



Identity Console

Telepítési útmutató

2022. szeptember

Jogi közlemény

A jogi megjegyzésekkel, védjegyekkel, jogi nyilatkozatokkal, garanciákkal, szabadalmakra vonatkozó szabályokkal, FIPS-kompatibilitással, exportálási és egyéb felhasználási korlátozásokkal, illetve az USA kormányát megillető jogokkal kapcsolatban lásd: <https://www.netiq.com/company/legal>.

Copyright © 2022 NetIQ Corporation. Minden jog fenntartva.

Tartalom

A könyv és a könyvtár rövid bemutatása	5
A NetIQ vállalatról	7
1 Az Identity Console telepítésének tervezése	11
A Docker telepítésének rendszerkövetelményei és előfeltételei	11
Rendszerekövetelmények	11
Előfeltételek	11
A környezet beállítása	13
Különálló telepítés (nem Docker) rendszerkövetelményei és előfeltételei	16
Rendszerekövetelmények	16
(Választható) Az OSP-konfiguráció előfeltételei	17
A munkaállomás rendszerkövetelményei és előfeltételei	18
Rendszerekövetelmények	18
RPM-aláírás ellenőrzése	19
2 Az Identity Console telepítése	21
Biztonsági javaslatok	21
Az Identity Console telepítése Docker-konténerként	22
Az OSP-konténer telepítése	22
Az Identity Console telepítése Docker-konténerként	24
Több fa csatlakoztatása az Identity Console-ban (Docker)	26
Különálló Identity Console telepítése	26
Különálló Identity Console (nem Docker) telepítése	27
Több fa csatlakoztatása különálló Identity Console-lal	28
Identity Console Windows rendszeren munkaállomásként	29
Több fa csatlakoztatása az Identity Console-ban (munkaállomás)	30
Az Identity Console leállítása és újraindítása	30
Az Identity Console leállítása és újraindítása Docker-konténerként	30
A különálló Identity Console leállítása és újraindítása	30
Az Identity Console-munkaállomás bezárása és újraindítása	31
Adatmegőrzés kezelése	31
Az Identity Console telepítése Azure Kubernetes-szolgáltatásokban	32
Identity Console telepítése AKS-fürtben	32
Kiszolgálói tanúsítvány módosítása	38
Docker-konténerben lévő kiszolgálói tanúsítvány módosítása	38
Kiszolgálói tanúsítvány módosítása a különálló Identity Console-ban	39
3 Az Identity Console frissítése	41
Az Identity Console frissítése Docker-konténerként	41
Különálló Identity Console frissítése (nem Docker)	43
Az OSP-konténer frissítése	44

4 Az Identity Console eltávolítása	45
Eltávolítási eljárás Docker-környezethez	45
A különálló Identity Console (nem Docker) eltávolítási eljárása	45

A könyv és a könyvtár rövid bemutatása

A *Telepítési útmutató* a NetIQ Identity Console (Identity Console) termék telepítésével és kezelésével kapcsolatos információkat tartalmaz. A könyv terminológiai meghatározásokat és megvalósítási forgatókönyveket tartalmaz.

Kiknek készült az útmutató?

A jelen útmutató hálózati rendszergazdák számára készült.

A könyvtárban megtalálható egyéb információk

A könyvtárban az alábbi információforrások találhatók meg:

Telepítési útmutató

Az Identity Console telepítését és frissítését ismerteti. A könyv hálózati rendszergazdák számára készült.

A NetIQ vállalatról

Globális jelenlétű szoftverfejlesztő vállalatunk főként a számítógépes munkakörnyezetekre leginkább jellemző három területen – a változás, az összetettség és a kockázat terén – felmerülő feladatok kezelésére kínál megoldásokat.

Vállalatunk nézőpontja

A változáshoz való alkalmazkodás, az összetettség és a kockázatok kezelése nem új feladat

Mégpedig annyira nem újak, hogy talán ezek a változók jelentik a legnagyobb akadályt a fizikai, a virtuális és a felhőalapú számítógépes környezetek biztonságos felmérésének, figyelésének és kezelésének szabályozhatósága terén.

A létfontosságú vállalati szolgáltatások hatékonyabb és gyorsabb üzemeltetése

Meggyőződésünk, hogy minden informatikai szervezetnek a lehető legnagyobb mértékű szabályozhatóságra van szüksége ahhoz, hogy időszerűen és költséghatékonyan tudja biztosítani szolgáltatásait. Ahogy a szervezet változik és a kezelésére felhasznált technológiák ezzel párhuzamosan szükségszerűen egyre összetettebbek lesznek, a szervezetre egyre nagyobb nyomást gyakorolnak az olyan állandó feladatok, mint a változás és az összetettség kezelése.

Vállalatunk filozófiája

Amit nyújtunk, nem csupán szoftver – intelligens megoldás

Annak érdekében, hogy megbízható szabályozási megoldást nyújthassunk, első lépésként arra törekszünk, hogy megismerjük azokat a valós helyzeteket, amelyekben az Önéhez hasonló informatikai szervezetek működnek nap mint nap. Ez az egyetlen módja annak, hogy olyan gyakorlatban alkalmazható, intelligens informatikai megoldásokat fejleszthessünk ki, amelyek igazolt és mérhető eredményeket biztosítanak. Ez pedig jóval lényegesebb számunkra, mint hogy csupán szoftvereket adjunk el.

A mi küldetésünk az Ön sikerének elősegítése

Törekvéseink középpontjában mindenekelőtt az Ön sikere áll. Termékeink kialakításától kezdve a telepítésükig folyamatosan szem előtt tartjuk, hogy olyan informatikai megoldásokra van szüksége, amelyek jól működnek és zökkenőmentesen integrálhatók a meglévő eszközeivel, hogy a telepítést követően is igényt tart a folyamatos támogatásra és képzésre, valamint hogy olyan partnerre van szüksége, akivel valóban könnyű együtt dolgozni. A lényeg mindebben, hogy az Ön sikere a mi sikerünk is.

Megoldásaink

- ♦ Azonosság- és hozzáférés-szabályozás
- ♦ Hozzáférés-kezelés

- ♦ Biztonságkezelés
- ♦ Rendszer- és alkalmazáskezelés
- ♦ Terheléskezelés
- ♦ Szolgáltatáskezelés

Értékesítési ügyfélszolgálatunk elérhetőségei

A termékekkel, árakkal és szoftverfunkciókkal kapcsolatos kérdéseivel forduljon helyi partnercégünkhöz. Ha erre nincs lehetősége, keresse fel értékesítési tanácsadó munkatársainkat.

Elérhetőségek világszerte: www.netiq.com/about_netiq/officelocations.asp

Az Egyesült Államokban és Kanadában: 1-888-323-6768

E-mail: info@netiq.com

Webhely: www.netiq.com

A technikai támogatás elérhetőségei

Ha valamely termékünkkel kapcsolatos konkrét problémát szeretne bejelenteni, forduljon technikai támogatási munkatársainkhoz.

Elérhetőségek világszerte: www.netiq.com/support/contactinfo.asp

Észak- és Dél-Amerikában: 1-713-418-5555

Európában, a Közel-Keleten és Afrikában: +353 (0) 91-782 677

E-mail: support@netiq.com

Webhely: www.netiq.com/support

A dokumentációhoz kapcsolódó támogatás elérhetősége

Fontos számunkra, hogy olyan dokumentációt nyújtsunk, amellyel Ön teljes mértékben elégedett lehet. Ha javaslata van arra vonatkozóan, hogy hogyan tökéletesíthetnénk dokumentumainkat, kattintson a www.netiq.com/documentation címen megtalálható, HTML-verzióban elérhető dokumentációs anyagok oldalainak az alján található **Add Comment** (Megjegyzés hozzáadása) hivatkozásra. A javaslatokat e-mailben is elküldheti nekünk a következő címre: Documentation-Feedback@netiq.com. Észrevételeit szívesen vesszük és előre is köszönjük!

Bekapcsolódás az online felhasználóközösségbe

A NetIQ vállalat Qmunity nevű online közössége olyan, együttműködésre alapuló hálózat, amelyen keresztül kapcsolatba léphet a szakterületén dolgozó más felhasználókkal és a NetIQ szakértőivel. Azáltal, hogy közvetlenül hozzáférhetővé teszi az információkat, hasznos hivatkozásokat nyújt a megoldandó problémákhoz, és a NetIQ szakértőit is elérhető közelségbe hozza. A Qmunity biztosítja Önnek mindazokat az ismereteket, amelyekkel kiaknázhhatja a meglévő informatikai eszközeiben rejlő összes lehetőséget. A részletekért látogasson el a <http://community.netiq.com> webhelyre.

1 Az Identity Console telepítésének tervezése

Ez a fejezet az Identity Console telepítésének előfeltételeit és rendszerkövetelményeit ismerteti. Mivel az Identity Console mind Docker-konténerként, mind különálló alkalmazásként futtatható, mindkét típusú telepítés előfeltételeit és rendszerkövetelményeit megtalálja a megfelelő szakaszokban.

