Identity Console

Inštalačná príručka

September 2022

Právne vyhlásenie

Obsah

Informácie o tejto publikácii a knižnici

Inštalačná príručka konzoly Identity Console poskytuje informácie o tom, ako inštalovať a spravovať produkt NetIQ Identity Console (Identity Console). Táto príručka definuje terminológiu a uvádza scenáre implementácie.

Komu je príručka určená

Táto príručka je určená správcom siete.

Ďalšie informácie v knižnici

Knižnica poskytuje prístup k týmto zdrojom informácií:

Inštalačná príručka

Opisuje, ako nainštalovať a inovovať aplikáciu Identity Console. Táto publikácia je určená správcom siete.

Informácie o spoločnosti NetIQ Corporation

Sme globálnou spoločnosťou, ktorá vyvíja podnikový softvér. Zameriavame sa na tri pretrvávajúce problémy vo vašom prostredí – zmeny, komplexnosť a riziká – a na spôsoby, ako vám ich môžeme pomôcť riadiť.

Náš postoj

Prispôsobenie sa zmenám a riadenie komplexnosti a rizík nie je ničím novým

Tieto problémy sú v podstate najpodstatnejšími zo všetkých problémov, ktorým čelíte. Bránia vám získať požadovanú kontrolu na zabezpečené meranie, sledovanie a správu fyzických, virtuálnych a cloudových počítačových prostredí.

Umožnenie kľúčových podnikových služieb – lepšie a rýchlejšie

Sme presvedčení, že jedine poskytnutie čo najväčšej kontroly umožní organizáciám v oblasti IT poskytovať včasnejšie a lacnejšie služby. Pretrvávajúce tlaky, napríklad na zmenu a komplexnosť, sa budú v súvislosti so zmenami organizácií neustále stupňovať a technológie potrebné na ich správu sa stanú nevyhnutne zložitejšími.

Naša filozofia

Predaj inteligentných riešení, nielen softvéru

Chceme zabezpečovať spoľahlivé riadenie, a preto musíme porozumieť scenárom zo skutočného sveta, s ktorými sa organizácie v oblasti IT ako tá vaša každodenne stretávajú. Jedine takto môžeme vyvíjať praktické a inteligentné riešenia IT, ktoré vedú k osvedčeným a merateľným výsledkom. To nám prináša oveľa väčšie potešenie než len predaj softvéru.

Odhodlanie pomôcť vám k úspechu

Váš úspech je základom našich obchodných aktivít. Od začiatku vývoja až po nasadenie produktu myslíme na to, že potrebujete: riešenia IT, ktoré dobre fungujú a bezproblémovo sa integrujú do existujúcich investícií, neustálu technickú podporu a školenia po nasadení, ako aj osoby, s ktorými sa ľahko spolupracuje. Napokon, váš úspech je úspechom nás všetkých.

Naše riešenia

- Kontrola identity a prístupu
- Riadenie prístupu
- Správa zabezpečenia
- Správa systémov a aplikácií

- Správa pracovného zaťaženia
- Správa služby

Kontaktovanie podpory predaja

Ak máte otázky týkajúce sa produktov, cien a funkcií, obráťte sa na svojho miestneho partnera. Ak sa s týmto partnerom nemôžete skontaktovať, obráťte sa na náš tím podpory predaja.

Celý svet:	www.netiq.com/about_netiq/officelocations.asp
USA a Kanada:	1-888-323-6768
E-mail:	info@netiq.com
Webová lokalita:	www.netiq.com

Kontaktovanie technickej podpory

Ak máte konkrétne problémy s produktom, obráťte sa na náš tím technickej podpory.

Celý svet:	www.netiq.com/support/contactinfo.asp
Severná a Južná Amerika:	1-713-418-5555
Európa, Blízky východ a Afrika:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Webová lokalita:	www.netiq.com/support

Kontaktovanie podpory pre oblasť dokumentácie

Naším cieľom je poskytovať dokumentáciu, ktorá spĺňa vaše požiadavky. Ak máte návrhy na zlepšenia, kliknite na položku **Add Comment** naspodku ľubovoľnej stránky dokumentácie vo verzii HTML, ktorá je zverejnená na lokalite www.netiq.com/documentation. Takisto môžete zaslať e-mail na adresu Documentation-Feedback@netiq.com. Vaše pripomienky si vážime a radi sa s nimi oboznámime.

Kontaktovanie komunity používateľov online

Qmunity – komunita spoločnosti NetIQ online – je sieť, pomocou ktorej môžete spolupracovať so svojimi kolegami a odborníkmi zo spoločnosti NetIQ. Komunita Qmunity poskytuje aktuálne informácie, užitočné prepojenia na praktické zdroje a prístup k odborníkom zo spoločnosti NetIQ. Vďaka tomu získate vedomosti potrebné na plné využitie potenciálu investícií do IT, na ktoré sa spoliehate. Ďalšie informácie nájdete na lokalite http://community.netiq.com.

1 Plánovanie inštalácie aplikácie Identity Console

Táto kapitola vysvetľuje systémové požiadavky a nevyhnutné podmienky na inštaláciu aplikácie Identity Console. Keďže aplikáciu Identity Console možno spúšťať ako kontajner Docker aj ako samostatnú aplikáciu, v príslušných častiach nájdete systémové požiadavky a nevyhnutné podmienky pre oba typy inštalácie.

POZNÁMKA: Aplikácia Identity Console podporuje eDirectory 9.2.4 HF2, Identity Manager Engine 4.8.3 HF2 a ich príslušné novšie verzie. Je potrebné, aby ste pred používaním aplikácie Identity Console inovovali svoje inštancie eDirectory a Identity Manager Engine.

Systémové požiadavky a nevyhnutné podmienky na inštaláciu ako kontajnera Docker

Táto časť vysvetľuje systémové požiadavky a nevyhnutné podmienky na inštaláciu aplikácie Identity Console ako kontajnera Docker.

Systémové požiadavky

Keďže aplikáciu Identity Console možno spúšťať ako kontajner Docker, ďalšie informácie o systémových požiadavkách a podporovaných platformách na jej inštaláciu nájdete v dokumentácii platformy Docker.

Požiadavky

❒ Nainštalujte platformu Docker, verziu 20.10.9-ce alebo novšiu. Ďalšie informácie o inštalácii platformy Docker nájdete na stránke inštalácie platformy Docker.

- ❒ Potrebujete získať certifikát servera pkcs12 so súkromným kľúčom na šifrovanie alebo dešifrovanie výmeny dát medzi serverom Identity Console a backendovým serverom. Tento certifikát servera sa používa na zabezpečenie pripojenia http. Môžete použiť certifikáty servera vygenerované ľubovoľným externým certifikačným úradom. Ďalšie informácie nájdete v časti Creating Server Certificate Objects (Vytváranie objektov certifikátu servera). Certifikát servera by mal obsahovať alternatívny názov subjektu s adresou IP a záznamom DNS servera Identity Console. Po vytvorení objektu certifikátu servera ho musíte exportovať vo formáte .pfx.
- ❒ Ak chcete overiť podpis certifikačného úradu na certifikátoch servera získaných v predchádzajúcom kroku, musíte získať certifikát certifikačného úradu pre všetky stromy vo formáte `.pem`. Tento certifikát rootCA tiež zaručuje vytvorenie zabezpečenej komunikácie ldap medzi klientom a serverom Identity Console. Napríklad certifikát certifikačného úradu pre službu eDirectory (`SSCert.pem`) môžete získať z cesty `/var/opt/novell/eDirectory/data/SSCert.pem`.
- ❒ (Voliteľné) Pomocou služby OSP (One SSO Provider) môžete používateľom povoliť overovanie jediným prihlásením na portál Identity Console. Pred inštaláciou aplikácie Identity Console musíte nainštalovať službu OSP. Ak chcete nakonfigurovať OSP pre aplikáciu Identity Console, postupujte podľa výziev na obrazovke a zadajte požadované hodnoty konfiguračných parametrov. Ďalšie informácie nájdete v časti „Nasadenie kontajnera služby OSP“ na strane 20. Ak chcete aplikáciu Identity Console zaregistrovať na existujúcom serveri OSP, do súboru `ism-configuration.properties` v priečinku `/opt/netiq/idm/apps/tomcat/conf/` musíte manuálne pridať nasledujúci text:

  ```
  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
  ```

  POZNÁMKA: Služba OSP vám umožňuje pripojiť sa len k jednému stromu eDirectory, pretože nepodporuje viacero stromov eDirectory.
- ❒ Uistite sa, že máte v adresári `/etc/hosts` k dispozícii správnu položku DNS pre hostiteľský počítač s úplným názvom hostiteľa.
- ❒ Ak chcete používať aplikáciu Identity Console v prehľadávači Edge, na dosiahnutie úplnej funkčnosti musíte prevziať najnovšiu verziu prehliadača Microsoft Edge.

