego założenia są dodawane do zastawu założeń uruchamiania programu obsługi. Program obsługi wykonuje te założenia tylko raz podczas uruchamiania programu obsługi. Aby uzyskać więcej informacji, zobacz Mapping Table Objects (Obiekty tabeli mapowania) w dokumencie *NetIQ Identity Manager Driver Administration Guide* (NetIQ Identity Manager Driver — podręcznik administracji).

Przy użyciu tabeli mapowania obiektów można wykonywać następujące działania:

- **Modyfikowanie istniejącego mapowania:** Aby zmodyfikować istniejącą tabelę mapowania obiektów, kliknij mapowanie na liście i na kolejnym ekranie wykonaj następujące działania:
  - Dodaj nową kolumnę.

    Określ wartość dla kolumny, a następnie wybierz, czy w wartości jest, czy nie jest uwzględniana wielkość liter lub czy wartość jest liczbowa.
  - Dodaj nowy wiersz i określ wartość dla wiersza.
  - Kliknij ikonę .
- **Usuwanie mapowania**: Aby usunąć mapowanie z listy, wybierz odpowiednie mapowanie na liście i kliknij ikonę .
- **Edytowanie w pliku XML**: Aby edytować mapowanie w pliku XML, kliknij mapowanie na liście i wybierz ikonę . Następnie zaznacz pole **Enable XML Editing** (Włącz edytowanie XML).

Zarządzanie zadaniami dla programów obsługi

Identity Console umożliwia planowanie zdarzeń przy użyciu opcji Zadania dla wszystkich poszczególnych programów obsługi.

Strona Zadania zawiera nazwę zadania, stan zadania (włączone lub wyłączone), zaplanowany czas uruchomienia i opis zadania. Kliknij nazwę zadania, aby wyświetlić stronę Zadania. Kliknij ikonę włączenia/wyłączenia w kolumnie Włączono, aby włączyć lub wyłączyć zadanie. Kliknij opis zadania, aby wyświetlić pełne informacje o zadaniu.

Na karcie Zadania znajduje się tabela zawierająca istniejące obiekty zadań wybranego programu obsługi, który jest wyświetlany pod w pełni kwalifikowaną nazwą we wpisie Program obsługi.

Na stronie Zadania można wykonać następujące zadania:

- **Utwórz zadanie**: kliknij ikonę +, aby utworzyć nowe zadanie.

  W oknie podręcznym **Nowe zadanie** wykonaj następujące czynności w celu utworzenia nowego zadania:

  1. Podaj nazwę zadania.
  2. Wybierz typ zadania.
  3. Kliknij ikonę ∨ i z dostępnej listy serwerów wybierz serwer, na którym zadanie ma być uruchamiane. W przeciwnym razie określ nazwę serwera, a następnie wybierz serwer.
  4. Kliknij przycisk **Utwórz**.
- **Uruchom wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ▷.
- **Zatrzymaj wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ⊡.
- **Włącz wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ✓.
- **Wyłącz wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ⊗.
- **Uzyskaj stan**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę ⓘ.
- **Usuń wybrane zadanie**: wybierz zadanie, klikając pole po lewej stronie zadania, a następnie kliknij ikonę 🗑.

Kliknij zadanie, aby uzyskać dostęp do strony **Właściwość zadania**. Na stronie tej możesz skonfigurować sposób uruchamiania zadania.

Ogólne: przedstawia nazwę klasy Java dla zadania. Na tej stronie możesz włączyć lub wyłączyć zadanie, usunąć zadanie po jego wykonaniu, wybrać serwer lub serwery, na których zadanie ma być uruchamiane, określić serwer poczty e-mail oraz nadać zadaniu inną nazwę i opis.

Plan: umożliwia ustawienie czasu uruchamiania zadania. Podaj wartość w polu Uruchom zadanie o, aby ustawić godzinę, i określ, czy zadanie ma być uruchamiane codziennie, co tydzień, co miesiąc czy co rok. Możesz też dostosować czas uruchamiania zadania lub włączyć przełącznik, aby uruchamiać zadanie ręcznie.

Zakres: umożliwia określenie obiektów, których dotyczy to zadanie. Obiekt może być kontenerem, grupą dynamiczną, grupą lub obiektem typu liść. Kliknij przycisk Dodaj, aby wybrać obiekt, którego ma dotyczyć to zadanie. Możesz użyć przycisku Przeglądaj, aby wybrać obiekt, a następnie kliknij przycisk OK. Aby usunąć obiekt z listy zakresu, wybierz obiekt zakresu, klikając pole po lewej stronie obiektu DN, a następnie kliknij przycisk Usuń.

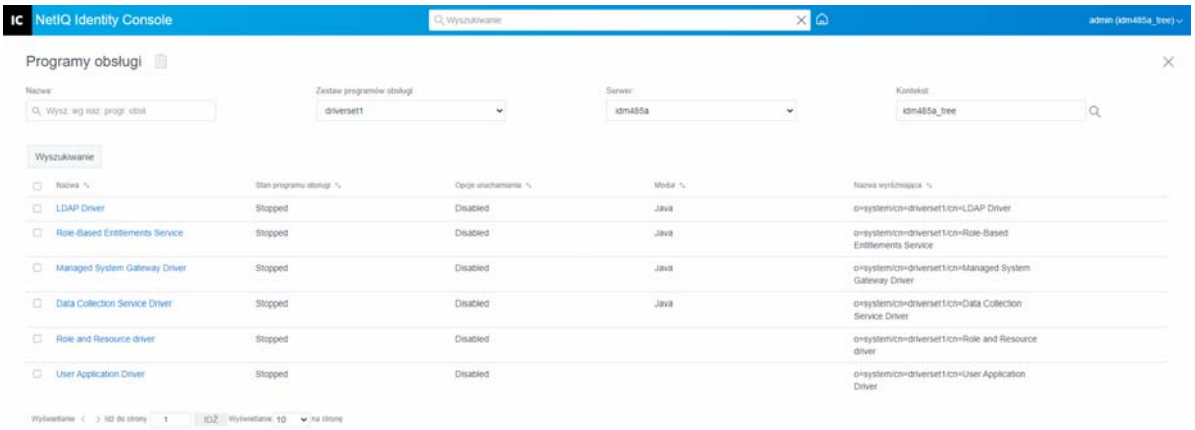
Po dodaniu obiektu wybierz go, aby wyświetlić więcej opcji. Jeśli wybierzesz obiekt grupy, masz możliwość zastosowania zadania do członków grupy lub tylko do grupy. Jeśli wybierzesz obiekt kontenera, masz możliwość zastosowania zadania do wszystkich elementów potomnych w tym kontenerze, do wszystkich elementów podrzędnych w kontenerze lub tylko do kontenera.

Parametry: umożliwia dodanie dodatkowych parametrów do zadania oraz podgląd parametrów w aktualnej konfiguracji. Parametry te zmieniają się w zależności od wybranego rodzaju zadania.

Wyniki: umożliwia określenie, co chcesz zrobić z wynikami zadania. Strona Wyniki jest podzielona na dwie części: Wynik pośredni i Wynik końcowy, przy czym dozwolone są następujące wyniki: Powodzenie, Ostrzeżenie, Błąd i Przerwano. Na prawo od kolumny Wyniki znajduje się kolumna Działanie. Kliknięcie kolumny Działanie pozwala ustawić sposób powiadamiania o każdym wyniku. Działania obejmują wysłanie wyniku audytu lub wysłanie wiadomości e-mail po zakończeniu wyniku. Jeśli nie wybierzesz opcji, nie zostanie podjęte żadne działanie dla wyniku.

Na karcie **Śledzenie** można skonfigurować śledzenie dla określonego programu obsługi. Aby uzyskać więcej informacji, zobacz „Konfigurowanie poziomu śledzenia” na stronie 177.

Rysunek 23-4 *Zarządzanie ustawieniami zaawansowanymi*



Konfigurowanie poziomów dziennika i śledzenia programów obsługi

Aby skonfigurować zapis w dzienniku i śledzenie dla programów obsługi, wybierz opcję **Drivers** (Programy obsługi) > kartę **Konfiguracja zapisu w dzienniku i śledzenia** na stronie głównej Identity Console. Ta sekcja jest podzielona na następujące kategorie:

- „Konfigurowanie poziomu dziennika” na stronie 176
- „Konfigurowanie poziomu śledzenia” na stronie 177

Konfigurowanie poziomu dziennika

Każdy program obsługi ma pole poziomu dziennika umożliwiające zdefiniowanie poziomu błędów, które powinny być śledzone. Wskazany w tym miejscu poziom określa, jakie komunikaty są dostępne w dziennikach. Domyślnie poziom dziennika jest ustawiony na śledzenie komunikatów o błędach. (Obejmuje to również komunikaty o błędach krytycznych). W celu śledzenia dodatkowych typów komunikatów należy zmienić poziom dziennika. Aby skonfigurować poziom dziennika, należy wybrać opcję **Konfiguracja zapisu w dzienniku i śledzenia** > kartę **Poziom dziennika**. W poniższej tabeli opisano ustawienia poziomu dziennika:

Opcja	Opis
Użyj ustawień dziennika z zestawu programów obsługi	Po zaznaczeniu tej opcji program obsługi zapisuje w dzienniku zdarzenia na podstawie ustawień dziennika obiektu zestawu programów obsługi.
Wyłącz zapis dziennika dla dzienników zestawu programów obsługi, subskrybenta i wydawcy	Wyłącza wszystkie zapisy dziennika dla tego programu obsługi w obiekcie zestawu programów obsługi, kanale subskrybenta i kanale wydawcy.
Maksymalna liczba pozycji w dzienniku (50–500)	Liczba pozycji w dzienniku. Wartość domyślna to 50.

Opcja	Opis
Poziom dziennika	Dostępne do wyboru są następujące poziomy dziennika: ◆ **Zapisuj w dzienniku błędy**: w dzienniku są zapisywane tylko błędy. ◆ Zapisuj w dzienniku błędy i ostrzeżenia: w dzienniku są zapisywane błędy i ostrzeżenia. ◆ **Zapisuj w dzienniku określone zdarzenia**: w dzienniku są zapisywane wybrane zdarzenia. Wybranie tej opcji powoduje włączenie następującej listy zdarzeń: ◆ **Zdarzenia mechanizmu metakatalogów** ◆ **Zdarzenia stanu** ◆ **Zdarzenia operacji** ◆ **Zdarzenia transformacji** ◆ **Zdarzenia zaopatrywania poświadczeń** ◆ **Aktualizuj tylko czas ostatniego zapisu dziennika**: powoduje aktualizację czasu ostatniego zapisu dziennika. ◆ **Zapis dziennika wyłączony**: powoduje wyłączenie zapisu dziennika dla programu obsługi.

Konfigurowanie poziomu śledzenia

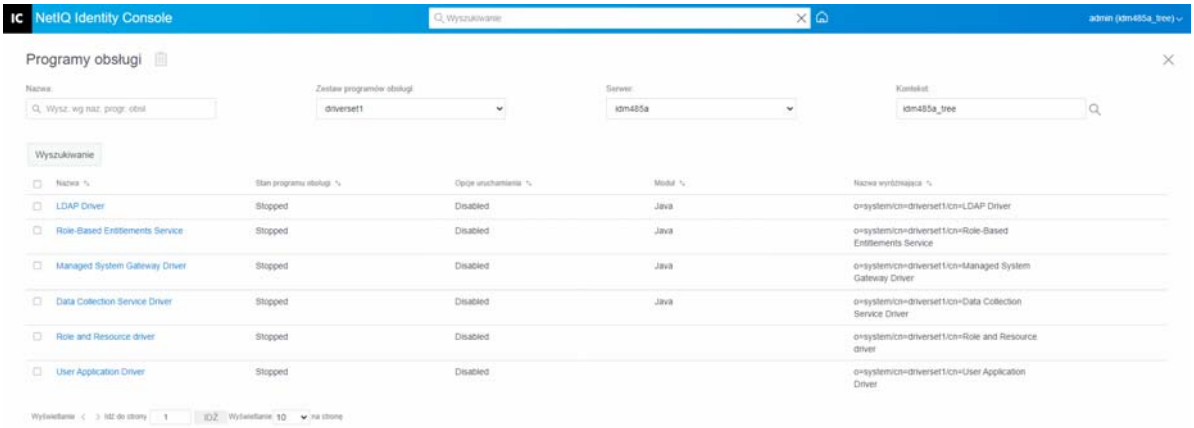
Dla określonego programu obsługi można skonfigurować śledzenie. W zależności od poziomu śledzenia określonego dla programu obsługi śledzenie wyświetla zdarzenia związane z programami obsługi podczas ich przetwarzania przez mechanizm. Poziom śledzenia programu obsługi ma wpływ tylko na program obsługi lub zestaw programów obsługi, w którym ustawiono śledzenie. W przypadku korzystania ze zdalnego modułu ładującego plik śledzenia zdalnego modułu ładującego jest ustawiany bezpośrednio w tym module i zawiera tylko śledzenie podkładki programu obsługi.

Aby skonfigurować śledzenie dla programu obsługi, należy wybrać opcję **Konfiguracja zapisu w dzienniku i śledzenia** > kartę **Śledzenie**. W poniższej tabeli opisano ustawienia śledzenia:

Parametr	Program obsługi
Poziom śledzenia	Wraz ze zwiększaniem poziomu śledzenia programu obsługi rośnie ilość informacji wyświetlanych przez funkcję Śledzenie. Pierwszy poziom śledzenia pokazuje błędy, ale nie ich przyczynę. Aby wyświetlać informacje o synchronizacji haseł, należy ustawić piąty poziom śledzenia. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.
Plik śledzenia	Umożliwia określenie nazwy pliku i lokalizacji, w której są zapisywane informacje Identity Manager dotyczące wybranego programu obsługi. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.

Parametr	Program obsługi
Nazwa śledzenia	Komunikaty śledzenia programu obsługi są dołączane z wartością wprowadzoną zamiast nazwy programu obsługi. Należy jej użyć, gdy nazwa programu obsługi jest bardzo długa.
Kodowanie pliku śledzenia	Plik śledzenia używa domyślnego kodowania systemu. W razie potrzeby można określić inne kodowanie.
Limit rozmiaru pliku śledzenia	Umożliwia ustawienie limitu dla pliku śledzenia Java. Jeśli zostanie ustawiony nieograniczony rozmiar pliku, plik będzie rósł, dopóki nie zabraknie miejsca na dysku. **UWAGA:** Określenie limitu rozmiaru pliku powoduje, że plik śledzenia jest dzielony na mniejsze pliki. Identity Manager automatycznie dzieli maksymalny rozmiar pliku przez dziesięć i tworzy oddzielne pliki. Połączony rozmiar tych plików jest równy maksymalnemu rozmiarowi pliku śledzenia. Po wybraniu opcji **Użyj ustawienia z zestawu programów obsługi** wartość jest brana z zestawu programów obsługi.

Rysunek 23-5 *Zarządzanie poziomami dziennika i śledzenia programów obsługi*



Badanie programów obsługi

Inspektor programu obsługi umożliwia wyświetlanie szczegółowych informacji o obiektach skojarzonych z programem obsługi. Ta sekcja jest podzielona na następujące kategorie:

- „Inspektor programu obsługi” na stronie 179
- „Inspektor pamięci podręcznej programu obsługi” na stronie 180
- „Inspektor pamięci podręcznej synchronizacji poza pasmem” na stronie 181
- „Manifest programu obsługi” na stronie 181
- „Monitorowanie kondycji programu obsługi” na stronie 182

Inspektor programu obsługi

Aby wyświetlić obiekty skojarzone z programem obsługi:

1. W portalu Identity Console wybierz opcję **Programy obsługi** > **Inspektor** > kartę **Inspektor programu obsługi**.
2. W polu **Program obsługi** określ w pełni kwalifikowaną nazwę programu obsługi, który chcesz zbadać, lub kliknij ikonę przeglądania, aby znaleźć i wybrać żądany program obsługi.
3. Po wybraniu programu obsługi do zbadania kliknij przycisk **OK**, aby wyświetlić stronę Inspektor programu obsługi.

