Identity Console

Podręcznik instalacji

Wrzesień 2022 r.

Informacje prawne

Informacje prawne, na temat znaków towarowych, zrzeczeń, gwarancji, eksportu i innych ograniczeń użytkowania, praw rządu Stanów Zjednoczonych, zasad dotyczących patentów oraz zgodności ze standardem FIPS można znaleźć na stronie https://www.netiq.com/company/legal.

Copyright © 2022 NetIQ Corporation. Wszelkie prawa zastrzeżone.

Spis treści

Informacje o niniejszym podręczniku i bibliotece

Podręcznik instalacji Identity Console zawiera informacje na temat instalowania produktu NetIQ Identity Console (Identity Console) i zarządzania nim. Podano w nim definicje terminów oraz przedstawiono scenariusze wdrażania.

Docelowi odbiorcy

Ten podręcznik jest przeznaczony dla administratorów sieci.

Inne informacje w bibliotece

Biblioteka udostępnia następujące zasoby informacyjne:

Podręcznik instalacji

Opisuje sposób instalowania i uaktualniania 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 Planowanie instalacji oprogramowania Identity Console

W tym rozdziale opisano wymagania systemowe i wymagania wstępne, jakie należy spełnić, aby zainstalować oprogramowanie Identity Console. Oprogramowanie Identity Console można uruchamiać jako kontener Dockera lub jako autonomiczną aplikację — wymagania systemowe i wymagania wstępne obu typów instalacji znajdziesz w odpowiednich sekcjach.

UWAGA: Identity Console obsługuje produkty eDirectory 9.2.4 HF2, Identity Manager Engine 4.8.3 HF2 i ich odpowiednie nowsze wersje. Przed użyciem oprogramowania Identity Console należy uaktualnić używane wystąpienia produktów eDirectory i Identity Manager Engine.

Wymagania systemowe i wymagania wstępne dotyczące instalacji Dockera

W tej części opisano wymagania systemowe i wymagania wstępne, jakie należy spełnić w celu zainstalowania oprogramowania Identity Console jako kontenera Dockera.

Wymagania systemowe

Oprogramowanie Identity Console można uruchamiać jako kontener Dockera — więcej informacji na temat wymagań systemowych i obsługiwanych platform umożliwiających zainstalowanie oprogramowania Identity Console można znaleźć w dokumentacji Dockera.

Wymagania wstępne

- ❒ Zainstaluj Dockera w wersji 20.10.9-ce lub nowszej. Aby uzyskać więcej informacji na temat instalowania Dockera, zobacz Docker Installation (Instalacja Dockera).
- ❒ Musisz uzyskać certyfikat serwera w formacie pkcs12 z kluczem prywatnym do szyfrowania/odszyfrowywania wymiany danych między serwerem Identity Console a serwerem zaplecza. Ten certyfikat serwera służy do zabezpieczania połączenia HTTP. Możesz używać certyfikatów

serwera wygenerowanych przez zewnętrzny ośrodek certyfikacji. Aby uzyskać więcej informacji, zobacz Tworzenie obiektów certyfikatu serwera. Certyfikat serwera powinien zawierać nazwę alternatywną podmiotu z adresem IP i nazwą DNS serwera Identity Console. Po utworzeniu obiektu certyfikatu serwera musisz go wyeksportować w formacie .pfx.

- Dla wszystkich drzew musisz uzyskać certyfikat ośrodka certyfikacji w formacie `.pem` do zatwierdzania podpisu ośrodka certyfikacji dla certyfikatów serwera uzyskanych w poprzednim kroku. Ten certyfikat głównego ośrodka certyfikacji zapewnia też ustanowienie bezpiecznej komunikacji LDAP między klientem a serwerem Identity Console. Możesz na przykład uzyskać certyfikat ośrodka certyfikacji eDirectory (`SSCert.pem`) z `/var/opt/novell/eDirectory/data/SSCert.pem`.
- (Opcjonalnie) Używając usługi One SSO Provider (OSP), możesz włączyć dla użytkowników uwierzytelnianie z jednokrotnym logowaniem do portalu Identity Console. Usługę OSP musisz zainstalować przed zainstalowaniem oprogramowania Identity Console. Aby skonfigurować usługę OSP pod kątem oprogramowania Identity Console, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie i podaj wymagane wartości parametrów konfiguracji. Aby uzyskać więcej informacji, zobacz „Wdrażanie kontenera OSP” na stronie 22. Aby zarejestrować Identity Console na istniejącym serwerze OSP, musisz ręcznie dodać plik `ism-configuration.properties` w folderze `/opt/netiq/idm/apps/tomcat/conf/`:

  ```
  com.netiq.edirapi.clientID = identityconsole
  com.netiq.edirapi.redirect.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/authcoderedirect
  com.netiq.edirapi.logout.url = https://<Identity Console Server IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/logoutredirect
  com.netiq.edirapi.logout.return-param-name = logoutURL
  com.netiq.edirapi.response-types = code,token
  com.netiq.edirapi.clientPass._attr_obscurity = NONE
  com.netiq.edirapi.clientPass = novell
  ```

  UWAGA: W przypadku usługi OSP możesz nawiązać połączenie tylko z jednym drzewem eDirectory, ponieważ usługa OSP nie obsługuje wielu drzew eDirectory.

- Upewnij się, że w pliku `/etc/hosts` jest dostępny poprawny wpis DNS dla komputera hosta, obejmujący w pełni zakwalifikowaną nazwę hosta.
- Jeśli chcesz używać oprogramowania Identity Console w przeglądarce Edge, w celu uzyskania pełnej funkcjonalności musisz pobrać najnowszą wersję Microsoft Edge.

UWAGA: Podczas używania oprogramowania Identity Console w przeglądarce Mozilla Firefox operacja może się nie powieść z komunikatem o błędzie `Niezgodność pochodzenia`. Aby rozwiązać ten problem, wykonaj następujące czynności:

1. Zaktualizuj przeglądarkę Safari do najnowszej wersji.
2. Na pasku adresu URL przeglądarki Firefox wprowadź `about:config` i naciśnij klawisz Enter.
3. Wyszukaj słowo Origin.
4. Kliknij dwukrotnie pozycję `network.http.SendOriginHeader` i zmień jej wartość na 1.

Konfigurowanie środowiska

Konieczne może być utworzenie pliku konfiguracyjnego zawierającego określone parametry. Jeśli chcesz skonfigurować oprogramowanie Identity Console z usługą OSP, musisz podać w pliku konfiguracyjnym parametry specyficzne dla usługi OSP. Na przykład utwórz poniższy plik `edirapi.conf` z parametrami usługi OSP:

UWAGA: Musisz podać nazwę drzewa eDirectory w polu `osp-redirect-url`.

```
listen = ":9000"
ldapserver = "2.168.1.1:636"
ldapuser = "cn=admin,ou=sa,o=system"
ldappassword = "novell"
pfxpassword = "novell"
ospmode = "true"
osp-token-endpoint = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/
getattributes"
osp-authorize-url = "https://10.10.10.10:8543/osp/a/idm/auth/oauth2/grant"
osp-logout-url = "https://10.10.10.10:8543/osp/a/idm/auth/app/logout"
osp-redirect-url = "https://10.10.10.10:9000/eDirAPI/v1/edirtree/
authcoderedirect"
osp-client-id = "identityconsole"
ospclientpass = "novell"
ospcert = "/etc/opt/novell/eDirAPI/cert/SSCert.pem"
bcert = "/etc/opt/novell/eDirAPI/cert/"
loglevel = "error"
check-origin = "true"
origin = "https://10.10.10.10:9000,https://192.168.1.1:8543"
```

Jeśli chcesz skonfigurować oprogramowanie Identity Console bez usługi OSP, utwórz poniższy plik konfiguracyjny bez parametrów usługi OSP:

```
listen = ":9000"
pfxpassword = "novell"
ospmode = "false"
bcert = "/etc/opt/novell/eDirAPI/cert/"
```

UWAGA: Jeśli chcesz skonfigurować oprogramowanie Identity Console z wieloma drzewami eDirectory, możesz pominąć parametry „*ldapserver*”, „*ldapuser*” oraz „*ldappassword*” i utworzyć plik konfiguracyjny.

Tabela 1-1 *Opis parametrów konfiguracji w pliku konfiguracyjnym*

Parametry konfiguracji	Opis
listen	Podaj 9000 jako port nasłuchiwania serwera Identity Console wewnątrz kontenera.
ldapserver	Podaj adres IP serwera hosta eDirectory oraz numer portu.