POZNÁMKA: Pri používaní aplikácie Identity Console v prehľadávači Mozilla Firefox môže operácia zlyhať s chybovým hlásením `Origin Mismatch` (Nezhoda pôvodu). Ak chcete problém vyriešiť, vykonajte tieto kroky:

1. Aktualizujte prehľadávač Firefox na najnovšiu verziu.
2. Do poľa s adresou v prehľadávači Firefox zadajte text `about:config` a stlačte kláves Enter.
3. Vyhľadajte text Origin.
4. Dvakrát kliknite na položku `network.http.SendOriginHeader` a zmeňte jej hodnotu na 1.

Nastavenie prostredia

Možno budete musieť vytvoriť konfiguračný súbor obsahujúci určité parametre. Ak chcete konfigurovať aplikáciu Identity Console pomocou služby OSP, v konfiguračnom súbore musíte zadať konkrétne parametre. Vytvorte napríklad nasledujúci súbor `edirapi.conf` s parametrami služby OSP:

POZNÁMKA: Do poľa `osp-redirect-url` zadajte názov stromu eDirectory.

```
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"
```

Ak chcete konfigurovať aplikáciu Identity Console bez služby OSP, vytvorte konfiguračný súbor uvedený nižšie bez parametrov služby OSP:

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

POZNÁMKA: Ak chcete nakonfigurovať aplikáciu Identity Console s viacerými stromami eDirectory, môžete vynechať parametre *ldapserver*, *ldapuser* a *ldappassword* a vytvoriť konfiguračný súbor.

Tabuľka 1-1 *Popis konfiguračných parametrov v konfiguračnom súbore*

Konfiguračné parametre	Popis
listen	Ako port prijímača servera Identity Console vnútri kontajnera zadajte port 9000.
ldapserver	Zadajte adresu IP hostiteľského servera eDirectory a číslo portu.

Konfiguračné parametre	Popis
ldapuser	Zadajte meno používateľa služby eDirectory. Tento parameter sa používa ako poverenie na iniciáciu volaní ldap do služby eDirectory pomocou ovládacieho prvku autorizácie proxy v prípade prihlásenia služby OSP. Používateľ ldap musí mať práva supervízora stromu eDirectory.
ldappassword	Zadajte heslo používateľa LDAP.
pfxpassword	Zadajte heslo súboru certifikátu servera pkcs12.
ospmode	Zadajte hodnotu `true` na integráciu služby OSP s aplikáciou Identity Console. Ak nastavíte hodnotu `false`, aplikácia Identity Console bude používať prihlásenie ldap.
osp-token-endpoint	Táto adresa URL sa používa na načítanie určitých atribútov zo servera OSP na overenie platnosti overovacieho tokenu.
osp-authorize-url	Túto adresu URL používa používateľ na poskytnutie poverení s cieľom získať overovací token.
osp-logout-url	Pomocou tejto adresy URL ukončite reláciu medzi používateľom a serverom OSP.
osp-redirect-url	Na túto adresu URL presmeruje server OSP používateľa po udelení overovacieho tokenu. **POZNÁMKA:** Pri konfigurácii aplikácie Identity Console nezabudnite uviesť názov stromu eDirectory malými písmenami. Ak názov stromu nie je zadaný malými písmenami, môže dôjsť k zlyhaniu prihlásenia na server Identity Console.
osp-client-id	Zadajte identifikátor klienta OSP poskytnutý v čase registrácie aplikácie Identity Console u OSP.
ospclientpass	Zadajte heslo klienta OSP poskytnuté v čase registrácie aplikácie Identity Console u OSP.
ospcert	Zadajte umiestnenie certifikátu CA servera OSP.
bcert	Zadajte umiestnenie certifikátu certifikačného úradu aplikácie Identity Console.
loglevel	Zadajte úrovne zápisu do denníka, ktoré chcete zahrnúť do súboru denníka. Tento parameter môže byť nastavený na hodnotu fatal, error, warn alebo info.
check-origin	Ak je tento parameter nastavený na hodnotu `true`, server Identity Console porovná hodnotu pôvodu požiadaviek. Dostupné sú možnosti `true` a `false`. Parameter *origin* je povinný aj v prípade, že pre parameter *check-origin* je nastavená hodnota `false` pri použití konfigurácie DNS.

Konfiguračné parametre	Popis
origin	Aplikácia Identity Console porovná hodnotu origin požiadaviek s hodnotami zadanými v tomto poli. **POZNÁMKA:** Od verzie Identity Console 1.4 je tento parameter nezávislý od parametra *check-origin* a v prípade použitia konfigurácie DNS je povinný.
maxclients	Maximálny počet súbežne spustených klientov, ktorí môžu získať prístup k objektu `IDConsole`. Všetci ostatní klienti nad úrovňou tohto limitu musia čakať vo fronte.

POZNÁMKA

- Konfiguračný parameter `ospmode` by ste mali použiť, iba ak plánujete integrovať OSP spoločne s aplikáciou Identity Console.
- Ak sú v nastavení aplikácie Identity Manager nakonfigurované aplikácie Identity Applications (Identity Apps) v režime klastra, musíte v poliach `osp-token-endpoint`, `osp-authorize-url` a `osp-logout-url` konfiguračného súboru zadať názov DNS servera vyrovnávača zaťaženia. Ak v týchto poliach uvediete podrobnosti o serveri OSP, prihlásenie do aplikácie Identity Console zlyhá.
- Ak je aplikácia Identity Console nakonfigurovaná s rovnakou inštanciou OSP ako aplikácie Identity Apps a Identity Reporting, pri prihlasovaní na portál Identity Console sa bude používať jediné prihlásenie (overovacia služba).
- V prípade verzie Identity Console 1.4 alebo novšej by mala byť adresa HTTPS URL služby OSP overená pomocou certifikátov obsahujúcich 2 048-bitový alebo novší kľúč.
- Ak chcete obmedziť prístup na portál Identity Console z rôznych domén, nastavte parameter `samesitecookie` na hodnotu `strict`. Ak chcete povoliť prístup na portál Identity Console z rôznych domén, nastavte parameter `samesitecookie` na hodnotu `lax`. Ak počas konfigurácie nezadáte tento parameter, predvolene sa použijú nastavenia prehľadávača.

Keď je konfiguračný súbor pripravený, pokračujte v nasadení kontajnera. Ďalšie informácie nájdete v časti „Nasadenie aplikácie Identity Console ako kontajnera Docker“ na strane 20.

Systémové požiadavky a nevyhnutné podmienky na samostatnú inštaláciu (nie kontajnera Docker)

Systémové požiadavky

Táto časť vysvetľuje systémové požiadavky a nevyhnutné podmienky na inštaláciu samostatnej aplikácie Identity Console.