MEGJEGYZÉS: Az Identity Console az eDirectory 9.2.4 HF2, az Identity Manager Engine 4.8.3 HF2 és ezek későbbi verzióit támogatja. Mielőtt használatba venné az Identity Console-t, frissítenie kell az eDirectoryt és az Identity Manager Engine példányait.

- ♦ „A Docker telepítésének rendszerkövetelményei és előfeltételei”, 11. oldal
- ♦ „Különálló telepítés (nem Docker) rendszerkövetelményei és előfeltételei”, 16. oldal
- ♦ „A munkaállomás rendszerkövetelményei és előfeltételei”, 18. oldal
- ♦ „RPM-aláírás ellenőrzése”, 19. oldal

A Docker telepítésének rendszerkövetelményei és előfeltételei

Ez a szakasz az Identity Console Docker-konténerként való telepítésének rendszerkövetelményeit és előfeltételeit ismerteti.

- ♦ „Rendszerkövetelmények”, 11. oldal
- ♦ „Előfeltételek”, 11. oldal
- ♦ „A környezet beállítása”, 13. oldal

Rendszerkövetelmények

Mivel az Identity Console Docker-konténerként futtatható, az Identity Console telepítésének rendszerkövetelményeiről és a támogatott platformokról a [Docker dokumentációja](#) nyújt további információt.

Előfeltételek

- Telepítse a Docker 20.10.9-ce vagy újabb verzióját. A Docker telepítésével kapcsolatos további információért lásd a [Docker telepítési útmutatóját](#).
- Az Identity Console-kiszolgáló és a háttérkiszolgáló közötti adatcsere titkosításához/dekódolásához be kell szereznie egy pkcs12 kiszolgálói tanúsítványt és a kapcsolódó személyes kulcsot. Ez a kiszolgálói tanúsítvány a http-kapcsolat védelmére szolgál. Bármelyik külső hitelesítésszolgáltató által létrehozott kiszolgálói tanúsítványokat használhat. További

információ: [Kiszolgálótanúsítvány-objektumok létrehozása](#). A kiszolgálói tanúsítványnak tartalmaznia kell a tulajdonos alternatív nevét az Identity Console-kiszolgáló IP-címével és DNS-címével együtt. A kiszolgálótanúsítvány-objektum létrehozását követően .pfx formátumban exportálnia kell azt.

- ❑ Az előző lépésben beszerzett kiszolgálói tanúsítványok hitelesítésszolgáltatói aláírásának az érvényesítéséhez minden egyes fához be kell szereznie egy .pem formátumú hitelesítésszolgáltatói tanúsítványt. Ez a legfelső szintű hitelesítésszolgáltatói tanúsítvány teszi lehetővé a biztonságos LDAP-kommunikáció létesítését az ügyfél és az Identity Console-kiszolgáló között. Az eDirectory hitelesítésszolgáltatói tanúsítványát (SSCert.pem) például a következő helyről szerezheti be: /var/opt/novell/eDirectory/data/SSCert.pem.
- ❑ (Választható) A One SSO Provider (OSP) használata esetén engedélyezheti az egyszerű bejelentkezési hitelesítést a felhasználók számára az Identity Console portáljához. Az Identity Console telepítése előtt telepítenie kell az OSP-t. Az OSP-nek az Identity Console számára történő konfigurálásához kövesse a képernyőn megjelenő utasításokat, és adja meg a konfigurációs paraméterek szükséges értékeit. További információ: „[Az OSP-konténer telepítése](#)”, 22. oldal. Ha egy meglévő OSP-kiszolgálóhoz szeretné regisztrálni az Identity Console-t, az /opt/netiq/idm/apps/tomcat/conf/ mappában lévő ism-configuration.properties fájlhoz manuálisan hozzá kell adnia a következőt:

```
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
```

MEGJEGYZÉS: Az OSP-vel csak egyetlen eDirectory-fához lehet csatlakozni, mivel az OSP nem támogatja több eDirectory-fa használatát.

- ❑ Győződjön meg arról, hogy a gazdagéphez teljesen meghatározott gazdanevet tartalmazó, megfelelő DNS-bejegyzés található az /etc/hosts fájlban.
- ❑ Ha az Identity Console-t Edge böngészőben szeretné használni, a teljes funkcionalitáshoz le kell töltenie a Microsoft Edge legújabb verzióját.

MEGJEGYZÉS: Ha az Identity Console-t a Mozilla Firefoxban használja, előfordulhat, hogy az Origin Mismatch (Eredeteltérés) hibaüzenet jelenik meg, és a művelet sikertelen lesz. A hibaelhárításhoz végezze el az alábbi lépéseket:

- 1 Frissítse a Firefoxot a legújabb verzióra.
 - 2 Írja be az about:config szöveget a Firefox URL-mezőjébe, és nyomja le az Enter billentyűt.
 - 3 Keressen az Origin szóra.
 - 4 Kattintson duplán a network.http.SendOriginHeader beállításra, és módosítsa az értékét 1-re.
-

A környezet beállítása

Előfordulhat, hogy létre kell hoznia egy bizonyos paramétereket tartalmazó konfigurációs fájlt. Ha az OSP-vel szeretné konfigurálni az Identity Console-t, a konfigurációs fájlban meg kell adni az OSP adott paramétereit. Hozza létre például az alábbi edirapi.conf fájlt OSP-paraméterekkel:

MEGJEGYZÉS: Meg kell adnia az eDirectory-fa nevét az osp-redirect-url mezőben.

```
listen = ":9000"
ldapservers = "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"
```

Amennyiben OSP nélkül szeretné konfigurálni az Identity Console-t, hozzon létre egy konfigurációs fájlt az alább látható módon, az OSP-paraméterek nélkül:

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

MEGJEGYZÉS: Ha több eDirectory-fával kívánja konfigurálni az Identity Console-t, kihagyhatja az „ldapservers”, az „ldapuser” és az „ldappassword” paramétert, és létrehozhatja a konfigurációs fájlt.

táblázat 1-1 A konfigurációs fájlban szereplő konfigurációs paraméterek leírása

Konfigurációs paraméterek	Leírás
listen	Adja meg a 9000-es értéket az Identity Console kiszolgáló figyelőportjához a konténeren belül.
ldapservers	Az eDirectory-kiszolgáló IP-címének és portszámának a megadására szolgál.

Konfigurációs paraméterek	Leírás
ldapuser	Az eDirectory-felhasználó felhasználónevének a meghatározására szolgál. Ez a paraméter OSP-bejelentkezés esetén hitelesítő adatként szolgál az eDirectory irányába proxyt használó hitelesítésvezérlő használatával kezdeményezett LDAP-hívásokhoz. Az LDAP-felhasználónak rendszergazdai jogokkal kell rendelkeznie az eDirectory-fához.
ldappassword	Az LDAP-felhasználó jelszavának a megadására szolgál.
pkcspassword	A pkcs12 kiszolgálótanúsítvány-fájl jelszavának a megadására szolgál.
ospmode	Az OSP Identity Console-ba való integrálásához adja meg a <code>true</code> (igaz) értéket. Ha <code>false</code> (hamis) értékre állítja, az Identity Console LDAP-bejelentkezést fog használni.
osp-token-endpoint	Ez az URL-cím használható bizonyos attribútumok lekéréséhez az OSP-kiszolgálótól a hitelesítési token érvényességének ellenőrzése céljából.
osp-authorize-url	A hitelesítési token beszerzésére szolgáló hitelesítő adatok megadásához a felhasználó által használt URL-cím.
osp-logout-url	Ezt az URL-címet használhatja a felhasználó és az OSP-kiszolgáló közötti kapcsolat befejezésére.
osp-redirect-url	Az OSP-kiszolgáló a hitelesítési token megadása után erre az URL-címre irányítja át a felhasználót. MEGJEGYZÉS: Az Identity Console konfigurálásakor ügyeljen arra, hogy az eDirectory-fa nevét kisbetűvel adja meg. Amennyiben a fa nevét nem kisbetűvel adja meg, a bejelentkezés az Identity Console-kiszolgálóra sikertelen lehet.
osp-client-id	Az Identity Console-nak az OSP-ben történő regisztrálásakor megadott OSP-ügyfélazonosító megadására szolgál.
ospclientpass	Az Identity Console-nak az OSP-ben történő regisztrálásakor megadott OSP-ügyféljelszó megadására szolgál.
ospcert	Az OSP-kiszolgáló hitelesítésszolgáltatói tanúsítványa helyének a megadására szolgál.
bcert	Az Identity Console hitelesítésszolgáltatói tanúsítványa helyének a megadására szolgál.