Parametry konfiguracji	Opis
ldapuser	Podaj nazwę użytkownika dla użytkownika usługi eDirectory. Ten parametr jest używany jako poświadczenie do inicjowania wywołań LDAP do usługi eDirectory przy użyciu kontroli autoryzacji proxy w przypadku logowania OSP. Użytkownik LDAP musi mieć uprawnienia nadzorcy w drzewie eDirectory.
ldappassword	Podaj hasło użytkownika LDAP.
pfxpassword	Podaj hasło pliku certyfikatu serwera w formacie pkcs12.
ospmode	Podaj wartość `true`, aby zintegrować usługę OSP z oprogramowaniem Identity Console. Jeśli ustawisz wartość `false`, oprogramowanie Identity Console będzie korzystać z logowania LDAP.
osp-token-endpoint	Ten adres URL służy do pobierania określonych atrybutów z serwera OSP w celu zweryfikowania poprawności tokena uwierzytelniania.
osp-authorize-url	Ten adres URL jest używany przez użytkownika do podawania poświadczeń w celu uzyskania tokenu uwierzytelniania.
osp-logout-url	Ten adres URL umożliwia zakończenie sesji między użytkownikiem a serwerem OSP.
osp-redirect-url	Serwer OSP przekierowuje użytkownika pod ten adres URL po przyznaniu tokenu uwierzytelniania. **UWAGA:** Pamiętaj, aby podając nazwę drzewa eDirectory podczas konfigurowania oprogramowania Identity Console użyć małych liter. Jeśli nazwa drzewa nie zostanie podana małymi literami, logowanie do serwera Identity Console może się nie powieść.
osp-client-id	Podaj identyfikator klienta OSP podany w momencie rejestracji oprogramowania Identity Console w OSP.
ospclientpass	Podaj hasło klienta OSP podane w momencie rejestracji oprogramowania Identity Console w OSP.
ospcert	Podaj lokalizację certyfikatu ośrodka certyfikacji serwera OSP.
bcert	Podaj lokalizację certyfikatu ośrodka certyfikacji oprogramowania Identity Console.
loglevel	Podaj poziomy dziennika, które mają zostać uwzględnione w pliku dziennika. Ten parametr może mieć wartość „fatal” (błąd krytyczny), „error” (błąd), „warn” (ostrzeżenie) lub „info” (informacje).

Parametry konfiguracji	Opis
check-origin	Jeśli ten parametr ma wartość `true`, serwer Identity Console porównuje wartość pochodzenia żądań. Dostępne opcje to `true` lub `false`. Parametr *origin* jest obowiązkowy, nawet jeśli parametr *check-origin* ma wartość `false`, w przypadku używania konfiguracji DNS.
origin	Identity Console porównuje wartość pochodzenia żądań z wartościami podanymi w tym polu. **UWAGA:** Od wersji Identity Console 1.4 wzwyż ten parametr jest niezależny od parametru *check-origin* i jest obowiązkowy w przypadku używania konfiguracji DNS.
maxclients	Maksymalna liczba klientów, którzy mogą jednocześnie uzyskać dostęp do `IDConsole`. Wszyscy dodatkowi klienci przekraczający ten limit muszą czekać w kolejce.

UWAGA

- Parametru konfiguracji `ospmode` należy użyć tylko w przypadku planowania zintegrowania usługi OSP z oprogramowaniem Identity Console.
- Jeśli w konfiguracji programu Identity Manager komponent Identity Apps jest skonfigurowany w trybie klastra, w polach `osp-token-endpoint`, `osp-authorize-url` i `osp-logout-url` w pliku konfiguracyjnym musisz podać nazwę DNS serwera równoważenia obciążenia. Jeśli w polach tych podasz szczegóły serwera OSP, logowanie do oprogramowania Identity Console nie powiedzie się.
- Jeśli oprogramowanie Identity Console jest skonfigurowane przy użyciu tego samego wystąpienia usługi OSP co komponenty Identity Apps i Identity Reporting, podczas logowania do portalu Identity Console zadziała jednokrotne logowanie (usługa uwierzytelniania).
- Od wersji Identity Console 1.4 wzwyż adres HTTPS URL usługi OSP należy zatwierdzać za pomocą certyfikatów zawierających klucz 2048-bitowy lub wyższy.
- Jeśli chcesz ograniczyć dostęp do portalu Identity Console z innych domen, ustaw parametr `samesitecookie` na `strict`. Jeśli chcesz zezwolić na dostęp do portalu Identity Console z innych domen, ustaw parametr `samesitecookie` na `lax`. Jeśli ten parametr nie zostanie określony podczas konfiguracji, domyślnie będą uwzględniane ustawienia przeglądarki.

Po przygotowaniu pliku konfiguracyjnego rozpocznij wdrażanie kontenera. Aby uzyskać więcej informacji, zobacz „Wdrażanie oprogramowania Identity Console jako kontenera Dockera” na stronie 22.

Wymagania systemowe i wymagania wstępne dotyczące instalacji autonomicznej (bez Dockera)

Wymagania systemowe

W tej części opisano wymagania systemowe i wymagania wstępne, jakie należy spełnić, aby zainstalować autonomiczną wersję oprogramowania Identity Console.

Kategoria	Wymaganie minimalne
Procesor	1,4 GHz 64-bitowy
Pamięć	2 GB
Miejsce na dysku twardym	200 MB w systemie Linux
Obsługiwana przeglądarka	◆ Najnowsza wersja przeglądarki **Microsoft Edge** ◆ Najnowsza wersja przeglądarki **Google Chrome** ◆ Najnowsza wersja przeglądarki **Mozilla Firefox** **UWAGA:** Podczas używania oprogramowania Identity Console w przeglądarce Mozilla Firefox operacja może się nie powieść z komunikatem o błędzie `Niezgodność pochodzenia`. Aby rozwiązać ten problem, wykonaj następujące czynności: **1** Zaktualizuj przeglądarkę Safari do najnowszej wersji. **2** Na pasku adresu URL przeglądarki Firefox wprowadź `about:config` i naciśnij klawisz Enter. **3** Wyszukaj słowo Origin. **4** Kliknij dwukrotnie pozycję `network.http.SendOriginHeader` i zmień jej wartość na 1.
Obsługiwany system operacyjny	◆ **Certyfikowane**: ◆ SUSE Linux Enterprise Server (SLES) 15 SP1, SP2 i SP3 ◆ SUSE Linux Enterprise Server (SLES) 12 SP1, SP2, SP3, SP4 i SP5 ◆ Red Hat Enterprise Linux (RHEL) 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 i 8.5 ◆ OpenSUSE 15.1 i 15.2 ◆ **Obsługiwane:** obsługiwane w nowszych wersjach pakietów Support Pack powyższych certyfikowanych systemów operacyjnych.

Kategoria	Wymaganie minimalne
Certyfikaty	◆ Musisz uzyskać certyfikat serwera w formacie pkcs12 z kluczem prywatnym do szyfrowania/odszyfrowywania wymiany danych między klientem a serwerem Identity Console. Ten certyfikat serwera służy do zabezpieczania połączenia HTTP. Możesz używać certyfikatów serwera wygenerowanych przez zewnętrzny ośrodek certyfikacji. Aby uzyskać więcej informacji, zobacz Tworzenie obiektów certyfikatu serwera. Certyfikat serwera powinien zawierać nazwę alternatywną podmiotu z adresem IP i nazwą DNS serwera Identity Console. Po utworzeniu obiektu certyfikatu serwera musisz go wyeksportować w formacie .pfx. ◆ Musisz uzyskać certyfikat ośrodka certyfikacji w formacie `.pem` do zatwierdzania podpisu ośrodka certyfikacji dla certyfikatów serwera uzyskanych w poprzednim kroku. Ten certyfikat głównego ośrodka certyfikacji zapewnia też ustanowienie bezpiecznej komunikacji LDAP między klientem a serwerem Identity Console. Możesz na przykład uzyskać certyfikat ośrodka certyfikacji eDirectory (`SSCert.pem`) z `/var/opt/novell/eDirectory/data/SSCert.pem`.

Gdy wszystko jest gotowe, przejdź do instalowania oprogramowania Identity Console. Aby uzyskać więcej informacji, zobacz „Wdrażanie oprogramowania Identity Console w wersji autonomicznej” na stronie 27.

(Opcjonalnie) Warunek wstępny konfiguracji usługi OSP

Używając usługi One SSO Provider (OSP), możesz włączyć dla użytkowników uwierzytelnianie z jednokrotnym logowaniem do portalu Identity Console. Usługę OSP musisz zainstalować przed zainstalowaniem oprogramowania Identity Console. Aby skonfigurować usługę OSP pod kątem oprogramowania Identity Console, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie i podaj wymagane wartości parametrów konfiguracji. Aby uzyskać więcej informacji, zobacz „Wdrażanie kontenera OSP” na stronie 22. Aby zarejestrować Identity Console na istniejącym serwerze OSP, musisz ręcznie dodać plik `ism-configuration.properties` w folderze `/opt/netiq/idm/apps/tomcat/conf/`:

```
com.netiq.edirapi.clientID = identityconsole
com.netiq.edirapi.redirect.url = https://<Identity Console Server
IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/
authcoderedirect
com.netiq.edirapi.logout.url = https://<Identity Console Server
IP>:<Identity Console Listener Port>/eDirAPI/v1/<eDirectory Tree Name>/
logoutredirect
com.netiq.edirapi.logout.return-param-name = logoutURL
com.netiq.edirapi.response-types = code,token
com.netiq.edirapi.clientPass._attr_obscurity = NONE
com.netiq.edirapi.clientPass = novell
```

UWAGA

- Jeśli instalujesz usługę OSP po raz pierwszy, podaj opcję `y` w polu **Konfiguruj OSP za pomocą eDir API** i postępuj zgodnie z monitami wyświetlanymi na ekranie, aby zarejestrować oprogramowanie Identity Console w usłudze OSP.
- Pamiętaj, aby podając nazwę drzewa eDirectory podczas konfigurowania oprogramowania Identity Console użyć małych liter. Jeśli nazwa drzewa nie zostanie podana małymi literami, logowanie do serwera Identity Console może się nie powieść.
- W przypadku usługi OSP możesz nawiązać połączenie tylko z jednym drzewem eDirectory, ponieważ usługa OSP nie obsługuje wielu drzew eDirectory.