Kategória	Minimálna požiadavka
Procesor	1,4 GHz, 64-bitový
Pamäť	2 GB
Miesto na disku	200 MB v systéme Linux
Podporovaný prehľadávač	◆ Najnovšia verzia prehľadávača **Microsoft Edge** ◆ Najnovšia verzia prehľadávača **Google Chrome** ◆ Najnovšia verzia prehľadávača **Mozilla Firefox** **POZNÁMKA:** Pri používaní aplikácie Identity Console v prehľadávači Mozilla Firefox môže operácia zlyhať s chybovým hlásením `Origin Mismatch` (Nezhoda pôvodu). Ak chcete problém vyriešiť, vykonajte tieto kroky: **1** Aktualizujte prehľadávač Firefox na najnovšiu verziu. **2** Do poľa s adresou v prehľadávači Firefox zadajte text `about:config` a stlačte kláves Enter. **3** Vyhľadajte text Origin. **4** Dvakrát kliknite na položku `network.http.SendOriginHeader` a zmeňte jej hodnotu na 1.
Podporovaný operačný systém	◆ **Certifikované**: ◆ SUSE Linux Enterprise Server (SLES) 15 SP1, SP2 a SP3 ◆ SUSE Linux Enterprise Server (SLES) 12 SP1, SP2, SP3, SP4 a SP5 ◆ Red Hat Enterprise Linux (RHEL) 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4 a 8.5 ◆ OpenSUSE 15.1 a 15.2 ◆ **Podporované:** Podporované v starších verziách balíkov podpory vyššie uvedených certifikovaných operačných systémov.

Kategória	Minimálna požiadavka
Certifikáty	◆ Na šifrovanie alebo dešifrovanie výmeny údajov medzi klientom a serverom Identity Console musíte získať certifikát servera vo formáte pkcs12 so súkromným kľúčom. Tento certifikát servera sa používa na zabezpečenie pripojenia http. Môžete použiť certifikáty servera vygenerované ľubovoľným externým certifikačným úradom. Ďalšie informácie nájdete v časti Creating Server Certificate Objects (Vytváranie objektov certifikátu servera). Certifikát servera by mal obsahovať alternatívny názov subjektu s adresou IP a záznamom DNS servera Identity Console. Po vytvorení objektu certifikátu servera ho musíte exportovať vo formáte .pfx. ◆ Ak chcete overiť podpis certifikačného úradu na certifikátoch servera získaných v predchádzajúcom kroku, musíte získať certifikát certifikačného úradu pre všetky stromy vo formáte `.pem`. Tento certifikát rootCA tiež zaručuje vytvorenie zabezpečenej komunikácie ldap medzi klientom a serverom Identity Console. Napríklad certifikát certifikačného úradu pre službu eDirectory (`SSCert.pem`) môžete získať z cesty `/var/opt/novell/eDirectory/data/SSCert.pem`.

Po dokončení týchto krokov pokračujte v inštalácii aplikácie Identity Console. Ďalšie informácie nájdete v časti „Nasadenie samostatnej aplikácie Identity Console“ na strane 24.

(Voliteľné) Nevyhnutné podmienky na konfiguráciu služby OSP

Pomocou služby OSP (One SSO Provider) môžete používateľom povoliť overovanie jediným prihlásením na portál Identity Console. Pred inštaláciou aplikácie Identity Console musíte nainštalovať službu OSP. Ak chcete nakonfigurovať OSP pre aplikáciu Identity Console, postupujte podľa výziev na obrazovke a zadajte požadované hodnoty konfiguračných parametrov. Ďalšie informácie nájdete v časti „Nasadenie kontajnera služby OSP“ na strane 20. Ak chcete aplikáciu Identity Console zaregistrovať na existujúcom serveri OSP, do súboru `ism-configuration.properties` v priečinku `/opt/netiq/idm/apps/tomcat/conf/` musíte manuálne pridať nasledujúci text:

```
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
```

POZNÁMKA

- Ak inštalujete aplikáciu OSP prvýkrát, pre položku `Configure OSP with eDir API` (Konfigurovať OSP pomocou rozhrania eDir API) zadajte voľbu `y` a podľa výziev na obrazovke zaregistrujte aplikáciu Identity Console v aplikácii OSP.
- Pri konfigurácii aplikácie Identity Console nezabudnite uviesť názov stromu eDirectory malými písmenami. Ak názov stromu nie je zadaný malými písmenami, môže dôjsť k zlyhaniu prihlásenia na server Identity Console.
- Služba OSP vám umožňuje pripojiť sa len k jednému stromu eDirectory, pretože nepodporuje viacero stromov eDirectory.

Systémové požiadavky a nevyhnutné podmienky pre verziu Workstation

Systémové požiadavky

Táto časť vysvetľuje systémové požiadavky a nevyhnutné podmienky na spúšťanie aplikácie Identity Console Workstation.

Kategória	Minimálna požiadavka
Procesor	1.5 GHz, 64-bitový
Pamäť	2 GB
Miesto na disku	1 GB v systéme Windows

Podporovaný operačný systém	• **Certifikované**:
	  • Windows Server 2016
	  • Windows Server 2019
	  • Windows Server 2022
	  • Windows 10
	  • Windows 11

Kategória	Minimálna požiadavka
Certifikáty	◆ Na výmenu údajov medzi klientom aplikácie Identity Console a serverom REST je potrebné získať certifikát servera vo formáte pfx. Tento certifikát servera musí mať vždy názov keys.pfx. Ďalšie informácie nájdete v časti Creating Server Certificate Objects (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/b1j4tpo3.html#b1j4u0cm) (Vytváranie objektov certifikátu servera). ◆ Ak chcete overiť podpis certifikačného úradu na certifikátoch servera získaných v predchádzajúcom kroku, musíte získať certifikát certifikačného úradu pre všetky stromy vo formáte `.pem`. Tento koreňový certifikát certifikačného úradu okrem toho zaručuje vytvorenie zabezpečenej komunikácie `ldap` medzi klientom a serverom Identity Console. Napríklad certifikát certifikačného úradu pre službu eDirectory (`SSCert.pem`) pre Linux môžete získať z cesty `/var/opt/novell/eDirectory/data/SSCert.pem`. Certifikát certifikačného úradu pre službu eDirectory `SSCert.pem` pre Windows získate z cesty c<`umiestnenie inštalácie služby eDirectory`>`\NetIQ\eDirectory\DIBFiles\CertServ\SSCert.pem`.

Po dokončení týchto krokov pokračujte v nasadení aplikácie Identity Console. Ďalšie informácie nájdete v časti „Identity Console v systéme Windows ako Workstation“ na strane 27.

Overenie podpisu RPM

Overenie podpisu RPM vykonáte podľa nasledujúcich krokov:

1. Prejdite do priečinka, do ktorého je zostava extrahovaná.

   Príklad: <`umiestnenie aplikácie Identity Console bez prípony tar`>`/IdentityConsole_150_Linux/license/MicroFocusGPGPackageSign.pub`.

2. Ak chcete importovať verejný kľúč, spustite nasledujúci príkaz:

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

3. (Voliteľné) Ak chcete overiť podpis RPM, spustite nasledujúci príkaz: `rpm --checksig -v` <`názov RPM`>

   Príklad:

   ```
   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 Nasadenie aplikácie Identity Console

Táto kapitola opisuje proces nasadenia aplikácie Identity Console a odporúčania týkajúce sa zabezpečenia. V rámci príprav na nasadenie skontrolujte predpoklady a systémové požiadavky uvedené v časti Kapitola 1, „Plánovanie inštalácie aplikácie Identity Console“, na straně 9.

Odporúčania týkajúce sa zabezpečenia

- V predvolenom nastavení nemajú kontajnery Docker žiadne obmedzenia prostriedkov. Tým sa každému kontajneru poskytuje prístup ku všetkým prostriedkom procesora a pamäte poskytovaným jadrom hostiteľa. Nastavením limitov pre množstvo prostriedkov, ktoré môže kontajner používať, tiež musíte zaručiť, že jeden spustený kontajner nespotrebúva viac prostriedkov a neobmedzuje ostatné spustené kontajnery.
  - Pomocou značky `--memory` v príkaze run platformy Docker musíte zaručiť používanie tvrdého limitu pre pamäť používanú kontajnerom Docker.
  - Pomocou značky `--cpuset-cpus` v príkaze run platformy Docker musíte zaručiť používanie limitu pre kapacitu procesora využívanú spusteným kontajnerom Docker.
- `--pids-limit` musíte nastaviť na 300, aby sa obmedzil počet vlákien jadra vytvorených vnútri kontajnera v danom čase. Tým sa zabraňuje útokom DoS.
- Pomocou značky `--restart` v príkaze run platformy Docker musíte nastaviť politiku reštartovania kontajnera pri zlyhaní na 5.
- Kontajner môžete používať, až keď sa po aktivácii kontajnera zobrazí stav **Healthy** (V poriadku). Ak chcete skontrolovať stav kontajnera, spustite tento príkaz:

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

- Kontajner Docker sa vždy spustí ako používateľ bez koreňových oprávnení (`nds`). Ako ďalšie bezpečnostné opatrenie povoľte opätovné priradenie priestoru mien používateľov v démonovi, aby ste zabránili útokom na eskaláciu oprávnení z kontajnera. Ďalšie informácie o opätovnom priradení priestoru mien používateľov nájdete v časti Isolate containers with a user namespace (Izolovanie kontajnerov s priestorom mien používateľov).

Nasadenie aplikácie Identity Console ako kontajnera Docker

Táto časť obsahuje nasledujúce procedúry:

Nasadenie kontajnera služby OSP

Na nasadenie kontajnera služby OSP vykonajte tieto kroky:

1. Prihláste sa na lokalitu Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a prevzatie softvéru) a prejdite na stránku Software Downloads (Softvér na prevzatie).
2. Vyberte nasledujúce možnosti:
   - Produkt: eDirectory
   - Názov produktu: eDirectory per User Sub SW E-LTU
   - Verzia: 9.2
3. Prevezmite súbor `IdentityConsole_<verzia>_Containers_tar.zip`.
4. Extrahujte prevzatý súbor do priečinka.
5. Upravte súbor vlastností pre tichú inštaláciu podľa vlastných požiadaviek. Vzorový súbor vlastností pre tichú inštaláciu je uvedený nižšie:

```
# 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
```

POZNÁMKA: Ak sa chcete vyhnúť priestorovým obmedzeniam pri použití súboru vlastností pre tichú inštaláciu (text vo formáte pre DOS), konvertujte textový súbor DOS na formát pre UNIX pomocou nástroja dos2unix. Ak chcete konvertovať textový súbor s ukončeniami riadka pre DOS na ukončenia riadka pre Unix, spustite nasledujúci príkaz:

```
dos2unix filename
```

Príklad:

```
dos2unix ukazkovysubor
```

---

6 Pomocou aplikácie iManager generujte certifikát servera (`cert.der`) a importujte ho do úložiska kľúčov (`tomcat.ks`). Kopírujte súbor vlastností pre tichú inštaláciu a úložisko kľúčov (`tomcat.ks`) do ľubovoľného adresára, napríklad do adresára `/data`. Ak chcete vytvoriť certifikát servera a importovať ho do úložiska kľúčov, vykonajte nasledujúce kroky:

6a Spustite nasledujúci príkaz na vytvorenie úložiska kľúčov (`tomcat.ks`). Generujte kľúč a uistite sa, že názov CN alebo úplný názov hostiteľa počítača je adresa 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 Spustite nasledujúci príkaz na vytvorenie žiadosti o podpísanie certifikátu. Príklad: `cert.csr`.

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

6c Postúpte žiadosť `cert.csr` do aplikácie iManager a načítajte certifikát servera `osp.der`. Zabezpečte, aby ste vybrali typ kľúča ako vlastný, možnosti použitia kľúča ako šifrovanie údajov, šifrovanie kľúča a digitálny podpis a aby pole pre alternatívny názov subjektu certifikátu obsahovalo adresu IP alebo názov hostiteľa servera OSP. Ďalšie informácie nájdete v časti Creating a Server Certificate Object (Vytvorenie objektu certifikátu servera).

6d Spustite nasledujúce príkazy na import certifikátu CÚ (SS`Cert.der`) a certifikátu servera (`cert.der`) do úložiska kľúčov `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 Spustite nasledujúci príkaz na načítanie obrazu služby OSP:

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

8 Nasaďte kontajner pomocou tohto príkazu:

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

Príklad:

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

Nasadenie aplikácie Identity Console ako kontajnera Docker

V tejto časti je vysvetlená procedúra nasadenia aplikácie Identity Console ako kontajnera Docker:

POZNÁMKA: Konfiguračné parametre, vzorové hodnoty a príklady uvedené v tejto procedúre slúžia iba na informačné účely. Musíte sa ubezpečiť, že sa nepoužívajú priamo vo vašom produkčnom prostredí.

---

1 Prihláste sa na lokalitu SLD (Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a prevzatie softvéru)) a prejdite na stránku Software Downloads (Softvér na prevzatie).

2 Vyberte nasledujúce možnosti:

- Produkt: eDirectory
- Názov produktu: eDirectory per User Sub SW E-LTU
- Verzia: 9.2

3 Prevezmite súbor `IdentityConsole_<verzia>_Container.tar.zip`.

4 Obraz musí byť načítaný do lokálneho registra prostredia Docker. Extrahujte a načítajte súbor `IdentityConsole_<version>_Containers.tar.gz` pomocou príkazov uvedených nižšie:

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

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

5 Vytvorte kontajner Docker aplikácie Identity Console pomocou tohto príkazu:

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

Príklad:

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

POZNÁMKA

- Nastavením premennej prostredia ACCEPT_EULA na hodnotu Y môžete prijať Licenčnú zmluvu koncového používateľa. Licenčnú zmluvu koncového používateľa môžete prijať aj prostredníctvom výzvy na obrazovke pri spúšťaní kontajnera pomocou možnosti `-it` v príkaze vytvorenia platformy Docker pre interaktívny režim.
- Parameter `--volume` v príkaze vyššie vytvorí zväzok na ukladanie údajov konfigurácie a denníkov. V tomto prípade sme vytvorili vzorový zväzok s názvom `IDConsole-volume`.

6 Skopírujte súbor certifikátu servera z lokálneho systému súborov do kontajnera ako `/etc/opt/novell/eDirAPI/cert/keys.pfx` pomocou tohto príkazu. Ďalšie informácie o vytvorení certifikátu servera nájdete v časti „Požiadavky“ na strane 9:

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

Príklad:

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

Pri pripojení k viacerým stromom eDirectory je potrebné získať aspoň jeden certifikát servera keys.pfx pre všetky pripojené stromy.

7 Skopírujte súbor certifikátu certifikačného úradu (`.pem`) z lokálneho systému súborov do kontajnera ako `/etc/opt/novell/eDirAPI/cert/sscert.pem` pomocou nasledujúceho príkazu. Ďalšie informácie o získaní certifikátu certifikačného úradu nájdete v časti „Požiadavky“ na strane 9:

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

Príklad:

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

Ak sa používateľ potrebuje pripojiť k viacerým stromom eDirectory, pozrite si časť: „Pripojenie aplikácie Identity Console ako kontajnera Docker k viacerým stromom“ na strane 24

8 Upravte konfiguračný súbor podľa vlastných požiadaviek a skopírujte konfiguračný súbor (`edirapi.conf`) z lokálneho systému súborov do kontajnera ako `/etc/opt/novell/eDirAPI/conf/edirapi.conf` pomocou nasledujúceho príkazu:

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

Príklad:

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

9 Spustite kontajner Docker pomocou tohto príkazu:

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

Príklad:

```
docker start identityconsole-container
```

POZNÁMKA: V adresári `/var/lib/docker/volumes/<volume_name>/_data/eDirAPI/var/log` môžete nájsť nasledujúce súbory denníka:

- edirapi.log - Používa sa na zapisovanie rôznych udalostí do denníka v edirapi a problémov s ladením.
- edirapi_audit.log - Používa sa na zapisovanie udalostí auditu edirapi do denníka. Denníky si zachovávajú formát auditu CEF.
- container-startup.log - Používa sa na zachytenie denníkov inštalácie kontajnera Docker aplikácie Identity Console.

Pripojenie aplikácie Identity Console ako kontajnera Docker k viacerým stromom

Aplikácia Identity Console umožňuje používateľovi pripojiť sa k viacerým stromom získaním individuálneho certifikátu certifikačného úradu príslušného stromu.

Ak sa napríklad pripojíte k trom stromom eDirectory, do kontajnera Docker je potrebné skopírovať všetky tri certifikáty certifikačného úradu:

```
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
```

Ak chcete reštartovať aplikáciu Identity Console, spustite nasledujúce príkazy:

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

Nasadenie samostatnej aplikácie Identity Console

- „Nasadenie samostatnej aplikácie Identity Console (nie kontajnera Docker)“ na strane 25
- „Pripojenie samostatnej inštalácie aplikácie Identity Console k viacerým stromom“ na strane 26

Nasadenie samostatnej aplikácie Identity Console (nie kontajnera Docker)

V tejto časti je vysvetlená procedúra nasadenia samostatnej aplikácie Identity Console:

1. Prihláste sa na lokalitu SLD (Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a prevzatie softvéru)) a prejdite na stránku Software Downloads (Softvér na prevzatie).
2. Vyberte nasledujúce možnosti:
   - Produkt: eDirectory
   - Názov produktu: eDirectory per User Sub SW E-LTU
   - Verzia: 9.2
3. Prevezmite najnovšiu zostavu aplikácie Identity Console.
4. Extrahujte prevzatý súbor do priečinka.
5. Otvorte prostredie a prejdite do priečinka, do ktorého ste extrahovali zostavu aplikácie Identity Console.
6. Kým ste prihlásení ako koreňový používateľ alebo jeho ekvivalent, spustite tento príkaz:

   ```
   ./identityconsole_install
   ```

7. Prečítajte si úvod a kliknite na položku **ENTER**.
8. Kliknutím na položku Y vyjadrite súhlas s Licenčnou zmluvou. Tým sa do systému nainštalujú všetky požadované súbory RPM.
9. Zadajte adresu IP alebo názov hostiteľa servera aplikácie Identity Console (ako plne kvalifikovaný rozlišujúci názov).
10. Zadajte číslo portu pre príjem aplikácie Identity Console. Predvolená hodnota je 9000.
11. Zadajte možnosť na integráciu aplikácie OSP s aplikáciou Identity Console alebo aplikáciu Identity Console na používanie prihlásenia ldap.
12. Ak chcete integrovať aplikáciu OSP s aplikáciou Identity Console, postupujte takto:
    1. Zadajte názov domény alebo adresu IP servera eDirectory alebo trezora identít s číslom portu LDAPS.

       Príklad:

       192.168.1.1:636
    2. Zadajte meno používateľa servera eDirectory alebo trezora identít.

       Príklad:

       cn=admin,ou=org_unit,o=org
    3. Zadajte heslo používateľa servera eDirectory alebo trezora identít.
    4. Znovu zadajte heslo používateľa servera eDirectory alebo trezora identít na potvrdenie hesla.
    5. Zadajte názov domény alebo adresu IP servera služby OSP s číslom portu SSL servera jediného prihlásenia.
    6. Zadajte ID klienta služby OSP.

7. Zadajte heslo klienta služby OSP.
8. Zadajte názov stromu servera eDirectory alebo trezora identít.

13 Zadajte cestu k dôveryhodným koreňovým certifikátom (`SSCert.pem`) vrátane priečinka.

Príklad:

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

POZNÁMKA: Používateľ musí dať pozor, aby v rámci priečinka certifikátov nevytvoril podadresár.

---

14 Zadajte cestu k certifikátu servera (`keys.pfx`) vrátane názvu súboru.

Príklad:

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

15 Zadajte heslo certifikátu servera. Na potvrdenie správneho zadania hesla znovu zadajte heslo certifikátu servera. Spustí sa inštalácia.

POZNÁMKA: V adresári `/var/opt/novell/eDirAPI/log` môžete nájsť nasledujúce súbory denníka:

- edirapi.log - Používa sa na zapisovanie rôznych udalostí do denníka v edirapi a problémov s ladením.
- edirapi_audit.log - Používa sa na zapisovanie udalostí auditu edirapi do denníka. Denníky si zachovávajú formát auditu CEF.
- identityconsole_install.log - Tento súbor sa používa na zachytenie denníkov inštalácie aplikácie Identity Console.

Denníky pre spustenie alebo zastavenie procesu aplikácie Identity Console je možné nájsť v súbore `/var/log/messages`.

POZNÁMKA: NetIQ odporúča, aby pri inštalácii aplikácie Identity Console a služby eDirectory v tom istom počítači v tomto počítači bola k dispozícii aspoň jedna inštancia služby eDirectory.

Pripojenie samostatnej inštalácie aplikácie Identity Console k viacerým stromom

Pri pripojení k viacerým stromom eDirectory je potrebné zaistiť získanie individuálneho certifikátu certifikačného úradu každého stromu.

Ak sa napríklad pripojíte k trom stromom eDirectory, je potrebné skopírovať všetky tri certifikáty certifikačného úradu do adresára `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
```

Spustite jeden z nasledujúcich príkazov na reštartovanie aplikácie Identity Console:

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

alebo

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

Identity Console v systéme Windows ako Workstation

Aplikácia Identity Console môže byť spustená v systéme Windows ako Workstation a vyžaduje, aby boli spustené služby REST. Preto sa pri jej spustení v príkazovom riadku edirapi.exe spúšťa proces eDirAPI. Ak je tento terminál edirapi.exe uzavretý, aplikácia Identity Console sa stáva nefunkčnou.

Nasledujúca procedúra opisuje, ako spúšťať aplikáciu Identity Console v systéme Windows.

1. Prihláste sa na lokalitu SLD (Software License and Download (https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0) (Licencie na softvér a prevzatie softvéru)) a prejdite na stránku Software Downloads (Softvér na prevzatie).
2. Vyberte nasledujúce možnosti:
   - Produkt: eDirectory
   - Názov produktu: eDirectory per User Sub SW E-LTU
   - Verzia: 9.2
3. Prevezmite súbor `IdentityConsole_<verzia>_workstation_win_x86_64.zip`.
4. Prevzatý súbor `IdentityConsole_<verzia>_workstation_win_x86_64.zip` extrahujte do priečinka.
5. Prejdite do extrahovaného priečinka: `IdentityConsole_150_workstation_win_x86_64\eDirAPI\cert` a skopírujte dôveryhodný koreňový certifikát certifikačného úradu SS`Cert.pem` a certifikát servera `keys.pfx`.

   Ak chcete získať certifikáty, pozrite si časť: „Systémové požiadavky a nevyhnutné podmienky pre verziu Workstation“ na strane 16

   Ak sa používateľ potrebuje pripojiť k viacerým stromom eDirectory, pozrite si časť: „Pripojenie aplikácie Identity Console v režime Workstation k viacerým stromom“ na strane 28

   POZNÁMKA: Názov certifikátu servera musí byť vždy `keys.pfx`.
6. Prejdite do priečinka, v ktorom je extrahovaná zostava, a dvakrát kliknite na súbor `run.bat` (dávkový súbor systému Windows).
7. V príkazovom riadku zadajte heslo certifikátu servera (`keys.pfx`).

   Spustí sa terminál procesu eDirAPI (edirapi.exe) a zobrazí sa prihlasovacia stránka aplikácie Identity Console.

POZNÁMKA:

- Ak terminál procesu `eDirAPI` (edirapi.exe) už je spustený, spustite súbor `identityconsole.exe` z priečinka extrahovanej zostavy.
- Používatelia nájdu na ceste `\IdentityConsole_150_workstation_win_x86_64\eDirAPI\log` nasledujúce denníky:

`edirapi.log` - Tento denník sa používa na zapisovanie rôznych udalostí v procese `edirapi` a problémov s ladením.