Konfigurációs paraméterek	Leírás
loglevel	A naplózási fájlban szerepeltetni kívánt naplózási szintek megadására szolgál. Ez a paraméter „fatal” (végzetes), „error” (hiba), „warn” (figyelmeztetés) vagy „info” (információ) értékre állítható be.
check-origin	Ha ez <code>true</code> (igaz) értékre van állítva, az Identity Console kiszolgáló összehasonlítja a kérések eredeti értékét. A választható lehetőségek a <code>true</code> (igaz) vagy a <code>false</code> (hamis). Az <code>origin</code> paraméter akkor is kötelező, ha a <code>check-origin</code> paraméter értéke <code>false</code> (hamis) a DNS-konfiguráció használatakor.
origin	Az Identity Console összehasonlítja a kérések származási értékét az ebben a mezőben megadott értékekkel. MEGJEGYZÉS: Az Identity Console 1.4-től kezdve ez a paraméter független a <code>check-origin</code> paramétertől, és a használata a DNS-konfiguráció használata esetén kötelező.
maxclients	Azon ügyfelek maximális száma, akik egyidejűleg hozzáférhetnek az Identity Console-hoz. A korlátot meghaladó minden további ügyfélnek sorban kell várakoznia.

MEGJEGYZÉS

- ♦ Az `ospmode` konfigurációs paraméter csak akkor használandó, ha az OSP integrálását tervezi az Identity Console-lal.
- ♦ Ha az Identity Applications (Identity Apps) fürt módban van konfigurálva az Identity Manager beállításában, meg kell adnia a terheléselosztó-kiszolgáló DNS-nevét a konfigurációs fájl `osp-token-endpoint`, `osp-authorize-url` és `osp-logout-url` mezőjében. Amennyiben az OSP-kiszolgáló adatait megadja ezekben a mezőkben, az Identity Console-bejelentkezés sikertelen lesz.
- ♦ Ha az Identity Console ugyanazzal az OSP-példánnyal van konfigurálva, mint az Identity Apps és az Identity Reporting, az egyszeri bejelentkezés (hitelesítési szolgáltatás) akkor lép érvénybe, amikor bejelentkezik az Identity Console portáljára.
- ♦ Az Identity Console 1.4. verziójától kezdődően az OSP HTTPS URL-címét 2048 bites kulcsot tartalmazó tanúsítványokkal kell érvényesíteni.
- ♦ Ha szeretné korlátozni az Identity Console portáljához való hozzáférést a különböző tartományokról, állítsa a `samesitecookie` paramétert `strict` értékre. Ha szeretné engedélyezni az Identity Console portáljához való hozzáférést a különböző tartományokról, állítsa a `samesitecookie` paramétert `lax` értékre. Ha a paramétert nem adja meg a konfiguráció során, a rendszer a böngészőbeállításokat veszi figyelembe.

Ha elkészült a konfigurációs fájjal, folytassa a műveletet a konténer telepítésével. További információ: [„Az Identity Console telepítése Docker-konténerként”, 22. oldal.](#)

Különálló telepítés (nem Docker) rendszerkövetelményei és előfeltételei

- ♦ „Rendszerkövetelmények”, 16. oldal
- ♦ „(Választható) Az OSP-konfiguráció előfeltételei”, 17. oldal

Rendszerkövetelmények

Ez a szakasz ismerteti a különálló Identity Console telepítésének rendszerkövetelményeit és előfeltételeit.

Kategória	Minimális követelmény
Processzor	1,4 GHz-es, 64 bites
Memória	2 GB
Lemezterület	200 MB Linuxon
Támogatott böngésző	<ul style="list-style-type: none">♦ A Microsoft Edge legújabb verziója♦ A Google Chrome legújabb verziója♦ A Mozilla Firefox legújabb verziója <p>MEGJEGYZÉS: Ha az Identity Console-t a Mozilla Firefoxban használja, előfordulhat, hogy az Origin Mismatch (Eredeteltérés) hibaüzenet jelenik meg, és a művelet sikertelen lesz. A hibaelhárításhoz végezze el az alábbi lépéseket:</p> <ol style="list-style-type: none">1 Frissítse a Firefoxot a legújabb verzióra.2 Írja be az <code>about:config</code> szöveget a Firefox URL-mezőjébe, és nyomja le az Enter billentyűt.3 Keressen az Origin szóra.4 Kattintson duplán a <code>network.http.SendOriginHeader</code> beállításra, és módosítsa az értékét 1-re.
Támogatott operációs rendszer	<ul style="list-style-type: none">♦ Minősített:<ul style="list-style-type: none">♦ SUSE Linux Enterprise Server (SLES) 15 SP1, SP2 és SP3♦ SUSE Linux Enterprise Server (SLES) 12 SP1, SP2, SP3, SP4 és SP5♦ Red Hat Enterprise Linux (RHEL) 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 és 8.5♦ OpenSUSE 15.1 és 15.2♦ Támogatott: A fenti minősített operációs rendszerek támogatási csomagjainak újabb verzióin támogatott.

Kategória	Minimális követelmény
Tanúsítványok	<ul style="list-style-type: none"> ◆ Be kell szereznie egy pkcs12 kiszolgálói tanúsítványt és a kapcsolódó személyes kulcsot az ügyfél és az Identity Console-kiszolgáló közötti adatcsere titkosításához/dekódolásához. Ez a kiszolgálói tanúsítvány a http-kapcsolat védelmére szolgál. Bármelyik külső hitelesítésszolgáltató által létrehozott kiszolgálói tanúsítványokat használhat. További információ: Kiszolgálóitanúsítvány-objektumok létrehozása. A kiszolgálói tanúsítványnak tartalmaznia kell a tulajdonos alternatív nevét az Identity Console-kiszolgáló IP-címével és DNS-címével együtt. A kiszolgálóitanúsítvány-objektum létrehozását követően .pfx formátumban exportálnia kell azt. ◆ Az előző lépésben beszerzett kiszolgálói tanúsítványok hitelesítésszolgáltatói aláírásának az érvényesítéséhez minden egyes fához be kell szereznie egy .pem formátumú hitelesítésszolgáltatói tanúsítványt. Ez a legfelső szintű hitelesítésszolgáltatói tanúsítvány teszi lehetővé a biztonságos LDAP-kommunikáció létesítését az ügyfél és az Identity Console-kiszolgáló között. Az eDirectory hitelesítésszolgáltatói tanúsítványát (SSCert.pem) például a következő helyről szerezheti be: /var/opt/novell/eDirectory/data/SSCert.pem.

Amint elkészült, folytassa az Identity Console telepítésével. További információ: „[Különálló Identity Console telepítése](#)”, 26. oldal.

(Választható) Az OSP-konfiguráció előfeltételei

A One SSO Provider (OSP) használata esetén engedélyezheti az egyszeri bejelentkezési hitelesítést a felhasználók számára az Identity Console portáljához. Az Identity Console telepítése előtt telepítenie kell az OSP-t. Az OSP-nek az Identity Console számára történő konfigurálásához kövesse a képernyőn megjelenő utasításokat, és adja meg a konfigurációs paraméterek szükséges értékeit. További információ: „[Az OSP-konténer telepítése](#)”, 22. oldal. Ha egy meglévő OSP-kiszolgálóhoz szeretné regisztrálni az Identity Console-t, az /opt/netiq/idm/apps/tomcat/conf/ mappában lévő ism-configuration.properties fájlhoz manuálisan hozzá kell adnia a következőt:

```
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
```

MEGJEGYZÉS

- ♦ Ha először telepíti az OSP-t, adja meg az „y” értéket a **Configure OSP with eDir API** (Az OSP konfigurálása az eDir API-val) beállításban, és a képernyőn megjelenő utasításokat követve regisztrálja az Identity Console-t az OSP-vel.
 - ♦ Az Identity Console konfigurálásakor ügyeljen arra, hogy az eDirectory-fa nevét kisbetűvel adja meg. Amennyiben a fa nevét nem kisbetűvel adja meg, a bejelentkezés az Identity Console-kiszolgálóra sikertelen lehet.
 - ♦ Az OSP-vel csak egyetlen eDirectory-fához lehet csatlakozni, mivel az OSP nem támogatja több eDirectory-fa használatát.
-

A munkaállomás rendszerkövetelményei és előfeltételei

- ♦ „Rendszerkövetelmények”, 18. oldal

Rendszerkövetelmények

Ez a szakasz ismerteti a munkaállomásként futtatott Identity Console telepítésének rendszerkövetelményeit és előfeltételeit.