Wymagania systemowe i wymagania wstępne dotyczące instalacji stacji roboczej

Wymagania systemowe

W tej części opisano wymagania systemowe i wymagania wstępne, jakie należy spełnić, aby zainstalować wersję oprogramowania Identity Console przeznaczoną na stację roboczą.

Kategoria	Wymaganie minimalne
Procesor	1.5 GHz 64-bitowy
Pamięć	2 GB
Miejsce na dysku twardym	1 GB w systemie Windows

Obsługiwany system operacyjny	• **Certyfikowane**:
	  • Windows Server 2016
	  • Windows Server 2019
	  • Windows Server 2022
	  • Windows 10
	  • Windows 11

Kategoria	Wymaganie minimalne
Certyfikaty	◆ Musisz uzyskać certyfikat serwera w formacie pfx do wymiany danych między klientem Identity Console a serwerem REST. Ten certyfikat serwera musi zawsze mieć nazwę keys.pfx. Aby uzyskać więcej informacji, zobacz Tworzenie obiektów certyfikatu serwera (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/b1j4tpo3.html#b1j4u0cm). ◆ Musisz uzyskać certyfikat ośrodka certyfikacji w formacie `.pem` do zatwierdzania podpisu ośrodka certyfikacji dla certyfikatów serwera uzyskanych w poprzednim kroku. Ten certyfikat głównego ośrodka certyfikacji zapewnia też ustanowienie bezpiecznej komunikacji `LDAP` między klientem a serwerem Identity Console. Certyfikat ośrodka certyfikacji eDirectory dla systemu Linux (`SSCert.pem`) możesz na przykład uzyskać z `/var/opt/novell/eDirectory/data/SSCert.pem`. Certyfikat ośrodka certyfikacji eDirectory `SSCert.pem` dla systemu Windows uzyskasz z `<Lokalizacja instalacji eDirectory>\NetIQ\eDirectory\DIBFiles\CertServ\SSCert.pem`.

Gdy wszystko jest gotowe, przejdź do wdrażania oprogramowania Identity Console. Aby uzyskać więcej informacji, zobacz „Identity Console w systemie Windows jako stacja robocza” na stronie 29.

Weryfikacja podpisu RPM

Wykonaj następujące czynności, aby przeprowadzić weryfikację podpisu RPM:

1. Przejdź do folderu, do którego wypakowano kompilację.

   Na przykład: `<rozpakowana lokalizacja Identity Console>/IdentityConsole_150_Linux/license/MicroFocusGPGPackageSign.pub`.

2. Uruchom następujące polecenie w celu zaimportowania klucza publicznego:

   ```
   rpm --import MicroFocusGPGPackageSign.pub
   ```

3. (Opcjonalnie) Uruchom następujące polecenie w celu zweryfikowania podpisu RPM: `rpm --checksig -v <nazwa RPM>`

   Na przykład:

   ```
   rpm --checksig -v identityconsole-1.5.0000.x86_64.rpm
   identityconsole-1.5.0000.x86_64.rpm:
   Header V4 RSA/SHA256 Signature, OK, key ID 786ec7c0: OK
   Header SHA1 digest: OK
   Header SHA256 digest: OK
   ```

```
Payload SHA256 digest: OK
V4 RSA/SHA256 Signature, key ID 786ec7c0: OK
MD5 digest: OK
```

2 Wdrażanie oprogramowania Identity Console

W tym rozdziale opisano proces wdrażania oprogramowania Identity Console oraz zalecenia dotyczące zabezpieczeń. Aby przygotować się do wdrażania, należy zapoznać się z wymaganiami wstępnymi i wymaganiami systemowymi (zob. Rozdział 1, „Planowanie instalacji oprogramowania Identity Console”, na stronie 11).

Zalecenia dotyczące zabezpieczeń

- Domyślnie kontenery Dockera nie mają żadnych ograniczeń dotyczących zasobów. W efekcie każdy kontener ma dostęp do wszystkich zasobów procesora i pamięci zapewnianych przez jądro hosta. Należy się upewnić, że jeden uruchomiony kontener nie zużywa większej ilości zasobów i nie pozbawia ich innych uruchomionych kontenerów, ustawiając ograniczenia ilości zasobów, jakich może używać kontener.
  - Kontener Dockera powinien zapewniać stosowanie stałego limitu dla pamięci używanej przez kontener, używając flagi `--memory` w poleceniu uruchamiania Dockera.
  - Kontener Dockera powinien zapewniać stosowanie limitu dla ilości zasobów procesora używanych przez kontener, używając flagi `--cpuset-cpus` w poleceniu uruchamiania Dockera.
- Parametr `--pids-limit` należy ustawić na 300, aby ograniczyć liczbę wątków jądra tworzonych w danej chwili wewnątrz kontenera. Ma to zapobiegać atakom DoS.
- Należy ustawić założenia ponownego uruchamiania kontenera w przypadku awarii na 5, używając flagi `--restart` w poleceniu uruchamiania Dockera.
- Z kontenera można korzystać tylko wtedy, gdy po pojawieniu się kontenera wyświetlanym stanem jest **Dobry stan**. Aby sprawdzić stan kontenera, uruchom następujące polecenie:

`docker ps <container_name/ID>`

- Kontener Dockera będzie zawsze uruchamiany jako użytkownik niebędący użytkownikiem root (`nds`). Jako dodatkowy środek bezpieczeństwa włącz ponowne mapowanie przestrzeni nazw użytkownika w demonie, aby zapobiec atakom eskalacji uprawnień z poziomu kontenera. Aby uzyskać więcej informacji na temat przestrzeni nazw użytkownika, zobacz Isolate containers with a user namespace (Izolowanie kontenerów za pomocą przestrzeni nazw użytkownika).

Wdrażanie oprogramowania Identity Console jako kontenera Dockera

W tej części omówiono następujące procedury:

Wdrażanie kontenera OSP

Wykonaj następujące czynności, aby wdrożyć kontener OSP:

1. Zaloguj się na stronie Software License and Download (https://sld.microfocus.com/) i przejdź do strony Software Downloads (Pobieranie oprogramowania).
2. Wybierz następujące opcje:
   - Produkt: eDirectory
   - Nazwa produktu: eDirectory per User Sub SW E-LTU
   - Wersja: 9.2
3. Pobierz plik: `IdentityConsole_<wersja>_Containers_tar.zip`.
4. Wypakuj pobrany plik do folderu.
5. Zmodyfikuj zgodnie z wymaganiami plik właściwości instalacji w trybie bez sygnalizacji. Przykładowy plik właściwości instalacji w trybie bez sygnalizacji przedstawiono poniżej:

```
# Silent file for osp with edirapi
## Static contents Do not edit - starts
INSTALL_OSP=true
DOCKER_CONTAINER=y
EDIRAPI_PROMPT_NEEDED=y
UA_PROMPT_NEEDED=n
SSPR_PROMPT_NEEDED=n
RPT_PROMPT_NEEDED=n
CUSTOM_OSP_CERTIFICATE=y
## Static contents Do not edit - ends

# OSP Details
SSO_SERVER_HOST=osp.example.com
SSO_SERVER_SSL_PORT=8543
OSP_COMM_TOMCAT_KEYSTORE_FILE=/config/tomcat.ks
OSP_COMM_TOMCAT_KEYSTORE_PWD=novell
SSO_SERVICE_PWD=novell
```

```
OSP_KEYSTORE_PWD=novell
IDM_KEYSTORE_PWD=novell
OSP_CUSTOM_NAME="Identity Console"
USER_CONTAINER="o=novell"
ADMIN_CONTAINER="o=novell"

# IDConsole Details
IDCONSOLE_HOST=192.168.1.1
IDCONSOLE_PORT=9000
EDIRAPI_TREENAME=ed913

#If ENABLE_CUSTOM_CONTAINER_CREATION is set to y
#ie., when you have user and admin container different from o=data
#    and they need to be created in eDir
#then CUSTOM_CONTAINER_LDIF_PATH should be entered as well
ENABLE_CUSTOM_CONTAINER_CREATION=n
#ENABLE_CUSTOM_CONTAINER_CREATION=y
#CUSTOM_CONTAINER_LDIF_PATH=/config/custom-osp.ldif

# eDir Details
ID_VAULT_HOST=192.168.1.1
ID_VAULT_LDAPS_PORT=636
ID_VAULT_ADMIN_LDAP="cn=admin,o=novell"
ID_VAULT_PASSWORD=novell
```

UWAGA: Aby uniknąć ograniczeń miejsca podczas używania pliku właściwości instalacji w trybie bez sygnalizacji (pliku tekstowego DOS), należy przekonwertować plik tekstowy DOS na format UNIX za pomocą narzędzia dos2unix. Uruchom poniższe polecenie, aby przekonwertować plik tekstowy z końcówek linii DOS na końcówki linii UNIX:

```
dos2unix filename
```

Na przykład:

```
dos2unix samplefile
```

6 Wygeneruj certyfikat serwera (`cert.der`), używając programu iManager, i zaimportuj go do magazynu kluczy (`tomcat.ks`). Skopiuj plik właściwości instalacji w trybie bez sygnalizacji oraz magazyn kluczy (`tomcat.ks`) do dowolnego katalogu. Na przykład `/data`. Wykonaj następujące czynności, aby utworzyć certyfikat serwera i zaimportować go do magazynu kluczy:

6a Uruchom następujące polecenie, aby utworzyć magazyn kluczy (`tomcat.ks`). Wygeneruj klucz, upewnij się, że nazwa zwykła (CN) lub w pełni kwalifikowana nazwa hosta urządzenia jest adresem IP.

```
keytool -genkey -alias osp -keyalg RSA -storetype pkcs12 -keystore /
opt/certs/tomcat.ks -validity 3650 -keysize 2048 -dname "CN=blr-
osp48-demo.labs.blr.novell.com" -keypass novell -storepass novell
```

6b Uruchom następujące polecenie, aby utworzyć żądanie podpisania certyfikatu. Na przykład `cert.csr`.

```
keytool -certreq -v -alias osp -file /opt/certs/cert.csr -keypass
novell -keystore /opt/certs/tomcat.ks -storepass novell
```

6c Przekaż to żądanie `cert.csr` do programu iManager i pobierz certyfikat serwera `osp.der`. Upewnij się, że jako typ klucza (key type)wybrano Custom, jako opcje użycia klucza (key usage) wybrano data encipherment, key encipherment i digital signature, a pole alternatywnej nazwy podmiotu (subject alternative name) certyfikatu zawiera adres IP lub nazwę hosta serwera OSP. Aby uzyskać więcej informacji, zobacz Tworzenie obiektu certyfikatu serwera.