   Na stronie zostaną wyświetlone informacje o obiektach skojarzonych z wybranym programem obsługi. Możesz wykonać dowolne z następujących działań:

   - **Usuń:** Usuwa skojarzenie między programem obsługi a obiektem. Zaznacz pole wyboru przed obiektem, który nie ma być dłużej skojarzony z programem obsługi, kliknij ikonę , a następnie kliknij przycisk **OK**, aby potwierdzić usunięcie.
   - **Odśwież:** Wybierz ikonę odświeżania , aby ponownie odczytać wszystkie obiekty skojarzone z programem obsługi i odświeżyć informacje.
   - **Pokaż:** Wybierz liczbę skojarzeń, które mają być wyświetlane na stronie. Możesz wybrać wstępnie zdefiniowaną liczbę (25, 50 lub 100) albo określić inną, dowolnie wybraną. Wartością domyślną jest 10 skojarzeń na stronę. Jeśli istnieje więcej skojarzeń niż wyświetlana liczba, następne i poprzednie strony skojarzeń możesz wyświetlić, używając przycisków strzałek.
   - **Działania:** Wykonaj działania na obiektach skojarzonych z programem obsługi. Kliknij opcję **Działania**, a następnie wybierz jedną z następujących opcji:
     - **Pokaż wszystkie skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi.
     - **Filtr wyświetlający wyłączone skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Wyłączone.
     - **Filtr wyświetlający ręczne skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Ręczne.
     - **Filtr wyświetlający migrowane skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Migrowane.
     - **Filtr wyświetlający oczekujące skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Oczekujące.
     - **Filtr wyświetlający przetworzone skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Przetworzone.
     - **Filtr wyświetlający niezdefiniowane skojarzenia:** Wyświetla wszystkie obiekty skojarzone z programem obsługi, które mają stan Niezdefiniowane.
     - **Podsumowanie skojarzeń:** Wyświetla stan wszystkich obiektów skojarzonych z programem obsługi.
   - **W pełni kwalifikowana nazwa obiektu:** Wyświetla w pełni kwalifikowane nazwy skojarzonych obiektów.
   - **Stan:** Wyświetla stan skojarzenia obiektu.
   - **Identyfikator obiektu:** Wyświetla wartość skojarzenia.

Inspektor pamięci podręcznej programu obsługi

Przy użyciu Identity Console można przeglądać transakcje w pliku pamięci podręcznej programu obsługi. **Inspektor pamięci podręcznej programu obsługi** wyświetla informacje o pliku pamięci podręcznej, w tym listę zdarzeń do przetworzenia przez program obsługi.

1. W portalu Identity Console wybierz opcję **Programy obsługi** > **Inspektor** > kartę **Inspektor pamięci podręcznej programu obsługi**.
2. W polu **Program obsługi** określ w pełni kwalifikowaną nazwę programu obsługi, którego pamięć podręczną chcesz zbadać, lub kliknij ikonę przeglądania, aby znaleźć i wybrać żądany program obsługi, a następnie kliknij przycisk **OK**, aby wyświetlić stronę Inspektor pamięci podręcznej programu obsługi.

   Plik pamięci podręcznej programu obsługi można odczytywać tylko wtedy, gdy program obsługi nie jest uruchomiony. Jeśli program obsługi jest zatrzymany, na stronie Inspektor pamięci podręcznej programu obsługi zostanie wyświetlona pamięć podręczna. Jeśli program obsługi działa, zamiast wpisów pamięci podręcznej na stronie zostaje wyświetlona uwaga `Program obsługi nie jest zatrzymany, nie można odczytać pamięci podręcznej`. Aby zatrzymać program obsługi, kliknij przycisk . Spowoduje to odczytanie i wyświetlenie pamięci podręcznej.

   - **Pamięć podręczna programu obsługi na serwerze:** Wyświetla serwer, na którym znajduje się to wystąpienie pliku pamięci podręcznej. Jeśli program obsługi działa na wielu serwerach, możesz wybrać inny serwer z listy, aby wyświetlić plik pamięci podręcznej programu obsługi dla tego serwera.
   - **Ikony Uruchomienie/Zatrzymanie programu obsługi:** Wyświetla bieżący stan programu obsługi i umożliwia jego uruchomienie lub zatrzymanie. Pamięć podręczną można odczytywać tylko wtedy, gdy program obsługi jest zatrzymany.
   - **Usuń:** Wybierz wpisy w pamięci podręcznej, a następnie kliknij ikonę , aby usunąć je z pliku pamięci podręcznej.
   - **Działania:** Umożliwia wykonywanie działań na wpisach w pliku pamięci podręcznej. Kliknij opcję **Działania**, aby rozwinąć menu, a następnie wybierz jedną z następujących opcji:
     - **Wyczyść wszystkie buforowane zdarzenia:** Umożliwia wyczyszczenie wszystkich buforowanych zdarzeń.
     - **Podsumowanie pamięci podręcznej:** Podsumowuje wszystkie zdarzenia przechowywane w pliku pamięci podręcznej.

Wyświetlanie szczegółów połączonego systemu dla programów obsługi

Aby wyświetlić szczegóły połączonego systemu dla określonego programu obsługi, wykonaj następujące czynności:

1. W portalu Identity Console kliknij moduł **Inspektor obiektu**.
2. Znajdź i wybierz określony obiekt programu obsługi, dla którego chcesz wyświetlić połączone systemy.
3. Na ekranie komputera zostaną wyświetlone wszystkie szczegóły połączonego systemu dla wybranego obiektu programu obsługi.

Inspektor pamięci podręcznej synchronizacji poza pasmem

Aby wyświetlić zdarzenia w pamięci podręcznej synchronizacji poza pasmem:

1. W portalu Identity Console wybierz opcję **Programy obsługi** > **Inspektor** > kartę **Inspektor pamięci podręcznej synchronizacji poza pasmem**.
2. W polu **Program obsługi** określ w pełni kwalifikowaną nazwę programu obsługi, którego pamięć podręczną chcesz zbadać, lub kliknij ikonę przeglądania, aby znaleźć i wybrać żądany program obsługi, a następnie kliknij przycisk **OK**.

   Plik pamięci podręcznej programu obsługi można odczytywać tylko wtedy, gdy program obsługi nie jest uruchomiony. Jeśli program obsługi jest zatrzymany, na stronie Inspektor pamięci podręcznej programu obsługi zostanie wyświetlona pamięć podręczna. Jeśli program obsługi działa, zamiast wpisów pamięci podręcznej na stronie zostaje wyświetlona uwaga `Program obsługi nie jest zatrzymany, nie można odczytać pamięci podręcznej`. Aby zatrzymać program obsługi, kliknij przycisk  . Spowoduje to odczytanie i wyświetlenie pamięci podręcznej.

   - **Nazwa pliku pamięci podręcznej:** Wyświetla nazwę pliku pamięci podręcznej.
   - **Pamięć podręczna programu obsługi na serwerze:** Wyświetla serwer, na którym znajduje się to wystąpienie pliku pamięci podręcznej. Jeśli program obsługi działa na wielu serwerach, możesz wybrać inny serwer z listy, aby wyświetlić plik pamięci podręcznej programu obsługi dla tego serwera.
   - **Ikony Uruchomienie/Zatrzymanie programu obsługi:** Wyświetla bieżący stan programu obsługi i umożliwia jego uruchomienie lub zatrzymanie. Pamięć podręczną można odczytywać tylko wtedy, gdy program obsługi jest zatrzymany.
   - **Usuń:** Wybierz wpisy w pamięci podręcznej, a następnie kliknij ikonę  , aby usunąć je z pliku pamięci podręcznej.
   - **Działania:** Umożliwia wykonywanie działań na wpisach w pliku pamięci podręcznej. Kliknij opcję **Działania**, aby rozwinąć menu, a następnie wybierz jedną z następujących opcji:
     - **Podsumowanie pamięci podręcznej:** Podsumowuje wszystkie zdarzenia przechowywane w pliku pamięci podręcznej.
     - **Wyczyść wszystkie buforowane zdarzenia:** Umożliwia wyczyszczenie wszystkich buforowanych zdarzeń.

Manifest programu obsługi

Manifest programu obsługi jest czymś w rodzaju podsumowania programu obsługi. Informuje o platformach obsługiwanych przez program obsługi i zawiera kilka ustawień konfiguracji. Manifest programu obsługi powinien zostać dostarczony przez dewelopera programu obsługi. Administrator sieci zazwyczaj nie musi edytować manifestu programu obsługi. W przypadku, gdy administrator chce edytować manifest programu obsługi, może to zrobić, wybierając opcję **Drivers** (Programy obsługi) > **Inspektor** > **Manifest programu obsługi** > **Enable XML Editing** (Włącz edytowanie XML).

Monitorowanie kondycji programu obsługi

Monitorowanie kondycji programu obsługi umożliwia wyświetlanie bieżącego stanu programu obsługi w kolorze zielonym, żółtym lub czerwonym oraz definiowanie działań do wykonania w odpowiedzi na każdy z tych stanów kondycji.

Użytkownik tworzy warunki (kryteria) określające każdy ze stanów kondycji, a także definiuje działania wykonywane przy każdej zmianie stanu kondycji programu obsługi. Na przykład jeśli stan kondycji programu obsługi zmienia się z zielonego na żółty, można wykonać takie działania jak ponowne uruchomienie programu obsługi, zamknięcie programu obsługi i wysłanie wiadomości e-mail do osoby wyznaczonej do rozwiązywania problemów z programem obsługi.

Przy użyciu tego modułu można wykonywać następujące zadania:

- „Modyfikowanie stanów kondycji programu obsługi” na stronie 182
- „Modyfikowanie działań kondycji programu obsługi” na stronie 185
- „Tworzenie stanu niestandardowego” na stronie 186
- „Modyfikowanie stanu niestandardowego” na stronie 187

Modyfikowanie stanów kondycji programu obsługi

Warunki określające poszczególne stany kondycji kontroluje użytkownik. Stan zielony ma reprezentować program obsługi w dobrym stanie, a czerwony — w złym.

W pierwszej kolejności oceniane są warunki dla stanu zielonego. Jeśli program obsługi nie spełnia warunków dla stanu zielonego, oceniane są warunki dla stanu żółtego. Jeśli program obsługi nie spełnia warunków dla stanu żółtego, do programu obsługi automatycznie jest przypisywany czerwony stan kondycji.

Aby zmodyfikować warunki dla stanu:

1. W portalu Identity Console otwórz stronę Konfiguracja kondycji programu obsługi dla programu obsługi, którego warunki chcesz zmodyfikować:
   - **1a** Otwórz stronę domową Identity Console.
   - **1b** Wybierz opcję **Programy obsługi** > **kliknij odpowiedni program obsługi z listy** > **Inspektor** > **Konfiguracja kondycji programu obsługi**.
2. Kliknij kartę stanu (Zielony lub Żółty), który chcesz zmodyfikować.

   Na karcie zostaną wyświetlone bieżące warunki stanu kondycji. Warunki są podzielone na grupy, a do łączenia poszczególnych warunków i grup służą operatory logiczne AND i OR. Rozważ następujący przykład stanu zielonego:

```
GROUP1
Condition1 and
Condition2
Or
GROUP2
Condition1 and
Condition2 and
Condition3
```

W tym przykładzie do programu obsługi jest przypisywany stan zielony, jeśli spełnione są warunki GROUP1 lub GROUP2. Jeśli nie są spełnione warunki żadnej z tych grup, oceniane są warunki dla stanu żółtego.

Warunki, które można oceniać, to:

- **Stan programu obsługi:** Uruchomiony, zatrzymany, uruchamiany, nieuruchomiony lub oczekiwanie na zamknięcie. Na przykład jednym z domyślnych warunków zielonego stanu kondycji jest to, że program obsługi jest uruchomiony.
- **Program obsługi w przepełnieniu pamięci podręcznej:** Stan pamięci podręcznej używanej do przechowywania transakcji programu obsługi. Jeśli program obsługi znajduje się w stanie przepełnienia pamięci podręcznej, cała dostępna pamięć podręczna została użyta. Na przykład domyślnym warunkiem zielonego stanu kondycji jest to, że warunek Program obsługi w przepełnieniu pamięci podręcznej jest fałszywy, natomiast domyślnym warunkiem żółtego stanu kondycji jest to, że warunek Program obsługi w przepełnieniu pamięci podręcznej jest prawdziwy.
- **Najnowsza:** Wiek najnowszej transakcji w pamięci podręcznej.
- **Najstarsza:** Wiek najstarszej transakcji w pamięci podręcznej.
- **Całkowity rozmiar:** Rozmiar pamięci podręcznej.
- **Rozmiar nieprzetworzonych:** Rozmiar wszystkich nieprzetworzonych transakcji w pamięci podręcznej.
- **Nieprzetworzone transakcje:** Liczba nieprzetworzonych transakcji w pamięci podręcznej. Możesz określić wszystkie typy transakcji lub tylko niektóre (na przykład dodania, usunięcia lub zmiany nazwy).
- **Historia transakcji:** Liczba transakcji przetworzonych w różnych punktach w kanale subskrybenta lub wydawcy w danym okresie. Ten warunek używa wielu elementów w następującym formacie:

  <*typ transakcji*> <*lokalizacja i okres transakcji* > <*operator relacyjny*> <*liczba transakcji*>.

  - <*typ transakcji*>: Określa oceniany typ transakcji. Mogą to być wszystkie transakcje, dodania, usunięcia, zmiany nazwy itd.
  - <*lokalizacja i okres transakcji*>: Określa oceniane miejsce w kanale subskrybenta lub wydawcy i okres. Na przykład można ocenić całkowitą liczbę transakcji przetworzonych jako zdarzenia zgłoszone przez wydawcę w ciągu ostatnich 48 godzin. Domyślnie dane historii transakcji są przechowywane przez dwa tygodnie, co oznacza, że nie można podać okresu większego niż dwa tygodnie, jeśli nie zostanie zmienione domyślne ustawienie Transaction Data Duration (Czas trwania danych transakcji).
  - <*operator relacyjny*>: Określa, że zidentyfikowane transakcje muszą być równe, inne, mniejsze, mniejsze lub równe, większe albo większe lub równe w stosunku do elementu <liczba transakcji>.
  - <*liczba transakcji*>: Określa liczbę transakcji używanych w procesie oceny.

  Poniżej przedstawiono przykład warunku Historia transakcji:

  ```
  <liczba dodań> <jako polecenia wydawcy> <w ciągu ostatnich 10 minut>
  <jest mniejsza niż> <1000>
  ```

- **Dostępna historia:** Ilość danych historii transakcji dostępnych do oceny. Podstawowym celem tego warunku jest zapewnienie, że warunek Historia transakcji nie spowoduje błędu bieżącego stanu ze względu na niewystarczającą ilość danych historii transakcji zebranych dla ocenianego okresu.

Na przykład załóżmy, że użytkownik chce za pomocą warunku Historia transakcji ocenić liczbę dodań jako poleceń wydawcy w ciągu ostatnich 48 godzin (przykład przedstawiony powyżej w sekcji Historia transakcji). Jednak nie chce, aby warunek spowodował błąd, gdy nie ma jeszcze danych z 48 godzin, co może mieć miejsce po początkowym skonfigurowaniu kondycji programu obsługi lub po ponownym uruchomieniu serwera programu obsługi (ponieważ dane historii transakcji są przechowywane w pamięci). Dlatego tworzy się grupy warunków podobne do następującej:

```
Group1 Dostępna historia <jest mniejsza niż> <48 godzin> lub Group2
Dostępna historia <jest większa niż lub równa> <48 godzin> i
Historia transakcji <liczba dodań> <jako polecenia wydawcy> <w ciągu
ostatnich 48 godzin> <jest mniejsza niż> <1000>
```

Stan jest oceniany jako prawdziwy, jeśli dowolna grupa warunków jest prawdziwa, co oznacza, że a) dostępne dane obejmują okres krótszy niż 48 godzin lub b) dostępne dane obejmują okres co najmniej 48 godzin, a liczba dodań jako poleceń wydawcy w ciągu ostatnich 48 godzin jest mniejsza niż 1000.

