



Identity Console

Instalační příručka

září 2022

Právní upozornění

Informace o právních upozorněních, ochranných známkách, prohlášeních o omezení odpovědnosti, zárukách, omezeních exportu a dalších omezeních, právech vlády USA, patentových zásadách a dodržování standardů FIPS naleznete na webu <https://www.netiq.com/company/legal>.

Copyright © 2022 NetIQ Corporation. Všechna práva vyhrazena.

Obsah

Informace o této příručce a knihovně	5
Informace o společnosti NetIQ Corporation	7
1 Plánování instalace konzoly Identity Console	9
Požadavky na systém a předpoklady pro instalaci v Dockeru	9
Požadavky na systém	9
Předpoklady	9
Nastavení prostředí	11
Požadavky na systém a předpoklady pro samostatnou instalaci (bez Dockeru)	13
Požadavky na systém	13
(Volitelné) Předpoklad pro konfiguraci poskytovatele OSP	15
Požadavky na systém a předpoklady pro pracovní stanici	16
Požadavky na systém	16
Ověření podpisu RPM	17
2 Nasazení konzoly Identity Console	19
Bezpečnostní doporučení	19
Nasazení konzoly Identity Console jako kontejneru Dockeru	20
Nasazení kontejneru poskytovatele OSP	20
Nasazení konzoly Identity Console jako kontejneru Dockeru	22
Více stromů s konzolou Identity Console jako Dockerem	24
Nasazení samostatné konzoly Identity Console	24
Nasazení samostatné konzoly Identity Console (bez Dockeru)	24
Více stromů se samostatnou konzolou Identity Console	26
Konzole Identity Console v systému Windows jako pracovní stanice	26
Více stromů s konzolou Identity Console jako pracovní stanicí	27
Zastavení a opětovné spuštění konzoly Identity Console	28
Zastavení a opětovné spuštění konzoly Identity Console instalované jako kontejner Dockeru	28
Zastavení a opětovné spuštění samostatně instalované konzoly Identity Console	28
Zavření a opětovné spuštění pracovní stanice konzoly Identity Console	29
Správa trvalosti dat	29
Nasazení konzoly Identity Console ve službách Azure Kubernetes	29
Nasazení konzoly Identity Console v clusteru AKS	29
Změna certifikátu serveru	35
Změna certifikátu serveru v kontejneru Dockeru	35
Změna certifikátu serveru v samostatné konzole Identity Console	36
3 Inovace konzoly Identity Console	37
Inovace konzoly Identity Console jako kontejneru Dockeru	37
Inovace samostatné konzoly Identity Console (bez Dockeru)	39
Inovace kontejneru poskytovatele OSP	40

4 Odinstalace konzoly Identity Console	41
Postup odinstalace v prostředí Dockeru	41
Postup odinstalace samostatné konzoly Identity Console (bez Dockeru).....	41

Informace o této příručce a knihovně

Tato *instalační příručka konzoly Identity Console* poskytuje informace k instalaci a správě produktu NetIQ Identity Console (konzola Identity Console). Kniha definuje terminologii a obsahuje scénáře implementace.

Komu je příručka určena

Tato příručka je určena správcům sítě.

Další informace v knihovně

Knihovna poskytuje následující zdroje informací:

Instalační příručka

Popisuje postup instalace a inovování konzoly Identity Console. Tato kniha je určena správcům sítě.

Informace o společnosti NetIQ Corporation

Jsme globální softwarová společnost, která se zaměřuje na tři stálé výzvy ve vašem prostředí, což jsou změna, složitost a rizika, a na to, jak vám můžeme pomoci s jejich zvládním.

Náš pohled na věc

Přizpůsobování se změnám a zvládnání komplexních problémů a rizik není ničím novým.

Ve skutečnosti jsou to ze všech výzev, kterým čelíte, pravděpodobně ty nejmarkantnější proměnné, které vám ubírají na kontrole potřebné k bezpečnému měření, monitorování a správě vašeho fyzického, virtuálního a cloudového výpočetního prostředí.

Aktivace zásadních obchodních služeb, lepší a rychlejší

Věříme, že zajištění nejlepší možné kontroly organizací IT představuje jediný způsob zajištění včasné a finančně nenákladné dodávky služeb. Neustálé tlaky, jako jsou změny a složitost, se budou stále zvyšovat s tím, jak se organizace stále mění a technologie potřebné k jejich správě jsou stále složitější.

Naše filozofie

Prodej inteligentních řešení, nejen softwaru

Z důvodu zajištění spolehlivější kontroly se nejprve snažíme porozumět situacím z praxe, do kterých se organizace IT, jako je ta vaše, denně dostávají. To je jediný způsob, jak můžeme vyvíjet praktická a inteligentní řešení IT, která úspěšně vedou k osvědčeným a změřitelným výsledkům. A to nám přináší větší uspokojení než pouhý prodej softwaru.

Posilování vašeho úspěchu je naším největším zájmem

Váš úspěch stojí v srdci našeho podnikání. Uvědomujeme si, že potřebujete řešení IT, která dobře fungují od založení až k nasazení a hladce se integrují s vašimi stávajícími investicemi, že potřebujete průběžnou podporu a školení i po nasazení a že potřebujete někoho, s kým se opravdu snadno pracuje – pro změnu. Koneckonců, váš úspěch je úspěchem nás všech.

Naše řešení

- ♦ Řízení identity a přístupu
- ♦ Správa přístupu
- ♦ Správa zabezpečení
- ♦ Správa systémů a aplikací

- ♦ Správa pracovního zatížení
- ♦ Správa služeb

Kontaktování prodejní podpory

Pokud máte otázky týkající se produktů, cen a možností, obraťte se na svého místního partnera. Pokud to není možné, kontaktujte náš tým podpory prodeje.

Celosvětově:	www.netiq.com/about_netiq/officelocations.asp
USA a Kanada	1-888-323-6768
E-mail:	info@netiq.com
Webové stránky:	www.netiq.com

Kontaktování technické podpory

Pokud potřebujete vyřešit konkrétní problémy s produkty, obraťte se na náš tým technické podpory.

Celosvětově:	www.netiq.com/support/contactinfo.asp
Severní a Jižní Amerika:	1-713-418-5555
Evropa, Střední východ a Afrika:	+353 (0) 91-782 677
E-mail:	support@netiq.com
Webové stránky:	www.netiq.com/support

Kontaktování podpory v oblasti dokumentace

Naším cílem je vytvářet takovou dokumentaci, která vyhovuje vašim potřebám. Pokud máte návrhy na zlepšení, klepněte na tlačítko **Add Comment** (Přidat komentář) v dolní části jakékoli stránky verzí HTML dokumentace publikované na stránkách www.netiq.com/documentation. Můžete také napsat e-mail na adresu Documentation-Feedback@netiq.com. Vážíme si vašich názorů a těšíme se, že se nám ozvete.

Kontaktování online komunity uživatelů

Qmunity, online komunita uživatelů aplikací NetIQ, je síť pro spolupráci, která vás spojí s ostatními uživateli a odborníky na NetIQ. Díky okamžitému poskytnutí informací, odkazům na užitečné prostředky a dostupnosti odborníků na NetIQ pomáhá Qmunity zajistit, že si osvojíte znalosti potřebné k využití plného potenciálu investic do IT, na které spoléháte. Další informace najdete na stránkách <http://community.netiq.com>.

1 Plánování instalace konzoly Identity Console

Tato kapitola obsahuje požadavky na systém a předpoklady pro instalaci konzoly Identity Console. Konzolu Identity Console lze spustit jako kontejner Dockeru nebo jako samostatnou aplikaci. Požadavky na systém a předpoklady pro každý typ instalace najdete v příslušné části příručky.

POZNÁMKA: Konzole Identity Console podporuje eDirectory 9.2.4 HF2, Identity Manager Engine 4.8.3 HF2 a jejich příslušné pozdější verze. Než začnete konzolu Identity Console používat, je nutné inovovat instance těchto součástí.