6d Uruchom następujące polecenie, aby zaimportować certyfikat ośrodka certyfikacji (`SSCert.der`) i certyfikat serwera (`cert.der`) do magazynu kluczy `tomcat.ks`.

```
keytool -import -trustcacerts -alias root -keystore /opt/certs/
tomcat.ks -file /opt/certs/SSCert.der -storepass novell -noprompt
```

```
keytool -import -alias osp -keystore /opt/certs/tomcat.ks -file /
opt/certs/cert.der -storepass novell -noprompt
```

7 Uruchom następujące polecenie w celu załadowania obrazu OSP:

```
docker load --input osp.tar.gz
```

8 Przeprowadź wdrożenie kontenera, używając następującego polecenia:

```
docker run -d --name OSP_Container --network=host -e
SILENT_INSTALL_FILE=/config/silent.properties -v /data:/config
osp:<version>
```

Na przykład:

```
docker run -d --name OSP_Container --network=host -e
SILENT_INSTALL_FILE=/config/silent.properties -v /data:/config
osp:6.3.9
```

Wdrażanie oprogramowania Identity Console jako kontenera Dockera

W tej części opisano procedurę wdrażania oprogramowania Identity Console jako kontenera Dockera:

UWAGA: Parametry konfiguracji, przykładowe wartości oraz przykłady wymienione w tej procedurze służą wyłącznie celom informacyjnym. Pamiętaj, aby nie używać ich bezpośrednio w środowisku produkcyjnym.

---

1 Zaloguj się na stronie SLD: Software License and Download (https://sld.microfocus.com/) i przejdź do strony Software Downloads (Pobieranie oprogramowania).

2 Wybierz następujące opcje:

- Produkt: eDirectory
- Nazwa produktu: eDirectory per User Sub SW E-LTU
- Wersja: 9.2

3 Pobierz plik: `IdentityConsole_<wersja>_Containers_tar.zip`.

4 Obraz należy załadować do lokalnego rejestru Dockera. Wypakuj i załaduj plik `IdentityConsole_<wersja>_Containers.tar.gz` przy użyciu poniższych poleceń:

```
tar -xvf IdentityConsole_<version>_Containers.tar.gz

docker load --input identityconsole.tar.gz
```

5 Utwórz kontener Dockera Identity Console, używając następującego polecenia:

```
docker create --name <identityconsole-container-name> --env
ACCEPT_EULA=Y --network=<network-type> --volume <volume-name>:/config/
identityconsole:<version>
```

Na przykład:

```
docker create --name identityconsole-container --env ACCEPT_EULA=Y --
network=host --volume IDConsole-volume:/config/
identityconsole:1.5.0.0000.
```

UWAGA

- Aby zaakceptować umowę EULA, można ustawić zmienną środowiskową `ACCEPT_EULA` na `Y`. Umowę EULA można też zaakceptować z poziomu monitu ekranowego podczas uruchamiania kontenera, używając opcji `-it` w poleceniu utworzenia Dockera w trybie interaktywnym.
- Parametr `--volume` w powyższym poleceniu spowoduje utworzenie wolumenu służącego do przechowywania danych konfiguracji i dzienników. W tym przypadku utworzyliśmy przykładowy wolumen o nazwie `IDConsole-volume`.

---

6 Skopiuj plik certyfikatu serwera z lokalnego systemu plików do dockera jako `/etc/opt/novell/eDirAPI/cert/keys.pfx`, używając następującego polecenia. Aby uzyskać więcej informacji na temat tworzenia certyfikatu serwera, zobacz „Wymagania wstępne” na stronie 11:

```
docker cp <absolute path of server certificate file> <identityconsole-
container-name>:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

Na przykład:

```
docker cp /home/user/keys.pfx identityconsole-container:/etc/opt/
novell/eDirAPI/cert/keys.pfx
```

W przypadku łączenia się z wieloma drzewami eDirectory należy uzyskać co najmniej jeden certyfikat serwera keys.pfx dla wszystkich połączonych drzew.

7 Skopiuj plik certyfikatu ośrodka certyfikacji (`.pem`) z lokalnego systemu plików do kontenera jako `/etc/opt/novell/eDirAPI/cert/sscert.pem`, używając następującego polecenia. Aby uzyskać więcej informacji na temat uzyskiwania certyfikatu ośrodka certyfikacji, zobacz „Wymagania wstępne” na stronie 11:

```
docker cp <absolute path of CA certificate file> <identityconsole-
container-name>:/etc/opt/novell/eDirAPI/cert/SSCert.pem
```

Na przykład:

```
docker cp /home/user/SSCert.pem identityconsole-container:/etc/opt/
novell/eDirAPI/cert/SSCert.pem
```

Jeśli użytkownik musi połączyć się z wieloma drzewami eDirectory, zapoznaj się z sekcją: „Wiele drzew w przypadku oprogramowania Identity Console jako Dockera” na stronie 26

8 Zmodyfikuj plik konfiguracyjny według potrzeb i skopiuj plik konfiguracyjny (`edirapi.conf`) z lokalnego systemu plików do kontenera jako `/etc/opt/novell/eDirAPI/conf/edirapi.conf`, używając następującego polecenia:

```
docker cp <absolute path of configuration file> <identityconsole-container-name>:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

Na przykład:

```
docker cp /home/user/edirapi.conf identityconsole-container:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

9 Uruchom kontener Dockera, używając następującego polecenia:

```
docker start <identityconsole-container-name>
```

Na przykład:

```
docker start identityconsole-container
```

UWAGA: W katalogu `/var/lib/docker/volumes/<nazwa_wolumenu>/_data/eDirAPI/var/log` znajdziesz następujące pliki dziennika:

- edirapi.log — służy do rejestrowania różnych zdarzeń w edirapi i problemów z debugowaniem.
- edirapi_audit.log — służy do rejestrowania zdarzeń audytu edirapi. Dzienniki są zgodne z formatem audytu CEF.
- container-startup.log — służy do przechwytywania dzienników instalacji kontenera Dockera Identity Console.

Wiele drzew w przypadku oprogramowania Identity Console jako Dockera

Identity Console umożliwia użytkownikowi łączenie się z wieloma drzewami przez uzyskanie indywidualnego certyfikatu ośrodka certyfikacji drzewa.

Na przykład jeśli łączysz się z trzema drzewami eDirectory, musisz skopiować wszystkie trzy certyfikaty ośrodka certyfikacji do kontenera Dockera:

```
docker cp /home/user/SSCert1.pem identityconsole-container:/etc/opt/novell/eDirAPI/cert/SSCert.pem

docker cp /home/user/SSCert2.pem identityconsole-container:/etc/opt/novell/eDirAPI/cert/SSCert1.pem

docker cp /home/user/SSCert3.pem identityconsole-container:/etc/opt/novell/eDirAPI/cert/SSCert2.pem
```

Uruchom następujące polecenia, aby uruchomić ponownie oprogramowanie Identity Console:

```
docker restart <identityconsole-container-name>
```

Wdrażanie oprogramowania Identity Console w wersji autonomicznej

Wdrażanie oprogramowania Identity Console w wersji autonomicznej (bez Dockera)

W tej części opisano procedurę wdrażania oprogramowania Identity Console w wersji autonomicznej:

1. Zaloguj się na stronie SLD: Software License and Download (https://sld.microfocus.com/) i przejdź do strony Software Downloads (Pobieranie oprogramowania).
2. Wybierz następujące opcje:
   - Produkt: eDirectory
   - Nazwa produktu: eDirectory per User Sub SW E-LTU
   - Wersja: 9.2
3. Pobierz najnowszą kompilację Identity Console.
4. Wypakuj pobrany plik do folderu.
5. Otwórz powłokę i przejdź do folderu, do którego została wypakowana kompilacja Identity Console.
6. Po zalogowaniu się jako użytkownik root lub użytkownik z uprawnieniami równoważnymi do użytkownika root uruchom następujące polecenie:

   ```
   ./identityconsole_install
   ```

7. Przeczytaj informacje na stronie Wprowadzenie, a następnie kliknij przycisk **ENTER**.
8. Kliknij opcję `Y`, aby zaakceptować umowę licencyjną. Spowoduje to zainstalowanie wszystkich wymaganych pakietów RPM w systemie.
9. Wprowadź nazwę hosta (w pełni kwalifikowaną nazwę domeny)/adres IP serwera Identity Console.
10. Wprowadź numer portu, który ma nasłuchiwać Identity Console. Wartość domyślna to 9000.
11. Wprowadź opcję integracji usługi OSP z Identity Console lub Identity Console będzie używać logowania LDAP.
12. Jeśli chcesz zintegrować usługę OSP z oprogramowaniem Identity Console:
    1. Wprowadź nazwę domeny/adres IP serwera eDirectory/bezpiecznego magazynu tożsamości z numerem portu LDAPS.

       Na przykład:

       192.168.1.1:636
    2. Wprowadź nazwę użytkownika eDirectory/bezpiecznego magazynu tożsamości.

       Na przykład:

cn=admin,ou=org_unit,o=org

3. Wprowadź hasło eDirectory/bezpiecznego magazynu tożsamości.
4. Ponownie wprowadź hasło eDirectory/bezpiecznego magazynu tożsamości, aby je potwierdzić.
5. Wprowadź nazwę domeny/adres IP serwera OSP z numerem portu SSL serwera SSO.
6. Wprowadź identyfikator klienta OSP.
7. Wprowadź hasło klienta OSP.
8. Wprowadź nazwę drzewa eDirectory/bezpiecznego magazynu tożsamości.

13 Wprowadź ścieżkę zaufanych certyfikatów głównych (`SSCert.pem`) wraz z folderem.

Na przykład:

```
/home/Identity_Console/certs
```

UWAGA: Użytkownik musi się upewnić, że nie tworzy podkatalogu w folderze cert.

14 Wprowadź ścieżkę certyfikatu serwera (`keys.pfx`) wraz z nazwą pliku.

Na przykład:

```
/home/Identity_Console/keys.pfx
```

15 Wprowadź hasło certyfikatu serwera. Aby potwierdzić, że hasło zostało wprowadzone poprawnie, wprowadź ponownie hasło certyfikatu serwera. Rozpoczyna się instalacja.

UWAGA: W katalogu `/var/opt/novell/eDirAPI/log` znajdziesz następujące pliki dziennika:

- edirapi.log — służy do rejestrowania różnych zdarzeń w edirapi i problemów z debugowaniem.
- edirapi_audit.log — służy do rejestrowania zdarzeń audytu edirapi. Dzienniki są zgodne z formatem audytu CEF.
- identityconsole_install.log — służy do przechwytywania dzienników instalacji Identity Console.

Dzienniki rozpoczęcia/zatrzymania przetwarzania Identity Console można znaleźć w pliku `/var/log/messages`.

UWAGA: NetIQ zaleca, aby podczas instalowania oprogramowania Identity Console i usługi eDirectory na tym samym komputerze było dostępne co najmniej jedno wystąpienie usługi eDirectory.

Wiele drzew w przypadku oprogramowania Identity Console w wersji autonomicznej

W przypadku łączenia się z wieloma drzewami eDirectory należy uzyskać indywidualny certyfikat ośrodka certyfikacji drzewa.

Na przykład jeśli łączysz się z trzema drzewami eDirectory, musisz skopiować wszystkie trzy certyfikaty ośrodka certyfikacji do katalogu `etc/opt/novell/eDirAPI/cert/`:

```
cp /home/user/SSCert.pem /etc/opt/novell/eDirAPI/cert/SSCert1.pem

cp /home/user/SSCert.pem /etc/opt/novell/eDirAPI/cert/SSCert2.pem
```

```
cp /home/user/SSCert.pem /etc/opt/novell/eDirAPI/cert/SSCert3.pem
```

Uruchom jedno z następujących poleceń, aby uruchomić ponownie oprogramowanie Identity Console:

```
/usr/bin/identityconsole restart
```

lub

```
systemctl restart netiq-identityconsole.service
```

Identity Console w systemie Windows jako stacja robocza

Oprogramowanie Identity Console można uruchomić w systemie Windows jako stację roboczą, co wymaga uruchomionych usług REST. Dlatego po jego uruchomieniu w wierszu poleceń edirapi.exe uruchamiany jest proces eDirAPI. Jeśli ten terminal edirapi.exe zostanie zamknięty, Identity Console przestanie działać.

Poniższa procedura opisuje sposób uruchamiania Identity Console w systemie Windows.

1. Zaloguj się na stronie SLD: Software License and Download (https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0) i przejdź do strony Software Downloads (Pobieranie oprogramowania).
2. Wybierz następujące opcje:
   - Produkt: eDirectory
   - Nazwa produktu: eDirectory per User Sub SW E-LTU
   - Wersja: 9.2
3. Pobierz plik `IdentityConsole_<wersja>_workstation_win_x86_64.zip`.
4. Wypakuj pobrany plik `IdentityConsole_<version>_workstation_win_x86_64.zip` do folderu.
5. Przejdź do wypakowanego folderu: `IdentityConsole_150_workstation_win_x86_64\eDirAPI\cert` i skopiuj zaufany certyfikat główny ośrodka certyfikacji `SSCert.pem` oraz certyfikat serwera `keys.pfx`.

   Aby pobrać certyfikat, zapoznaj się z częścią: „Wymagania systemowe i wymagania wstępne dotyczące instalacji stacji roboczej” na stronie 18

   Jeśli użytkownik musi połączyć się z wieloma drzewami eDirectory, zapoznaj się z częścią: „Wiele drzew w przypadku oprogramowania Identity Console jako stacji roboczej” na stronie 30

   UWAGA: Certyfikat serwera musi zawsze mieć nazwę `keys.pfx`.

   ---
6. Przejdź do folderu, do którego wypakowano kompilację, i kliknij dwukrotnie plik `run.bat` (plik wsadowy Windows).
7. W wierszu poleceń wprowadź hasło certyfikatu serwera `(keys.pfx)`.

   Zostanie uruchomiony terminal procesu eDirAPI (edirapi.exe) i pojawi się strona logowania do Identity Console.

UWAGA:

- Jeśli terminal procesu `eDirAPI` (edirapi.exe) jest już uruchomiony, uruchom plik `identityconsole.exe` z folderu, do którego wypakowano kompilację.
- Użytkownicy znajdą następujące dzienniki w katalogu:`\IdentityConsole_150_workstation_win_x86_64\eDirAPI\log`

  `edirapi.log` — służy do rejestrowania różnych zdarzeń w `edirapi` i problemów z debugowaniem.

  `edirapi_audit.log` — służy do rejestrowania zdarzeń audytu `edirapi`. Dzienniki są zgodne z formatem audytu CEF.
- Logowanie oparte na usłudze OSP nie jest obsługiwane w trybie stacji roboczej.
- Stacja robocza Identity Console nasłuchuje tylko `port 9000`. Nie modyfikuj pliku `edirapi_win.conf`.

Wiele drzew w przypadku oprogramowania Identity Console jako stacji roboczej

Identity Console umożliwia użytkownikowi łączenie się z wieloma drzewami przez uzyskanie indywidualnego certyfikatu ośrodka certyfikacji drzewa.

1. Zamknij stację roboczą Identity Console i terminal eDirAPI.
2. Skopiuj certyfikaty ośrodka certyfikacji `SSCert.pem` do lokalizacji: `IdentityConsole_150_workstation_win_x86_64\eDirAPI\cert.`

   Na przykład jeśli chcesz połączyć się z trzema drzewami eDirectory, skopiuj certyfikaty ośrodka certyfikacji odpowiednio jako `SSCert1.pem`, `SSCert2.pem` i `SSCert3.pem`.
3. Przejdź do folderu, do którego wypakowano kompilację, i kliknij dwukrotnie plik `run.bat` (plik wsadowy Windows).
4. Wprowadź hasło `keys.pfx` w wierszu polecenia i zaloguj się do żądanego drzewa eDirectory.

Zatrzymywanie i ponowne uruchamianie oprogramowania Identity Console

- „Zatrzymywanie i ponowne uruchamianie oprogramowania Identity Console jako kontenera Dockera” na stronie 30
- „Zatrzymywanie i ponowne uruchamianie autonomicznej wersji oprogramowania Identity Console” na stronie 31
- „Zamykanie i ponowne uruchamianie stacji roboczej Identity Console” na stronie 31

Zatrzymywanie i ponowne uruchamianie oprogramowania Identity Console jako kontenera Dockera

Aby zatrzymać oprogramowanie Identity Console, uruchom następujące polecenie:

`docker stop <identityconsole-container-name>`

Aby ponownie uruchomić oprogramowanie Identity Console, uruchom następujące polecenie:

```
docker restart <identityconsole-container-name>
```

Aby uruchomić oprogramowanie Identity Console, uruchom następujące polecenie:

```
docker start <identityconsole-container-name>
```

Zatrzymywanie i ponowne uruchamianie autonomicznej wersji oprogramowania Identity Console

Aby zatrzymać oprogramowanie Identity Console, uruchom jedno z następujących poleceń:

```
/usr/bin/identityconsole stop
```

lub

```
systemctl stop netiq-identityconsole.service
```

Aby ponownie uruchomić Identity Console, uruchom jedno z następujących poleceń:

```
/usr/bin/identityconsole restart
```

lub

```
systemctl restart netiq-identityconsole.service
```

Aby uruchomić Identity Console, uruchom jedno z następujących poleceń:

```
/usr/bin/identityconsole start
```

lub

```
systemctl start netiq-identityconsole.service
```

Zamykanie i ponowne uruchamianie stacji roboczej Identity Console

Aby zamknąć aplikację i proces, postępuj zgodnie z następującą procedurą:

1. Zamknij aplikację komputerową Identity Console dla systemu Windows.
2. Zatrzymaj proces eDirAPI, zamykając terminal procesu `eDirAPI`.

Aby ponownie uruchomić stację roboczą Identity Console, przejdź do folderu, do którego wypakowano kompilację, i kliknij dwukrotnie plik `run.bat` (plik wsadowy Windows).

UWAGA: Jeśli terminal procesu `eDirAPI` jest już uruchomiony, uruchom plik `identityconsole.exe` z folderu, do którego wypakowano kompilację, aby ponownie uruchomić stację roboczą Identity Console.

Zarządzanie trwałością danych

Wraz z kontenerami Identity Console są też tworzone wolumeny do obsługi trwałości danych. Aby użyć parametrów konfiguracyjnych starego kontenera przy użyciu woluminów, wykonaj następujące czynności:

1. Zatrzymaj bieżący kontener Dockera, używając następującego polecenia:

   ```
   docker stop identityconsole-container
   ```

2. Utwórz drugi kontener, używając danych aplikacji starego kontenera przechowywanych na wolumenie Dockera (`edirapi-volume-1`):

   ```
   docker create --name identityconsole-container-2 --network=host --
   volume edirapi-volume-1:/config/ identityconsole:1.0.0
   ```

3. Uruchom drugi kontener, używając następującego polecenia:

   ```
   docker start identityconsole-container-2
   ```

4. (Opcjonalnie) Pierwszy kontener można teraz usunąć, używając następującego polecenia:

   ```
   docker rm identityconsole-container
   ```

Wdrażanie oprogramowania Identity Console w usłudze Azure Kubernetes Services

Azure Kubernetes Service (AKS) to zarządzana usługa Kubernetes, która umożliwia wdrażanie klastrów i zarządzanie nimi. W tej części omówiono następujące procedury:

Wdrażanie oprogramowania Identity Console w klastrze usługi AKS

W tej części opisano następujące procedury wdrażania oprogramowania Identity Console w klastrze usługi AKS:

- „Tworzenie rejestru Azure Container Registry (ACR)” na stronie 33
- „Ustawianie klastra Kubernetes” na stronie 34
- „Tworzenie standardowego publicznego adresu IP jednostki SKU” na stronie 34
- „Konfigurowanie usługi Cloud Shell i nawiązywanie połączenia z klastrem Kubernetes” na stronie 34
- „Wdrażanie aplikacji” na stronie 35

Tworzenie rejestru Azure Container Registry (ACR)

Azure Container Registry (ACR) to oparty na platformie Azure prywatny rejestr dla obrazów kontenerów Dockera.

Aby uzyskać więcej informacji, zobacz Tworzenie rejestru kontenerów platformy Azure przy użyciu Azure Portal w sekcji Tworzenie rejestru kontenerów — portal lub wykonaj następujące czynności w celu utworzenia rejestru Azure Container Registry (ACR):

1. Zaloguj się do portalu Azure.
2. Wybierz kolejno opcje **Utwórz zasób** > **Kontenery** > **Container Registry**.
3. Na karcie **Podstawy** podaj wartości w polach **Grupa zasobów** i **Nazwa rejestru**. Nazwa rejestru musi być unikatowa w obrębie platformy Azure i może zawierać od 5 do 50 znaków alfanumerycznych.

   Zaakceptuj wartości domyślne pozostałych ustawień.
4. Następnie wybierz pozycję **Przejrzyj i utwórz**.
5. Kliknij przycisk **Utwórz**.
6. Zaloguj się w interfejsie wiersza polecenia platformy Azure i uruchom następujące polecenie w celu zalogowania się do Azure Container Registry.

   ```
   az acr login --name registryname
   ```

   Na przykład:

   ```
   az acr login --name < idconsole >
   ```
7. Pobierz serwer logowania Azure Container Registry za pomocą polecenia:

   ```
   az acr show --name registryname --query loginServer --output table
   ```

   Na przykład:

   ```
   az acr show --name < idconsole > --query loginServer --output table
   ```
8. Oznacz lokalny obraz Identity Console nazwą serwera logowania ACR (registryname.azureacr.io), używając następującego polecenia:

   ```
   docker tag idconsole-image <login server>/idconsole-image
   ```

   Na przykład:

   ```
   docker tag identityconsole:<version> registryname.azurecr.io/
   identityconsole:<version>
   ```
9. Wypchnij oznaczony obraz do rejestru.

   ```
   docker push <login server>/idconsole: <version>
   ```

   Na przykład:

   ```
   docker push registryname.azurecr.io/identityconsole:<version>
   ```
10. Pobierz listę obrazów w rejestrze za pomocą polecenia:

    ```
    az acr show --name registryname --query loginServer --output table
    ```

Ustawianie klastra Kubernetes

Utwórz zasób usługi Kubernetes za pomocą portalu Azure lub interfejsu wiersza polecenia.

Aby uzyskać bardziej szczegółowe kroki tworzenia zasobu usługi Kubernetes na platformie Azure z węzłem, zobacz Tworzenie klastra AKS w przewodniku Szybki start dla platformy Azure.

UWAGA:

- Upewnij się, że jako sieć wybierasz Azure CNI.
- Wybierz istniejącą sieć wirtualną (w której w podsieci jest wdrożony serwer eDirectory).
- Wybierz istniejący rejestr kontenerów, w którym dostępny jest obraz Identity Console.

Tworzenie standardowego publicznego adresu IP jednostki SKU

Zasób publicznego adresu IP w grupie zasobów klastra Kubernetes działa jako adres IP modułu równoważenia obciążenia dla aplikacji.

Aby uzyskać szczegółowe kroki, zobacz Tworzenie publicznego adresu IP przy użyciu Azure Portal w sekcji Tworzenie publicznego adresu IP — portal.

Konfigurowanie usługi Cloud Shell i nawiązywanie połączenia z klastrem Kubernetes

Do wszystkich operacji korzystaj z usługi Cloud Shell, która jest dostępna w portalu Azure.

Aby skonfigurować usługę Cloud Shell w portalu Azure, zobacz Uruchamianie usługi Cloud Shell w sekcji Bash — Szybki start, lub wykonaj następujące czynności w celu skonfigurowania usługi Cloud Shell i nawiązania połączenia z klastrem Kubernetes:

1. W portalu Azure kliknij przycisk  , aby otworzyć Cloud Shell.

   UWAGA: Aby zarządzać klastrem Kubernetes, użyj klienta wiersza poleceń Kubernetes `kubectl`. Jeśli korzystasz z Azure Cloud Shell, kubectl jest już zainstalowany.

   ---

2. Skonfiguruj kubectl do łączenia się z klastrem Kubernetes, używając następującego polecenia:

   ```
   az aks get-credentials --resource-group "resource group name" --name
   "Kubernetes cluster name"
   ```

   Na przykład:

   ```
   az aks get-credentials --resource-group myResourceGroup --name
   myAKSCluster
   ```

3. Sprawdź listę węzłów klastra za pomocą polecenia:

   ```
   kubectl get nodes
   ```

Wdrażanie aplikacji

Do wdrożenia Identity Console możesz użyć przykładowych plików `idc-services.yaml`, `idc-statefulset.yaml`, `idc-storageclass.yaml` i `idc-pvc.yaml`.

Możesz także tworzyć własne pliki yaml zgodnie z wymaganiami.

1. Utwórz zasób klasy pamięci masowej, używając poniższego polecenia:

   ```
   kubectl apply -f <location of the YAML file>
   ```

   Na przykład:

   ```
   kubectl apply -f idc-storageclass.yaml
   ```

   (Opcjonalnie) Aby uzyskać więcej informacji na temat dynamicznego tworzenia i używania trwałego wolumenu przy użyciu udziału Azure Files, zobacz Dynamiczne tworzenie i korzystanie z trwałego woluminu za pomocą usługi Azure Files w usłudze Azure Kubernetes Service (AKS)

   Przykładowy plik zasobów klasy pamięci masowej przedstawiono poniżej:

   ```
   kind: StorageClass
   apiVersion: storage.k8s.io/v1
   metadata:
     name: azurefilesc
   provisioner: kubernetes.io/azure-file
   mountOptions:
     - dir_mode=0777
     - file_mode=0777
     - uid=0
     - gid=0
     - mfsymlinks
     - cache=strict
     - actimeo=30
   parameters:
     skuName: Standard_LRS
     shareName: fileshare
   ~
   ```

   Zasób klasy pamięci masowej umożliwia dynamiczne zaopatrywanie pamięci masowej. Definiuje on sposób tworzenia udziału Azure Files.

2. Szczegóły klasy pamięci masowej możesz wyświetlić, używając poniższego polecenia:

   ```
   kubectl get sc
   ```

3. Utwórz zasób PVC, używając pliku `idc-pvc.yaml`:

   ```
   kubectl apply -f <location of the YAML file>
   ```

   Na przykład:

   ```
   kubectl apply -f idc.pvc.yaml
   ```

   Przykładowy plik zasobu PVC przedstawiono poniżej:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvcforsc
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: azurefilesc
  resources:
    requests:
      storage: 5Gi
```

Zasób PVC tworzy udział pliku. PVC (persistent volume claim) używa obiektu klasy pamięci masowej do dynamicznego zaopatrywania udziału plików platformy Azure.