Kategória	Minimális követelmény
Processzor	1,5 GHz-es, 64 bites
Memória	2 GB
Lemezterület	1 GB Windows esetén
Támogatott operációs rendszer	<ul style="list-style-type: none">♦ Minősített:<ul style="list-style-type: none">♦ Windows Server 2016♦ Windows Server 2019♦ Windows Server 2022♦ Windows 10♦ Windows 11

Kategória	Minimális követelmény
Tanúsítványok	<ul style="list-style-type: none"> ♦ Az Identity Console-ügyfél és a REST-kiszolgáló közötti adatcseréhez pfx formátumú kiszolgálói tanúsítványt kell beszereznie. Ennek a kiszolgálói tanúsítványnak mindig a keys.pfx nevet kell viselnie. További információ: Kiszolgálóitanúsítvány-objektumok létrehozása (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/b1j4tpo3.html#b1j4u0cm). ♦ Az előző lépésben beszerzett kiszolgálói tanúsítványok hitelesítésszolgáltatói aláírásának az érvényesítéséhez minden egyes fához be kell szereznie egy .pem formátumú hitelesítésszolgáltatói tanúsítványt. Ez a legfelső szintű hitelesítésszolgáltatói tanúsítvány egy biztonságos LDAP-kommunikáció létesítését is lehetővé teszi az ügyfél és az Identity Console-kiszolgáló között. <p>Az eDirectory Linux rendszerhez való hitelesítésszolgáltatói tanúsítványát (SSCert.pem) például a következő helyről szerezheti be: /var/opt/novell/edirectory/data/SSCert.pem.</p> <p>Az eDirectory Windows rendszerhez való hitelesítésszolgáltatói tanúsítványát (SSCert.pem) a következő helyről szerezheti be: <eDirectory telepítési helye>\NetIQ\edirectory\DIBFiles\CertServ\SSCert.pem.</p>

Amint elkészült, folytassa az Identity Console telepítésével. További információ: „[Identity Console Windows rendszeren munkaállomásként](#)”, 29. oldal.

RPM-aláírás ellenőrzése

Az RPM-aláírás ellenőrzéséhez végezze el az alábbi lépéseket:

- 1 Navigáljon abba a mappába, ahová a buildet kicsomagolta.

Például: <Identity Console kicsomagolt helye>/IdentityConsole_150_Linux/license/MicroFocusGPGPackageSign.pub.

- 2 A nyilvános kulcs importálásához futtassa a következő parancsot:

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

- 3 (Választható) Futtassa a következő parancsot az RPM-aláírás ellenőrzéséhez: rpm --checksig -v <RPM neve>

Például:

```
rpm --checksig -v identityconsole-1.5.0000.x86_64.rpm
```

```
identityconsole-1.5.0000.x86_64.rpm:  
V4 RSA fejléc / SHA256 aláírás, OK, 786ec7c0 kulcsazonosító: OK  
SHA1 fejléc kivonata: OK  
SHA256 fejléc kivonata: OK  
SHA256 adattartalom kivonata: OK  
V4 RSA/SHA256 aláírás, 786ec7c0 kulcsazonosító: OK  
MD5 kivonat: OK
```

2 Az Identity Console telepítése

Ez a fejezet ismerteti az Identity Console telepítési folyamatát a biztonsági javaslatokkal együtt. A telepítésre való felkészülésként ellenőrizze, hogy teljesülnek-e a következő szakaszban felsorolt előfeltételek és rendszerkövetelmények: [1. Fejezet, „Az Identity Console telepítésének tervezése”, 11. oldal.](#)

- ♦ [„Biztonsági javaslatok”, 21. oldal](#)
- ♦ [„Az Identity Console telepítése Docker-konténerként”, 22. oldal](#)
- ♦ [„Különálló Identity Console telepítése”, 26. oldal](#)
- ♦ [„Identity Console Windows rendszeren munkaállomásként”, 29. oldal](#)
- ♦ [„Az Identity Console leállítása és újraindítása”, 30. oldal](#)
- ♦ [„Adatmegőrzés kezelése”, 31. oldal](#)
- ♦ [„Az Identity Console telepítése Azure Kubernetes-szolgáltatásokban”, 32. oldal](#)
- ♦ [„Kiszolgálói tanúsítvány módosítása”, 38. oldal](#)

Biztonsági javaslatok

- ♦ A Docker-konténerekhez alapértelmezés szerint nem tartoznak erőforrás-korlátozások. Ez minden konténernek hozzáférést ad az állomás kernelje által biztosított összes processzor- és memória-erőforráshoz. Az egy konténer által használható erőforrások mennyiségéhez korlátot beállítva biztosítani kell azt is, hogy egyetlen működő konténer se használjon több erőforrást, és más működő konténerek ne szenvedjenek hiányt.
 - ♦ A Docker futtatási parancsán a `--memory` jelzőt használva a Docker-konténernek biztosítani kell, hogy a konténer által használt memóriára szigorú korlát vonatkozzon.
 - ♦ A Docker futtatási parancsán a `--cpuset-cpus` jelzőt használva a Docker-konténernek biztosítani kell, hogy egy működő konténer által használt processzor memóriájára szigorú korlát vonatkozzon.
- ♦ A `--pids-limit` értékét 300-ra kell állítani a konténeren belül bármilyen adott időben létrehozott kernelszálak számának korlátozásához. Ez a szolgáltatásmegtagadási (DoS) támadások megakadályozására szolgál.
- ♦ A Docker futtatási parancsán a `--restart` jelzőt használva 5-ös értékre kell állítani a konténer hiba esetén érvényes újraindítási házirendjét.
- ♦ A konténert csak azt követően szabad használnia, miután az állapota **kifogástalan** értéket mutat a konténer megjelenése után. A konténer állapotának ellenőrzéséhez futtassa a következő parancsot:

```
docker ps <container_name/ID>
```

- A Docker-konténer mindig nem gyökérszintű felhasználóként (nds) indul el. További biztonsági beállításként engedélyezze a felhasználói névtér újbóli hozzárendelését a démonon a jogosultságellenőrzési támadások megakadályozásához a konténeren belül. A felhasználói névtér újbóli hozzárendeléséről a [Isolate containers with a user namespace](#) (Konténerek elkülönítése felhasználói névtérrel) című fejezetben olvashat.

Az Identity Console telepítése Docker-konténerként

Ez a szakasz az alábbi eljárásokat tartalmazza:

- „Az OSP-konténer telepítése”, 22. oldal
- „Az Identity Console telepítése Docker-konténerként”, 24. oldal
- „Több fa csatlakoztatása az Identity Console-ban (Docker)”, 26. oldal

Az OSP-konténer telepítése

Az OSP-konténer telepítéséhez végezze el az alábbi lépéseket:

- 1 Jelentkezzen be a [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalon, majd navigáljon a Software Downloads (Szoftvertöltések) oldalra.
- 2 Válassza ki a következőt:
 - Termék: eDirectory
 - Termék neve: eDirectory per User Sub SW E-LTU
 - Verzió: 9.2
- 3 Töltse le a következő fájlt: IdentityConsole_<verzió>_Containers_tar.zip.
- 4 Csomagolja ki a letöltött fájlt egy mappába.
- 5 Módosítsa az elosztott tulajdonságfájlt a követelménye szerint. Alább látható egy példa az elosztott tulajdonságfájlról:

```
# 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

```

MEGJEGYZÉS: Az elosztott tulajdonságfájl (DOS-szövegfájl) használata során a helyhiány elkerülése érdekében a DOS-szövegfájl a dos2unix eszközzel UNIX-formátumra kell konvertálni. Futtassa az alábbi parancsot a szöveges fájlban lévő DOS-sorvégződések Unix-sorvégződésekékké történő átalakításához:

```
dos2unix filename
```

Például:

```
dos2unix samplefile
```

-
- 6** Hozzon létre egy kiszolgálótanúsítványt (`cert.der`) az iManager használatával, és importálja a kulcstárba (`tomcat.ks`). Másolja az elosztott tulajdonságfájl és a kulcstárat (`tomcat.ks`) bármelyik könyvtárba. Például: `/data`. Az alábbi lépéseket elvégezve hozzon létre egy kiszolgálótanúsítványt, és importálja a kulcstárba:

- 6a** Futtassa a következő parancsot egy kulcstár (`tomcat.ks`) létrehozásához. Hozzon létre kulcsot, és biztosítsa, hogy a gép közös neve vagy teljesen minősített állomásneve az IP-cím legyen.

```
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** Tanúsítvány-aláírási kérés létrehozásához futtassa a következő parancsot. Például: `cert.csr`.

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

- 6c** Továbbítsa ezt a `cert.csr` parancsot az iManagernek, és szerezze be az `osp.der` kiszolgálótanúsítványt. A kulcs típusánál válassza az Egyéni típust; a kulcshasználati beállítások, például az Adatok rejtjelezése, a Kulcs rejtjelezése és a Digitális aláírás,

valamint a tanúsítványra vonatkozó Tulajdonos alternatív neve mező az OSP-kiszolgáló IP-címét vagy állomásnevét tartalmazza. További információt a [Kiszolgálótanúsítvány-objektumok létrehozása](#) című fejezetben talál.

- 6d Futtassa a következő parancsokat a hitelesítésszolgáltatói tanúsítvány (SSCert.der) és a kiszolgálótanúsítvány (cert.der) importálásához a tomcat.ks kulcstárba.

```
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 Az OSP-rendszerkép betöltéséhez futtassa a következő parancsot:

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

- 8 Telepítse a második konténert az alábbi paranccsal:

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

Például:

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

Az Identity Console telepítése Docker-konténerként

Ez a szakasz az Identity Console Docker-konténerként történő telepítésének eljárását ismerteti:

MEGJEGYZÉS: A jelen eljárásban említett konfigurációs paraméterek, mintaértékek és példák csak tájékoztatói célokra szolgálnak. Ügyeljen arra, hogy ne használja őket közvetlenül az éles környezetében.