- ♦ „Požadavky na systém a předpoklady pro instalaci v Dockeru“ na straně 9
- ♦ „Požadavky na systém a předpoklady pro samostatnou instalaci (bez Dockeru)“ na straně 13
- ♦ „Požadavky na systém a předpoklady pro pracovní stanici“ na straně 16
- ♦ „Ověření podpisu RPM“ na straně 17

Požadavky na systém a předpoklady pro instalaci v Dockeru

V této části jsou shrnuty požadavky na systém a předpoklady pro instalaci konzoly Identity Console jako kontejneru Dockeru.

- ♦ „Požadavky na systém“ na straně 9
- ♦ „Předpoklady“ na straně 9
- ♦ „Nastavení prostředí“ na straně 11

Požadavky na systém

Konzolu Identity Console lze spustit jako kontejner Dockeru. Další informace o požadavcích na systém a podporovaných platformách pro její instalaci najdete v [dokumentaci k Dockeru](#).

Předpoklady

- ❑ Nainstalujte Docker 20.10.9-ce nebo novější. Další informace najdete na stránce [o instalaci Dockeru](#).
- ❑ Je nutné získat certifikát serveru pkcs12 se soukromým klíčem k šifrování a dešifrování výměny dat mezi serverem konzoly Identity Console a backendovým serverem. Tento certifikát serveru se používá k zabezpečení připojení přes HTTP. Můžete použít certifikáty serveru vygenerované libovolným vnějším certifikačním úřadem. Další informace najdete v tématu [Vytváření objektů](#)

[certifikátu serveru](#). Certifikát serveru by měl obsahovat alternativní název subjektu s adresou IP a DNS serveru konzoly Identity Console. Jakmile vytvoříte objekt certifikátu serveru, je třeba jej exportovat ve formátu .pfx.

- ❑ K ověření podpisu certifikačního úřadu u certifikátů serveru je třeba pro všechny stromy získat certifikát certifikačního úřadu ve formátu .pem. Tento kořenový certifikát certifikačního úřadu zároveň zajišťuje zabezpečenou komunikaci LDAP mezi klientem a serverem Identity Console. Můžete například získat certifikát certifikačního úřadu služby eDirectory CA (SSCert.pem) z umístění /var/opt/novell/eDirectory/data/SSCert.pem.
- ❑ (Volitelné) Pomocí poskytovatele One SSO Provider (OSP) můžete uživatelům na portálu Identity Console zpřístupnit ověřování službou Single Sign-on. Poskytovatele OSP je nutné nainstalovat před instalací konzoly Identity Console. Poskytovatele OSP pro konzolu Identity Console nakonfigurujte podle pokynů na obrazovce a zadejte povinné hodnoty konfiguračních parametrů. Další informace najdete v části „[Nasazení kontejneru poskytovatele OSP](#)“ na straně 20. Pokud chcete konzolu Identity Console registrovat k existujícímu serveru OSP, je třeba do souboru ism-configuration.properties ve složce /opt/netiq/idm/apps/tomcat/conf/ přidat následující 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: S poskytovatelem OSP se můžete připojit pouze k jednomu stromu služby eDirectory, protože poskytovatel OSP nepodporuje více stromů služby eDirectory.

- ❑ Pro hostitelský počítač musíte mít k dispozici správný záznam DNS v umístění /etc/hosts s úplným názvem hostitele.
- ❑ Pokud chcete konzolu Identity Console používat v prohlížeči Edge, je třeba k plnohodnotnému fungování stáhnout nejnovější verzi prohlížeče.

POZNÁMKA: Při používání konzoly Identity Console v prohlížeči Mozilla Firefox může operace selhat a může se zobrazit chybová zpráva o neshodě zdroje. Tyto potíže odstraní takto:

- 1 Aktualizujte Firefox na nejnovější verzi.
 - 2 Do pole pro adresu URL v prohlížeči Firefox zadejte about:config a stiskněte klávesu Enter.
 - 3 Vyhledejte výraz „origin“.
 - 4 Poklepejte na položku network.http.SendOriginHeader a změňte její hodnotu na 1.
-

Nastavení prostředí

Možná bude nutné vytvořit konfigurační soubor s konkrétními parametry. Pokud chcete konfigurovat konzolu Identity Console pomocí poskytovatele OSP, musíte do konfiguračního souboru zadat parametry specifické pro tohoto poskytovatele. Vytvořte tedy například níže uvedený soubor `edirapi.conf` s parametry poskytovatele OSP:

POZNÁMKA: Do pole `osp-redirect-url` je nutné zadat název 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"
```

Jestliže chcete konzolu Identity Console konfigurovat bez poskytovatele OSP, vytvořte konfigurační soubor tak, jak je vidět níže, bez parametrů OSP:

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

POZNÁMKA: Pokud chcete konzolu Identity Console nakonfigurovat s několika stromy služby eDirectory, můžete přeskočit parametry „`ldapserver`“, „`ldapuser`“ a „`ldappassword`“ a vytvořit konfigurační soubor.

Tabulka 1-1 Popis konfiguračních parametrů v konfiguračním souboru:

Konfigurační parametry	Popis
<code>listen</code>	Jako port naslouchacího procesu serveru konzoly Identity Console v kontejneru zadejte 9000.
<code>ldapserver</code>	Zadejte adresu IP hostitelského serveru eDirectory a číslo portu.

Konfigurační parametry	Popis
ldapuser	Zadejte uživatelské jméno uživatele služby eDirectory. Tento parametr se používá jako pověření k inicializaci volání LDAP do služby eDirectory za použití řízení autorizace prostřednictvím proxy v případě přihlášení poskytovatele OSP. Uživatel LDAP musí mít na daném stromu služby eDirectory práva supervizora.
ldappassword	Zadejte heslo uživatele LDAP.
pfxpassword	Zadejte heslo souboru certifikátu serveru pkcs12.
ospmode	Pokud chcete s konzolou Identity Console integrovat poskytovatele OSP, zadejte hodnotu <code>True</code> . Jestliže nastavíte hodnotu <code>False</code> , bude se u konzoly Identity Console používat přihlášení LDAP.
osp-token-endpoint	Tato adresa URL se používá k načtení určitých atributů ze serveru OSP s cílem ověřit platnost ověřovacího tokenu.
osp-authorize-url	Tuto adresu URL používá uživatel k poskytnutí pověření, aby mohl získat ověřovací token.
osp-logout-url	Tuto adresu URL použijte k ukončení relace mezi uživatelem a serverem OSP.
osp-redirect-url	Na tuto adresu URL přesměruje server OSP uživatele po udělení ověřovacího tokenu. POZNÁMKA: Při konfiguraci konzoly Identity Console nezapomeňte zadat název stromu eDirectory malými písmeny. Jestliže název stromu není zadán malými písmeny, nemusí se přihlášení k serveru Identity Console zdařit.
osp-client-id	Zadejte ID klienta OSP použité při registraci konzoly Identity Console u poskytovatele OSP.
ospclientpass	Zadejte heslo klienta OSP použité při registraci konzoly Identity Console u poskytovatele OSP.
ospcert	Zadejte umístění certifikátu CA serveru OSP.
bcert	Zadejte umístění certifikátu certifikačního úřadu konzoly Identity Console.
loglevel	Zadejte úroveň protokolování, které chcete zahrnout do souboru protokolu. Tento parametr lze nastavit na hodnoty „fatal“, „error“, „warn“ nebo „info“.
check-origin	Pokud je tato možnost nastavena na hodnotu <code>True</code> , server konzoly Identity Console porovná původní hodnotu požadavků. Dostupné možnosti jsou <code>True</code> nebo <code>False</code> . Parametr <i>origin</i> je povinný, i když je hodnota parametru <i>check-origin</i> při použití konfigurace DNS nastavena na <code>False</code> .

Konfigurační parametry	Popis
origin	Konzola Identity Console porovná hodnotu parametru origin požadavků s hodnotami zadanými v tomto poli. POZNÁMKA: Počínaje verzí konzoly Identity Console 1.4 je tento parametr nezávislý na parametru <i>check-origin</i> a je povinný, pokud se používá konfigurace DNS.
maxclients	Maximální počet souběžně připojených klientů s přístupem ke konzole IDConsole. Případní další klienti nad tento limit musí čekat ve frontě.

POZNÁMKA

- ♦ Parametr konfigurace `ospmode` je vhodné použít jen v případě, že plánujete s konzolou Identity Console integrovat poskytovatele OSP.
- ♦ Pokud máte aplikace Identity Applications (Identity Apps) v nastavení nástroje Identity Manager konfigurovány v režimu clusteru, musíte v konfiguračním souboru do polí `osp-token-endpoint`, `osp-authorize-url` a `osp-logout-url` zadat název DNS serveru vyrovnávání zatížení. Pokud do těchto polí zadáte informace o serveru OSP, přihlášení ke konzole Identity Console se nezdaří.
- ♦ Jestliže je konzola Identity Console konfigurována se stejnou instancí poskytovatele OSP jako aplikace Identity Apps a Identity Reporting, uplatní se při přihlašování na portál Identity Console ověřovací služba Single Sign-on.
- ♦ Adresa HTTPS URL poskytovatele OSP musí být počínaje verzí konzoly Identity Console 1.4 ověřena pomocí certifikátů obsahujících 2048bitový klíč nebo vyšší.
- ♦ Chcete-li omezit přístup k portálu Identity Console z jiných domén, nastavte parametr `samesitecookie` na hodnotu `strict`. Chcete-li povolit přístup k portálu Identity Console z jiných domén, nastavte parametr `samesitecookie` na hodnotu `lax`. Pokud parametr během konfigurace nezadáte, uplatní se jako výchozí nastavení prohlížeče.

Jakmile budete mít konfigurační soubor připraven, pokračujte nasazením kontejneru. Další informace najdete v části „[Nasazení konzoly Identity Console jako kontejneru Dockeru](#)“ na straně 20.

Požadavky na systém a předpoklady pro samostatnou instalaci (bez Dockeru)

- ♦ „[Požadavky na systém](#)“ na straně 13
- ♦ „[\(Volitelné\) Předpoklad pro konfiguraci poskytovatele OSP](#)“ na straně 15

Požadavky na systém

V této části jsou vysvětleny požadavky na systém a předpoklady pro samostatnou instalaci konzoly Identity Console.

Kategorie	Minimální požadavek
Procesor	64bitový o frekvenci 1,4 GHz
Paměť	2 GB
Prostor na disku	200 MB v systému Linux
Podporovaný prohlížeč	<ul style="list-style-type: none"> ♦ Nejnovější verze prohlížeče Microsoft Edge ♦ Nejnovější verze prohlížeče Google Chrome ♦ Nejnovější verze prohlížeče Mozilla Firefox <p>POZNÁMKA: Při používání konzoly Identity Console v prohlížeči Mozilla Firefox může operace selhat a může se zobrazit chybová zpráva o neshodě zdroje. Tyto potíže odstraní takto:</p> <ol style="list-style-type: none"> 1 Aktualizujte Firefox na nejnovější verzi. 2 Do pole pro adresu URL v prohlížeči Firefox zadejte <code>about:config</code> a stiskněte klávesu Enter. 3 Vyhledejte výraz „origin“. 4 Poklepejte na položku <code>network.http.SendOriginHeader</code> a změňte její hodnotu na 1.
Podporovaný operační systém	<ul style="list-style-type: none"> ♦ Certifikováno: <ul style="list-style-type: none"> ♦ 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 ♦ Podporováno: Podporováno v novějších verzích aktualizací Support Pack výše uvedených certifikovaných operačních systémů.

Kategorie	Minimální požadavek
Certifikáty	<ul style="list-style-type: none"> ♦ K šifrování a dešifrování dat vyměňovaných mezi klientem a serverem Identity Console je třeba získat certifikát serveru pkcs12 se soukromým klíčem. Tento certifikát serveru se používá k zabezpečení připojení přes HTTP. Můžete použít certifikáty serveru vygenerované libovolným vnějším certifikačním úřadem. Další informace najdete v tématu Vytváření objektů certifikátu serveru. Certifikát serveru by měl obsahovat alternativní název subjektu s adresou IP a DNS serveru konzoly Identity Console. Jakmile vytvoříte objekt certifikátu serveru, je třeba jej exportovat ve formátu .pfx. ♦ K ověření podpisu certifikačního úřadu u certifikátů serveru je třeba pro všechny stromy získat certifikát certifikačního úřadu ve formátu .pem. Tento kořenový certifikát certifikačního úřadu zároveň zajišťuje zabezpečenou komunikaci LDAP mezi klientem a serverem Identity Console. Můžete například získat certifikát certifikačního úřadu služby eDirectory CA (SSCert.pem) z umístění /var/opt/novell/eDirectory/data/SSCert.pem.

Jakmile budete připraveni, pokračujte v instalaci konzoly Identity Console. Další informace najdete v části „[Nasazení samostatné konzoly Identity Console](#)“ na straně 24.

(Volitelné) Předpoklad pro konfiguraci poskytovatele OSP

Pomocí poskytovatele One SSO Provider (OSP) můžete uživatelům na portálu Identity Console zpřístupnit ověřování službou Single Sign-on. Poskytovatele OSP je nutné nainstalovat před instalací konzoly Identity Console. Poskytovatele OSP pro konzolu Identity Console nakonfigurujte podle pokynů na obrazovce a zadejte povinné hodnoty konfiguračních parametrů. Další informace najdete v části „[Nasazení kontejneru poskytovatele OSP](#)“ na straně 20. Pokud chcete konzolu Identity Console registrovat k existujícímu serveru OSP, je třeba do souboru `ism-configuration.properties` ve složce `/opt/netiq/idm/apps/tomcat/conf/` přidat následující 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

- ♦ Jestliže poskytovatele OSP instalujete poprvé, zadejte u možnosti `Configure OSP with eDir API` (Konfigurovat OSP s rozhraním eDir API) hodnotu `y` a podle pokynů na obrazovce zaregistrujte konzolu Identity Console u poskytovatele OSP.
 - ♦ Při konfiguraci konzoly Identity Console nezapomeňte zadat název stromu eDirectory malými písmeny. Jestliže název stromu není zadán malými písmeny, nemusí se přihlášení k serveru Identity Console zdařit.
 - ♦ S poskytovatelem OSP se můžete připojit pouze k jednomu stromu služby eDirectory, protože poskytovatel OSP nepodporuje více stromů služby eDirectory.
-

Požadavky na systém a předpoklady pro pracovní stanici

- ♦ [„Požadavky na systém“ na straně 16](#)

Požadavky na systém

V této části jsou vysvětleny požadavky na systém a předpoklady pro spuštění pracovní stanice konzoly Identity Console.

Kategorie	Minimální požadavek
Procesor	64bitový o frekvenci 1.5 GHz
Paměť	2 GB
Prostor na disku	1 GB v systému Windows
Podporovaný operační systém	<ul style="list-style-type: none">♦ Certifikováno:<ul style="list-style-type: none">♦ Windows Server 2016♦ Windows Server 2019♦ Windows Server 2022♦ Windows 10♦ Windows 11

Kategorie	Minimální požadavek
Certifikáty	<ul style="list-style-type: none"> Pro výměnu dat mezi klientem konzoly Identity Console a serverem REST je třeba získat certifikát serveru ve formátu pfx. Tento certifikát serveru musí být vždy pojmenován keys.pfx. Další informace najdete v tématu Vytváření objektů certifikátu serveru (https://www.netiq.com/documentation/edirectory-92/edir_admin/data/b1j4tpo3.html#b1j4u0cm). K ověření podpisu certifikačního úřadu u certifikátů serveru je třeba pro všechny stromy získat certifikát certifikačního úřadu ve formátu .pem. Tento kořenový certifikát certifikačního úřadu zároveň zajišťuje zabezpečenou komunikaci LDAP mezi klientem a serverem Identity Console. <p>Můžete například získat certifikát certifikačního úřadu služby eDirectory pro Linux SSCert.pem z umístění /var/opt/novell/eDirectory/data/SSCert.pem.</p> <p>Certifikát certifikačního úřadu služby eDirectory SSCert.pem pro Windows získáte z umístění <umístění instalace služby eDirectory>\NetIQ\eDirectory\DIBFiles\CertServ\SSCert.pem.</p>

Jakmile budete připraveni, pokračujte v nasazení konzoly Identity Console. Další informace najdete v části „Konzole Identity Console v systému Windows jako pracovní stanice“ na straně 26.

Ověření podpisu RPM

Ověření podpisu RPM provedete následovně:

- 1 Přejděte do složky, ve které je extrahováno sestavení.

Příklad: <neoznačené umístění konzoly Identity Console>/IdentityConsole_150_Linux/license/MicroFocusGPGPackageSign.pub

- 2 Spuštěním následujícího příkazu importujte veřejný klíč:

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

- 3 (Volitelné) Spuštěním následujícího příkazu ověřte podpis RPM: rpm --checksig -v <název RPM>

Příklad:

```
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 Nasazení konzoly Identity Console

Tato kapitola popisuje postup nasazení konzoly Identity Console spolu s bezpečnostními doporučeními. Při přípravě na nasazení si projděte seznam předpokladů a požadavků na systém, který najdete v části [Kapitola 1, „Plánování instalace konzoly Identity Console“](#), na straně 9.

- ♦ „Bezpečnostní doporučení“ na straně 19
- ♦ „Nasazení konzoly Identity Console jako kontejneru Dockeru“ na straně 20
- ♦ „Nasazení samostatné konzoly Identity Console“ na straně 24
- ♦ „Konzole Identity Console v systému Windows jako pracovní stanice“ na straně 26
- ♦ „Zastavení a opětovné spuštění konzoly Identity Console“ na straně 28
- ♦ „Správa trvalosti dat“ na straně 29
- ♦ „Nasazení konzoly Identity Console ve službách Azure Kubernetes“ na straně 29
- ♦ „Změna certifikátu serveru“ na straně 35

Bezpečnostní doporučení

- ♦ U kontejnerů Dockeru neexistují ve výchozím nastavení žádná omezení prostředků. Každý kontejner tak má zajištěn přístup ke všem prostředkům procesoru a paměti poskytovaným jádrem hostitele. Dále je třeba zajistit, aby jeden běžící kontejner nespotřeboval větší množství prostředků a neubíral dalším běžícím kontejnerům. Provedete to nastavením limitů pro objem prostředků, které může využít jeden kontejner.
 - ♦ U kontejnerů Dockeru je třeba nastavit použití pevného limitu paměti používané kontejnerem pomocí příznaku `--memory` v příkazu pro spuštění kontejneru Dockeru.
 - ♦ U kontejnerů Dockeru je třeba nastavit použití limitu na kapacitu procesoru využitou běžícím kontejnerem pomocí příznaku `--cpuset-cpus` v příkazu pro spuštění kontejneru Dockeru.
- ♦ Příznak `--pids-limit` je třeba nastavit na 300 a omezit tak počet vláken jádra spuštěných v libovolný okamžik uvnitř kontejneru. Toto opatření pomáhá zabránit útokům DoS.
- ♦ Je nutné nastavit zásady restartování kontejnerů při selhání na 5 pomocí příznaku `--restart` v příkazu pro spuštění kontejneru Dockeru.
- ♦ Po zprovoznění nelze kontejner začít používat dříve, než se jako jeho stav zobrazí **Healthy** (V pořádku). Stav kontejneru zjistíte následujícím příkazem:

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

- ♦ Kontejner Dockeru se vždy spustí jako jiný než kořenový uživatel (`nds`). Jako další bezpečnostní opatření aktivujte přemapování oboru názvů uživatelů na démona. Předejdete tak útokům eskalace oprávnění zevnitř kontejneru. Další informace o přemapování oboru názvů uživatelů najdete v tématu [Isolate containers with a user namespace](#) (Izolace kontejnerů pomocí oboru názvů uživatelů).

Nasazení konzoly Identity Console jako kontejneru Dockeru

Tato část se věnuje následujícím postupům:

- ♦ „Nasazení kontejneru poskytovatele OSP“ na straně 20
- ♦ „Nasazení konzoly Identity Console jako kontejneru Dockeru“ na straně 22
- ♦ „Více stromů s konzolou Identity Console jako Dockerem“ na straně 24

Nasazení kontejneru poskytovatele OSP

Při nasazování kontejneru poskytovatele OSP postupujte takto:

- 1 Přihlaste se na stránce softwarové licence a stahování [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) a přejděte na stránku Software Downloads (Stažení softwaru).
- 2 Vyberte následující:
 - ♦ Produkt: eDirectory
 - ♦ Název produktu: eDirectory per User Sub SW E-LTU
 - ♦ Verze: 9.2
- 3 Stáhněte soubor: IdentityConsole_<verze>_Containers_tar.zip.
- 4 Extrahujte stažený soubor do složky.
- 5 Upravte soubor vlastností tiché instalace podle svých požadavků. Níže najdete příklad souboru vlastností tiché instalace:

```
# 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: Aby se předešlo omezení místa při používání souboru vlastností tiché instalace (text DOS), musíte textový soubor DOS převést na formát UNIX pomocí nástroje dos2unix. Spuštěním příkazu níže převedete textový soubor z ukončení řádku DOS na ukončení řádku Linux:

```
dos2unix filename
```

Příklad:

```
dos2unix samplefile
```

-
- 6** Pomocí nástroje iManager vygenerujte certifikát serveru (`cert.der`) a importujte ho do úložiště klíčů (`tomcat.ks`). Zkopírujte soubor vlastností tiché instalace a úložiště klíčů (`tomcat.ks`) do libovolného adresáře. Můžete použít například svazek `/data`. Pomocí následujícího postupu vytvořte certifikát serveru a importujte ho do úložiště klíčů:

- 6a** Spuštěním následujícího příkazu vytvořte úložiště klíčů (`tomcat.ks`). Vygenerujte klíč a ověřte, že název CN nebo plně kvalifikovaný název hostitele počítače 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** Spuštěním následujícího příkazu vytvořte žádost o podepsání certifikátu. Může to být například `cert.csr`.

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

- 6c** Předějte tuto žádost `cert.csr` do nástroje iManager a získejte certifikát serveru `osp.der`. Je třeba vybrat typ klíče Vlastní a možnosti využití klíče Šifrování dat, Šifrování klíče a Digitální podpis a pole alternativního názvu subjektu certifikátu musí obsahovat adresu IP nebo název hostitele serveru poskytovatele OSP. Další informace najdete v tématu [Creating a Server Certificate Object](#) (Vytvoření objektu certifikátu serveru).

- 6d** Spuštěním následujících příkazů importujte certifikát certifikačního úřadu (`SSCert.der`) a certifikát serveru (`cert.der`) do úložiště klíčů `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 Spuštěním následujícího příkazu načtete bitovou kopii poskytovatele OSP:

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

8 Pomocí následujícího příkazu nasadíte kontejner:

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

Příklad:

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

Nasazení konzoly Identity Console jako kontejneru Dockeru

Tato část vysvětluje postup nasazení konzoly Identity Console jako kontejneru Dockeru:

POZNÁMKA: Parametry konfigurace, vzorové hodnoty a příklady zmíněné v tomto postupu slouží jen jako reference. Nepoužívejte je přímo ve vašem produkčním prostředí.

1 Přihlaste se na stránce SLD: [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) a přejděte na stránku Software Downloads (Stažení softwaru).

2 Vyberte následující:

- ♦ Produkt: eDirectory
- ♦ Název produktu: eDirectory per User Sub SW E-LTU
- ♦ Verze: 9.2

3 Stáhněte soubor: IdentityConsole_<verze>_Container.tar.zip.

4 Bitovou kopii je třeba načíst do místního registru Dockeru. Rozbalte a načtete soubor IdentityConsole_<verze>_Containers.tar.gz pomocí následujících příkazů:

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

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

5 Pomocí následujícího příkazu vytvořte kontejner Dockeru konzoly Identity Console:

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

Příklad:

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

POZNÁMKA

- ♦ Smlouvu EULA můžete přijmout nastavením proměnné prostředí `ACCEPT_EULA` na hodnotu `Y`. Smlouvu EULA můžete přijmout také po zobrazení výzvy při spuštění kontejneru Dockeru. Stačí pomocí možnosti `-it` v příkazu k jeho vytvoření nastavit interaktivní režim.
- ♦ Parametr `--volume` ve výše uvedeném příkazu vytvoří svazek, kam se uloží konfigurace a data protokolu. V našem příkladu jsme vytvořili vzorový svazek s názvem `IDConsole-volume`.

-
- 6 Pomocí následujícího příkazu zkopírujte soubor certifikátu serveru z místního systému souborů do kontejneru jako `/etc/opt/novell/eDirAPI/cert/keys.pfx`. Další informace o vytvoření certifikátu serveru najdete v tématu „[Předpoklady](#)“ na straně 9:

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

Příklad:

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

Když se připojíte k více stromům služby eDirectory, musíte získat alespoň jeden certifikát serveru `keys.pfx` pro všechny připojené stromy.

- 7 Pomocí následujícího příkazu zkopírujte soubor certifikátu certifikačního úřadu (`.pem`) z místního systému souborů do kontejneru jako `/etc/opt/novell/eDirAPI/cert/sscert.pem`: Další informace o získání certifikátu certifikačního úřadu najdete v části „[Předpoklady](#)“ na straně 9:

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

Příklad:

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

Pokud se uživatel potřebuje připojit k více stromům eDirectory, prostudujte si oddíl: „[Více stromů s konzolou Identity Console jako Dockerem](#)“ na straně 24

- 8 Změňte konfigurační soubor podle potřeby a pomocí následujícího příkazu zkopírujte soubor (`edirapi.conf`) z místního systému souborů do kontejneru jako `/etc/opt/novell/eDirAPI/conf/edirapi.conf`:

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

Příklad:

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

- 9 Pomocí následujícího příkazu spusťte kontejner Dockeru:

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

Příklad:

```
docker start identityconsole-container
```

POZNÁMKA: V adresáři `/var/lib/docker/volumes/<název_s vazku>/_data/eDirAPI/var/log` najdete následující soubory protokolu:

- ♦ `edirapi.log` – Používá se k protokolování různých událostí v edirapi a odstraňování problémů.
 - ♦ `edirapi_audit.log` – Používá se k protokolování událostí auditu edirapi. Protokoly mají formát auditu CEF.
 - ♦ `container-startup.log` – Používá se k zachycení protokolů instalace kontejneru Dockeru konzoly Identity Console.
-

Více stromů s konzolou Identity Console jako Dockerem

Identity Console umožňuje uživatelům připojit více stromů získáním jednotlivých certifikátů certifikačního úřadu.

Pokud se například připojíte ke třem stromům služby eDirectory, musíte do kontejneru Dockeru zkopírovat všechny tři certifikáty certifikačního úřadu:

```
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
```

Spuštěním následujících příkazů spusťte konzolu Identity Console:

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

Nasazení samostatné konzoly Identity Console

- ♦ „[Nasazení samostatné konzoly Identity Console \(bez Dockeru\)](#)“ na straně 24
- ♦ „[Více stromů se samostatnou konzolou Identity Console](#)“ na straně 26

Nasazení samostatné konzoly Identity Console (bez Dockeru)

V této části je vysvětlen postup nasazení samostatné konzoly Identity Console:

- 1 Přihlaste se na stránce SLD: [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) a přejděte na stránku Software Downloads (Stažení softwaru).
- 2 Vyberte následující:
 - ♦ Produkt: eDirectory
 - ♦ Název produktu: eDirectory per User Sub SW E-LTU
 - ♦ Verze: 9.2
- 3 Stáhněte nejnovější sestavení konzoly Identity Console.
- 4 Extrahujte stažený soubor do složky.
- 5 Otevřete prostředí a přejděte do složky, kam jste sestavení konzoly Identity Console rozbalili.

6 Přihlaste se jako kořenový nebo ekvivalentní uživatel a spusťte následující příkaz:

```
./identityconsole_install
```

7 Přečtěte si úvod a stiskněte klikněte na možnost **ENTER**.

8 Kliknutím na možnost **Y** přijměte licenční smlouvu. Poté se do systému nainstalují všechny potřebné balíčky RPM.

9 Zadejte název hostitele serveru konzoly Identity Console (plně kvalifikovaný název domény) nebo jeho adresu IP.

10 Zadejte číslo portu, na kterém má konzola Identity Console naslouchat. Výchozí hodnota je 9000.

11 Zadejte možnost pro integraci poskytovatele OSP s konzolou Identity Console nebo pro to, aby konzola Identity Console použila přihlášení LDAP.

12 Pokud chcete integrovat poskytovatele OSP s konzolou Identity Console:

1. Zadejte název domény nebo adresu IP serveru služby eDirectory / Sejfu identit s číslem portu LDAPS.

Příklad:

```
192.168.1.1:636
```

2. Zadejte uživatelské jméno služby eDirectory / sejfu identit.

Příklad:

```
cn=admin,ou=org_unit,o=org
```

3. Zadejte heslo služby eDirectory / sejfu identit.

4. Zadejte heslo služby eDirectory / sejfu identit znovu a potvrďte ho.

5. Zadejte název domény nebo adresu IP serveru OSP s číslem portu SSL serveru SSO.

6. Zadejte ID klienta poskytovatele OSP.

7. Zadejte heslo klienta poskytovatele OSP.

8. Zadejte název stromu služby eDirectory / Sejfu identit.

13 Zadejte cestu k důvěryhodnému kořenovému certifikátu (`SSCert.pem`) včetně složky.

Příklad:

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

POZNÁMKA: Uživatel nesmí ve složce certifikátu vytvářet podsložky.

14 Zadejte cestu k certifikátu serveru (`keys.pfx`) včetně názvu souboru.

Příklad:

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

15 Zadejte heslo certifikátu serveru. Zadejte znovu heslo certifikátu serveru a potvrďte tak jeho správnost. Instalace se inicializuje.

POZNÁMKA: V adresáři `/var/opt/novell/eDirAPI/log` najdete následující soubory protokolů:

- ♦ `edirapi.log` – Používá se k protokolování různých událostí v `edirapi` a odstraňování problémů.

- ♦ `edirapi_audit.log` – Používá se k protokolování událostí auditu edirapi. Protokoly mají formát auditu CEF.
- ♦ `identityconsole_install.log` – Používá se k zachycení protokolů instalace konzoly Identity Console.

Protokoly ke spuštění a zastavení procesu konzoly Identity Console jsou k dispozici v souboru `/var/log/messages`.

POZNÁMKA: NetIQ doporučuje, aby při instalaci konzoly Identity Console a služby eDirectory na stejném počítači byla na počítači k dispozici alespoň jedna instance služby eDirectory.

Více stromů se samostatnou konzolou Identity Console

Když se připojíte k více stromům služby eDirectory, musíte získat jednotlivé certifikáty certifikační autority stromu.

Pokud se například připojíte ke třem stromům služby eDirectory, musíte do adresáře `etc/opt/novell/eDirAPI/cert/` zkopírovat všechny tři certifikáty certifikačního úřadu:

```
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
```

Spuštěním jednoho z následujících příkazů spustíte konzolu Identity Console:

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

nebo

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

Konzole Identity Console v systému Windows jako pracovní stanice

Konzoli Identity Console lze spustit v systému Windows jako pracovní stanici a vyžaduje spuštěné služby REST. Po spuštění proto v příkazovém řádku `edirapi.exe` běží proces `eDirAPI`. Pokud je tento terminál `edirapi.exe` uzavřen, konzola Identity Console nebude funkční.

Následující postup popisuje, jak spustit konzolu Identity Console v systému Windows.

- 1 Přihlaste se na stránce 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) a přejděte na stránku Software Downloads (Stažení softwaru).
- 2 Vyberte následující:
 - ♦ Produkt: eDirectory
 - ♦ Název produktu: eDirectory per User Sub SW E-LTU
 - ♦ Verze: 9.2
- 3 Stáhněte soubor `IdentityConsole_<verze>_workstation_win_x86_64.zip`.

4 Extrahujte stažený soubor `IdentityConsole_<verze>_workstation_win_x86_64.zip` do složky.

5 Přejděte do extrahované složky:

`IdentityConsole_150_workstation_win_x86_64\edirapi\cert` a zkopírujte důvěryhodný kořenový certifikát certifikačního úřadu `SSCert.pem` a certifikát serveru `keys.pfx`.

Postup získání certifikátů naleznete v oddílu: „[Požadavky na systém a předpoklady pro pracovní stanici](#)“ na straně 16

Pokud se uživatel potřebuje připojit k více stromům eDirectory, prostudujte si oddíl: „[Více stromů s konzolou Identity Console jako pracovní stanici](#)“ na straně 27

POZNÁMKA: Název certifikátu serveru musí být vždy ve formátu `keys.pfx`.

6 Přejděte do složky, do které bylo sestavení extrahováno, a dvakrát klikněte na soubor `run.bat` (dávkový soubor Windows).

7 Do příkazového řádku zadejte heslo certifikátu serveru (`keys.pfx`).

Terminál procesu eDirAPI (`edirapi.exe`) se spustí a zobrazí se přihlašovací stránka konzoly Identity Console.

POZNÁMKA:

- ♦ Pokud terminál procesu eDirAPI (`edirapi.exe`) již běží, spusťte soubor `identityconsole.exe` ze složky s extrahovaným sestavením.
 - ♦ Uživatelé najdou následující protokoly
`v:\IdentityConsole_150_workstation_win_x86_64\edirapi\log`
`edirapi.log` – Používá se k protokolování různých událostí v `edirapi` a odstraňování problémů.
`edirapi_audit.log` – Používá se k protokolování událostí auditu `edirapi`. Protokoly mají formát auditu CEF.
 - ♦ Přihlášení na základě poskytovatele OSP není v režimu pracovní stanice podporováno.
 - ♦ Pracovní stanice konzoly Identity Console naslouchá pouze na portu 9000. Soubor `edirapi_win.conf` neměňte.
-

Více stromů s konzolou Identity Console jako pracovní stanici

Identity Console umožňuje uživatelům připojit více stromů získáním jednotlivých certifikátů certifikačního úřadu.

1 Zavřete pracovní stanici konzoly Identity Console a terminál eDirAPI.

2 Zkopírujte certifikáty certifikační autority `SSCert.pem` do umístění:

`IdentityConsole_150_workstation_win_x86_64\edirapi\cert`.

Pokud se například chcete připojit ke třem stromům služby eDirectory, zkopírujte certifikáty certifikační autority jako `SSCert1.pem`, `SSCert2.pem` a `SSCert3.pem`.

- 3 Přejděte do složky, do které bylo sestavení extrahováno, a dvakrát klikněte na soubor `run.bat` (dávkový soubor Windows).
- 4 Zadejte heslo `keys.pfx` do řádku terminálu a přihlaste se k požadovanému stromu eDirectory.

Zastavení a opětovné spuštění konzoly Identity Console

- ♦ „Zastavení a opětovné spuštění konzoly Identity Console instalované jako kontejner Dockeru“ na straně 28
- ♦ „Zastavení a opětovné spuštění samostatně instalované konzoly Identity Console“ na straně 28
- ♦ „Zavření a opětovné spuštění pracovní stanice konzoly Identity Console“ na straně 29

Zastavení a opětovné spuštění konzoly Identity Console instalované jako kontejner Dockeru

Konzolu Identity Console zastavíte následujícím příkazem:

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

Konzolu Identity Console restartujete následujícím příkazem:

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

Konzolu Identity Console spustíte následujícím příkazem:

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

Zastavení a opětovné spuštění samostatně instalované konzoly Identity Console

Konzoli Identity Console zastavíte jedním z následujících příkazů:

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

nebo

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

Konzoli Identity Console restartujete jedním z následujících příkazů:

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

nebo

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

Konzoli Identity Console spustíte jedním z následujících příkazů:

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

nebo

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

Zavření a opětovné spuštění pracovní stanice konzoly Identity Console

Aplikaci a proces ukončíte následovně:

- 1 Ukončete desktopovou aplikaci konzoly Identity Console v systému Windows.
- 2 Zastavte proces eDirAPI zavřením terminálu procesu eDirAPI.

Chcete-li znovu spustit pracovní stanici konzoly Identity Console, přejděte do složky, do které bylo sestavení extrahováno, a dvakrát klikněte na soubor `run.bat` (dávkový soubor Windows).

POZNÁMKA: Pokud terminál procesu eDirAPI již běží, spusťte `identityconsole.exe` ze složky s extrahovaným sestavením a znovu spusťte pracovní stanici Identity Console.

Správa trvalosti dat

Spolu s kontejnery konzoly Identity Console se vytvoří také svazky pro zajištění trvalosti dat. Pokud chcete použít konfigurační parametry starého kontejneru, který svazky používá, postupujte takto:

- 1 Pomocí následujícího příkazu zastavte aktuální kontejner Dockeru:

```
docker stop identityconsole-container
```

- 2 S použitím dat aplikace o starém kontejneru uloženém ve svazku Dockeru (`edirapi-volume-1`) vytvořte druhý kontejner:

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

- 3 Spusťte druhý kontejner pomocí následujícího příkazu:

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

- 4 (Volitelné) Nyní můžete první kontejner pomocí následujícího příkazu odebrat:

```
docker rm identityconsole-container
```

Nasazení konzoly Identity Console ve službách Azure Kubernetes

Služba Azure Kubernetes Service (AKS) je spravovaná služba Kubernetes, která umožňuje nasazovat a spravovat clustery. Tato část se věnuje následujícím postupům:

Nasazení konzoly Identity Console v clusteru AKS

Tento oddíl vysvětluje následující postupy pro nasazení konzoly Identity Console v clusteru AKS:

- ♦ „Vytvoření registru Azure Container Registry (ACR)“ na straně 30
- ♦ „Nastavení clusteru Kubernetes“ na straně 31
- ♦ „Vytvoření standardní veřejné adresy IP pro SKU“ na straně 31

- ♦ „Nastavení služby Cloud Shell a připojení ke clusteru Kubernetes“ na straně 31
- ♦ „Nasazení aplikace“ na straně 32

Vytvoření registru Azure Container Registry (ACR)

Azure Container Registry (ACR) je privátní registr využívající služby Azure pro obrázky kontejneru Dockeru.

Podrobnější kroky naleznete v oddílu [Vytvoření registru kontejneru Azure pomocí portálu Azure](#) v tématu Vytvoření registru kontejneru – Portál nebo registr Azure Container Registry (ACR) vytvořte následujícím postupem:

1. Přihlaste se na [portálu Azure](#).
2. Přejděte do nabídky **Vytvořit prostředek > Kontejnery > Registr kontejneru**.
3. Na kartě **Základy** zadejte hodnoty pro **Skupinu prostředků** a **Název registru**. Název registru musí být ve službách Azure jedinečný a musí obsahovat minimálně 5 a maximálně 50 alfanumerických znaků.
Přijměte výchozí hodnoty pro zbývající nastavení.
4. Klikněte na **Zkontrolovat a vytvořit**.
5. Klikněte na tlačítko **Vytvořit**.
6. Přihlaste se k Azure CLI a spuštěním následujícího příkazu se přihlaste do registru Azure Container Registry.

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

Příklad:

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

7. Načtete přihlašovací server registru Azure Container Registry pomocí příkazu:

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

Příklad:

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

8. Pomocí následujícího příkazu označte místní bitovou kopii konzoly Identity Console názvem přihlašovacího serveru ACR (registryname.azurecr.io):

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

Příklad:

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

9. Odešlete označenou bitovou kopii do registru.

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

Příklad:

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

10. Pomocí následujícího příkazu načtete seznam bitových kopií v registru:

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

Nastavení clusteru Kubernetes

Vytvoří prostředek služby Kubernetes pomocí portálu Azure nebo CLI.

Podrobnější kroky vytvoření prostředku služby Kubernetes v Azure s uzlem naleznete v tématu [Create an AKS Cluster](#) (Vytvoření clusteru AKS) ve stručné příručce [Azure Quickstart](#).

POZNÁMKA:

- ♦ Jako síť je třeba vybrat Azure CNI.
 - ♦ Vyberte existující virtuální síť (kde je server služby eDirectory nasazen v podsíti).
 - ♦ Vyberte existující registr kontejneru, kde je k dispozici bitová kopie konzoly Identity Console.
-

Vytvoření standardní veřejné adresy IP pro SKU

Prostředek veřejné adresy IP v rámci skupiny prostředků clusteru Kubernetes funguje jako IP pro vyvážení zatížení aplikace.

Podrobné kroky naleznete v oddílu [Vytvoření veřejné adresy IP pomocí portálu Azure](#) v tématu [Vytvoření veřejné adresy IP – Portál](#).

Nastavení služby Cloud Shell a připojení ke clusteru Kubernetes

Použijte službu Cloud Shell, která je k dispozici na portálu Azure pro všechny operace.

Chcete-li nakonfigurovat službu Cloud Shell na portálu Azure, prostudujte si část [Start Cloud Shell](#) (Spuštění služby Cloud Shell) ve stručné příručce [Bash – Quickstart](#) nebo následujícími kroky nakonfigurujte službu Cloud Shell a připojte ji ke clusteru Kubernetes:

1. Na portálu Azure klikněte na tlačítko  a otevřete službu Cloud Shell.

POZNÁMKA: Ke správě clusteru Kubernetes použijte klienta příkazového řádku Kubernetes `kubectl`. Pokud používáte službu Azure Cloud Shell, je klient `kubectl` již nainstalován.

2. Pomocí následujícího příkazu nakonfigurujte klienta `kubectl` pro připojení ke clusteru Kubernetes:

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

Příklad:

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

3. Ověřte seznam uzlů clusteru pomocí příkazu:

```
kubectl get nodes
```

Nasazení aplikace

K nasazení konzoly Identity Console můžete použít ukázkové soubory `idc-services.yaml`, `idc-statefulset.yaml`, `idc-storageclass.yaml` a `idc-pvc.yaml`.

Podle požadavku můžete také vytvořit vlastní soubory yaml.

1. Pomocí příkazu níže vytvořte prostředek třídy úložiště:

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

Příklad:

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

(Volitelné) Další informace o tom, jak dynamicky vytvářet a používat trvalý svazek se sdílenou složkou Azure, naleznete v tématu [Dynamically create and use a persistent volume with Azure Files in Azure Kubernetes Service \(AKS\)](#) (Dynamické vytváření a používání trvalého svazku se soubory Azure ve službě Azure Kubernetes Service (AKS)).

Níže je uveden ukázkový soubor prostředku třídy úložiště:

```
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
~
```

Prostředek třídy úložiště umožňuje poskytování dynamického úložiště. Používá se k definování toho, jak se vytváří sdílená složka Azure.

2. Pomocí příkazu níže si můžete zobrazit podrobnosti třídy úložiště:

```
kubectl get sc
```

3. Pomocí souboru `idc-pvc.yaml` vytvořte prostředek pvc:

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

Příklad:


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

Níže je uveden ukázkový soubor prostředku pvc:

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

Prostředek nároku trvalého svazku vytvoří sdílenou složku. Nárok trvalého svazku (Persistent Volume Claim, PVC) využívá objekt třídy úložiště k dynamickému poskytování sdílené složky Azure.

4. Nahrajte edirapi.conf, certifikát certifikačního úřadu a certifikát serveru do prostředí cloudu.

Klikněte na ikonu tlačítka **Nahrát/stáhnout soubory**  v prostředí cloudu a nahrajte soubory edirapi.conf, SSCert.pem a keys.pfx.

POZNÁMKA: edirapi.conf má parametr „origin“. Zde je potřeba poskytnout adresu IP, pomocí které lze přistupovat k aplikaci konzoly Identity Console. (použijte adresu IP, která se vytvoří v oddílu „[Vytvoření standardní veřejné adresy IP pro SKU](#)“ na straně 31.)

Nasazení konzoly Identity Console vyžaduje certifikát serveru (keys.pfx).

Při vytváření certifikátu serveru je jako alternativní název subjektu třeba zadat platný název DNS.

Kroky sestavení platného názvu DNS:

Typický pod nasazený pomocí StatefulSet má název DNS podobný názvu níže - {statefulsetname}-{ordinal}.{servicename}.{namespace}.svc.cluster.local

- ♦ Pokud je název StatefulSet v souboru idconsole-statefulset.yaml idconsole-app, pak statefulsetname = idconsole-app
- ♦ Pokud se jedná o první pod, pak pořadí = 0
- ♦ Pokud definujete serviceName v souboru idconsole-statefulset.yaml jako idconsole, pak serviceName = idconsole
- ♦ Pokud je to ve výchozím nastavení obor názvů, pak obor názvů=výchozí

Výstup: idconsole-app-0.idconsole.default.svc.cluster.local

5. Vytvořte prostředek configmap v clusteru Kubernetes, který obsahuje konfigurační soubory společně s certifikáty.

Před spuštěním příkazu zkontrolujte, že jsou v adresáři obsaženy soubory (edirapi.conf, SSCert.pem a keys.pfx).

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

Příklad:

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

6. Pomocí příkazu popisu kubectl zobrazte podrobnosti objektu configmap:


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

Příklad:

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

7. Vytvořte prostředek StatefulSet k nasazení kontejneru.

Spuštěním příkazu níže nasadíte kontejner:

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

Příklad:

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

Níže je uveden ukázkový soubor prostředku StatefulSet:

```
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. Spuštěním následujícího příkazu ověřte stav nasazeného podu:

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

9. Vytvořte prostředek služby typu loadBalancer.

Typ služby uvedený v souboru yaml je loadBalancer.

Pomocí příkazu níže vytvořte prostředek služby:

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

Příklad:

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

Níže je uveden ukázkový soubor prostředku služby:

```
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
```

Pomocí příkazu níže zkontrolujte EXTERNÍ adresu IP (nebo loadBalancerIP):

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

10. Spusťte adresu URL pomocí EXTERNÍ adresy IP (nebo adresy loadBalancerIP).

Příklad:

```
https://<EXTERNÍ IP>:9000/identityconsole
```

Změna certifikátu serveru

Tento oddíl obsahuje informace o změně certifikátu serveru v kontejneru Dockeru a samostatné konzole Identity Console.

- ♦ [„Změna certifikátu serveru v kontejneru Dockeru“ na straně 35](#)
- ♦ [„Změna certifikátu serveru v samostatné konzole Identity Console“ na straně 36](#)

Změna certifikátu serveru v kontejneru Dockeru

Následujícím postupem změňte certifikát serveru v kontejneru Dockeru:

- 1 Spuštěním následujícího příkazu zkopírujte nový certifikát serveru do libovolného umístění kontejneru.