Stan jest oceniany jako fałszywy, jeśli oba warunki są oceniane jako fałszywe, co oznacza, że a) dostępne dane obejmują okres co najmniej 48 godzin i b) liczba dodań jako poleceń wydawcy w ciągu ostatnich 48 godzin jest większa niż 1000.

3 Zmodyfikuj kryteria stosownie do potrzeb.

- Aby dodać nową grupę, kliknij ikonę + obok opcji **Grupy warunków**.
- Aby dodać warunek, kliknij ikonę + obok operatorów logicznych (AND/OR). Możesz również kliknąć łącze **Dodaj nowy warunek**.
- Aby zmienić kolejność grup warunków lub pojedynczych warunków, zaznacz pole wyboru obok grupy lub warunku, które chcesz przenieść, a następnie klikaj przyciski strzałek, aby przesuwać grupę lub warunek w górę i w dół. Przy użyciu przycisków strzałek możesz również przenieść warunek z jednej grupy do innej.

4 Po zakończeniu zapisz zmiany, klikając przycisk **Zapisz**.

5 Jeśli chcesz zmienić działania skojarzone z ustawionymi warunkami, przejdź do sekcji „Modyfikowanie działań kondycji programu obsługi” na stronie 185.

Modyfikowanie działań kondycji programu obsługi

Istnieje możliwość określenia działań, które mają być wykonywane po zmianie stanu kondycji programu obsługi. Na przykład jeśli stan zmienia się z zielonego na żółty, można zamknąć lub uruchomić ponownie program obsługi, wygenerować zdarzenie lub uruchomić przepływ pracy. Albo, jeśli stan zmienia się z żółtego na zielony, wykonać wszystkie działania skojarzone ze stanem zielonym.

Działania stanu kondycji są wykonywane tylko raz przy każdym spełnieniu warunków. Dopóki stan pozostaje prawdziwy, działania nie są powtarzane. Gdy stan zmienia się ze względu na to, że warunki przestają być spełniane, w momencie ich spełnienia po raz kolejny działania są wykonywane ponownie.

1 W portalu Identity Console otwórz stronę Konfiguracja kondycji programu obsługi dla programu obsługi, którego działania chcesz zmodyfikować:

   1a Otwórz stronę domową Identity Console.

   1b Wybierz opcję **Programy obsługi** > **kliknij odpowiedni program obsługi z listy** > **Inspektor** > **Konfiguracja kondycji programu obsługi**.

2 Kliknij kartę **Zielony**, **Żółty** lub **Czerwony** dla stanu, którego działania chcesz zmodyfikować.

3 Kliknij ikonę plusa (+) obok nagłówka **Działania**, aby dodać działanie, a następnie wybierz odpowiedni typ działania:

   - **Uruchomienie programu obsługi:** Uruchamia program obsługi.
   - **Zatrzymanie programu obsługi:** Zatrzymuje program obsługi.
   - **Uruchom ponownie program obsługi:** Zatrzymuje, a następnie uruchamia ponownie program obsługi.
   - **Wyczyść pamięć podręczną programu obsługi:** Usuwa z pamięci podręcznej wszystkie transakcje, w tym również nieprzetworzone.
   - **Wyślij e-mail:** Wysyła wiadomość e-mail do co najmniej jednego odbiorcy. Szablon, który ma być używany w treści wiadomości e-mail, musi już istnieć. Aby uwzględnić w wiadomości e-mail nazwę programu obsługi, nazwę serwera i informacje o bieżącym stanie kondycji, dodaj do szablonu wiadomości e-mail tokeny `$Driver$`, `$Server$` i `$HealthState$`, a następnie dołącz je w tekście wiadomości. Na przykład:

     ```
     The current health state of the $Driver$ driver running on $Server$
     is $HealthState$.
     ```

     WAŻNE: Aby wysyłać wiadomości do wielu użytkowników, poszczególne adresy e-mail należy oddzielać przecinkami (,). Nie należy używać średników zamiast przecinków.

   - **Zapisz komunikat o śledzeniu:** Zapisuje komunikat w pliku dziennika zadania Kondycja programu obsługi lub w pliku dziennika zestawu programów obsługi, jeśli plik śledzenia nie jest skonfigurowany w zadaniu Kondycja programu obsługi.
   - **Generuj zdarzenie:** Generuje zdarzenie, które może być używane przez składniki Audit i Sentinel.
   - **Wykonaj ECMAScript:** Wykonuje istniejący skrypt ECMAScript.

Aby uzyskać informacje na temat sposobu tworzenia skryptów ECMA, zobacz Using ECMAScript in Policies (Używanie skryptu ECMAScript w założeniach) w dokumencie *NetIQ Identity Manager — Using Designer to Create Policies* (NetIQ Identity Manager — tworzenie założeń przy użyciu programu Designer).

- **Rozpocznij przepływ pracy:** Uruchamia przepływ pracy zaopatrywania.
- **W przypadku błędu:** Gdy działanie kończy się niepowodzeniem, informuje, co zrobić z pozostałymi działaniami, bieżącym stanem kondycji i zadaniem Kondycja programu obsługi.
  - **Wpływaj na działania przez:** Możesz kontynuować wykonywanie pozostałych działań, zatrzymać wykonywanie pozostałych działań lub przywrócić domyślną wartość bieżącego ustawienia. Bieżące ustawienie jest stosowane tylko wtedy, gdy istnieje wiele działań W przypadku błędu i w jednym z poprzednich działań W przypadku błędu została ustawiona opcja Wpływaj na działania przez.
  - **Wpływaj na stan przez:** Możesz zapisać bieżący stan, odrzucić bieżący stan lub przywrócić domyślną wartość bieżącego ustawienia. Zapisanie stanu powoduje, że warunki stanu są nadal oceniane jako prawdziwe. Odrzucenie stanu powoduje ocenę warunków stanu jako fałszywych. Bieżące ustawienie jest stosowane tylko wtedy, gdy istnieje wiele działań W przypadku błędu i w jednym z poprzednich działań W przypadku błędu została ustawiona opcja Wpływaj na stan przez.
  - **Wpływaj na zadanie kondycji programu obsługi przez:** Możesz kontynuować uruchamianie zadania, przerwać i wyłączyć zadanie lub przywrócić domyślną wartość bieżącego ustawienia. Dalsze uruchamianie zadania powoduje, że zadanie kończy ocenianie warunków, aby określić stan kondycji programu obsługi i wykonać wszystkie działania skojarzone ze stanem. Przerwanie i wyłączenie zadania zatrzymuje bieżące działanie zadania i zamyka zadanie. Zadanie nie uruchamia się ponownie, dopóki nie zostanie włączone. Bieżące ustawienie jest stosowane tylko wtedy, gdy istnieje wiele działań W przypadku błędu i w jednym z poprzednich działań W przypadku błędu zostało wybrane ustawienie Wpływaj na zadanie kondycji programu obsługi przez.

4 Po zakończeniu zapisz zmiany, klikając przycisk **Zapisz**.

Tworzenie stanu niestandardowego

Istnieje możliwość utworzenia co najmniej jednego stanu niestandardowego w celu wykonywania działań niezależnych od bieżącego stanu kondycji programu obsługi (zielonego, żółtego, czerwonego). W przypadku spełnienia warunków stanu niestandardowego jego działania są wykonywane niezależnie od bieżącego stanu kondycji.

Podobnie jak w przypadku zielonego, żółtego i czerwonego stanu kondycji, działania stanu niestandardowego są wykonywane raz po każdym spełnieniu warunków. Dopóki stan pozostaje prawdziwy, działania nie są powtarzane. Gdy stan zmienia się ze względu na to, że warunki przestają być spełniane, w momencie ich spełnienia po raz kolejny działania są wykonywane ponownie.

1 W Identity Console otwórz stronę Konfiguracja kondycji programu obsługi dla programu obsługi, w przypadku którego chcesz utworzyć stan niestandardowy:

1a Otwórz stronę domową Identity Console.

1b Wybierz opcję **Programy obsługi** > **kliknij odpowiedni program obsługi z listy** > **Inspektor** > **Konfiguracja kondycji programu obsługi**.

2 Kliknij ikonę + obok ikon stanu kondycji programu obsługi (zielonej, żółtej i czerwonej)

3 Wykonaj instrukcje podane w sekcjach „Modyfikowanie stanów kondycji programu obsługi” na stronie 182 i „Modyfikowanie działań kondycji programu obsługi” na stronie 185, aby zdefiniować warunki i działania stanu niestandardowego.

Modyfikowanie stanu niestandardowego

Aby zmodyfikować stany niestandardowe, wykonaj następujące czynności:

1 W Identity Console otwórz stronę Konfiguracja kondycji programu obsługi dla programu obsługi, w przypadku którego chcesz utworzyć stan niestandardowy:

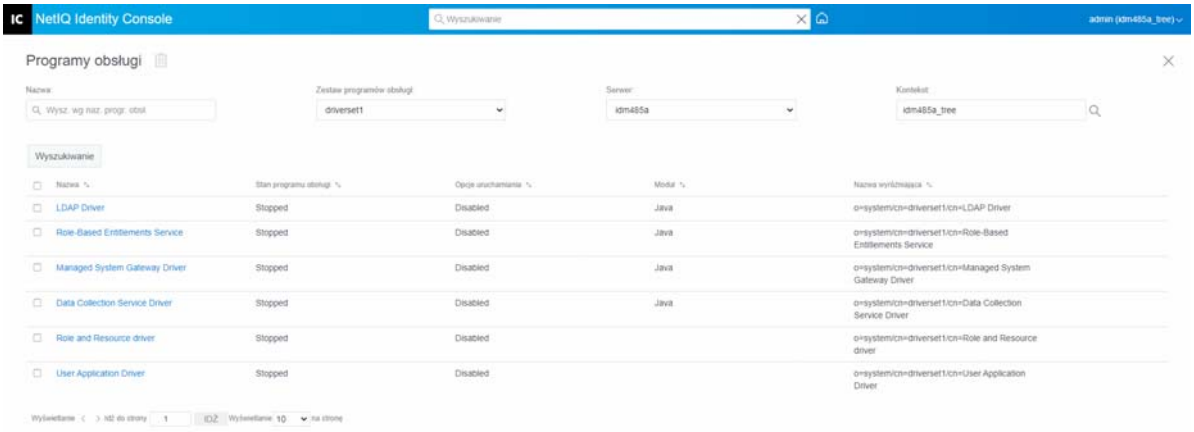
1a Otwórz stronę domową Identity Console.

1b Wybierz opcję **Programy obsługi** > **kliknij odpowiedni program obsługi z listy** > **Inspektor** > **Konfiguracja kondycji programu obsługi**.

2 Kliknij ikonę obok ikon stanu kondycji programu obsługi (zielonej, żółtej i czerwonej)

3 Wykonaj instrukcje podane w sekcjach „Modyfikowanie stanów kondycji programu obsługi” na stronie 182 i „Modyfikowanie działań kondycji programu obsługi” na stronie 185, aby zdefiniować warunki i działania stanu niestandardowego.

Rysunek 23-6 *Zarządzanie inspektorami programów obsługi*



24 Zarządzanie statystykami zestawu programów obsługi

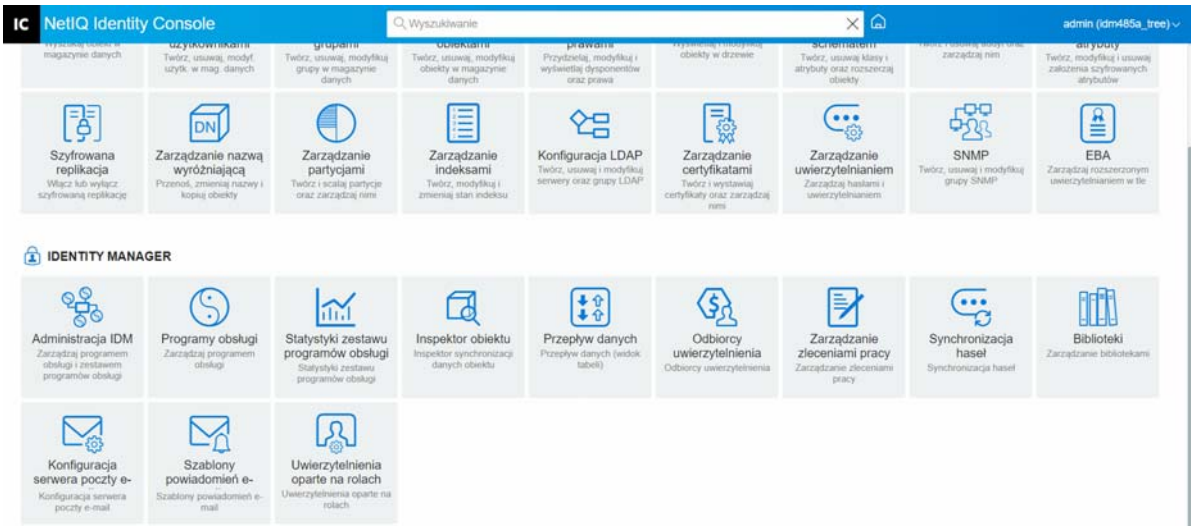
W portalu Identity Console można wyświetlić różne statystyki dotyczące pojedynczego programu obsługi lub całego zestawu programów obsługi. Należą do nich takie statystyki jak: rozmiar pliku pamięci podręcznej, rozmiar nieprzetworzonych transakcji w pliku pamięci podręcznej, najstarsze i najnowsze transakcje oraz całkowita liczba nieprzetworzonych transakcji według kategorii (dodawanie, usuwanie, modyfikowanie itd.). Aby wyświetlić statystyki dotyczące zestawu programów obsługi:

1. W Identity Console otwórz stronę **Statystyki zestawu programów obsługi**.
2. Wybierz odpowiedni serwer z listy rozwijanej.

   Zostanie wyświetlona strona, na której można przejrzeć statystyki dotyczące wszystkich programów obsługi zawartych w zestawie programów obsługi.

   - Aby odświeżyć statystyki, kliknij ikonę .
   - Aby zamknąć statystyki dotyczące programu obsługi, kliknij przycisk w prawym górnym rogu okna statystyk programu obsługi.
   - Aby otworzyć statystyki dotyczące wszystkich programów obsługi, kliknij opcje **Działania** > **Pokaż wszystko**.
   - Aby zwinąć listę nieprzetworzonych transakcji programu obsługi, kliknij przycisk znajdujący się nad listą. Aby zwinąć listę nieprzetworzonych transakcji wszystkich programów obsługi, kliknij opcje **Działania** > **Zwiń wszystkie transakcje**.
   - Aby rozwinąć listę transakcji, kliknij przycisk . Aby rozwinąć listę nieprzetworzonych transakcji wszystkich programów obsługi, kliknij opcje **Działania** > **Rozwiń wszystkie transakcje**.
   - Aby zamknąć pulpit statystyki wyłączonych programów obsługi, kliknij opcję **Działania**, a następnie wybierz opcję **Ukryj wyłączone programy obsługi**.

Rysunek 24-1 *Zarządzanie statystykami zestawu programów obsługi*



25 Badanie obiektów programu Identity Manager

Przy użyciu inspektora obiektu można przeglądać szczegółowe informacje o udziale obiektu w relacjach programu Identity Manager. Relacje te obejmują połączone systemy skojarzone z obiektem, sposób przepływu danych między bezpiecznym magazynem tożsamości a połączonymi systemami, wartości atrybutów przechowywane obecnie w bezpiecznym magazynie tożsamości i w połączonych systemach, konfiguracje programów obsługi połączonych systemów itd.