- 1 Jelentkezzen be az SLD: [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalon, majd navigáljon a Software Downloads (Szoftvertöltések) oldalra.
- 2 Válassza ki a következőt:
 - ♦ Termék: eDirectory
 - ♦ Termék neve: eDirectory per User Sub SW E-LTU
 - ♦ Verzió: 9.2
- 3 Töltse le a következő fájlt: IdentityConsole_<verzió>_Container.tar.zip.
- 4 A rendszerképet be kell töltenie a Docker rendszerleíró adatbázisába. Bontsa ki és töltsse be az IdentityConsole_<verziószám>_Containers.tar.gz fájlt az alábbi parancsokkal:

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

```
docker load --input identityconsole.tar.gz
```
- 5 Hozza létre az Identity Console Docker-konténert a következő paranccsal:

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

Például:

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

MEGJEGYZÉS

- ♦ A Végfelhasználói licencszerződés (EULA) az ACCEPT_EULA környezeti változó „Y” (I) értékre állításával fogadható el. A Végfelhasználói licencszerződést a képernyőn megjelenő utasításból is elfogadhatja a konténer indítása során az `-it` kapcsolót használva az interaktív mód Docker create (Docker létrehozása) parancsában.
- ♦ `--volume` a fenti paraméterben lévő parancs létrehoz egy kötetet a konfigurációs és a naplódatok tárolásához. Ebben az esetben létrehoztunk egy `IDConsole-volume` nevű mintakötetet.

-
- 6 Másolja a kiszolgálói tanúsítványfájlt a helyi fájlrendszerből a konténerbe az `/etc/opt/novell/eDirAPI/cert/keys.pfx` elérési úton az alábbi paranccsal. A kiszolgálói tanúsítvány létrehozásáról további információt talál a következő fejezetben: [„Előfeltételek”, 11. oldal](#):

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

Például:

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

Ha több eDirectory-fához csatlakozik, legalább egy `keys.pfx` kiszolgálói tanúsítványt be kell szereznie az összes csatlakoztatott fához.

- 7 Másolja a hitelesítésszolgáltatói tanúsítványfájlt (`.pem`) a helyi fájlrendszerből a konténerbe az `/etc/opt/novell/eDirAPI/cert/SSCert.pem` elérési úton az alábbi paranccsal. A kiszolgálói tanúsítvány beszerzéséről további információt talál a következő fejezetben: [„Előfeltételek”, 11. oldal](#):

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

Például:

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

Ha a felhasználónak több eDirectory-fához kell csatlakoznia, lásd a következő fejezetet: [„Több fa csatlakoztatása az Identity Console-ban \(Docker\)”, 26. oldal](#)

- 8 Módosítsa a konfigurációs fájlt az igényeinek megfelelően, majd másolja a konfigurációs fájlt (`edirapi.conf`) a helyi fájlrendszerből a konténerbe az `/etc/opt/novell/eDirAPI/conf/edirapi.conf` elérési úton a következő parancs segítségével:

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

Például:

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

9 Indítsa el a Docker-konténert a következő paranccsal:

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

Például:

```
docker start identityconsole-container
```

MEGJEGYZÉS: A következő naplófájlokat a `/var/lib/docker/volumes/<kötet_neve>/_data/eDirAPI/var/log` könyvtárban találja:

- ♦ `edirapi.log` – Az edirapi különböző eseményeinek a naplózására és hibakeresésre szolgál.
 - ♦ `edirapi_audit.log` – Ez az edirapi ellenőrzési eseményeinek a naplózására szolgál. A naplók a CEF naplózási formátumot követik.
 - ♦ `container-startup.log` – Az Identity Console Docker-konténer telepítési naplóinak a rögzítésére szolgál.
-

Több fa csatlakoztatása az Identity Console-ban (Docker)

Az Identity Console lehetővé teszi a felhasználó számára, hogy az egyes fák egyedi hitelesítésszolgáltatói tanúsítványának a beszerzésével több fához is csatlakozzon.

Ha például három eDirectory-fához csatlakozik, akkor mindhárom hitelesítésszolgáltatói tanúsítványt be kell másolnia a Docker-konténerbe:

```
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/SSCert1.pem
```

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

Az Identity Console újraindításához futtassa a következő parancsokat:

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

Különálló Identity Console telepítése

- ♦ [„Különálló Identity Console \(nem Docker\) telepítése”, 27. oldal](#)
- ♦ [„Több fa csatlakoztatása különálló Identity Console-lal”, 28. oldal](#)

Különálló Identity Console (nem Docker) telepítése

Ez a szakasz ismerteti a különálló Identity Console telepítési eljárását:

- 1 Jelentkezzen be az SLD: [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalon, majd navigáljon a Software Downloads (Szoftvertöltések) oldalra.
- 2 Válassza ki a következőt:
 - ◆ Termék: eDirectory
 - ◆ Termék neve: eDirectory per User Sub SW E-LTU
 - ◆ Verzió: 9.2
- 3 Töltse le az Identity Console legújabb buildjét.
- 4 Csomagolja ki a letöltött fájlt egy mappába.
- 5 Nyisson meg egy kezelőfelületet, és keresse meg a mappát, ahová kibontotta az Identity Console-buildet.
- 6 Futtassa az alábbi parancsot, miközben gyökérszintű vagy a gyökérszinttel egyenértékű felhasználóként van bejelentkezve:

```
./identityconsole_install
```
- 7 Olvassa el a bevezetést, majd kattintson az **ENTER** gombra.
- 8 Az „Y” (I) lehetőségre kattintva fogadja el a licencszerződést. Ezzel telepíti az összes szükséges RPM-et a rendszerén.
- 9 Adja meg az Identity Console-kiszolgáló állomásnevét (teljesen minősített tartománynevét)/IP-címét.
- 10 Adja meg az Identity Console által figyelt port számát. Alapértéke 9000.
- 11 Válasszon a következő két lehetőség közül: az OSP és az Identity Console integrálása vagy LDAP-bejelentkezés használata az Identity Console-hoz.
- 12 Ha integrálni szeretné az OSP-t az Identity Console-lal:
 1. Adja meg az eDirectory/identitástár kiszolgálójának tartománynevét/IP-címét az LDAPS-portszámmal együtt.
Például:
192.168.1.1:636
 2. Adja meg az eDirectory/identitástár felhasználónevét.
Például:
cn=admin,ou=org_unit,o=org
 3. Adja meg az eDirectory/identitástár jelszavát.
 4. A megerősítés érdekében adja meg ismét az eDirectory/identitástár jelszavát.
 5. Adja meg az OSP-kiszolgáló tartománynevét/IP-címét az SSO-kiszolgáló SSL-portszámával együtt.
 6. Adja meg az OSP-ügyfél azonosítóját.
 7. Adja meg az OSP-ügyfél jelszavát.
 8. Adja meg az eDirectory-/identitástárfa nevét.

13 Adja meg a megbízható főtanúsítványok (`SSCert.pem`) elérési útját a mappával együtt.

Például:

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

MEGJEGYZÉS: A felhasználó nem hozhat létre alkönyvtárat a cert mappán belül.

14 Adja meg a kiszolgálótanúsítvány (`keys.pfx`) elérési útját a fájlnevvvel együtt.

Például:

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

15 Adja meg a kiszolgálói tanúsítvány jelszavát. A helyes jelszó megerősítéséhez adja meg újra a kiszolgálói tanúsítvány jelszavát. A telepítés megkezdődik.

MEGJEGYZÉS: A következő naplófájlokat a `/var/opt/novell/eDirAPI/log` könyvtárban találja:

- ♦ `edirapi.log` – Az edirapi különböző eseményeinek a naplózására és hibakeresésre szolgál.
- ♦ `edirapi_audit.log` – Ez az edirapi ellenőrzési eseményeinek a naplózására szolgál. A naplók a CEF naplózási formátumot követik.
- ♦ `identityconsole_install.log` – Az Identity Console telepítési naplóinak a rögzítésére szolgál.

Az Identity Console indítási/leállítási folyamatának naplói a `/var/log/messages` fájlban található.

MEGJEGYZÉS: A NetIQ azt ajánlja, hogy az Identity Console és az eDirectory ugyanazon a gépen történő telepítésekor a gépen legalább egy eDirectory-példány legyen elérhető.

Több fa csatlakoztatása különálló Identity Console-lal

Ha több eDirectory-fához csatlakozik, gondoskodnia kell a fák egyedi hitelesítésszolgáltatói tanúsítványának beszerzéséről.

Ha például három eDirectory-fához csatlakozik, akkor mindhárom hitelesítésszolgáltatói tanúsítványt be kell másolnia az `etc/opt/novell/eDirAPI/cert/` mappába:

```
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
```

Az Identity Console újraindításához futtassa a következő parancsok valamelyikét:

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

vagy

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

Identity Console Windows rendszeren munkaállomásként

Az Identity Console Windows rendszeren munkaállomásként is indítható; ehhez az szükséges, hogy a REST-szolgáltatások fussanak a rendszeren. Ezért indításakor egy eDirAPI-folyamat fut le az edirapi.exe parancssoron. Az edirapi.exe termináljának bezárásakor az Identity Console nem használható.