`edirapi_audit.log` - Používa sa na zapisovanie udalostí auditu `edirapi` do denníka. Denníky si zachovávajú formát auditu CEF.

- Prihlásenie na základe služby OSP nie je v režime Workstation podporované.
- Aplikácia Identity Console v režime Workstation prijíma údaje len na `porte 9000`. Neupravujte súbor `edirapi_win.conf`.

Pripojenie aplikácie Identity Console v režime Workstation k viacerým stromom

Aplikácia Identity Console umožňuje používateľovi pripojiť sa k viacerým stromom získaním individuálneho certifikátu certifikačného úradu príslušného stromu.

1. Zatvorte aplikáciu Identity Console Workstation a terminál eDirAPI.
2. Skopírujte certifikáty certifikačného úradu `SSCert.pem` do umiestnenia: `IdentityConsole_150_workstation_win_x86_64\eDirAPI\cert.`

   Ak sa napríklad chcete pripojiť k trom stromom eDirectory, skopírujte certifikáty certifikačného úradu ako `SSCert1.pem`, `SSCert2.pem` a `SSCert3.pem`.
3. Prejdite do priečinka, v ktorom je extrahovaná zostava, a dvakrát kliknite na súbor `run.bat` (dávkový súbor systému Windows).
4. Zadajte heslo súboru `keys.pfx` do príkazového riadka terminálu a prihláste sa do požadovaného stromu eDirectory.

Zastavenie a reštartovanie aplikácie Identity Console

- „Zastavenie a reštartovanie aplikácie Identity Console ako kontajnera Docker“ na strane 28
- „Zastavenie a reštartovanie samostatnej aplikácie Identity Console“ na strane 29
- „Zatvorenie a opätovné spustenie aplikácie identity Console Workstation“ na strane 29

Zastavenie a reštartovanie aplikácie Identity Console ako kontajnera Docker

Ak chcete aplikáciu Identity Console zastaviť, spustite tento príkaz:

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

Ak chcete aplikáciu Identity Console reštartovať, spustite tento príkaz:

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

Ak chcete spustiť aplikáciu Identity Console, spustite tento príkaz:

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

Zastavenie a reštartovanie samostatnej aplikácie Identity Console

Ak chcete aplikáciu Identity Console zastaviť, spustite niektorý z nasledujúcich príkazov:

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

alebo

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

Ak chcete aplikáciu Identity Console reštartovať, spustite niektorý z nasledujúcich príkazov:

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

alebo

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

Ak chcete spustiť aplikáciu Identity Console, spustite niektorý z nasledujúcich príkazov:

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

alebo

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

Zatvorenie a opätovné spustenie aplikácie identity Console Workstation

Ak chcete zavrieť aplikáciu a proces, postupujte podľa tejto procedúry:

1. Zatvorte počítačovú aplikáciu Identity Console pre Windows.
2. Zastavte proces eDirAPI zatvorením terminálu procesu `eDirAPI`.

Ak chcete znovu spustiť aplikáciu Identity Console Workstation, prejdite do priečinka, v ktorom je extrahovaná zostava, a dvakrát kliknite na súbor `run.bat` (dávkový súbor systému Windows).

POZNÁMKA: Ak terminál procesu `eDirAPI` už je spustený, znovu spustite aplikáciu Identity Console Workstation spustením súboru `identityconsole.exe` z priečinka extrahovanej zostavy.

Správa perzistencie údajov

Spoločne s kontajnermi Identity Console sa vytvárajú aj zväzky na perzistenciu údajov. Ak chcete použiť konfiguračné parametre starého kontajnera pomocou zväzkov, postupujte takto:

1. Zastavte aktuálny kontajner Docker pomocou tohto príkazu:

   ```
   docker stop identityconsole-container
   ```

2. Vytvorte druhý kontajner pomocou údajov aplikácie starého kontajnera uloženého vo zväzku Docker (`edirapi-volume-1`):

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

3 Spustite druhý kontajner Docker pomocou tohto príkazu:

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

4 (Voliteľné) Prvý kontajner môžete odstrániť pomocou tohto príkazu:

```
docker rm identityconsole-container
```

Nasadenie aplikácie Identity Console v službách Azure Kubernetes Service

Azure Kubernetes Service (AKS) je spravovaná služba Kubernetes, ktorá vám umožňuje nasadzovať a spravovať klastre. Táto časť obsahuje nasledujúce procedúry:

Nasadenie aplikácie Identity Console v klastri AKS

V tejto časti sú vysvetlené nasledujúce procedúry na nasadenie aplikácie Identity Console v klastri AKS:

- „Vytvorenie registra Azure Cointainer Registry (ACR)“ na strane 30
- „Nastavenie klastra Kubernetes“ na strane 31
- „Vytvorenie verejnej adresy IP štandardnej jednotky SKU“ na strane 32
- „Nastavenie prostredia Cloud Shell a pripojenie ku klastru Kubernetes“ na strane 32
- „Nasadenie aplikácie“ na strane 32

Vytvorenie registra Azure Cointainer Registry (ACR)

Azure Container Registry (ACR) je súkromný register na báze platformy Azure pre obrazy kontajnera Docker.

Podrobnejší postup nájdete na stránke Create an Azure container registry using the Azure portal (Vytvorenie registra kontajnera Azure pomocou portálu Azure) v časti Create container registry - Portal (Vytvorenie registra kontajnera - portál) alebo vykonajte nasledujúce kroky na vytvorenie registra Azure Container Registry (ACR):

1. Prihláste sa na lokalitu Azure Portal.
2. Prejdite do sekcie **Create a resource** (Vytvoriť prostriedok) > **Containers** (Kontajnery) > **Container Registry** (Register kontajnera).
3. Na karte **Basics** (Základy) zadajte hodnoty do polí **Resource group** (Skupina prostriedkov) a **Registry name** (Názov registra). Názov registra musí byť na portáli Azure jedinečný a musí obsahovať najmenej 5 a najviac 50 alfanumerických znakov.

   Pre ostatné nastavenia prijmite predvolené hodnoty.
4. Kliknite na položku **Review + create** (Skontrolovať a vytvoriť).
5. Kliknite na položku **Create** (Vytvoriť).

6. Prihláste sa do rozhrania príkazového riadka Azure a spustením nasledujúceho príkazu sa prihláste do registra Azure Container Registry

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

   Príklad:

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

7. Vyhľadajte prihlasovací server registra Azure Container Registry pomocou príkazu:

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

   Príklad:

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

8. Označte lokálny obraz aplikácie Identity Console názvom prihlasovacieho servera registra ACR (registryname.azureacr.io) pomocou nasledujúceho príkazu:

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

   Príklad:

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

9. Odošlite označkovaný obraz do registra.

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

   Príklad:

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

10. Vyhľadajte zoznam obrazov v registri pomocou príkazu:

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

Nastavenie klastra Kubernetes

Vytvorte prostriedok služby Kubernetes pomocou portálu Azure alebo rozhrania príkazového riadka.

Podrobnejší postup na vytvorenie prostriedku služby Kubernetes na platforme Azure s uzlom nájdete v časti Create an AKS Cluster (Vytvorenie klastra AKS) v príručke Azure Quickstart (Azure - rýchle spustenie).

POZNÁMKA:

- Vyberte Azure CNI ako sieť.
- Vyberte existujúcu virtuálnu sieť (kde server eDirectory je nasadený v podsieti).
- Vyberte existujúci register kontajnera, v ktorom je k dispozícii obraz aplikácie Identity Console.

Vytvorenie verejnej adresy IP štandardnej jednotky SKU

Prostriedok verejnej adresy IP v skupine prostriedkov klastra Kubernetes vystupuje ako adresa IP zariadenia na vyrovnávanie záťaže pre aplikáciu.