Aby zbadać obiekty programu Identity Manager, kliknij opcję **Inspektor obiektu** na stronie głównej Identity Console. Określ w pełni kwalifikowaną nazwę obiektu, który chcesz zbadać, lub kliknij ikonę przeglądania, aby znaleźć i wybrać żądany obiekt.

W sekcji Połączone systemy znajduje się lista połączonych systemów, z którymi jest skojarzony obiekt. Przy użyciu strony **Inspektor obiektu** możesz wykonywać następujące działania:

- **Dodawanie skojarzenia**: Aby dodać nowe skojarzenie z połączonym systemem, kliknij ikonę +. Wyszukaj i wybierz **Obiekt programu obsługi integracji** i określ **Identyfikator skojarzonego obiektu**.
- **Usuwanie skojarzenia**: Aby usunąć skojarzenie z połączonym systemem, zaznacz pole wyboru po lewej stronie skojarzenia i kliknij ikonę 🗑. Aby usunąć wszystkie skojarzenia, zaznacz pole wyboru poniżej kolumny Usuń, a następnie kliknij ikonę 🗑.

Rysunek 25-1 *Badanie obiektów programu Identity Manager*

26 Zarządzanie przepływem danych

Przepływ danych przedstawia kanały wydawcy i subskrybenta dla kilku programów obsługi w pojedynczym widoku. Przy użyciu tej opcji można wyświetlać i aktualizować własność danych dla wszystkich programów obsługi.

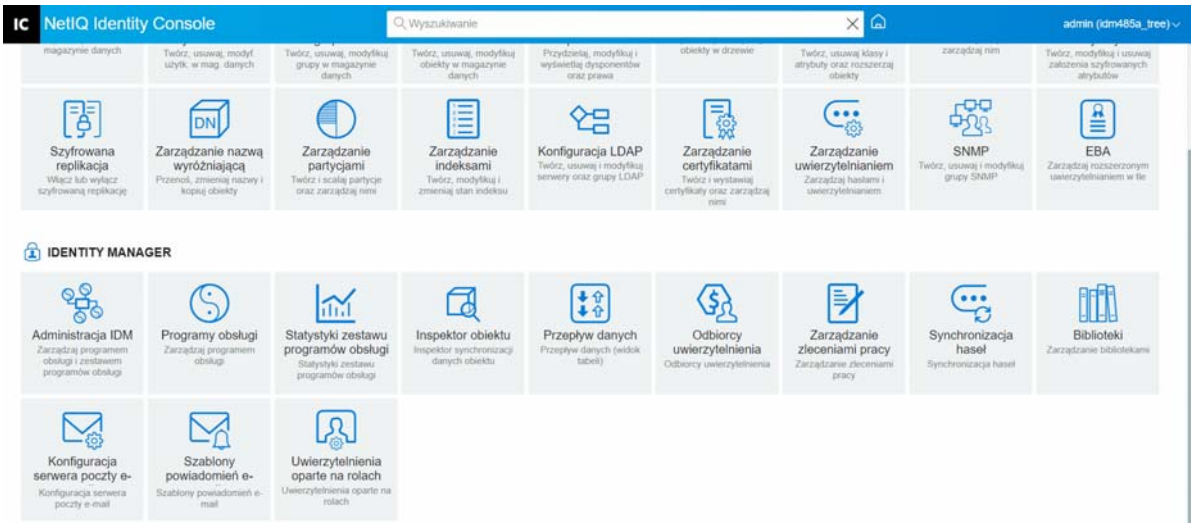
Aby uzyskać dostęp do widoku tabeli przepływu danych, kliknij moduł **Przepływ danych (widok tabeli)** na stronie głównej Identity Console. Następnie znajdź i wybierz odpowiedni kontener, aby wyświetlić listę programów obsługi.

Aby zarządzać własnością danych poszczególnych programów obsługi, wykonaj następujące czynności:

1. Każdy program obsługi ma dwa przyciski do zarządzania przepływem danych w kanałach wydawcy i subskrybenta. Przycisk po lewej stronie służy do zarządzania przepływem danych w kanale wydawcy, w przycisk po prawej — w kanale subskrybenta.
   - 1a **Synchronizuj**: Wybierz tę opcję, aby zsynchronizować określony atrybut. Po wybraniu tej opcji ikona w kanale wydawcy zmieni się na ↑, a ikona na kanale subskrybenta zmieni się na ↓.
   - 1b **Ignoruj**: Wybierz tę opcję, aby zatrzymać synchronizację określonego atrybutu. Po wybraniu tej opcji ikona zmieni się na ⊘.
   - 1c **Powiadom**: Wybierz tę opcję, aby otrzymywać powiadomienia o wszystkich zmianach określonego atrybutu. Jednak zmiana nie będzie automatycznie synchronizowana. Po wybraniu tej opcji ikona zmieni się na 🔔.
   - 1d **Resetuj**: Wybierz tę opcję, aby zresetować wartość atrybutu do wartości określonej przez drugi kanał. Po wybraniu tej opcji ikona zmieni się na ↻.

     UWAGA: Tę wartość można ustawić albo na kanale wydawcy, albo na kanale subskrybenta. Nie można ustawić jej jednocześnie na obu kanałach.

Rysunek 26-1 *Zarządzanie przepływem danych*



27 Zarządzanie odbiorcami uwierzytelnienia

Odwołania do uwierzytelnienia i wyniki są zachowywane w obiektach, którym nadano lub unieważniono uwierzytelnienie. Odwołania do uwierzytelnienia i wyniki zawierają informacje o tym, czy uwierzytelnienie w danym obiekcie jest obecnie nadane, czy unieważnione. Odbiorcami uwierzytelnienia są dowolne obiekty, które zawierają odwołania do uwierzytelnienia.

Odwołania do uwierzytelnienia

Aby wyświetlić odwołania do uwierzytelnienia i wyniki, kliknij opcję **Odbiorcy uwierzytelnienia** na stronie głównej Identity Console i wybierz opcję Odwołania do uwierzytelnienia. Następnie wpisz w pełni kwalifikowaną nazwę obiektu, którą jest `DirXML-EntitlementRecipient`. W celu wybrania obiektu możesz kliknąć przycisk  Selektor obiektów.

Wyniki uwierzytelnienia

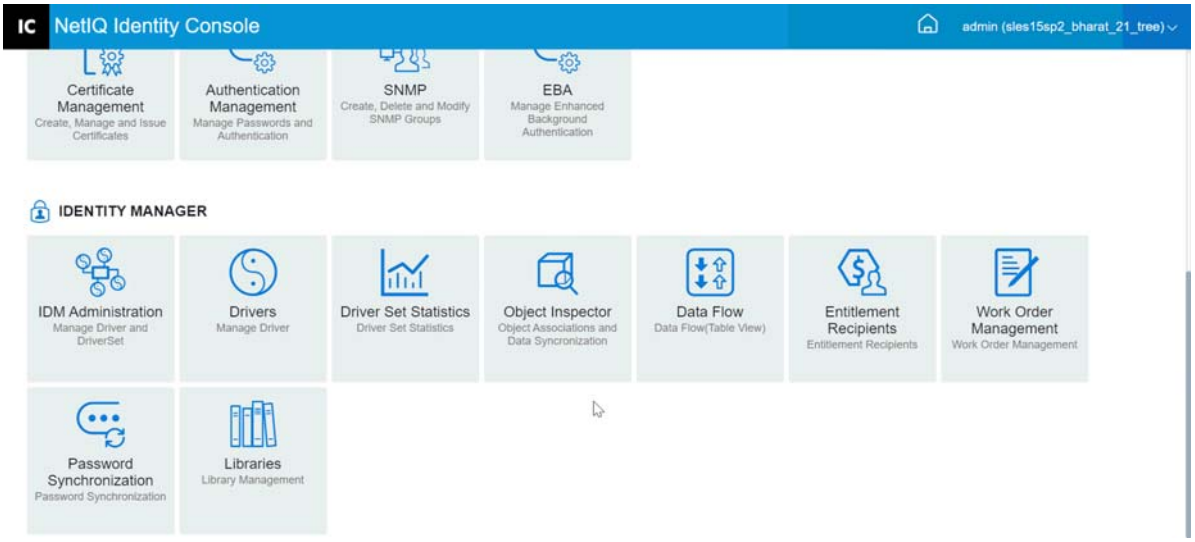
W tabeli Wyniki uwierzytelnienia w portalu Identity Console są wyświetlane wyniki uwierzytelnienia skojarzone z wybranym obiektem. Aby wyświetlić skojarzone uwierzytelnienie, wybierz w pełni kwalifikowaną nazwę uwierzytelnienia. Aby wyświetlić wyniki uwierzytelnienia w formacie XML, wybierz odpowiedni identyfikator wyniku.

- **Nagłówki kolumn wyników uwierzytelnienia:** Nagłówki kolumn obejmują w pełni kwalifikowaną nazwę uwierzytelnienia, jego aktualny stan — przyznane lub unieważnione, źródło wyników (skąd pochodzą), stan wyniku, wszelkie komunikaty, które wystąpiły wraz z wynikiem, znacznik czasu wyniku oraz identyfikację wyniku.
  - **W pełni kwalifikowana nazwa uwierzytelnienia**: Kliknij w pełni kwalifikowaną nazwę uprawnienia dla obiektu, aby wyświetlić stronę Modyfikacja obiektu. Ta strona umożliwia wyświetlenie sposobu przydzielenia atrybutów eDirectory do obiektu. Można też na niej modyfikować atrybuty obiektu. Liczba kategorii wyświetlana na stronie Modyfikacja obiektu zależy od wybranego obiektu.
  - **Stan**: Wyświetla stan uwierzytelnienia — przyznane lub unieważnione. Jeśli dodatek typu plug-in znajdzie jakąkolwiek inną wartość w strumieniu XML, wyświetli tę wartość bezpośrednio.
  - **Komunikat**: Wszelkie komunikaty skojarzone przez podkładkę DirXML ze stanem wyników. Informacje przechowywane w części <msg></msg> pliku XML wyników. Kliknij wpis Identyfikator wyników, aby wyświetlić pełne szczegóły wyniku na stronie Przeglądarka XML.

- **Znacznik czasu**: Czas, w którym mechanizm uwierzytelnienia przetworzył i zapisał wynik. Kliknij wpis Identyfikator wyników, aby wyświetlić pełne szczegóły wyniku na stronie Przeglądarka XML.
- **Identyfikator wyniku**: Kliknij wpis Identyfikator wyników, aby wyświetlić pełne szczegóły wyniku na stronie Przeglądarka XML. Po zakończeniu przeglądania wyników kliknij przycisk Zamknij.

Aby usunąć wpis wyników uwierzytelnienia, kliknij pole wyboru po lewej stronie wpisu wyników uwierzytelnienia, a następnie kliknij opcję Usuń.

Rysunek 27-1 *Zarządzanie odbiorcami uwierzytelnienia*



28 Zarządzanie zleceniami pracy

Programy obsługi Identity Manager mogą tworzyć zlecenia pracy jako wynik przetworzonych przez nie zdarzeń. Na przykład jeśli jest używany program obsługi kadr (SAP HR, PeopleSoft itd.), może on generować zlecenie pracy przy każdym dodaniu nowego użytkownika.

Identity Console umożliwia tworzenie zleceń pracy dla różnych programów obsługi, które mogą korzystać z tej funkcji, i zarządzanie nimi.

Tworzenie nowego zlecenia pracy

Aby utworzyć nowe zlecenie pracy, wykonaj następujące czynności:

1. Kliknij opcję **Zlecenie pracy** na stronie docelowej Identity Console.
2. Kliknij ikonę +, aby utworzyć nowe zlecenie pracy.
3. Podaj nazwę zlecenia pracy, a następnie kliknij przycisk **OK**.

   Nazwa jest używana jako nazwa obiektu WorkOrder (Zlecenie pracy) w bezpiecznym magazynie tożsamości.
4. Wypełnij następujące pola:

   Stan: Nowe zlecenie pracy może mieć stan **Oczekujące** lub **Wstrzymane**. Zazwyczaj zlecenie pracy ma stan **Oczekujące**. Zlecenie pracy można zatrzymać, wybierając opcję **Wstrzymane**. Po przetworzeniu zlecenia pracy w tym polu pojawia się jego stan wynikowy.

   Termin: Program obsługi może wykonać zlecenie pracy natychmiast, ale możesz również zaplanować zlecenie pracy. Aby zaplanować termin, kliknij ikonę kalendarza. Przy użyciu kalendarza wybierz datę. Wybierz miesiąc, rok i godzinę za pomocą strzałek.

   Powtórz zlecenie pracy: Wybierz tę opcję, aby zlecenie pracy było przetwarzane wielokrotnie. Określ przedział czasu, wybierając liczbę tygodni, dni, godzin lub minut, jakie muszą upłynąć przed powtórzeniem zlecenia pracy. Zlecenie pracy przestaje się powtarzać w dniu usunięcia, chyba że zostanie usunięte lub zmodyfikowane ręcznie albo program obsługi zwróci komunikat o błędzie.

   Data usunięcia: Użyj elementu sterującego kalendarza, aby wybrać datę usunięcia skonfigurowanych zleceń pracy. Zlecenia pracy w stanie błędu nie są usuwane, chyba że została wybrana opcja **Usuń zlecenie pracy, nawet jeśli zawiera błąd**.

   Zależne zlecenia pracy: Po utworzeniu nowego zlecenia pracy można uzależnić je od co najmniej jednego zlecenia pracy. Kliknij ikonę 🔍, aby znaleźć i wybrać zależne zlecenia pracy. Aby usunąć zlecenie pracy z listy, wybierz je, a następnie kliknij ikonę 🗑.

Typ: Użyj tego pola, aby określić typ zlecenia pracy. Program obsługi nie zmienia tego atrybutu. Atrybut jest przekazywany do obiektu WorkToDo (Zlecenie do wykonania) po przetworzeniu zlecenia pracy.

Numer zlecenia pracy: Unikatowy numer zlecenia pracy. Tę wartość może przypisać firmowy system zleceń pracy inny niż NetIQ eDirectory, na przykład baza danych zleceń pracy.

Informacje kontaktowe: Informacje kontaktowe osoby odpowiedzialnej za zlecenie pracy.

Dziennik przetwarzania zlecenia pracy: Po przetworzeniu zlecenia pracy program obsługi rejestruje w tym polu jego wyniki, między innymi stan. Umożliwia to sprawdzanie bieżącego stanu zlecenia pracy oraz identyfikowanie wszelkich problemów, jakie wystąpiły w programie obsługi podczas próby skonfigurowania zlecenia pracy.

Atrybut stanu zlecenia pracy pozostaje w stanie oczekiwania do czasu przetworzenia zlecenia pracy. Zlecenie pracy jest przetwarzane po upływie terminu. Program obsługi raportuje wyniki przetwarzania, ustawiając stan atrybutu na Skonfigurowane, Ostrzeżenie lub Błąd. Zlecenie pracy w stanie Wstrzymane jest ignorowane.

- **Oczekujące:** Program obsługi czeka na termin, aby ukończyć zlecenie pracy.
- **Skonfigurowane:** Zlecenie pracy zostało pomyślnie przetworzone.
- **Błąd:** Program obsługi nie mógł wykonać zlecenia pracy.
- **Ostrzeżenie:** Wystąpiło ostrzeżenie dotyczące zlecenia pracy. Program obsługi wysyła ostrzeżenie na przykład wtedy, gdy zlecenie pracy ma zależne zlecenie pracy z późniejszym terminem.

Opis: Opis zlecenia pracy.

Zawartość zlecenia pracy: Dane w tym polu są używane przez reguły programu obsługi do przetwarzania zlecenia pracy. Na przykład może to być plik XML używany do przetwarzania zlecenia pracy przez program Command Transformation.