4. Przekaż plik edirapi.conf, certyfikat ośrodka certyfikacji i certyfikat serwera do Cloud Shell.

   Kliknij ikonę przycisku **Przekaż/Pobierz pliki**  w Cloud Shell i przekaż pliki `edirapi.conf`, `SSCert.pem` oraz `keys.pfx`.

UWAGA: Plik edirapi.conf ma parametr „origin”. W tym miejscu należy podać adres IP, za pomocą którego będzie uzyskiwany dostęp do aplikacji Identity Console. (Użyj adresu IP utworzonego w części „Tworzenie standardowego publicznego adresu IP jednostki SKU” na stronie 34).

Wdrożenie Identity Console wymaga certyfikatu serwera (`keys.pfx`).

Podczas tworzenia certyfikatu serwera upewnij się, że w polu Alternatywna nazwa podmiotu została podana poprawna nazwa DNS.

Kroki tworzenia prawidłowej nazwy DNS:

Typowy zasobnik wdrożony przy użyciu obiektu StatefulSet ma nazwę DNS jak poniżej — {nazwa_zestawu_stanowego}-{liczba_porządkowa}.{nazwa_usługi}.{przestrzeń_nazw}.svc.cluster.local

- Jeśli nazwa StatefulSet w pliku idconsole-statefulset.yaml to idconsole-app, wówczas nazwa_zestawu_stanowego = idconsole-app
- Jeśli jest to pierwszy zasobnik, to liczba_porządkowa = 0
- Jeśli jako nazwa_usługi w pliku idconsole -statefulset.yaml zdefiniujesz idconsole, to nazwa_usługi = idconsole
- Jeśli jest to domyślna przestrzeń nazw, to przestrzeń_nazw = default

Wynik: idconsole-app-0.idcosole.default.svc.cluster.local

---

5. Utwórz zasób configmap w klastrze Kubernetes, który przechowuje pliki konfiguracyjne wraz z certyfikatami.

   Przed uruchomieniem polecenia upewnij się, że pliki (`edirapi.conf`, `SSCert.pem` i `keys.pfx`) znajdują się w katalogu.

   ```
   kubectl create configmap <confgimapName> --from-file= "path where the files are present"
   ```

   Na przykład:

   ```
   kubectl create configmap config-data --from-file=/data
   ```

6. Wyświetl szczegóły obiektu configmap, używając polecenia kubectl describe:

   ```
   kubectl describe configmap <configmapName>
   ```

   Na przykład:

   ```
   kubectl describe configmap confg-data
   ```

7. Utwórz zasób StatefulSet w celu wdrożenia kontenera.

   Uruchom następujące polecenie w celu wdrożenia kontenera:

   ```
   kubectl apply -f <location of the YAML file>
   ```

   Na przykład:

   ```
   kubectl apply -f idc-statefulset.yaml
   ```

   Przykładowy plik zasobu StatefulSet przedstawiono poniżej:

   ```
   apiVersion: apps/v1
   kind: StatefulSet
   metadata:
     name: idconsole-app
   spec:
     serviceName: idconsole
     selector:
       matchLabels:
         app: idconsole
     replicas: 1
     template:
       metadata:
         labels:
           app: idconsole
       spec:
         containers:
         - name: idconsole-container
           image: registryname.azurecr.io/identityconsole:<version>
           env:
           - name: ACCEPT_EULA
             value: "Y"
           ports:
           - containerPort: 9000
           volumeMounts:
             - name: configfiles
               mountPath: /config/data
             - name: datapersistenceandlog
               mountPath: /config
               subPath: log
         volumes:
           - name: configfiles
             configMap:
               name: config-data
           - name: datapersistenceandlog
             persistentVolumeClaim:
               claimName: pvcforsc
   ```

8. Uruchom następujące polecenie, aby sprawdzić stan wdrożonego zasobnika:

```
kubectl get pods -o wide
```

9. Utwórz zasób usługi typu loadBalancer.

   Typ usługi określony w pliku yaml to loadBalancer.

   Utwórz zasób usługi, używając następującego polecenia:

   ```
   kubectl apply -f <location of the YAML file>
   ```

   Na przykład:

   ```
   kubectl apply -f ids-service.yaml
   ```

   Przykładowy plik zasobu usługi przedstawiono poniżej:

   ```
   apiVersion: v1
   kind: Service
   metadata:
     name: idconsole-service
     labels:
       run: idconsole-service
   spec:
     type: LoadBalancer
     loadBalancerIP: xx.xx.xx.xx
     selector:
       app: idconsole
     ports:
      - port: 9000
        targetPort: 9000
        protocol: TCP
   ```

   Sprawdź adres ZEWNĘTRZNY-IP (lub adres IP modułu równoważenia obciążenia), używając następującego polecenia:

   ```
   kubectl get svc -o wide
   ```

10. Uruchom adres URL, używając adresu ZEWNĘTRZNY-IP (lub adresu IP modułu równoważenia obciążenia).

    Na przykład:

    https://<ZEWNĘTRZNY-IP>:9000/identityconsole

Modyfikowanie certyfikatu serwera

W tych częściach przedstawiono informacje dotyczące modyfikowania certyfikatu serwera w kontenerze Dockera oraz autonomicznej wersji oprogramowania Identity Console.

- „Modyfikowanie certyfikatu serwera w kontenerze Dockera” na stronie 39
- „Modyfikowanie certyfikatu serwera w autonomicznej wersji oprogramowania Identity Console” na stronie 39

Modyfikowanie certyfikatu serwera w kontenerze Dockera

Aby zmodyfikować certyfikat serwera w kontenerze Dockera, wykonaj następujące czynności:

1. Uruchom następujące polecenie, aby skopiować nowy certyfikat serwera w dowolnej lokalizacji kontenera.

   Na przykład:

   ```
   docker cp /path/to/new-keys.pfx <container_id/name>:/tmp/new-keys.pfx
   ```

2. Zaloguj się do kontenera, używając następującego polecenia:

   ```
   docker exec -it <container_name> bash
   ```

3. Uruchom narzędzie NLPCERT, aby zapisać klucze jako pseudoużytkownik:

   ```
   LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/lib64/:/opt/
   netiq/common/openssl/lib64/ /opt/novell/eDirAPI/sbin/nlpcert -i /tmp/
   new-keys.pfx -o /etc/opt/novell/eDirAPI/conf/ssl/private/cert.pem
   ```

4. Zakończ pracę konsoli kontenera za pomocą polecenia:

   ```
   exit
   ```

5. Uruchom ponownie kontener, wprowadzając:

   ```
   docker restart <container name>
   ```

Modyfikowanie certyfikatu serwera w autonomicznej wersji oprogramowania Identity Console

Aby zmodyfikować certyfikat serwera w autonomicznej wersji oprogramowania Identity Console, wykonaj następujące czynności:

1. Uruchom narzędzie NLPCERT, aby zapisać klucze:

   ```
   su - nds -c "LD_LIBRARY_PATH=/opt/novell/lib64/:/opt/novell/eDirectory/
   lib64/:/opt/netiq/common/openssl/lib64/ /opt/novell/eDirAPI/sbin/
   nlpcert -i /Expiredcert/noexpire/new-keys.pfx -o /etc/opt/novell/
   eDirAPI/conf/ssl/private/cert.pem"
   ```

2. Uruchom ponownie oprogramowanie Identity Console:

   ```
   systemctl restart netiq-identityconsole.service
   ```

3 Uaktualnianie oprogramowania Identity Console

W tym rozdziale opisano proces uaktualniania oprogramowania Identity Console do najnowszych wersji. Aby przygotować się do uaktualniania, należy zapoznać się z wymaganiami wstępnymi i wymaganiami systemowymi (zob. Rozdział 1, „Planowanie instalacji oprogramowania Identity Console”, na stronie 11).

W tej części omówiono następujące procedury:

Uaktualnianie oprogramowania Identity Console jako kontenera Dockera

Gdy pojawi się nowa wersja obrazu Identity Console, administrator może wykonać procedurę uaktualniania w celu wdrożenia kontenera z najnowszą wersją oprogramowania Identity Console. Przed wykonaniem uaktualnienia należy trwale zachować wszystkie niezbędne dane związane z aplikacją na wolumenach Dockera. Aby uaktualnić oprogramowanie Identity Console przy użyciu kontenera Dockera, wykonaj następujące czynności:

1. Pobierz i załaduj najnowszą wersję obrazu Dockera ze strony Software License and Download (https://sld.microfocus.com/) i wykonaj czynności z części „Wdrażanie oprogramowania Identity Console” na stronie 21 w celu zainstalowania najnowszej wersji oprogramowania Identity Console.
2. Po załadowania najnowszego obrazu Dockera zatrzymaj bieżący kontener Dockera, używając następującego polecenia:

   ```
   docker stop identityconsole-container
   ```

3. (Opcjonalnie) Wykonaj kopię zapasową wolumenu współużytkowanego.
4. Usuń istniejący kontener Identity Console, uruchamiając następujące polecenie:

   ```
   docker rm <container name>
   ```

   Na przykład:

   ```
   docker rm identityconsole-container
   ```

5. (Opcjonalnie) Usuń starszy obraz Dockera Identity Console, uruchamiając następujące polecenie:

   ```
   docker rmi identityconsole
   ```

6 Utwórz kontener Dockera Identity Console, używając następującego polecenia:

```
docker create --name <identityconsole-container-name> --env
ACCEPT_EULA=Y --network=<network-type> --volume <volume-name>:/config/
identityconsole:<version>
```

Na przykład:

```
docker create --name identityconsole-container --env ACCEPT_EULA=Y --
network=host --volume IDConsole-volume:/config/
identityconsole:1.5.0.0000
```

UWAGA

- Aby zaakceptować umowę EULA, można ustawić zmienną środowiskową `ACCEPT_EULA` na `Y`. Umowę EULA można też zaakceptować z poziomu monitu ekranowego podczas uruchamiania kontenera, używając opcji `-it` w poleceniu utworzenia Dockera w trybie interaktywnym.
- Parametr `--volume` w powyższym poleceniu spowoduje utworzenie wolumenu służącego do przechowywania danych konfiguracji i dzienników. W tym przypadku utworzyliśmy przykładowy wolumen o nazwie `IDConsole-volume`.