A következő eljárás az Identity Console Windows rendszerben történő futtatását ismerteti.

- 1 Jelentkezzen be az SLD: [Software License and Download \(https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0\)](https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0) (Szoftverlicenc és -letöltés) oldalon, majd navigáljon a Software Downloads (Szoftvertöltések) oldalra.
 - 2 Válassza ki a következőt:
 - ♦ Termék: eDirectory
 - ♦ Termék neve: eDirectory per User Sub SW E-LTU
 - ♦ Verzió: 9.2
 - 3 Töltse le az IdentityConsole_<verzió>_workstation_win_x86_64.zip fájlt.
 - 4 Csomagolja ki az IdentityConsole_<verzió>_workstation_win_x86_64.zip fájlt egy mappába.
 - 5 Navigáljon a kicsomagolt mappába:
IdentityConsole_150_workstation_win_x86_64\edirAPI\cert, majd másolja a megbízható legfelső szintű hitelesítésszolgáltatói SSCert.pem és a kiszolgálói tanúsítványt keys.pfx.

A tanúsítványok megszerzésével kapcsolatos információkért lásd a következő fejezetet: „[A munkaállomás rendszerkövetelményei és előfeltételei](#)”, 18. oldal

Ha a felhasználónak több eDirectory-fához kell csatlakoznia, lásd a következő fejezetet: „[Több fa csatlakoztatása az Identity Console-ban \(munkaállomás\)](#)”, 30. oldal
-
- MEGJEGYZÉS:** A kiszolgálói tanúsítvány nevének mindig keys.pfx-nek kell lennie.
-
- 6 Navigáljon abba a mappába, ahová a buildet kicsomagolta, majd kattintson duplán a run.bat (Windows-kötegfájl) fájlra.
 - 7 Adja meg a kiszolgálói tanúsítvány (keys.pfx) jelszavát a parancssorban.
Ekkor elindul az eDirAPI folyamatterminál (edirapi.exe), és megjelenik az Identity Console bejelentkezési oldala.

MEGJEGYZÉS:

- ♦ Ha az edirAPI folyamatterminál (edirapi.exe) már fut, akkor futtassa az identityconsole.exe programot abból a mappából, ahová a buildet kicsomagolta.
- ♦ A felhasználók a következő naplófájlokat találják az \IdentityConsole_150_workstation_win_x86_64\edirAPI\log mappában

`edirapi.log` – Az edirapi különböző eseményeinek a naplózására és hibakeresésre szolgál.
`edirapi_audit.log` – Ez az edirapi ellenőrzési eseményeinek a naplózására szolgál. A naplók a CEF naplózási formátumot követik.

- ♦ Az OSP-alapú bejelentkezés nem támogatott munkaállomás üzemmódban.
- ♦ Az Identity Console-munkaállomás kizárólag a 9000-es portot figyeli. Ne módosítsa az `edirapi_win.conf` fájlt.

Több fa csatlakoztatása az Identity Console-ban (munkaállomás)

Az Identity Console lehetővé teszi a felhasználó számára, hogy az egyes fák egyedi hitelesítésszolgáltatói tanúsítványának a beszerzésével több fához is csatlakozzon.

- 1 Zárja be az Identity Console-munkaállomást és az eDirAPI-terminált.
- 2 Másolja a hitelesítésszolgáltatói tanúsítványokat `SSCert.pem` a következő helyre:
`IdentityConsole_150_workstation_win_x86_64\edirAPI\cert`.
Ha például három eDirectory-fához szeretne csatlakozni, a hitelesítésszolgáltatói tanúsítványokat `SSCert1.pem`, `SSCert2.pem` és `SSCert3.pem` néven másolja be.
- 3 Navigáljon abba a mappába, ahová a buildet kicsomagolta, majd kattintson duplán a `run.bat` (Windows-kötegfájl) fájlra.
- 4 Írja be a `keys.pfx` jelszót a terminál promptjába, és jelentkezzen be a kívánt eDirectory-fába.

Az Identity Console leállítása és újraindítása

- ♦ [„Az Identity Console leállítása és újraindítása Docker-konténerként”, 30. oldal](#)
- ♦ [„A különálló Identity Console leállítása és újraindítása”, 30. oldal](#)
- ♦ [„Az Identity Console-munkaállomás bezárása és újraindítása”, 31. oldal](#)

Az Identity Console leállítása és újraindítása Docker-konténerként

Az Identity Console leállításához futtassa a következő parancsot:

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

Az Identity Console újraindításához futtassa a következő parancsot:

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

Az Identity Console indításához futtassa a következő parancsot:

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

A különálló Identity Console leállítása és újraindítása

Az Identity Console leállításához futtassa a következő parancsok valamelyikét:

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

vagy

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

Az Identity Console újraindításához futtassa a következő parancsok valamelyikét:

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

vagy

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

Az Identity Console elindításához futtassa a következő parancsok valamelyikét:

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

vagy

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

Az Identity Console-munkaállomás bezárása és újraindítása

Az alkalmazás és a folyamat bezárásához kövesse a következő eljárást:

- 1 Zárja be az Identity Console asztali Windows-alkalmazást.
- 2 Állítsa le az eDirAPI folyamatot a eDirAPI folyamatterminál bezárásával.

Az Identity Console munkaállomás újraindításához navigáljon abba a mappába, ahová a buildet kicsomagolta, majd kattintson duplán a `run.bat` (Windows-kötegfájl) fájlra.

MEGJEGYZÉS: Ha az eDirAPI folyamatterminál már fut, akkor az Identity Console-munkaállomás újraindításához futtassa az `identityconsole.exe` fájlt a kicsomagolt mappából.

Adatmegőrzés kezelése

Az Identity Console-konténerekkel együtt kötetek is létrejönnek az adatmegőrzéshez. A köteteket használó régi konténer konfigurációs paramétereinek használatához végezze el az alábbi lépéseket:

- 1 Állítsa le az aktuális Docker-konténert az alábbi paranccsal:

```
docker stop identityconsole-container
```

- 2 Hozza létre a második konténert a Docker-kötetben (`edirapi-volume-1`) tárolt régi konténer alkalmazásadatai használatával:

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

- 3 Indítsa el a második konténert az alábbi paranccsal:

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

- 4 (Választható) Az első konténer most már eltávolítható az alábbi paranccsal:

```
docker rm identityconsole-container
```

Az Identity Console telepítése Azure Kubernetes-szolgáltatásokban

Az Azure Kubernetes Service (AKS) egy felügyelt, fürtök telepítésére és kezelésére szolgáló Kubernetes-szolgáltatás. Ez a szakasz az alábbi eljárásokat tartalmazza:

Identity Console telepítése AKS-fürtben

Ez a szakasz a következő eljárásokat ismerteti az Identity Console AKS-fürtben történő telepítéséhez:

- ♦ „Azure Container Registry (ACR) létrehozása”, 32. oldal
- ♦ „Kubernetes-fürt beállítása”, 33. oldal
- ♦ „Szabványos SKU-hoz tartozó nyilvános IP-cím létrehozása”, 34. oldal
- ♦ „Cloud Shell beállítása és csatlakozás a Kubernetes-fürthöz”, 34. oldal
- ♦ „Az alkalmazás telepítése”, 34. oldal

Azure Container Registry (ACR) létrehozása

Az Azure Container Registry (ACR) egy Azure-alapú, privát tárolóregisztrációs adatbázis a Docker-konténerek rendszerképei számára.

Azure Container Registryt (ACR-t) a Tárolóregisztrációs adatbázis létrehozása – Portál című témakör [Azure Container Registry \(ACR\) létrehozása az Azure Portal használatával](#) című részében található részletes leírást követve, illetve az alábbi lépéseket elvégezve hozhat létre:

1. Jelentkezzen be az [Azure Portalra](#).
2. Válassza az **Erőforrás létrehozása > Tárolók > Container Registry** lehetőséget.
3. Az **Alapok** lapon adja meg az **Erőforráscsoport** és a **Regisztrációs adatbázis neve** értékét. A tárolóregisztrációs adatbázis nevének egyedinek kell lennie az Azure-ban, és 5–50 közötti számú alfanumerikus karaktert kell tartalmaznia.
A többi beállítás esetén fogadja el az alapértelmezett értékeket.
4. Kattintson az **Áttekintés + létrehozás** gombra.
5. Kattintson a **Létrehozás** gombra.
6. Jelentkezzen be az Azure CLI-be, majd futtassa a következő parancsot az Azure Container Registrybe való bejelentkezéshez

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

Például:

```
az acr login --name < idconsole >
```

7. Kérje le az Azure Container Registry bejelentkezési kiszolgálóját a következő paranccsal:

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

Például:

```
az acr show --name < idconsole > --query loginServer --output table
```

8. Címkézze fel az Identity Console helyi rendszerképét az ACR bejelentkezési kiszolgáló nevével (registryname.azureacr.io) a következő parancs segítségével:

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

Például:

```
docker tag identityconsole:<version> registryname.azurecr.io/  
identityconsole:<version>
```

9. Küldje el a felcímkézett rendszerképet a tárolóregisztrációs adatbázisba.

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

Például:

```
docker push registryname.azurecr.io/identityconsole:<version>
```

10. Kérje le a tárolóregisztrációs adatbázisban lévő rendszerképek listáját a következő paranccsal:

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

Kubernetes-fürt beállítása

Hozzon létre egy Kubernetes szolgáltatási erőforrást az Azure Portal vagy a CLI segítségével.