Usuwanie istniejącego zlecenia pracy

Aby usunąć istniejące zlecenie pracy, wykonaj następujące czynności:

1. Kliknij opcję **Zlecenie pracy** na stronie docelowej Identity Console.
2. Wybierz zlecenie pracy, które chcesz usunąć.
3. Kliknij ikonę  .

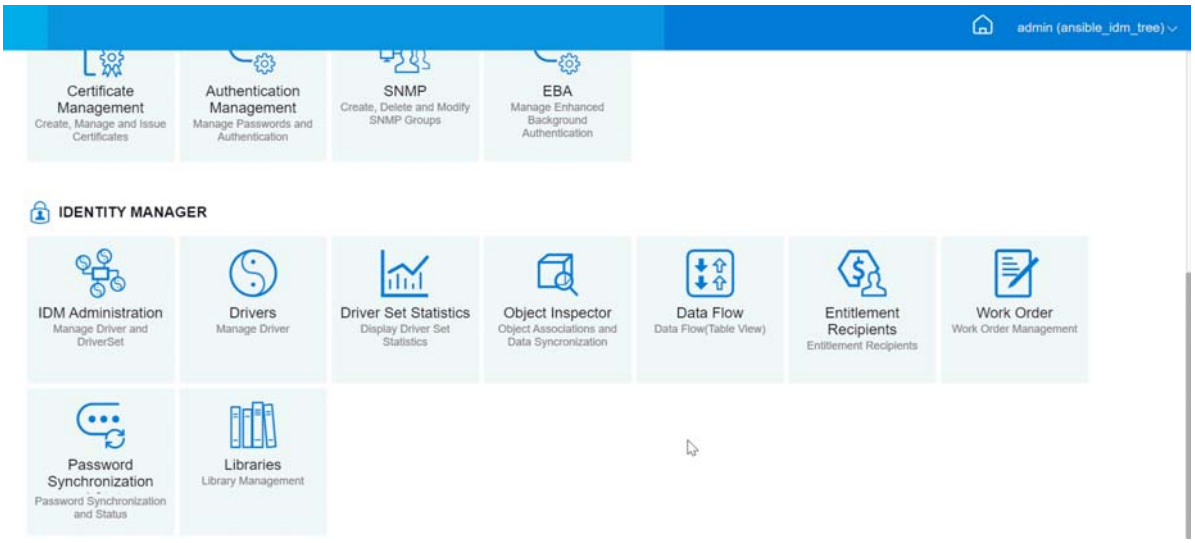
Filtrowanie listy zleceń pracy

Aby odfiltrować listę zleceń pracy, wykonaj następujące czynności:

1. Kliknij opcję **Zlecenie pracy** na stronie docelowej Identity Console.
2. Kliknij opcję **Działania** w obszarze Zarządzanie zleceniami pracy.
3. Z menu rozwijanego wybierz typ filtru:
   - **Pokaż wszystko:** Na liście są wyświetlane wszystkie zlecenia pracy skojarzone z programem obsługi.

- **Skonfigurowane:** Na liście są wyświetlane tylko skonfigurowane zlecenia pracy skojarzone z programem obsługi.
- **Błąd:** Na liście są wyświetlane tylko zlecenia pracy w stanie błędu.
- **Wstrzymane:** Na liście są wyświetlane zlecenia pracy, które zostały ręcznie wstrzymane.
- **Oczekujące:** Na liście są wyświetlane zlecenia pracy, których termin jeszcze nie upłynął.

Rysunek 28-1 *Zarządzanie zleceniami pracy*



29 Zarządzanie stanem i synchronizacją haseł

Przy użyciu portalu Identity Console można weryfikować synchronizację i stan haseł poszczególnych programów obsługi. W celu przeprowadzenia weryfikacji należy wybrać moduł **Synchronizacja haseł** na stronie głównej Identity Console.

Przy użyciu tego modułu można wykonywać następujące działania:

- „Sprawdzanie stanu synchronizacji haseł” na stronie 201
- „Weryfikowanie ustawień synchronizacji haseł” na stronie 202

Sprawdzanie stanu synchronizacji haseł

Istnieje możliwość ustalenia, czy hasło dystrybucyjne dla określonego użytkownika jest takie samo jak hasło w połączonym systemie. Aby sprawdzić stan synchronizacji haseł, wykonaj następujące czynności:

1. W portalu Identity Console wybierz opcję **Synchronizacja haseł** > **Stan hasła**.
2. Znajdź i wybierz użytkownika, w przypadku którego chcesz sprawdzić stan hasła.
3. Mogą być widoczne następujące stany hasła:
   - Hasła są synchronizowane.
   - Hasła NIE są synchronizowane.
   - Stan hasła jest nieznany, ponieważ nie można skontaktować się z połączonym systemem, aby zażądać sprawdzenia hasła.
   - Wystąpił błąd.

UWAGA: Aby wyświetlić więcej szczegółów na temat każdego z powyższych stanów, musisz najechać kursorem myszy na stan w kolumnie **Stan hasła**.

Zadanie Stan hasła powoduje, że program obsługi wykonuje działanie Sprawdzenie hasła obiektu. Nie wszystkie programy obsługi umożliwiają sprawdzanie hasła. Te, które umożliwiają, muszą zawierać funkcję password-check w manifeście programu obsługi. Identity Console nie pozwala na wysyłanie operacji sprawdzania hasła do programów obsługi, które nie zawierają tej funkcji w manifeście.

Działanie Sprawdzenie hasła obiektu sprawdza hasło dystrybucyjne. Jeśli hasło dystrybucyjne nie jest aktualizowane, Sprawdzenie hasła obiektu może zgłaszać, że hasła nie są zsynchronizowane.

Hasło dystrybucyjne nie jest aktualizowane, jeśli wystąpi jedna z następujących sytuacji:

- Używana jest metoda synchronizacji korzystająca z hasła NDS lub hasła uniwersalnego. Aby uzyskać więcej informacji, zobacz „Tworzenie założeń haseł za pomocą ustawień niestandardowych” na stronie 118.

UWAGA: Działanie Stan hasła sprawdza hasło NDS, zamiast hasła uniwersalnego w bezpiecznym magazynie tożsamości. W związku z tym jeśli w założeniach haseł użytkownika nie określono synchronizacji hasła NDS z hasłem uniwersalnym, hasła są zawsze zgłaszane jako niezsynchronizowane. W rzeczywistości hasło dystrybucyjne może być zsynchronizowane z hasłem w połączonym systemie, ale sprawdzenie stanu hasła nie będzie dokładne, dopóki hasło NDS i hasło dystrybucyjne nie zostaną zsynchronizowane z hasłem uniwersalnym.

Weryfikowanie ustawień synchronizacji haseł

Synchronizacja haseł pozwala synchronizować hasła w połączonych systemach przy użyciu programu Identity Manager. Aby wyświetlić ustawienia synchronizacji haseł dla połączonych systemów, wybierz odpowiedni zestaw programów obsługi z menu rozwijanego.

Przy użyciu synchronizacji haseł można skonfigurować połączone systemy tak, aby wykonywały następujące zadania:

- Publikowanie haseł w programie Identity Manager.
- Subskrybowanie haseł z programu Identity Manager lub z innych połączonych systemów.
- Wymuszanie założeń haseł w połączonych systemach.
- Wysyłanie wiadomości e-mail z powiadomieniami.

Aby sprawdzić ustawienia synchronizacji haseł, wykonaj następujące czynności:

1. Na stronie głównej Identity Console wybierz opcję **Synchronizacja haseł** > **Synchronizacja haseł**.
2. Wybierz zestaw programów obsługi zawierający program obsługi, którego ustawienia chcesz sprawdzić.
3. Kliknij nazwę programu obsługi na liście.

   UWAGA: Ustawienia, które są włączone i wyłączone, zależą od programu obsługi. Dostępne są tylko ustawienia funkcji obsługiwanych przez program obsługi.

4. Zweryfikuj, czy ustawienia są prawidłowo skonfigurowane.

   Program Identity Manager akceptuje hasła (kanał wydawcy): Jeśli ta opcja jest włączona, Identity Manager umożliwia przepływ haseł z połączonego systemu do bezpiecznego magazynu tożsamości. Wyłączenie tej opcji oznacza, że żadne elementy `<hasło>` nie mogą przepływać do programu Identity Manager. Są one usuwane z pliku XML przez założenia synchronizacji haseł w kanale wydawcy.

   To ustawienie dotyczy haseł użytkownika dostarczanych przez sam połączony system oraz wartości haseł tworzonych przez założenia w kanale wydawcy.

   Jeśli ta opcja jest włączona, ale opcja hasła dystrybucyjnego poniżej jest wyłączona, wartość `<hasło>` pochodząca z połączonego systemu jest zapisywana bezpośrednio w haśle uniwersalnym w bezpiecznym magazynie tożsamości. Jeśli założenia haseł użytkownika nie pozwalają na korzystanie z hasła uniwersalnego, hasło jest zapisywane w haśle NDS.

   Użyj hasła dystrybucyjnego do synchronizacji haseł: To ustawienie jest dostępne tylko w przypadku włączenia ustawienia **Program Identity Manager akceptuje hasła (kanał wydawcy)**.

Jeśli ta opcja jest włączona wartość hasła pochodząca z połączonego systemu jest zapisywana w haśle dystrybucyjnym. Hasło dystrybucyjne jest odwracalne, co oznacza, że można je pobrać z danych bezpiecznego magazynu tożsamości na potrzeby synchronizacji haseł. Identity Manager używa go do dwukierunkowej synchronizacji haseł z połączonymi systemami. Aby Identity Manager mógł dystrybuować hasła z tego systemu do innych systemów, ta opcja musi być włączona.

Akceptuj hasło tylko wtedy, jeśli jest zgodne z założeniami haseł użytkownika: To ustawienie jest dostępne tylko w przypadku włączenia ustawienia **Użyj hasła dystrybucyjnego do synchronizacji haseł**.

Jeśli ta opcja jest wybrana, Identity Manager nie zapisuje hasła z tego połączonego systemu w haśle dystrybucyjnym w bezpiecznym magazynie tożsamości, dopóki hasło nie spełnia założeń haseł użytkownika.

Jeśli hasło jest niezgodne z założeniami, należy włączyć ustawienie **Reset the user's password to the Distribution Password** (Resetuj hasło użytkownika do hasła dystrybucyjnego), aby zresetować hasło użytkownika w połączonym systemie. Umożliwia to wymuszenie założeń haseł w połączonym systemie, a także w bezpiecznym magazynie tożsamości. Jeśli ta opcja nie zostanie zaznaczona, hasła użytkowników mogą stracić synchronizację w połączonych systemach. Jednak podejmując decyzję o użyciu tej opcji, należy wziąć pod uwagę założenia haseł połączonego systemu. Niektóre połączone systemy mogą nie zezwalać na resetowanie, ponieważ nie umożliwiają one powtarzania haseł.

Używając ustawienia **Powiadom użytkownika o błędzie synchronizacji haseł pocztą e-mail**, można informować użytkowników o niepowodzeniu ustawiania lub resetowania hasła. Powiadamianie jest szczególnie przydatne w przypadku tej opcji. Gdy użytkownik zmienia hasło na takie, które jest dozwolone przez połączony system, ale odrzucane przez Identity Manager z powodu złożeń haseł, nie wie, że hasło zostało zresetowane, dopóki nie otrzyma powiadomienia lub nie spróbuje zalogować się do połączonego systemu za pomocą starego hasła.

Zawsze akceptuj hasło; ignoruj założenia haseł: To ustawienie jest dostępne tylko w przypadku włączenia ustawienia **Użyj hasła dystrybucyjnego do synchronizacji haseł**.

Po wybraniu tej opcji Identity Manager nie wymusza założeń haseł użytkownika dla tego połączonego systemu. Identity Manager zapisuje hasło z tego połączonego systemu w haśle dystrybucyjnym w bezpiecznym magazynie tożsamości i dystrybuuje je do innych połączonych systemów, niezależnie od zgodności z założeniami haseł.

Aplikacja akceptuje hasła (kanał subskrybenta): Po włączeniu tej opcji program obsługi wysyła hasła z bezpiecznego magazynu tożsamości do tego połączonego systemu. Oznacza to również, że jeśli użytkownik zmienia hasło w innym połączonym systemie, który publikuje hasła w haśle dystrybucyjnym w bezpiecznym magazynie tożsamości, hasło jest zmieniane na to z połączonego systemu.

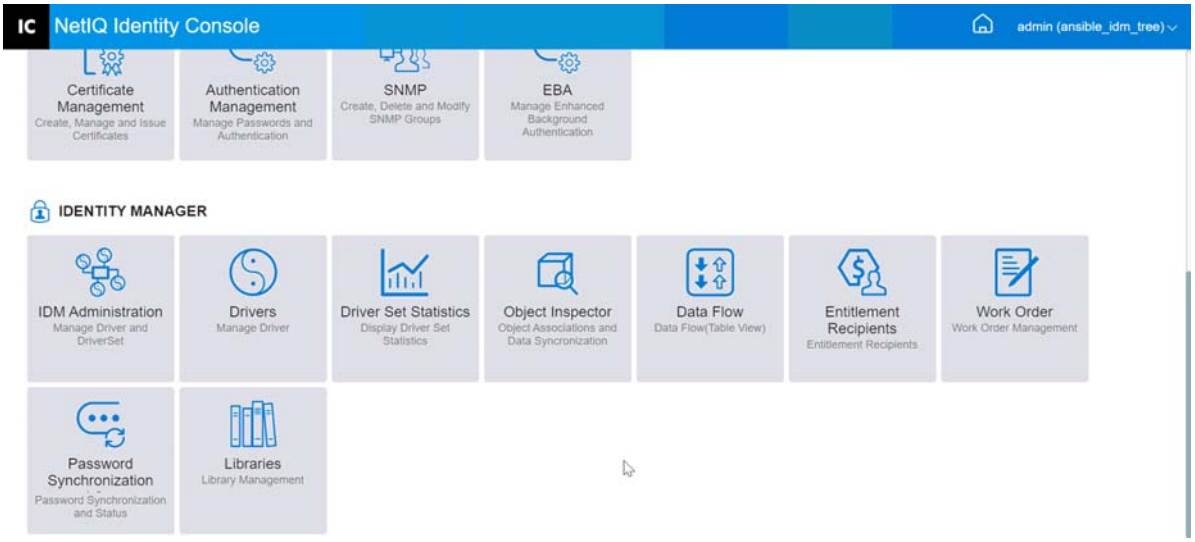
Domyślnie hasło dystrybucyjne jest takie samo jak hasło uniwersalne w bezpiecznym magazynie tożsamości, dlatego zmiany hasła uniwersalnego wprowadzone w bezpiecznym magazynie tożsamości są również wysyłane do połączonego systemu.

Powiadom użytkownika o błędzie synchronizacji haseł pocztą e-mail: Po włączeniu tej opcji do użytkownika jest wysyłana wiadomość e-mail, gdy hasło nie zostało zsynchronizowane, ustawione lub zresetowane. Wiadomość e-mail wysyłana do użytkownika jest oparta na szablonie wiadomości e-mail. Ten szablon jest dostarczany przez aplikację Synchronizacja haseł. Jednak aby szablon mógł działać, należy go dostosować i określić serwer e-mail do wysyłania

wiadomości z powiadomieniami. Aby uzyskać instrukcje, zobacz Configuring E-Mail Notification (Konfigurowanie powiadomienia e-mail) w dokumencie *NetIQ Identity Manager Password Management Guide* (NetIQ Identity Manager — podręcznik zarządzania hasłami).

5 Po zakończeniu kliknij przycisk **Zapisz**, aby zapisać zmiany. Ustawienia są zapisywane jako globalne wartości konfiguracyjne.