7 Skopiuj plik certyfikatu serwera z lokalnego systemu plików do nowo utworzonego kontenera jako `/etc/opt/novell/eDirAPI/cert/keys.pfx`, używając następującego polecenia:

```
docker cp <absolute path of server certificate file> identityconsole-
container:/etc/opt/novell/eDirAPI/cert/keys.pfx
```

Na przykład:

```
docker cp /home/user/keys.pfx identityconsole-container:/etc/opt/
novell/eDirAPI/cert/keys.pfx
```

W przypadku połączenia się z wieloma drzewami eDirectory należy skopiować co najmniej jeden certyfikat serwera keys.pfx dla wszystkich połączonych drzew.

8 Skopiuj plik certyfikatu ośrodka certyfikacji (`.pem`) z lokalnego systemu plików do nowo utworzonego kontenera jako `/etc/opt/novell/eDirAPI/cert/sscert.pem`, używając następującego polecenia:

```
docker cp <absolute path of CA certificate file> identityconsole-
container:/etc/opt/novell/eDirAPI/cert/SScert.pem
```

Na przykład:

```
docker cp /home/user/SSCert.pem identityconsole-container:/etc/opt/
novell/eDirAPI/cert/SSCert.pem
```

W przypadku łączenia się z wieloma drzewami eDirectory należy uzyskać indywidualny certyfikat ośrodka certyfikacji drzewa dla wszystkich połączonych drzew. Na przykład jeśli łączysz się z trzema drzewami eDirectory, musisz skopiować wszystkie trzy certyfikaty ośrodka certyfikacji do kontenera Dockera:

```
docker cp /home/user/SSCert.pem identityconsole-container:/etc/opt/
novell/eDirAPI/cert/SSCert.pem
docker cp /home/user/SSCert1.pem identityconsole-container:/etc/opt/
novell/eDirAPI/cert/SSCert1.pem
docker cp /home/user/SSCert2.pem identityconsole-container:/etc/opt/
novell/eDirAPI/cert/SSCert2.pem
```

UWAGA: Od wersji Identity Console 1.4 wzwyż plik konfiguracyjny edirapi.conf) nie zawiera jawnie parametrów „*ldapuser*”,„*ldappassword*” ani „*ldapserver*”. Wartość parametru „*bcert*” musi zawierać ścieżkę katalogu z zaufanymi certyfikatami głównymi. Na przykład: bcert = "/etc/opt/novell/eDirAPI/cert/". Parametr „*origin*” jest niezależny od parametru „*check-origin*” i jest obowiązkowy w przypadku używania konfiguracji DNS.

---

9 Skopiuj plik konfiguracyjny (`edirapi.conf`) z lokalnego systemu plików do nowo utworzonego kontenera jako `/etc/opt/novell/eDirAPI/conf/edirapi.conf`, używając następującego polecenia:

```
docker cp <absolute path of configuration file> identityconsole-
container:/etc/opt/novell/eDirAPI/conf/edirapi.conf
```

Na przykład:

```
docker cp /home/user/edirapi.conf identityconsole-container:/etc/opt/
novell/eDirAPI/conf/edirapi.conf
```

10 Uruchom drugi kontener, używając następującego polecenia:

```
docker start identityconsole-container
```

11 Aby sprawdzić stan uruchomionego kontenera, uruchom następujące polecenie:

```
docker ps -a
```

Uaktualnianie oprogramowania Identity Console w wersji autonomicznej (bez Dockera)

W tej części opisano procedurę uaktualniania oprogramowania Identity Console w wersji autonomicznej:

1 Pobierz plik `IdentityConsole_<wersja>_Containers.tar.gz` ze strony Software License and Download (https://sld.microfocus.com/).

2 Zaloguj się do SLD, przejdź do strony Software Download SLD i kliknij opcję **Pobierz**.

3 Wybierz Produkt: **eDirectory** > Nazwa produktu: **eDirectory per User Sub SW E-LTU** > Wersja: **9.2**

4 Pobierz najnowszą kompilację Identity Console.

5 Wypakuj pobrany plik przy użyciu następującego polecenia:

```
tar -zxvf IdentityConsole_<version>_Linux.tar.gz
```

6 Przejdź do folderu, do którego została wypakowana kompilacja Identity Console.

7 Skopiuj do folderu wszystkie zaufane certyfikaty główne drzew eDirectory, z którymi chcesz się połączyć. Aby skopiować zaufany certyfikat główny do folderu, uruchom następujące polecenie:

```
cp /var/opt/novell/eDirectory/data/SSCert.pem <folder path>
```

Na przykład:

```
cp /var/opt/novell/eDirectory/data/SSCert.pem /home/Identity_Console/
certs
```

8 Uruchom następujące polecenie:

```
./identityconsole_install
```

9 Określ ścieżkę folderu zaufanych certyfikatów głównych używaną w **kroku 4**.

10 Oprogramowanie Identity Console zostało pomyślnie uaktualnione.

Uaktualnianie kontenera OSP

Wykonaj następujące czynności, aby uaktualnić kontener OSP:

1 Pobierz i załaduj najnowszą wersję obrazu OSP ze strony Software License and Download (https://sld.microfocus.com/).

Na przykład:

```
docker load --input osp.tar.gz
```

2 Po załadowaniu najnowszego obrazu OSP zatrzymaj bieżący kontener OSP, używając następującego polecenia:

```
docker stop <OSP container name>
```

3 (Opcjonalnie) Wykonaj kopię zapasową wolumenu współużytkowanego.

4 Usuń istniejący kontener OSP, uruchamiając następujące polecenie:

```
docker rm <OSP container name>
```

Na przykład:

```
docker rm OSP_Container
```

5 Przejdź do katalogu zawierającego magazyn kluczy (`tomcat.ks`) oraz plik właściwości instalacji w trybie bez sygnalizacji (`tomcat.ks`) i zachowaj istniejący folder OSP. Wygeneruj nowy magazyn kluczy (`tomcat.ks`) o rozmiarze klucza 2048. Aby dowiedzieć się więcej, zobacz **krok 4** w części Wdrażanie kontenera OSP Podręcznika instalacji Identity Console.

6 Przeprowadź wdrożenie kontenera, używając następującego polecenia:

```
docker run -d --name OSP_Container --network=host -e
SILENT_INSTALL_FILE=/config/silent.properties -v /data:/config
osp:<version>
```

Na przykład:

```
docker run -d --name OSP_Container --network=host -e
SILENT_INSTALL_FILE=/config/silent.properties -v /data:/config
osp:6.5.3
```

4 Odinstalowywanie oprogramowania Identity Console

W tym rozdziale opisano proces deinstalacji oprogramowania Identity Console:

- „Procedura deinstalacji dla środowiska Dockera” na stronie 45
- „Procedura deinstalacji dla oprogramowania Identity Console w wersji autonomicznej (bez Dockera)” na stronie 45

Procedura deinstalacji dla środowiska Dockera

Aby odinstalować kontener Dockera Identity Console, wykonaj następujące czynności:

1. Zatrzymaj kontener Identity Console:

   ```
   docker stop <container-name>
   ```

2. Uruchom następujące polecenie w celu usunięcia kontenera Dockera Identity Console:

   ```
   docker rm -f <container_name>
   ```

3. Uruchom następujące polecenie w celu usunięcia obrazu Dockera:

   ```
   docker rmi -f <docker_image_id>
   ```

4. Usuń wolumen Dockera:

   ```
   docker volume rm <docker-volume>
   ```

UWAGA: Jeśli usuniesz wolumen, dane zostaną też usunięte z serwera.

Procedura deinstalacji dla oprogramowania Identity Console w wersji autonomicznej (bez Dockera)

Aby odinstalować autonomiczną wersję Identity Console, wykonaj następujące czynności:

1. Przejdź do katalogu `/usr/bin` na komputerze, na którym jest zainstalowane oprogramowanie Identity Console.
2. Uruchom następujące polecenie:

   ```
   ./identityconsoleUninstall
   ```

3. Oprogramowanie Identity Console zostało pomyślnie odinstalowane.

UWAGA: Gdy na komputerze jest zainstalowany eDirectory lub inny produkt NetIQ, użytkownik musi ręcznie odinstalować pliki *nici* i *openssl*.