Az egy csomóponttal rendelkező Kubernetes szolgáltatási erőforrás Azure-ban történő létrehozásának részletesebb lépéseit az [Azure rövid útmutatójának AKS-fürt létrehozása](#) című részében találja.

MEGJEGYZÉS:

- ♦ Hálózatként az Azure CNI-t válassza ki.
 - ♦ Válassza ki a meglévő virtuális hálózatot (ahol az eDirectory-kiszolgálót az alhálózatra telepítették).
 - ♦ Válassza ki azt a meglévő tárolóregisztrációs adatbázist, ahol az Identity Console-rendszerkép található.
-

Szabványos SKU-hoz tartozó nyilvános IP-cím létrehozása

A Kubernetes-fürt erőforráscsoportja alatti Nyilvános IP-cím erőforrás az alkalmazás terhelés kiegyenlítő IP-jeként működik.

A részletes lépéseket a Nyilvános IP-cím létrehozása – Portál című témakör [Nyilvános IP-cím létrehozása az Azure Portal használatával](#) című részében találja.

Cloud Shell beállítása és csatlakozás a Kubernetes-fürthöz

Minden művelethez használja az Azure Portalon elérhető Cloud Shellt.

A Cloud Shell Azure Portalon történő beállításával kapcsolatos információkért olvassa el a [Bash – Rövid útmutató A Cloud Shell elindítása](#) című szakaszt, illetve a Cloud Shell beállításához és a Kubernetes-fürthöz való csatlakozáshoz hajtsa végre az alábbi lépéseket:

1. Az Azure Portalon kattintson a  gombra a Cloud Shell megnyitásához.

MEGJEGYZÉS: A Kubernetes-fürtök kezeléséhez használja a `kubectl` nevű Kubernetes parancssori ügyletet. Ha az Azure Cloud Shellt használja, a `kubectl` már telepítve van.

2. A következő parancs használatával állítsa be a `kubectl` ügyletet a Kubernetes-fürthöz való csatlakozáshoz:

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

Például:

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

3. Ellenőrizze a fürtcsomópontok listáját a következő parancs segítségével:

```
kubectl get nodes
```

Az alkalmazás telepítése

Az Identity Console telepítéséhez használhatja az `idc-services.yaml`, az `idc-statefulset.yaml`, az `idc-storageclass.yaml` és az `idc-pvc.yaml` mintafájlokat.

A követelményeknek megfelelően saját yml-fájlokat is létrehozhat.

1. Hozzon létre egy tárolási osztály-erőforrást az alábbi paranccsal:

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

Például:

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

(Választható) Ha további információkra van szüksége arról, hogy hogyan hozhat létre állandó köteteket dinamikusan, illetve hogyan felügyelheti azokat Azure Files-megosztással, olvassa el az [Állandó kötet dinamikusan létrehozása és használata a Azure Files segítségével Azure Kubernetes Service \(AKS\) környezetben](#) című témakört.

Alább látható egy példa a tárolásosztályerőforrás-fájltra:

```
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
~
```

A tárolásosztály-erőforrások dinamikus tárolókiosztást tesznek lehetővé. Az Azure-fájlmegosztás létrehozásának a meghatározására szolgál.

2. Tekintse meg a tárolási osztály részleteit az alábbi parancs használatával:

```
kubectl get sc
```

3. Hozzon létre egy PVC-erőforrást az `idc-pvc.yaml` fájl segítségével:

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

Például:


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

Alább látható egy példa a PVC-erőforrásfájltra:

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

A fájlmegosztást egy állandókötet-igénylési erőforrás hozza létre. Az állandókötet-igénylés (PVC) a tárolásosztály-objektumot használja az Azure-fájlmegosztás dinamikus kiosztásához.

4. Töltse fel az `edirapi.conf` fájlt, a hitelesítésszolgáltatói tanúsítványt és a kiszolgálói tanúsítványt a Cloud Shellbe.

Kattintson a **Fájlok feltöltése/letöltése** gomb ikonjára  a Cloud Shellen, majd töltsse fel az `edirapi.conf`, az `SSCert.pem` és a `keys.pfx` fájlt.

MEGJEGYZÉS: Az `edirapi.conf` tartalmaz egy „origin” paramétert. Itt kell megadnia azt az IP-címet, amellyel az Identity Console alkalmazást el kívánja érni. (használja a „[Szabványos SKU-hoz tartozó nyilvános IP-cím létrehozása](#)”, 34. oldal című szakaszban létrehozott IP-címet).

Az Identity Console telepítése kiszolgálói tanúsítványt (`keys.pfx`) igényel.

A kiszolgálói tanúsítvány létrehozása során ügyeljen arra, hogy érvényes DNS-nevet adjon meg a Tulajdonos alternatív neve mezőben.

Egy érvényes DNS-név létrehozásának lépései:

Egy tipikus, a StatefulSet használatával telepített pod DNS-neve a következő: `{statefulsetname}-{ordinal}.{servicename}.{namespace}.svc.cluster.local`

- ♦ Ha a StatefulSet neve az `idconsole-statefulset.yaml` fájlban `idconsole-app`, akkor `statefulsetname = idconsole-app`
- ♦ Ha ez az 1. pod, akkor `ordinal = 0`
- ♦ Ha az `idconsole-statefulset.yaml` fájlban a `serviceName` paramétert értékeként az `idconsole` értéket állítja be, akkor `serviceName = idconsole`
- ♦ Ha ez az alapértelmezett névtér, akkor `namespace=default`

Kimenet: `idconsole-app-0.idconsole.default.svc.cluster.local`

5. Hozzon létre egy configmap erőforrást a Kubernetes-fürtben, amely a tanúsítványokkal együtt tárolja a konfigurációs fájlokat.

A parancs futtatása előtt győződjön meg arról, hogy a fájlok (`edirapi.conf`, `SSCert.pem` és `keys.pfx`) megtalálhatók-e a könyvtárban.

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

Például:

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

6. A configmap objektum részletei a `kubectl describe` parancs segítségével tekinthetők meg:

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

Például:

```
kubectl describe configmap config-data
```

7. A konténer telepítéséhez hozza létre a StatefulSet erőforrást.

A konténer telepítéséhez futtassa az alábbi parancsot:

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

Például:

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

Alább látható egy példa a StatefulSet erőforrásfájltra:

```

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: pvcforsec

```

8. A telepített pod állapotának ellenőrzéséhez futtassa a következő parancsot:

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

9. Hozzon létre LoadBalancer típusú szolgáltatás-erőforrást.

A yaml fájlban megadott szolgáltatás típusa loadBalancer.

Hozzon létre egy szolgáltatás-erőforrást az alábbi paranccsal:

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

Például:

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

Alább látható egy példa a szolgáltatáserőforrás-fájltra:

```
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
```

Az alábbi parancs segítségével ellenőrizze az EXTERNAL-IP címet (vagy a loadBalancerIP címet):

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

10. Indítsa el az URL-t az EXTERNAL-IP (vagy a loadBalancerIP cím) használatával.

Például:

```
https://<EXTERNAL-IP>:9000/identityconsole
```

Kiszolgálói tanúsítvány módosítása

Ez a szakasz a Docker-konténer és a különálló Identity Console kiszolgálói tanúsítványának a módosításával kapcsolatos információkat tartalmaz.

- [„Docker-konténerben lévő kiszolgálói tanúsítvány módosítása”, 38. oldal](#)
- [„Kiszolgálói tanúsítvány módosítása a különálló Identity Console-ban”, 39. oldal](#)

Docker-konténerben lévő kiszolgálói tanúsítvány módosítása

Egy Docker-konténerben lévő kiszolgálói tanúsítvány módosításához végezze el a következő lépéseket:

- 1 Futtassa a következő parancsot, és másolja az új kiszolgálói tanúsítványt bárhová a konténerben.