Rysunek 29-1 *Zarządzanie synchronizacją haseł*



30 Zarządzanie bibliotekami

W obiektach bibliotek są przechowywane liczne założenia i inne zasoby współdzielone przez programy obsługi. Obiekt biblioteki można utworzyć w obiekcie zestawu programów obsługi lub w dowolnym kontenerze usługi eDirectory. W drzewie usługi eDirectory może istnieć wiele bibliotek. Programy obsługi mogą odwoływać się do dowolnej biblioteki w drzewie, dopóki na serwerze z uruchomionym programem obsługi jest przechowywana replika do odczytu/zapisu lub replika główna obiektu biblioteki.

Arkusze stylów, założenia, reguły i inne obiekty zasobów mogą być przechowywane w bibliotece i używane przez programy obsługi.

Przy użyciu modułu Zarządzanie bibliotekami można wykonywać następujące zadania:

- „Wyświetlanie i usuwanie istniejącej biblioteki” na stronie 205
- „Wyświetlanie i usuwanie obiektów z biblioteki” na stronie 205

Wyświetlanie i usuwanie istniejącej biblioteki

Aby wyświetlić i usunąć istniejącą bibliotekę, wykonaj następujące czynności:

1. Na stronie domowej Identity Console wybierz moduł **Biblioteki**.
2. Wybierz odpowiednią bibliotekę z listy.
3. Kliknij ikonę  . Kliknij przycisk **OK**, aby potwierdzić.

Wyświetlanie i usuwanie obiektów z biblioteki

Istnieje możliwość wyświetlania i usuwania założeń oraz tabel mapowania z obiektów bibliotek. Aby usunąć obiekty, wykonaj następujące czynności:

1. Na stronie domowej Identity Console wybierz moduł **Biblioteki**.
2. Kliknij odpowiednią bibliotekę na liście.
3. Aby usunąć założenia, wybierz kartę **Założenia**.
4. Wybierz odpowiednie założenia z listy i kliknij ikonę  .
5. Aby usunąć tabele mapowania, wybierz kartę **Tabele mapowania**.
6. Wybierz odpowiednią tabelę mapowania z listy i kliknij ikonę  .
7. Kliknij przycisk **OK**, aby potwierdzić.

Rysunek 30-1 *Zarządzanie bibliotekami*

31 Zarządzanie opcjami serwera e-mail

Za pomocą opcji serwera poczty e-mail możesz określić ustawienia serwera SMTP poczty e-mail.

Nazwa hosta

Nazwa hosta używanego serwera poczty elektronicznej SMTP. Może to być również adres IP. Można także podać niestandardowy port po nazwie hosta lub adresie IP.

WAŻNE: Nazwę hosta lub adres IP należy oddzielić od portu dwukropkiem (:).

Od

Możesz określić prawidłowy adres e-mail, który zostanie wyświetlony jako pole Od w nagłówku wiadomości e-mail.

Wartość limitu czasu

Opcja limitu czasu pozwala ustawić limit czasu (w sekundach) na wysłanie wiadomości e-mail z powiadomieniami.

Włącz SSL

W razie potrzeby możesz włączyć opcję SSL.

Uwierzytelnij na serwerze za pomocą poświadczeń

Używane w przypadku zabezpieczonego serwera SMTP. Jeśli przed wysłaniem wiadomości e-mail serwer wymaga uwierzytelnienia, należy określić w tym miejscu nazwę użytkownika oraz hasło.

Pomimo określenia informacji uwierzytelniania w tym miejscu, konieczne może być również określenie ich osobno w aplikacji wysyłającej powiadomienia pocztą e-mail.

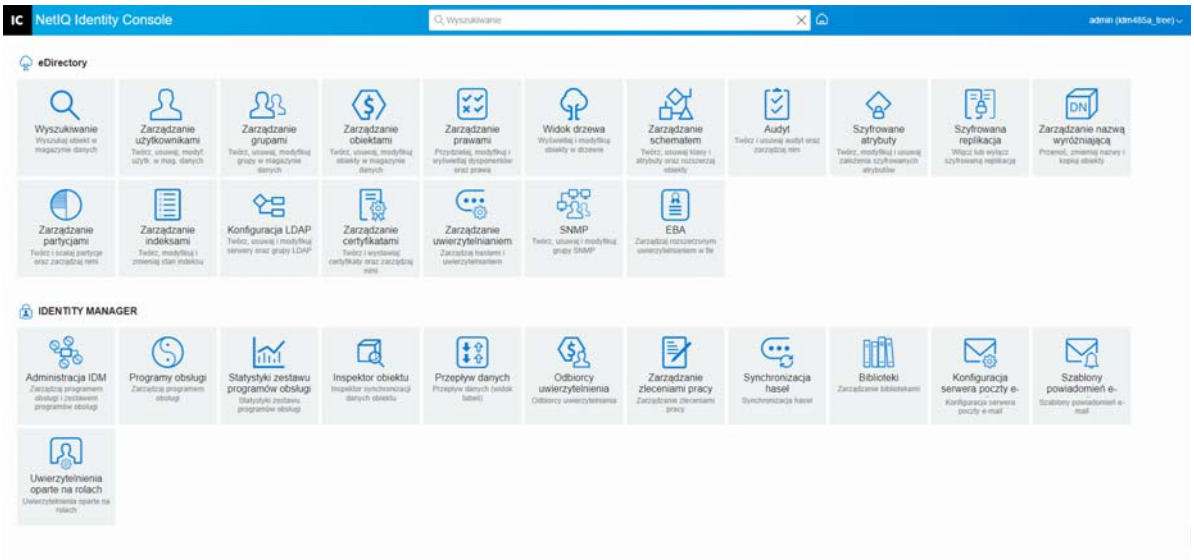
Przykładowo podawanych w tym miejscu danych uwierzytelniania można użyć do wysyłania powiadomień z przypomnieniem hasła poczty e-mail. Aplikacja synchronizacji hasła programu Identity Manager wysyła jednak powiadomienia pocztą e-mail przy użyciu założeń programu obsługi. Może być również wymagane podanie danych uwierzytelniania w tym programie obsługi.

Aby uwierzytelnić serwer, wykonaj następujące czynności:

1. Wybierz opcję **Uwierzytelnij na serwerze za pomocą poświadczeń**.
2. Podaj **nazwę użytkownika** i **hasło**.
3. Kliknij opcję **Testuj połączenie z serwerem**, aby zweryfikować połączenie.
4. Kliknij pozycję **Zapisz**.

UWAGA: Po zapisaniu szczegółów poświadczeń opcja **Testuj połączenie z serwerem** zostaje wyłączona.

Rysunek 31-1 *Konfiguracja serwera e-mail*



32 Zarządzanie szablonami poczty e-mail

Na tej liście wymieniono dostępne szablony powiadomień. Szablony służą do wysyłania wiadomości e-mail do użytkowników należących do danego drzewa. Szablony te można dostosowywać przy użyciu własnego tekstu.

Niektóre aplikacje udostępniają własne szablony. Obiekty szablonów zawarte są w kontenerze zabezpieczeń znajdującym się zwykle w głównym katalogu drzewa.

Listę można sortować według nazwy, daty lub tematu.

Temat

Tekst widoczny dla użytkownika w nagłówku tematu wiadomości e-mail. Aby edytować szablon, kliknij nagłówek tematu szablonu. Przy użyciu interfejsu Edytuj szablon powiadomień e-mail można modyfikować szablon i jego szczegóły.

Nazwa szablonu

Każdy szablon ma unikalną nazwę. Aplikacja wysyłająca wiadomości e-mail używa tej nazwy.

Ostatnia modyfikacja

Data i godzina ostatniej modyfikacji szablonu.

Nowość

Umożliwia utworzenie nowego szablonu wiadomości e-mail.

1. Kliknij ikonę +.
2. Podaj nazwę nowego szablonu (na przykład Zatwierdzenie) i kliknij przycisk **OK**.

Jeśli wyłączono okienka podręczne, nastąpi powrót do okna Edytuj szablon powiadomień e-mail. W kolumnie Nazwa pojawi się nazwa nowego szablonu, ale w kolumnie nagłówka tematu zostanie wyświetlony tekst [No Subject] ([Brak tematu]). W takim przypadku kliknij pozycję [Brak tematu], aby podać szczegóły w nowym szablonie.

Edytuj szablon powiadomień e-mail

Strona Edytuj szablon powiadomień e-mail umożliwia modyfikowanie szablonu e-mail. Szablony można dostosowywać przy użyciu własnego tekstu.

Nazwa szablonu

Wyświetla nazwę szablonu.

Temat

Tekst widoczny dla użytkownika w nagłówku tematu wiadomości e-mail. Tekst w wierszu tematu można zmienić. Rzeczywista nazwa szablonu pozostanie nadal taka sama.

Wyślij jako

Format wysyłania wiadomości e-mail przez serwer SMTP: Tekst lub HTML.

Tokeny lub Znaczniki zastępcze

Znaczniki zastępcze pozwalają dostosowywać wiadomości pod kątem użytkowników. Można skopiować znaczniki zastępcze z listy dostępnych znaczników, a następnie je wkleić do wiadomości.

Każdy z szablonów zawiera domyślne tokeny lub znaczniki zastępcze, czyli zmienne wymagane do dostosowania wiadomości e-mail pod kątem użytkownika. Na przykład szablon wiadomości e-mail funkcji Zapomniane hasło, służący do wysyłania do użytkownika hasła, zawiera domyślny token lub znacznik zastępczy o nazwie „CurrentPassword”.

Dodaj: definiować można również inne tokeny lub znaczniki zastępcze, które będą stosowane w treści wiadomości.

Aby dodać token lub znacznik zastępczy, wykonaj następujące czynności:

1. Kliknij ikonę  .
2. Podaj **nazwę** i **opis** w oknie **Dodaj znacznik zastępczy**.
3. Kliknij przycisk **OK**.
4. Nowy token lub znacznik zastępczy pojawi się w kolumnie Znaczniki zastępcze.

Kopiuj znacznik: kliknij opcję  , aby skopiować wybrany znacznik do bufora systemowego, a następnie możesz kliknąć myszą, aby go wkleić i wykorzystać w wierszu tematu lub treści wiadomości.

Usuń: wybierz token lub znacznik zastępczy na liście i kliknij opcję  , aby usunąć znacznik z listy. Upewnij się, że nie usuwasz znaczników potrzebnych w treści wiadomości.

Treść wiadomości

Tekst wiadomości e-mail.

Po wprowadzeniu wszystkich modyfikacji szablonu powiadomień e-mail kliknij opcję **Aktualizuj**.

Usuń

Usuwa (z Magazynu tożsamości) szablony utworzone przez użytkownika. Nie można usuwać szablonów domyślnych dostarczanych z aplikacjami, takimi jak Identity Manager.

1. Wybierz szablon, który chcesz usunąć.

   Jeśli klikniesz nagłówek tematu szablonu, Identity Console wyświetli okno dialogowe Edit Email Templates (Edytuj szablony poczty e-mail).
2. Kliknij ikonę Usuń.
3. Kliknij przycisk **OK**.

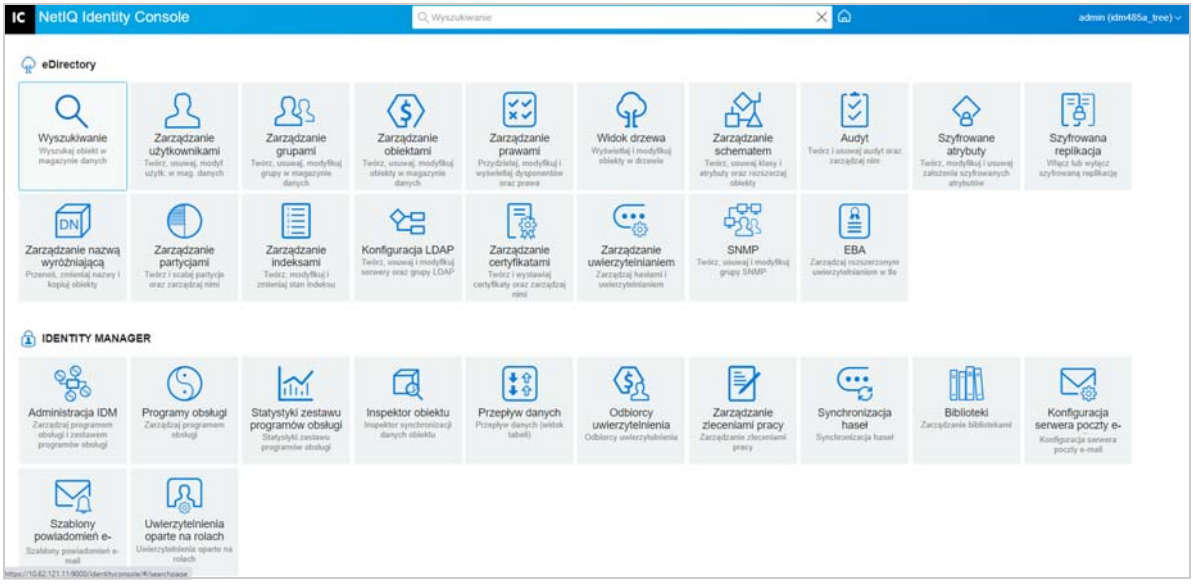
Filtruj szablony

Umożliwia filtrowanie szablonu wiadomości e-mail, który ma być wyświetlany. Zostaną wyświetlone tylko wybrane szablony. Opcja Filter by all (Filtruj wg wszystkich) powoduje wyświetlenie wszystkich szablonów.

Odśwież szablony

Kliknij ikonę , aby odświeżyć i usunąć wszelkie zastosowane filtry szablonów.

Rysunek 32-1 *Szablony powiadomień e-mail*



33 Zarządzanie uwierzytelnieniami opartymi na rolach

Uwierzytelnienie RBE umożliwia przyznanie uwierzytelnień w połączonych systemach grupie użytkowników NetIQ® Identity Console. Dzięki założeniom RBE można usprawnić zarządzanie założeniami biznesowymi i zmniejszyć potrzebę konfigurowania programów obsługi Identity Manager.

Moduł dotyczący uwierzytelnienia opartego na roli obejmuje następujące części:

Uwierzytelnienie oparte na roli

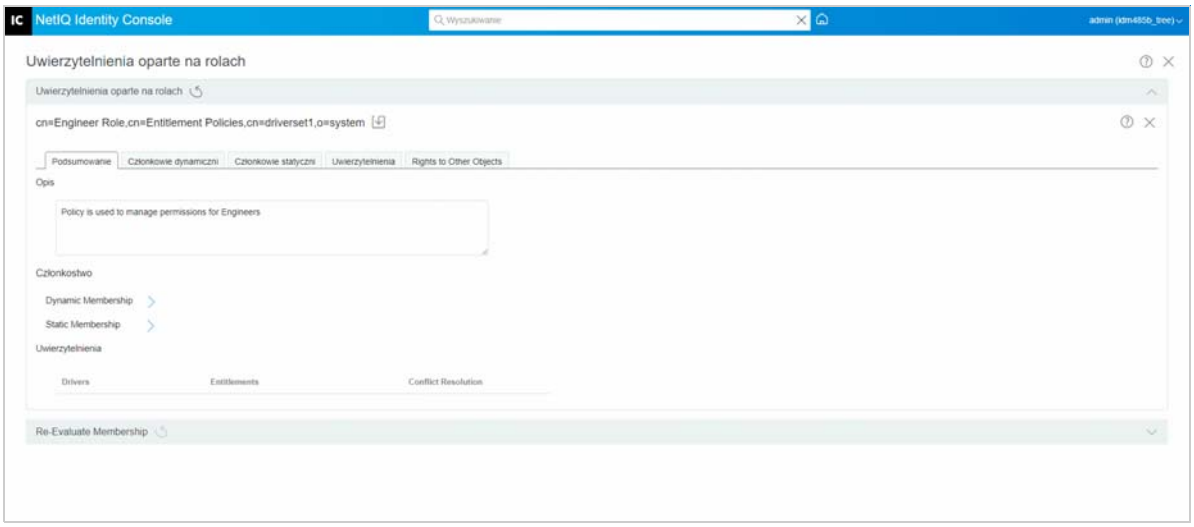
Założenie RBE to obiekt grupy dynamicznej Identity Console z dodatkowymi funkcjami pozwalającymi na przyznawanie uwierzytelnień opartych na rolach w połączonych systemach. Podczas tworzenia założenia RBE definiuje się członkostwo dla założenia, a także uwierzytelnienia, które powinny zostać przyznane członkom założenia RBE. Każde założenie RBE jest skojarzone z pojedynczym obiektem zestawu programów obsługi przypisanym do konkretnego serwera. Podobnie jak program obsługi Identity Manager, każde założenie dotyczące uwierzytelnienia może zarządzać tylko obiektami znajdującymi się w replice głównej lub replice do odczytu/zapisu na serwerze, do którego jest przypisane.