Podrobný postup nájdete na stránke Create a public IP address using the Azure portal (Vytvorenie verejnej adresy IP pomocou portálu Azure) v časti Create public IP address – Portal (Vytvorenie verejnej adresy IP - portál).

Nastavenie prostredia Cloud Shell a pripojenie ku klastru Kubernetes

Používajte prostredie Cloud Shell, ktoré je k dispozícii na portáli Azure, na všetky operácie.

Ak chcete nastaviť prostredie Cloud Shell na portáli Azure, pozrite si časť Start Cloud Shell (Spustenie prostredia Cloud Shell) v príručke Bash – Quickstart (Bash - rýchle spustenie) alebo vykonajte nasledujúce kroky na nastavenie prostredia Cloud Shell a pripojenie ku klastru Kubernetes:

1. Na portáli Azure kliknutím na tlačidlo  otvorte prostredie Cloud Shell.

   POZNÁMKA: Ak chcete spravovať klaster Kubernetes, použite klienta príkazového riadka Kubernetes `kubectl`. Ak používate Azure Cloud Shell, klient kubectl už je nainštalovaný.

2. Nakonfigurujte klienta kubectl na pripojenie ku klastru Kubernetes pomocou nasledujúceho príkazu:

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

   Príklad:

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

3. Overte zoznam uzlov klastra pomocou príkazu:

   ```
   kubectl get nodes
   ```

Nasadenie aplikácie

Na nasadenie aplikácie Identity Console môžete použiť ukážkové súbory `idc-services.yaml`, `idc-statefulset.yaml`, `idc-storageclass.yaml` a `idc-pvc.yaml`.

Môžete si tiež vytvoriť svoje súbory yaml podľa vlastných požiadaviek.

1. Vytvorte prostriedok triedy úložiska pomocou príkazu nižšie:

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

   Príklad:

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

(Voliteľné) Ďalšie informácie o tom, ako dynamicky vytvoriť a používať trvalý zväzok so zdieľaným umiestnením pre súbory Azure, nájdete v časti Dynamically create and use a persistent volume with Azure Files in Azure Kubernetes Service (AKS) (Dynamické vytvorenie a používanie trvalého zväzku so súbormi Azure v službe Azure Kubernetes Service (AKS).

Ukážkový súbor prostriedku triedy úložiska je zobrazený nižšie:

```
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
~
```

Prostriedok triedy úložiska umožňuje dynamické poskytovanie úložiska. Používa sa na definovanie, ako vytvoriť zdieľané umiestnenie pre súbory Azure.

2. Detaily triedy úložiska zobrazíte pomocou príkazu nižšie:

   ```
   kubectl get sc
   ```

3. Vytvorte prostriedok požiadavky na trvalý zväzok pomocou súboru `idc-pvc.yaml`:

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

   Príklad:

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

   Ukážkový súbor prostriedku požiadavky na trvalý zväzok je zobrazený nižšie:

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

   Prostriedok požiadavky na trvalý zväzok vytvára zdieľané umiestnenie pre súbory. Požiadavka na trvalý zväzok (PTZ) používa objekt triedy úložiska na dynamické poskytovanie zdieľaného umiestnenia pre súbory Azure.

4. Odovzdajte súbor edirapi.conf, certifikát certifikačného úradu a certifikát servera do prostredia Cloud Shell.

   Kliknite na ikonu **Upload/Download files** (Odovzdať alebo prevziať súbory)  v prostredí Cloud Shell a odovzdajte súbory `edirapi.conf`, `SSCert.pem` a `keys.pfx`.

   POZNÁMKA: Súbor edirapi.conf má parameter „origin“. Tu potrebujeme poskytnúť adresu IP, s ktorou získame prístup k aplikácii Identity Console. (použite adresu IP, ktorá je vytvorená v časti „Vytvorenie verejnej adresy IP štandardnej jednotky SKU“ na strane 32.)

   Nasadenie aplikácie Identity Console vyžaduje certifikát servera (`keys.pfx`).

   Počas vytvárania certifikátu servera zadajte platný názov DNS do poľa alternatívneho názvu subjektu.

   Kroky na zostavenie platného názvu DNS:

   Typický pod nasadený pomocou StatefulSet má názov DNS, ako je uvedené nižšie - {statefulsetname}-{ordinal}.{servicename}.{namespace}.svc.cluster.local

   - Ak názov pre StatefulSet v súbore idconsole-statefulset.yaml je idconsole-app, potom statefulsetname = idconsole-app
   - Ak ide o prvý pod, ordinal = 0
   - Ak definujete serviceName v súbore idconsole-statefulset.yaml ako idconsole, potom serviceName = idconsole
   - Ak ide o predvolený priestor názvov, potom namespace=default

   Výstup teda bude vyzerať takto: idconsole-app-0.idcosole.default.svc.cluster.local

   ---

5. Vytvorte v klastri Kubernetes prostriedok configmap, ktorý uchováva konfiguračné súbory spolu s certifikátmi.

   Pred spustením príkazu sa uistite, že v adresári sú prítomné súbory (`edirapi.conf`, `SSCert.pem` a `keys.pfx`).

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

   Príklad:

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

6. Zobrazte detaily objektu configmap pomocou príkazu kubectl describe:

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

   Príklad:

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

7. Vytvorte prostriedok StatefulSet na nasadenie kontajnera.

   Spustením príkazu nižšie nasaďte kontajner:

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

   Príklad:

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

Ukážkový súbor prostriedku StatefulSet je zobrazený nižšie:

```
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. Spustením nasledujúceho príkazu overte stav nasadeného podu:

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

9. Vytvorte prostriedok služby typu loadBalancer.

   Typ služby zadanej v súbore yaml je loadBalancer.

   Vytvorte prostriedok služby pomocou príkazu nižšie:

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

   Príklad:

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

   Ukážkový súbor prostriedku služby je zobrazený nižšie:

```
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
```

Skontrolujte adresu EXTERNAL-IP (alebo loadBalancerIP) pomocou príkazu nižšie:

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

10. Spustite url pomocou adresy EXTERNAL-IP (alebo loadBalancerIP).

    Príklad:

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

Úprava certifikátu servera

Táto časť poskytuje informácie o úprave certifikátu servera v kontajneri Docker a samostatnej aplikácii Identity Console.

- „Úprava certifikátu servera v kontajneri Docker“ na strane 36
- „Úprava certifikátu servera v samostatnej aplikácii Identity Console“ na strane 37

Úprava certifikátu servera v kontajneri Docker

Vykonaním nasledujúcich krokov upravte certifikát servera v kontajneri Docker:

1 Spustením nasledujúceho príkazu skopírujte nový certifikát servera do ľubovoľného umiestnenia v kontajneri.

Príklad:

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

2 Prihláste sa do kontajnera pomocou nasledujúceho príkazu:

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

3 Spustite príkaz NLPCERT na uloženie kľúčov ako pseudopoužívateľ:

```
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 Ukončite konzolu kontajnera pomocou príkazu:

```
exit
```

5 Reštartujte kontajner tak, že zadáte:

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

Úprava certifikátu servera v samostatnej aplikácii Identity Console

Vykonaním nasledujúcich krokov upravte certifikát servera v samostatnom kontajneri:

1 Spustením príkazu NLPCERT uložte kľúče:

```
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 Reštartujte aplikáciu Identity Console:

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

3 Inovácia aplikácie Identity Console

Táto kapitola opisuje proces inovácie aplikácie Identity Console na najnovšie verzie. V rámci príprav na inováciu skontrolujte predpoklady a systémové požiadavky uvedené v časti Kapitola 1, „Plánovanie inštalácie aplikácie Identity Console“, na strane 9.

Táto časť obsahuje nasledujúce procedúry:

Inovácia aplikácie Identity Console ako kontajnera Docker

Keď je dostupná nová verzia obrazu aplikácie Identity Console, správca môže vykonať procedúru inovácie na nasadenie kontajnera pomocou najnovšej verzie aplikácie Identity Console. Skôr než vykonáte inováciu, natrvalo uložte všetky potrebné údaje súvisiace s aplikáciou do zväzkov Docker. Ak chcete aplikáciu Identity Console inovovať pomocou kontajnera Docker, vykonajte tieto kroky:

1. Prevezmite a načítajte najnovšiu verziu obrazu Docker z lokality Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a prevzatie softvéru) a vykonajte kroky na inštaláciu najnovšej verzie aplikácie Identity Console, ako sú uvedené v časti „Nasadenie aplikácie Identity Console“ na strane 19.
2. Po načítaní najnovšieho obrazu Docker zastavte aktuálny kontajner Docker pomocou tohto príkazu:

   ```
   docker stop identityconsole-container
   ```

3. (Voliteľné) Vytvorte zálohu zdieľaného zväzku.
4. Spustením nasledujúceho príkazu odstráňte existujúci kontajner aplikácie Identity Console:

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

   Príklad:

   ```
   docker rm identityconsole-container
   ```

5. (Voliteľné) Spustením nasledujúceho príkazu odstráňte zastaraný obraz Docker aplikácie Identity Console:

   ```
   docker rmi identityconsole
   ```

6. Vytvorte kontajner Docker aplikácie Identity Console pomocou tohto príkazu:

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

   Príklad:

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

POZNÁMKA

- Nastavením premennej prostredia ACCEPT_EULA na hodnotu Y môžete prijať Licenčnú zmluvu koncového používateľa. Licenčnú zmluvu koncového používateľa môžete prijať aj prostredníctvom výzvy na obrazovke pri spúšťaní kontajnera pomocou možnosti `-it` v príkaze vytvorenia platformy Docker pre interaktívny režim.
- Parameter `--volume` v príkaze vyššie vytvorí zväzok na ukladanie údajov konfigurácie a denníkov. V tomto prípade sme vytvorili vzorový zväzok s názvom `IDConsole-volume`.

7 Skopírujte súbor certifikátu servera z lokálneho systému súborov do práve vytvoreného kontajnera ako `/etc/opt/novell/eDirAPI/cert/keys.pfx` pomocou tohto príkazu:

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

Príklad:

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

Pri pripojení k viacerým stromom eDirectory je potrebné skopírovať aspoň jeden certifikát servera keys.pfx pre všetky pripojené stromy.

8 Skopírujte súbor certifikátu certifikačného úradu (`.pem`) z lokálneho systému súborov do práve vytvoreného kontajnera ako `/etc/opt/novell/eDirAPI/cert/sscert.pem` pomocou tohto príkazu:

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

Príklad:

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

Pri pripojení k viacerým stromom eDirectory je potrebné zaistiť získanie individuálneho certifikátu certifikačného úradu pre všetky pripojené stromy. Ak sa napríklad pripojíte k trom stromom eDirectory, do kontajnera Docker je potrebné skopírovať všetky tri certifikáty certifikačného úradu:

```
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
```

POZNÁMKA: Od verzie Identity Console 1.4 konfiguračný súbor (edirapi.conf) explicitne neobsahuje parametre *ldapuser*, *ldappassword* a *ldapserver*. Hodnota parametra *bcert* musí zahŕňať cestu k adresáru pre dôveryhodné koreňové certifikáty. Príklad: bcert = "/etc/opt/novell/eDirAPI/cert/". A parameter *origin* je nezávislý od parametra *check-origin* a pri používaní konfigurácie DNS je povinný.

9 Skopírujte konfiguračný súbor (`edirapi.conf`) z lokálneho systému súborov do práve vytvoreného kontajnera ako `/etc/opt/novell/eDirAPI/conf/edirapi.conf` pomocou tohto príkazu:

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

Príklad:

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

10 Spustite druhý kontajner Docker pomocou tohto príkazu:

```
docker start identityconsole-container
```

11 Ak chcete skontrolovať stav spusteného kontajnera, spustite nasledujúci príkaz:

```
docker ps -a
```

Inovácia samostatnej aplikácie Identity Console (inej než Docker)

V tejto časti je vysvetlená procedúra inovácie samostatnej aplikácie Identity Console:

1 Prevezmite súbor `IdentityConsole_<verzia>_Containers.tar.gz` z lokality Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a softvér na prevzatie)

2 Prihláste na lokalitu SLD, prejdite na stránku softvéru na prevzatie a kliknite na položku **Download** (Prevziať).

3 Postupne vyberte hodnoty Product (Produkt): **eDirectory** > Product Name (Názov produktu): **eDirectory per User Sub SW E-LTU** > Version (Verzia): **9.2**

4 Prevezmite najnovšiu zostavu aplikácie Identity Console.

5 Extrahujte prevzatý súbor pomocou nasledujúceho príkazu:

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

6 Prejdite do priečinka, do ktorého ste extrahovali zostavu Identity Console.

7 Skopírujte všetky dôveryhodné koreňové certifikáty stromov eDirectory, ktoré chcete pripojiť k priečinku. Ak chcete kopírovať dôveryhodný koreňový certifikát do priečinka, spustite nasledujúci príkaz:

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

Príklad:

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

8 Spustite nasledujúci príkaz:

```
./identityconsole_install
```

9 Zadajte cestu priečinka dôveryhodných koreňových certifikátov použitého v **kroku 4**.

10 Aplikácia Identity Console sa úspešne inovuje.

Inovácia kontajnera služby OSP

Na inováciu kontajnera služby OSP vykonajte tieto kroky:

1. Prevezmite a načítajte najnovšiu verziu obrazu služby OSP z lokality Software License and Download (https://sld.microfocus.com/) (Licencie na softvér a softvér na prevzatie).

   Príklad:

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

2. Po načítaní najnovšieho obrazu služby OSP zastavte aktuálny kontajner služby OSP pomocou tohto príkazu:

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

3. (Voliteľné) Vytvorte zálohu zdieľaného zväzku.
4. Spustením nasledujúceho príkazu odstráňte existujúci kontajner služby OSP:

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

   Príklad:

   ```
   docker rm OSP_Container
   ```

5. Prejdite do adresára, ktorý obsahuje ukladací priestor kľúčov (`tomcat.ks`) a súbor vlastností pre tichú inštaláciu, odstráňte existujúci ukladací priestor kľúčov (`tomcat.ks`) a ponechajte existujúci priečinok služby OSP. Generujte nový ukladací priestor kľúčov (`tomcat.ks`) s veľkosťou kľúčov 2 048. Ďalšie informácie nájdete v **kroku 4** v časti Nasadenie kontajnera služby OSP Inštalačnej príručky aplikácie Identity Console.
6. Nasaďte kontajner pomocou tohto príkazu:

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

   Príklad:

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

4 Odinštalovanie aplikácie Identity Console

Táto kapitola opisuje proces odinštalovania aplikácie Identity Console:

Procedúra odinštalovania pre prostredie Docker

Ak chcete odinštalovať kontajner Docker aplikácie Identity Console, vykonajte tieto kroky:

1. Zastavte kontajner aplikácie Identity Console:

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

2. Spustením nasledujúceho príkazu odstráňte kontajner Docker aplikácie Identity Console:

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

3. Spustením nasledujúceho príkazu odstráňte obraz kontajnera Docker:

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

4. Odstráňte zväzok kontajnera Docker:

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

POZNÁMKA: Ak odstránite zväzok, zo servera sa odstránia aj údaje.

Procedúra odinštalovania pre samostatnú aplikáciu Identity Console (nie kontajner Docker)

Ak chcete odinštalovať samostatnú aplikáciu Identity Console, vykonajte tieto kroky:

1. V počítači, v ktorom je nainštalovaná aplikácia Identity Console, prejdite do adresára `/usr/bin`.
2. Spustite nasledujúci príkaz:

   ```
   ./identityconsoleUninstall
   ```

3. Aplikácia Identity Console sa úspešne odinštaluje.

POZNÁMKA: Pri nainštalovaní služby eDirectory alebo iného produktu NetIQ v počítači používateľ musí manuálne odinštalovať *nici* a *openssl*.