Például:

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

- 2 Jelentkezzen be a konténerbe a következő paranccsal:

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

- 3 Futtassa az NLPcert-t a kulcsok pszeudofelhasználóként történő tárolásához:

```
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 Lépjen ki a konténer konzoljából a következő paranccsal:

```
exit
```

5 A következő megadásával indítsa újra a konténert:

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

Kiszolgálói tanúsítvány módosítása a különálló Identity Console-ban

Az alábbi lépésekkel módosíthatja a kiszolgálói tanúsítványt a különálló konténerben:

1 A kulcsok tárolásához futtassa az NLPCERT-t:

```
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 Indítsa újra az Identity Console-t:

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

3 Az Identity Console frissítése

Ez a fejezet ismerteti az Identity Console legújabb verzióra történő frissítésének folyamatát. A frissítésre való felkészülésként ellenőrizze, hogy teljesülnek-e a következő fejezetben felsorolt előfeltételek és rendszerkövetelmények: [1. Fejezet, „Az Identity Console telepítésének tervezése”, 11. oldal.](#)

Ez a szakasz az alábbi eljárásokat tartalmazza:

- „Az Identity Console frissítése Docker-konténerként”, 41. oldal
- „Különálló Identity Console frissítése (nem Docker)”, 43. oldal
- „Az OSP-konténer frissítése”, 44. oldal

Az Identity Console frissítése Docker-konténerként

Amikor rendelkezésre áll az Identity Console-rendszerkép új verziója, a rendszergazda egy frissítési eljárást végrehajtva telepítheti az Identity Console legújabb verzióját tartalmazó konténert. A frissítések előtt az alkalmazással kapcsolatos összes szükséges adatot tárolja véglegesen a Docker-kötetekben. Az Identity Console Docker-konténer használatával történő frissítéséhez végezze el az alábbi lépéseket:

- 1 Töltse le és töltsé be a Docker-rendszerkép legújabb verzióját a [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalon, majd végezze el az Identity Console legújabb verziójának telepítését a következő szakaszban ismertetett módon: „[Az Identity Console telepítése](#)”, 21. oldal.

- 2 Amint betöltődött a legújabb docker-rendszerkép, állítsa le az aktuális docker-konténert az alábbi paranccsal:

```
docker stop identityconsole-container
```

- 3 (Választható) Készítse el a megosztott kötet biztonsági másolatát.

- 4 A következő parancsot futtatva törölje a meglévő Identity Console-konténert:

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

Például:

```
docker rm identityconsole-container
```

- 5 (Választható) A következő parancsot futtatva törölje az elavult Identity Console Docker-rendszerképet:

```
docker rmi identityconsole
```

- 6 Hozza létre az Identity Console Docker-konténert a következő paranccsal:

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

Például:

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

MEGJEGYZÉS

- ♦ A Végfelhasználói licencszerződés (EULA) az ACCEPT_EULA környezeti változó „Y” (l) értékre állításával fogadható el. A Végfelhasználói licencszerződést a képernyőn megjelenő utasításból is elfogadhatja a konténer indítása során az `-it` kapcsolót használva az interaktív mód Docker create (Docker létrehozása) parancsában.
- ♦ `--volume` a fenti paraméterben lévő parancs létrehoz egy kötetet a konfigurációs és a naplódokumentumok tárolásához. Ebben az esetben létrehoztunk egy `IDConsole-volume` nevű mintakötetet.

-
- 7** Másolja a kiszolgálói tanúsítványfájlt a helyi fájlrendszerből az újonnan létrehozott konténerbe az `/etc/opt/novell/eDirAPI/cert/keys.pfx` elérési úton az alábbi paranccsal:

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

Például:

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

Ha több eDirectory-fához csatlakozik, legalább egy `keys.pfx` kiszolgálói tanúsítványt kell bemásolnia minden egyes csatlakoztatott fához.

- 8** Másolja a hitelesítésszolgáltatói tanúsítványfájlt (`.pem`) a helyi fájlrendszerből az újonnan létrehozott konténerbe az `/etc/opt/novell/eDirAPI/cert/SSCert.pem` elérési úton az alábbi paranccsal:

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

Például:

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

Ha több eDirectory-fához csatlakozik, minden egyes fa esetén gondoskodnia kell az egyedi hitelesítésszolgáltatói tanúsítvány beszerzéséről. Ha például három eDirectory-fához csatlakozik, akkor mindhárom hitelesítésszolgáltatói tanúsítványt be kell másolnia a Docker-konténerbe:

```
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
```

MEGJEGYZÉS: Az Identity Console 1.4-től kezdve a konfigurációs fájl (`edirapi.conf`) nem tartalmazza explicit módon az „`ldapuser`”, az „`ldappassword`” és az „`ldapserver`” paramétert. A „`bcert`” paraméterértéknek tartalmaznia kell a megbízható főtanúsítványok könyvtárának

elérési útját. Például: `bcert = "/etc/opt/novell/eDirAPI/cert/"`. Az „*origin*” paraméter pedig független a „*check-origin*”, paramétertől, a használata pedig a DNS-konfiguráció használata esetén kötelező.

- 9 Másolja a konfigurációs fájlt (`edirapi.conf`) a helyi fájlrendszerből az újonnan létrehozott konténerbe az `/etc/opt/novell/eDirAPI/conf/edirapi.conf` elérési úton az alábbi paranccsal:

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

Például:

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

- 10 Indítsa el a második konténert az alábbi paranccsal:

```
docker start identityconsole-container
```

- 11 A futó konténer állapotának ellenőrzéséhez futtassa a következő parancsot:

```
docker ps -a
```

Különálló Identity Console frissítése (nem Docker)

Ez a szakasz ismerteti a különálló Identity Console frissítési eljárását:

- 1 Töltse le az `IdentityConsole_<verzió>_Containers.tar.gz` fájlt a [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalról.
- 2 Jelentkezzen be az SLD oldalon, navigáljon a szoftverletöltési SLD oldalra, majd kattintson a **Letöltés** gombra.
- 3 Navigáljon a Termék: **eDirectory** > Termék neve: **eDirectory per User Sub SW E-LTU** > Verzió: **9.2** elemeket kiválasztva.
- 4 Töltse le az Identity Console legújabb buildjét.
- 5 A következő parancsot használva csomagolja ki a letöltött fájlt:

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

- 6 Navigáljon abba a mappába, ahova az Identity Console buildjét kicsomagolta.
- 7 Másolja annak azoknak az eDirectory-fáknak az összes megbízható főtanúsítványát egy mappába, amelyekhez kapcsolódni szeretve. A megbízható főtanúsítvány mappába másolásához futtassa a következő parancsot:

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

Például:

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

- 8 Futtassa a következő parancsot:

```
./identityconsole_install
```


- 9 Adja meg a **4. lépésben** használt megbízható főtanúsítványok mappájának elérési útját.
- 10 Az Identity Console sikeresen frissül.

Az OSP-konténer frissítése

Az OSP-konténer frissítéséhez hajtsa végre a következő lépéseket:

- 1 Töltse le és töltsse be az OSP-rendszerkép legújabb verzióját a [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) (Szoftverlicenc és -letöltés) oldalról.

Például:

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

- 2 Amint betöltődött a legújabb OSP-rendszerkép, állítsa le az aktuális OSP-konténert az alábbi paranccsal:

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

- 3 (Választható) Készítse el a megosztott kötet biztonsági másolatát.

- 4 A következő parancsot futtatva törölje a meglévő OSP-konténert:

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

Például:

```
docker rm OSP_Container
```

- 5 Lépjen a kulcstárat (`tomcat.ks`) és az elosztott tulajdonságfájlt tartalmazó könyvtárba, törölje a meglévő kulcstárat (`tomcat.ks`), és tartsa meg a meglévő OSP mappát. Generáljon egy új kulcstárolót (`tomcat.ks`) 2048-as kulcsmérettel. További információt az [Identity Console – Telepítési útmutató Az OSP-konténer telepítése](#) című fejezetében talál a **4. lépés** leírásában.

- 6 Telepítse a második konténert az alábbi paranccsal:

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

Például:

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

4 Az Identity Console eltávolítása

Ez a fejezet az Identity Console eltávolításának folyamatát ismerteti:

- „Eltávolítási eljárás Docker-környezethez”, 45. oldal
- „A különálló Identity Console (nem Docker) eltávolítási eljárása”, 45. oldal

Eltávolítási eljárás Docker-környezethez

Az Identity Console Docker-konténer eltávolításához végezze el az alábbi lépéseket:

- 1 Állítsa le az Identity Console konténert:

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

- 2 Az Identity Console Docker-konténer eltávolításához futtassa a következő parancsot:

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

- 3 A Docker-rendszerkép eltávolításához futtassa a következő parancsot:

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

- 4 Távolítsa el a Docker-kötetet:

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

MEGJEGYZÉS: Ha eltávolítja a kötetet, az adatokat is eltávolítja a kiszolgálóról.

A különálló Identity Console (nem Docker) eltávolítási eljárása

A különálló Identity Console eltávolításához végezze el az alábbi lépéseket:

- 1 Keresse meg az `/usr/bin` könyvtárat azon a gépen, amelyen az Identity Console telepítve van.
- 2 Futtassa a következő parancsot:

```
./identityconsoleUninstall
```

- 3 A rendszer sikeresen eltávolítja az Identity Console-t.

MEGJEGYZÉS: Ha az eDirectory vagy más NetIQ termék telepítve van a gépre, a felhasználónak manuálisan kell eltávolítania a `nici` és `openssl` szolgáltatásokat.