W poniższych sekcjach wyjaśniono szczegółowo uwierzytelnienie oparte na roli:

Podsumowanie

Ta strona przedstawia ogólny widok kryteriów członkostwa i uwierzytelnień w ramach założenia dotyczącego uwierzytelnienia.

Rysunek 33-1 *Strona podsumowania*



Członkostwo:

Kryteria określone dla członkostwa dynamicznego są wyświetlane w składni filtru LDAP. Informacje w polu Tożsamość wyszukiwania wskazują, które prawa obiektu są używane podczas odpytywania o członkostwo dynamiczne, a informacje w polach Podstawowa nazwa wyróżniająca i Zakres wskazują, która część drzewa jest uwzględniona w zapytaniu.

Uwzględnienia w członkostwie statycznym i wykluczenia z niego można wyświetlić, zaznaczając pole wyboru.

Połączona lista wszystkich członków nie jest wyświetlana na stronie Podsumowanie, ponieważ lista ta może być długa. Aby wyświetlić połączoną listę wszystkich członków założenia dotyczącego uwierzytelnienia, zarówno dynamicznych, jak i statycznych, użyj karty Członkostwo > Wyświetl członkostwo.

Uwierzytelnienia:

Uwierzytelnienia w połączonych systemach przyznane członkom założenia dotyczącego uwierzytelnienia. Należy pamiętać, że uwierzytelnienia oparte na rolach są luźno spójne z połączonymi systemami. Oznacza to, że stan uwierzytelnienia w połączonym systemie nie jest wyświetlany w interfejsie Uwierzytelnienie oparte na roli. Jeśli przyznasz uwierzytelnienie założeniu dotyczącemu uwierzytelnienia, a później to uwierzytelnienie nie jest już dostępne w połączonym systemie, uwierzytelnienie nadal widnieje w założeniu dotyczącym uwierzytelnienia, dopóki nie usuniesz go ręcznie z listy.

Rozwiązywanie konfliktów:

W przypadku założeń RBE mających wartości te metody są używane do określania, które wartości są przyznawane użytkownikowi, jeśli co najmniej dwa założenia RBE przyznają temu użytkownikowi różne wartości. Przykładem uwierzytelnienia, które ma wartości, jest członkostwo w listach dystrybucyjnych poczty e-mail, gdzie wartości to nazwy list dystrybucyjnych.

Metoda rozwiązywania konfliktów jest ustawiana osobno dla każdego indywidualnego uwierzytelnienia w każdym obiekcie programu obsługi. Jeśli uwierzytelnienie jest używane w wielu założeniach RBE, metoda rozwiązywania konfliktów jest taka sama we wszystkich założeniach RBE. Aby zmienić metodę rozwiązywania konfliktów dla uwierzytelnienia, należy zmienić ustawienie tego uwierzytelnienia w manifeście programu obsługi dla programu obsługi.

- **Nierozpoznane:** uwierzytelnienie RBE nie zostało ukończone w kreatorze lub ustawienie zostało niepoprawnie wpisane w manifeście programu obsługi.
- **Scalenie:** ustawienie domyślne to Scalenie (`union` w manifeście programu obsługi). Oznacza to, że użytkownikowi zostają przyznane wszystkie wartości tego uwierzytelnienia ze wszystkich założeń RBE, których jest członkiem.

  W przypadku korzystania z domyślnego ustawienia Scalenie kolejność priorytetów listy założeń nie ma znaczenia dla tego konkretnego uwierzytelnienia.

  Na przykład użytkownikowi przyznawane jest członkostwo w listach dystrybucyjnych poczty e-mail dla programu obsługi GroupWise® A na podstawie dwóch różnych założeń RBE — założenia Menedżerowie i założenia Członkowie zespołu. W założeniu 1 użytkownik otrzymuje członkostwo w liście dystrybucyjnej poczty e-mail Menedżerowie, a w założeniu 2 — członkostwo w liście dystrybucyjnej poczty e-mail Członkowie zespołu. W przypadku ustawienia Scalenie użytkownik otrzymuje członkostwo w obu listach dystrybucyjnych poczty e-mail.
- **Priorytet:** to ustawienie oznacza, że jeśli wiele założeń RBE przyznaje użytkownikowi różne wartości dla tego samego uwierzytelnienia z tego samego obiektu programu obsługi, użytkownik otrzymuje tylko te wartości, które są określone w założeniu RBE znajdującym się najwyżej na liście.

  W przypadku korzystania z ustawienia Priorytet kolejność priorytetów listy założeń ma znaczenie dla tego konkretnego uwierzytelnienia.

  Na przykład użytkownikowi przyznawane jest członkostwo w listach dystrybucyjnych poczty e-mail dla programu obsługi GroupWise A na podstawie dwóch różnych założeń RBE — założenia Menedżerowie i założenia Członkowie zespołu. W założeniu Menedżerowie użytkownik otrzymuje członkostwo w liście dystrybucyjnej poczty e-mail Menedżerowie, a w założeniu Członkowie zespołu — członkostwo w liście dystrybucyjnej poczty e-mail Członkowie zespołu. Założenie Menedżerowie znajduje się wyżej na liście założeń niż założenie Członkowie zespołu. W przypadku ustawienia Priorytet użytkownik otrzymuje członkostwo tylko w liście dystrybucyjnej poczty e-mail Menedżerowie.

  Używanie priorytetu do rozwiązywania konfliktów może być przydatne na przykład wtedy, gdy atrybut w połączonym systemie dopuszcza tylko jedną wartość. Jeśli dwa różne założenia RBE przyznają wartość tego atrybutu temu samemu użytkownikowi, użytkownik otrzyma wartość przyznaną przez założenie RBE, które jest najwyżej na liście.

UWAGA: Ustawienie rozwiązywania konfliktów nie jest dostępne dla uwierzytelnień, które nie mają wartości, takich jak konto. Uwierzytelnienia bez wartości są zawsze przyznawane członkom założeń RBE, niezależnie od priorytetu założeń na liście.

Członkowie dynamiczni

Kryteria określone dla członkostwa dynamicznego są wyświetlane w składni filtru LDAP. Informacje w polu Tożsamość wyszukiwania wskazują, które prawa obiektu są używane podczas odpytywania o członkostwo dynamiczne, a informacje w polach Podstawowa nazwa wyróżniająca i Zakres wskazują, która część drzewa jest uwzględniona w zapytaniu.

Filtr członkostwa

Możliwe jest zdefiniowanie kryteriów członkostwa, takich jak położenie w drzewie i atrybuty obiektu. Na przykład członkostwo może zależeć od tego, czy użytkownik znajduje się w aktywnym kontenerze lub czy nazwa stanowiska zawiera słowo Menedżer. Użytkownicy spełniający kryteria stają się automatycznie członkami założenia RBE, bez konieczności dodawania każdego użytkownika do założenia. Członkostwo dynamiczne jest takie samo jak obiekt grupy dynamicznej.

Jeśli obiekt zmieni się tak, że nie spełnia już kryteriów członkostwa dynamicznego, uwierzytelnienia zostają automatycznie unieważnione przy następnej ponownej ocenie użytkownika.

Ustawianie parametrów wyszukiwania

Określ lokalizację użytkowników, którymi ma zarządzać założenie dotyczące uwierzytelnienia. Wybierz kontener, w którym znajdują się użytkownicy (Podstawowa nazwa wyróżniająca) oraz jak daleko od tego kontenera w dół ma przebiegać wyszukiwanie (Zakres wyszukiwania). Aby założenie dotyczące uwierzytelnienia mogło zarządzać użytkownikami w określonych kontenerach, użytkownicy muszą znajdować się w replice do odczytu/zapisu lub replice głównej na serwerze.

Dla ustawienia Zakres wyszukiwania dostępne są następujące opcje:

- Ten kontener i kontenery podrzędne: użytkownicy poniżej tego kontenera w drzewie są członkami założenia dotyczącego uwierzytelnienia, jeśli spełniają kryteria określone dla członkostwa dynamicznego. Użytkownicy wewnątrz kontenerów podrzędnych również są członkami, jeśli spełniają kryteria.
- Tylko ten kontener: użytkownicy wewnątrz tego kontenera są członkami założenia dotyczącego uwierzytelnienia, tylko jeśli spełniają kryteria określone dla członkostwa dynamicznego. Użytkownicy wewnątrz kontenerów podrzędnych poniżej tego kontenera nie są członkami, nawet jeśli spełniają kryteria.

Definiowanie kryteriów filtru

Podaj cechy określające, którzy użytkownicy są członkami założenia dotyczącego uwierzytelnienia.

Na stronie Podsumowanie dla założenia dotyczącego uwierzytelnienia kryteria określone dla członkostwa dynamicznego są wyświetlane w składni filtru LDAP.

Domyślnie członkostwo dynamiczne jest ustawione na uwzględnianie wszystkich obiektów klasy Użytkownik (i obiektów klas pochodnych od klasy Użytkownik) w zakresie wyszukiwania jako członków założenia dotyczącego uwierzytelnienia.

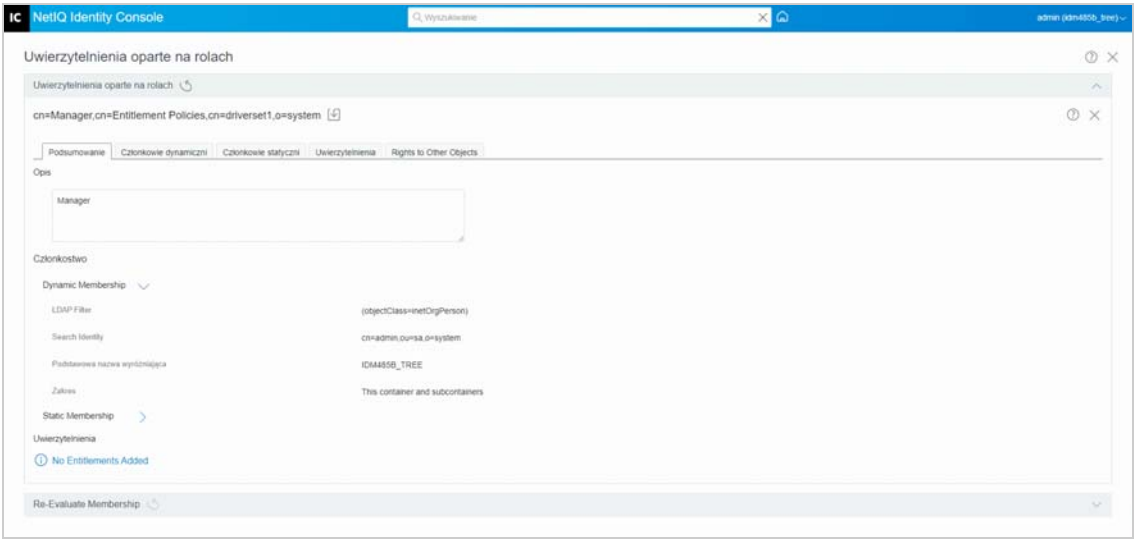
UWAGA: Jeśli utworzysz nową klasę obiektu pochodną od klasy Użytkownik, istniejące założenie dotyczące uwierzytelnienia nie będzie znało tej klasy, dopóki nie zmodyfikujesz założenia dotyczącego uwierzytelnienia. Zapobiega to niezamierzonemu przyznawaniu uwierzytelnień użytkownikom nowej klasy. Wprowadzenie jakiejkolwiek modyfikacji do założenia dotyczącego uwierzytelnienia powoduje zaktualizowanie listy klas pochodnych od użytkownika dla tego założenia.

Tworzenie członkostwa dynamicznego

Na karcie Członkowie dynamiczni wykonaj następujące czynności:

1. Kliknij kartę **Członkowie dynamiczni**.
2. Użyj filtrów **Tożsamość wyszukiwania**, **Rozpocznij wyszukiwania w** i **Zakres wyszukiwania** zgodnie z wymaganiami.
3. Kliknij konkretną opcję **Utwórz grupę**, aby utworzyć nowy warunek lub wiersz, a następnie podaj wymagane kryteria wyszukiwania lub warunek.

Rysunek 33-2 *Członkowie dynamiczni*



Zakres wyszukiwania: zakres wyszukiwania wskazuje zestaw wpisów na poziomie lub poniżej podstawowej nazwy wyróżniającej wyszukiwania, które mogą być uznane za potencjalne dopasowanie dla operacji wyszukiwania.

Kryteria wyszukiwania: wyszukiwanie można ograniczyć, aby ułatwić zlokalizowanie określonego rekordu lub grupy rekordów z dużej liczby rekordów.

Podstawowa nazwa wyróżniająca: podstawowa nazwa wyróżniająca to punkt, od którego serwer będzie szukać użytkowników.

Grupa LDAP: jest to hierarchiczna organizacja użytkowników, grup i jednostek organizacyjnych, które są kontenerami dla użytkowników i grup.

UWAGA: Użytkownik może tworzyć jedną lub wiele grup z warunkami. Warunki składają się z atrybutów, operatorów i wartości. Domyślnie wypełniany jest warunek **Klasa obiektu** > **jest równe** > **Użytkownik**.

Członkowie statyczni

Członkowie statyczni to klasa członków, którzy są deklarowani przy użyciu statycznych słów kluczowych. Członek statyczny ma pewnie ograniczone dostępy.

Na karcie Członkowie statyczni można wykonywać następujące operacje:

Uwzględnij członków:

Dodaj statycznie członków, którzy nie są uwzględnieni przez filtr członkostwa dynamicznego.

Wyklucz członków:

Wyklucz członków, którzy spełniają kryteria filtru, ale nie powinni być uwzględnieni w założeniu dotyczącym uwierzytelnienia.

Uwierzytelnienia

Uwierzytelnienie RBE umożliwia przyznanie uwierzytelnień w połączonych systemach oraz praw w programie Identity Manager. Uwierzytelnienia mogą być następujące:

- Konta w połączonych systemach.
- Członkostwo w listach dystrybucyjnych poczty e-mail w połączonych systemach.
- Członkostwo w grupie w połączonych systemach.
- Atrybuty odpowiednich obiektów w połączonych systemach, wypełnione wartościami, które podasz.

UWAGA: Funkcjonalność Uwierzytelnienia jest częścią programu Identity Manager, dlatego zanim będzie można przyznawać uwierzytelnienia w połączonych systemach, należy zainstalować i skonfigurować programy obsługi Identity Manager do obsługi funkcji Uwierzytelnienia.

Tworzenie uwierzytelnienia

Na karcie Uwierzytelnienia wykonaj następujące czynności:

1. Kliknij kartę **Uwierzytelnienie**.
2. Kliknij przycisk +, aby **dodać programy obsługi** i zapewnić uwierzytelnienia w połączonych systemach.

   Pojawi się ekran **Dodaj program obsługi**.
3. Wybierz program obsługi z menu rozwijanego.
4. Kliknij przycisk **Dodaj**.

   Pojawi się ekran **Dodaj uwierzytelnienia**.
5. Z menu rozwijanego **wybierz grupę uwierzytelnień**, którą chcesz dodać.
6. Wybierz **typ zapytania**:
   - **Buforowane:** gdy zapytania zostały wcześniej uruchomione.
   - **Zapytanie zewnętrzne:** gdy zapytania są nowe.

   Pojawi się ekran **Dodaj uwierzytelnienie grupowe**.
7. Wybierz uwierzytelnienie grupowe z menu rozwijanego, a następnie kliknij przycisk **Wybierz**.

Rights to other Objects (Prawa do innych obiektów)

Ta strona umożliwia nadanie praw dysponenta założenia dotyczącego uwierzytelnienia do obiektu eDirectory. Każdy członek założenia dotyczącego uwierzytelnienia staje się dysponentem obiektu.

Oprócz przypisywania praw do wszystkich atrybutów można kliknąć przycisk Dodaj właściwość, aby przypisać prawa do określonych właściwości.

Pole wyboru Dziedziczenie określa, czy prawa są przenoszone w dół drzewa. Na przykład jeśli przypisujesz prawa do obiektu kontenera i chcesz, aby założenie dotyczące uwierzytelnienia miało takie same prawa do obiektów i kontenerów podrzędnych znajdujących się poniżej tego kontenera, zaznacz pole wyboru Dziedziczenie.

Prawa do obiektów w eDirectory są przyznawane członkom założenia dotyczącego uwierzytelnienia po dokonaniu zmian na tej stronie. Natomiast uwierzytelnienia w połączonych systemach są przyznawane każdemu członkowi założenia dotyczącego uwierzytelnienia następnym razem, gdy atrybut używany do członkostwa dynamicznego jest modyfikowany dla tego użytkownika lub gdy użytkownik jest przenoszony lub zmienia nazwę. (Podobnie jest w przypadku unieważnienia praw i uwierzytelnień). Aby wymusić aktualizację, użyj zadania Ponownie oceń członkostwo.

Tworzenie praw do innych obiektów

Aby utworzyć prawa:

1 Kliknij kartę **Prawa do innych obiektów**

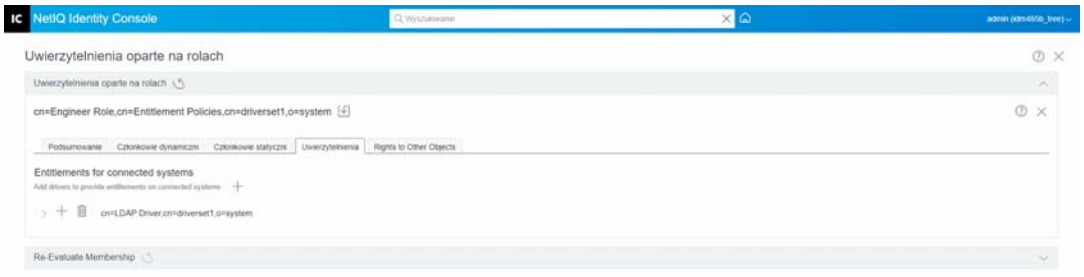
Na tej stronie możesz dodać nowy obiekt i wyszukać te obiekty, które mają być dysponentem tego założenia dotyczącego uwierzytelnienia.

1a Kliknij przycisk +, aby dodać obiekt.

Pojawi się strona **PRZEGLĄDARKA KONTEKSTOWA**. Strona zawiera listę `Obiekty`.

1b Rozwiń listę `Obiekty`, a następnie zgodnie z wymaganiami wybierz grupy lub indywidualnych użytkowników i przypisz im prawa.

Rysunek 33-3 *Prawa do innych obiektów*

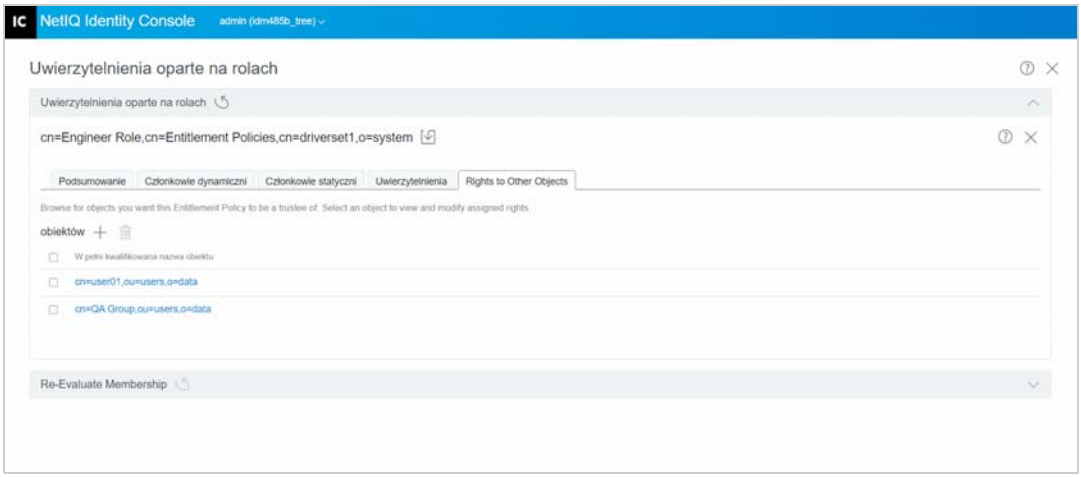


1c Aby dodać więcej właściwości, wybierz przycisk +.

Pojawi się strona **WYBIERZ WŁAŚCIWOŚCI**. Ta strona zawiera listę właściwości, które może mieć obiekt.

1d Kliknij przycisk **Gotowe**.

Rysunek 33-4 *Wybierz opcję Właściwości*



2 (Opcjonalnie) Przy użyciu strzałek **W górę** i **W dół** nadaj priorytet założeniom RBE.

Nadawanie priorytetu założeniom służy rozwiązywaniu konfliktów uwierzytelnień pomiędzy wieloma założeniami. Najwyżej położone założenie ma najwyższy priorytet. Więcej informacji można znaleźć w sekcji: „Nadawanie priorytetu założeniom RBE” na stronie 220

Nadawanie priorytetu założeniom RBE

Podczas tworzenia założeń RBE może się zdarzyć, że założenia mające wpływ na danego użytkownika są ze sobą w konflikcie.

Kolejność założeń RBE na liście odpowiada ich priorytetowi. Kolejność na liście można zmieniać za pomocą przycisków strzałek w górę i w dół.

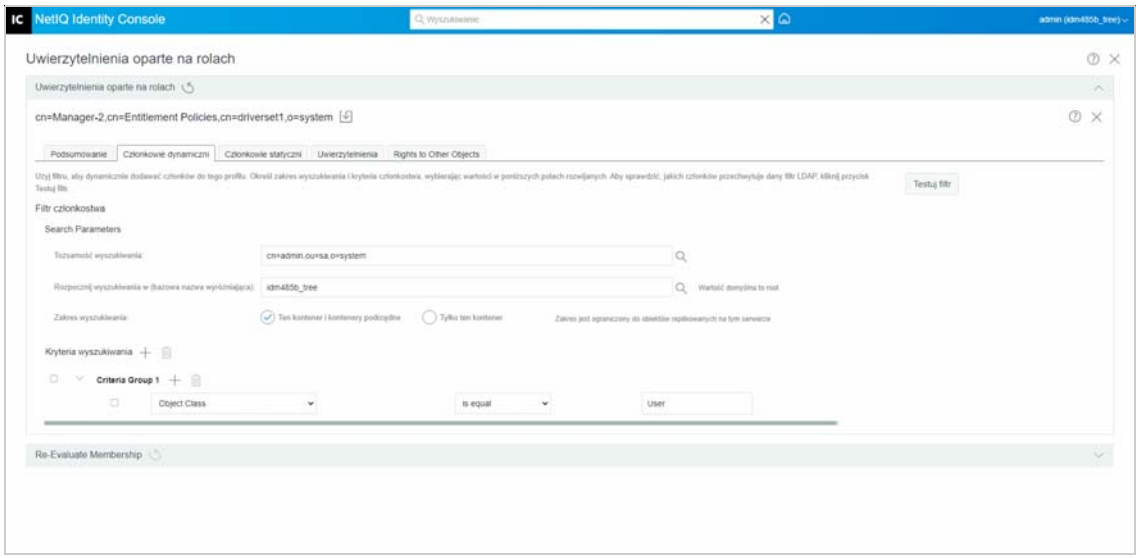
- To ustawienie może być na przykład przydatne, jeśli atrybut w połączonym systemie dopuszcza tylko jedną wartość. Jeśli dwa różne założenia RBE przyznają wartość tego atrybutu temu samemu użytkownikowi, użytkownik otrzyma wartość przyznaną przez założenie RBE, które jest najwyżej na liście. Innym przykładem może być skonfigurowanie środowiska tak, aby używało uwierzytelnień do umieszczania użytkowników w strukturze hierarchicznej w innym systemie. W takiej sytuacji chcesz, aby użytkownik był umieszczony w jednym lub drugim miejscu, a nie w dwóch miejscach jednocześnie.
- Pamiętaj, że ustawienie jest niezależne dla każdego uwierzytelnienia oferowanego przez każdy program obsługi.
- Z reguły założenia administratora lub menedżera należy umieszczać wyżej na liście niż założenia użytkowników końcowych lub poszczególnych współtwórców. Grupy o węższym członkostwie należy umieszczać wyżej niż grupy o szerszym.

Aby nadać priorytet założeniom RBE:

1 Wybierz założenie dotyczące uwierzytelnienia, któremu chcesz zwiększyć lub zmniejszyć priorytet.

2 Przy użyciu strzałek **W górę** lub **W dół** nadaj priorytet założeniom RBE.

Rysunek 33-5 *Ustalanie priorytetów założeń*

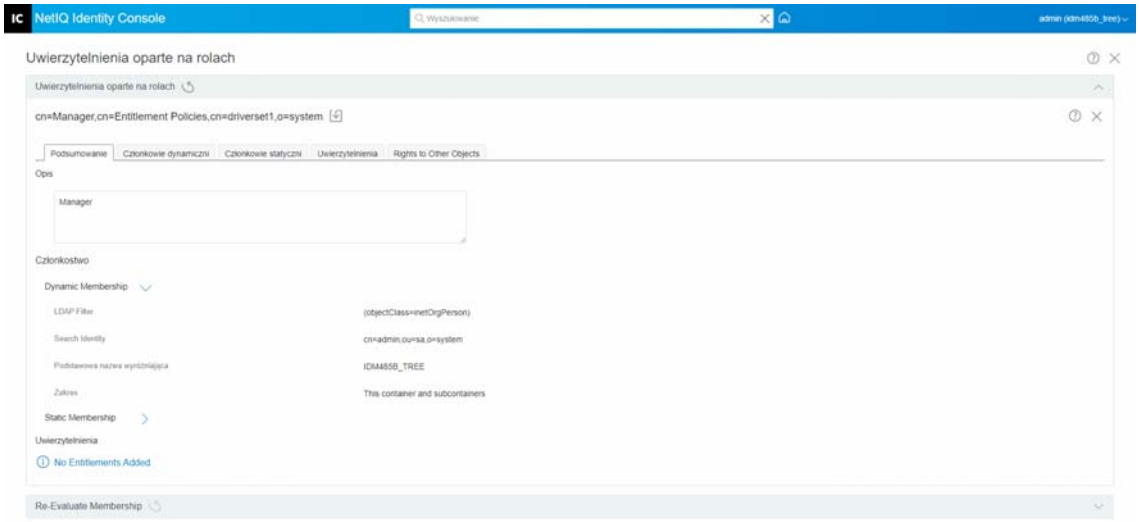


3 Kliknij przycisk Zapisz .

Podsumowanie szczegółów członkostwa w założeniu jest wyświetlane na karcie **Podsumowanie**.

4 Uruchom ponownie program obsługi.

Rysunek 33-6 *Zamknięcie i ponowne uruchomienie*



UWAGA: Ponowne uruchomienie programu obsługi jest niezbędne, aby zmiany zaczęły obowiązywać.

Ponowna ocena członkostwa

Uwierzytelnienia oparte na rolach umożliwiają przyznawanie uwierzytelnień w połączonych systemach grupie użytkowników.

Podczas tworzenia lub edytowania założeń RBE członkostwo każdego użytkownika musi zostać ponownie ocenione w celu określenia, czy uwierzytelnienia w połączonych systemach muszą zostać przyznane, zmienione lub unieważnione. Domyślnie ponowna ocena jest przeprowadzana dla użytkowników pojedynczo, przy następnej zmianie atrybutu, który ma wpływ na członkostwo dla każdego użytkownika, lub gdy użytkownik jest przenoszony lub zmienia nazwę. To domyślne zachowanie minimalizuje użycie zasobów systemowych, ale oznacza, że może wystąpić znaczne opóźnienie między zmianą założenia RBE a przyznaniem, zmianą lub unieważnieniem uwierzytelnień dla konkretnego użytkownika.

Aby uwierzytelnienia użytkowników zostały zaktualizowane od razu, możesz użyć zadania „Ponowna ocena założeń RBE” na stronie 222 w celu określenia użytkowników, którzy powinni zostać natychmiast ponownie ocenieni. Zalecamy wykonywanie tego zadania przy każdym tworzeniu lub edytowaniu założenia RBE.

Przed wersją Identity Manager 3.6 ponowna ocena członkostwa była przeprowadzana dla wszystkich założeń RBE w zestawie programów obsługi, a nie dla poszczególnych założeń dotyczących uwierzytelnień. Program Identity Manager 3.6 umożliwia jednak **ocenę** założenia RBE i **dodanie** jego członków do wybranej **listy obiektów**. Jeśli zdefiniujesz założenie dotyczące uwierzytelnienia i utworzysz listę członków, to obok wybranego wpisu Obiekty zobaczysz nagłówek Oceń założenie dotyczące uwierzytelnienia, aby **dodać** jego członków do listy. Wybierz założenie, a następnie kliknij ikonę +, aby dodać członków założenia do **listy obiektów**. Możesz dodawać lub usuwać członków lub obiekty z wybranej **listy obiektów**.

Aby jak najlepiej wykorzystać zasoby systemowe, należy wprowadzić wszystkie zmiany w założeniach RBE w danym zestawie programów obsługi przed użyciem zadania „Ponowna ocena założeń RBE” na stronie 222.

UWAGA: Ponowna ocena założeń jest konieczna tylko w przypadku uwierzytelnień w połączonych systemach. Gdy prawa oprogramowania Identity Console są zmieniane dla założeń RBE, zmiany obowiązują natychmiast dla każdego użytkownika. Aby można było przeprowadzić ponowną ocenę członkostwa, musi być uruchomiony program obsługi usługi uwierzytelnienia.

Ponowna ocena założeń RBE

Aby ponownie ocenić członkostwo:

1. Kliknij kolejno opcje **Ponownie oceń członkostwo** > **Wybierz zestaw programów obsługi**.

   Pojawi się lista utworzonych założeń.

2. Wybierz założenie wymagające ponownej oceny i kliknij przycisk **Oceń** Evaluate.

   Na karcie **Obiekty** pojawią się użytkownicy będący częścią grupy.

3. (Opcjonalnie) Aby dodać konkretnego użytkownika, kliknij przycisk +.

   Tej funkcji **Dodaj** + możesz użyć tylko wtedy, gdy na liście nie ma użytkowników, a chcesz dodać konkretnych użytkowników.

4 (Opcjonalnie) Aby usunąć konkretnego użytkownika, kliknij przycisk .

Tej funkcji **Usuń** możesz użyć tylko wtedy, gdy konkretnych użytkowników trzeba usunąć z listy.

5 Kliknij przycisk Ponownie oceń członkostwo .

Rysunek 33-7 *Ponowna ocena członkostwa*