Příklad:

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

- 2 Pomocí následujícího příkazu se přihlaste ke kontejneru:

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

- 3 Spuštěním příkazu NLPCERT uložíte klíče jako pseudo uživatel:

```
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 Ukončete konzolu kontejneru pomocí příkazu:

```
exit
```

- 5 Restartujte kontejner zadáním:

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

Změna certifikátu serveru v samostatné konzole Identity Console

Následujícím postupem změňte certifikát serveru v samostatném kontejneru:

- 1 Spuštěním příkazu NLPCERT uložte klíče:

```
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 Restartujte konzolu Identity Console:

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

3 Inovace konzoly Identity Console

Tato kapitola popisuje postup inovace konzoly Identity Console na nejnovější verzi. V rámci přípravy na instalaci si projděte seznam předpokladů a požadavků na systém, který najdete v části [Kapitola 1, „Plánování instalace konzoly Identity Console“](#), na straně 9.

Tato část se věnuje následujícím postupům:

- „Inovace konzoly Identity Console jako kontejneru Dockeru“ na straně 37
- „Inovace samostatné konzoly Identity Console (bez Dockeru)“ na straně 39
- „Inovace kontejneru poskytovatele OSP“ na straně 40

Inovace konzoly Identity Console jako kontejneru Dockeru

Jakmile je k dispozici nová verze bitové kopie konzoly Identity Console, může správce provést inovaci, při níž nasadí kontejner s nejnovější verzí konzoly. Před inovací ověřte, že jste všechna potřebná data související s aplikací trvale uložili ve svazcích Dockeru. Postup inovace konzoly Identity Console pomocí kontejneru Dockeru:

- 1 Stáhněte a načtěte ze stránky softwarové licence a stahování [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/) nejnovější verzi bitové kopie Dockeru a nainstalujte nejnovější verzi konzoly Identity Console podle pokynů v části „[Nasazení konzoly Identity Console](#)“ na straně 19.

- 2 Jakmile načtete nejnovější bitovou kopii Dockeru, zastavte pomocí následujícího příkazu aktuální kontejner Dockeru:

```
docker stop identityconsole-container
```

- 3 (Volitelné) Vytvořte zálohu sdíleného svazku.

- 4 Spuštěním následujícího příkazu odstraňte stávající kontejner konzoly Identity Console:

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

Příklad:

```
docker rm identityconsole-container
```

- 5 (Volitelné) Odstraňte zastaralou bitovou kopii Dockeru pro konzolu Identity Console spuštěním následujícího příkazu:

```
docker rmi identityconsole
```

- 6 Pomocí následujícího příkazu vytvořte kontejner Dockeru konzoly Identity Console:

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

Příklad:

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

POZNÁMKA

- ♦ Smlouvu EULA můžete přijmout nastavením proměnné prostředí `ACCEPT_EULA` na hodnotu `Y`. Smlouvu EULA můžete přijmout také po zobrazení výzvy při spuštění kontejneru Dockeru. Stačí pomocí možnosti `-it` v příkazu k jeho vytvoření nastavit interaktivní režim.
- ♦ Parametr `--volume` ve výše uvedeném příkazu vytvoří svazek, kam se uloží konfigurace a data protokolu. V našem příkladu jsme vytvořili vzorový svazek s názvem `IDConsole-volume`.

-
- 7 Pomocí následujícího příkazu zkopírujte soubor certifikátu serveru z místního systému souborů do nově vytvořeného kontejneru jako `/etc/opt/novell/eDirAPI/cert/keys.pfx`:

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

Příklad:

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

Když se připojíte k více stromům služby eDirectory, musíte zkopírovat alespoň jeden certifikát serveru `keys.pfx` pro všechny připojené stromy.

- 8 Pomocí následujícího příkazu zkopírujte soubor certifikátu certifikačního úřadu (`.pem`) z místního systému souborů do nově vytvořeného kontejneru jako `/etc/opt/novell/eDirAPI/cert/SSCert.pem`:

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

Příklad:

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

Když se připojíte k více stromům služby eDirectory, musíte získat jednotlivé certifikáty certifikační autority pro všechny připojené stromy. Pokud se například připojíte ke třem stromům služby eDirectory, musíte do kontejneru Dockeru zkopírovat všechny tři certifikáty certifikačního úřadu:

```
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: Počínaje konzolou Identity Console 1.4 konfigurační soubor (`edirapi.conf`) výslovně nezahrnuje parametry „`ldapuser`“, „`ldappassword`“ a „`ldapserver`“. Hodnota parametru „`bcert`“ musí zahrnovat cestu k adresáři pro důvěryhodné kořenové certifikáty. Příklad: `bcert = "/etc/opt/novell/eDirAPI/cert/"`. A parametr „`origin`“ je nezávislý na parametru „`check-origin`“ a je povinný při použití konfigurace DNS.

- 9 Pomocí následujícího příkazu zkopírujte konfigurační soubor (`edirapi.conf`) z místního systému souborů do nově vytvořeného kontejneru jako `/etc/opt/novell/eDirAPI/conf/edirapi.conf`:

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

Příklad:

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

- 10 Spusťte druhý kontejner pomocí následujícího příkazu:

```
docker start identityconsole-container
```

- 11 Stav běžícího kontejneru zjistíte spuštěním následujícího příkazu:

```
docker ps -a
```

Inovace samostatné konzoly Identity Console (bez Dockeru)

V této části je vysvětlen postup inovace samostatné konzoly Identity Console:

- 1 Stáhněte `IdentityConsole_<verze>_Containers.tar.gz` ze stránky [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/)
- 2 Přihlaste se k SLD, přejděte na stránku Software Download SLD a klikněte na **Download** (Stáhnout).
- 3 Vyberte produkt: **eDirectory** > Název produktu: **eDirectory per User Sub SW E-LTU** > Verze: **9.2**
- 4 Stáhněte nejnovější sestavení konzoly Identity Console.
- 5 Pomocí následujícího příkazu extrahujte stažený soubor:

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

- 6 Přejděte do složky, do které jste extrahovali sestavení Identity Console.
- 7 Zkopírujte všechny důvěryhodné kořenové certifikáty stromů služby eDirectory, ke kterým se chcete připojit, do složky. Ke kopírování důvěryhodného kořenového certifikátu do složky použijte následující příkaz:

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

Příklad:

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

- 8 Spusťte následující příkaz:

```
./identityconsole_install
```

- 9 Zadejte cestu ke složce důvěryhodných kořenových certifikátů použité v **kroku 4**.
- 10 Konzole Identity Console se úspěšně inovuje.

Inovace kontejneru poskytovatele OSP

Při inovaci kontejneru poskytovatele OSP postupujte takto:

- 1 Stáhněte a načtěte nejnovější verzi bitové kopie poskytovatele OSP se stránky [Software License and Download \(https://sld.microfocus.com/\)](https://sld.microfocus.com/).

Příklad:

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

- 2 Jakmile načtete nejnovější bitovou kopii poskytovatele OSP, zastavte pomocí následujícího příkazu aktuální kontejner poskytovatele OSP:

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

- 3 (Volitelné) Vytvořte zálohu sdíleného svazku.

- 4 Spuštěním následujícího příkazu odstraňte stávající kontejner poskytovatele OSP:

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

Příklad:

```
docker rm OSP_Container
```

- 5 Přejděte do adresáře, který obsahuje úložiště klíčů (`tomcat.ks`) a soubor vlastností tiché instalace, odstraňte existující úložiště klíčů (`tomcat.ks`) a zachovejte existující složku poskytovatele OSP. Vygenerujte nové úložiště klíčů (`tomcat.ks`) s velikostí klíče 2048. Další informace naleznete v **kroku 4** v části [Nasazení kontejneru poskytovatele OSP](#) Instalační příručky konzoly Identity Console.

- 6 Pomocí následujícího příkazu nasadte kontejner:

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

Příklad:

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

4 Odinstalace konzoly Identity Console

Tato kapitola popisuje proces odinstalace konzoly Identity Console:

- ♦ „Postup odinstalace v prostředí Dockeru“ na straně 41
- ♦ „Postup odinstalace samostatné konzoly Identity Console (bez Dockeru)“ na straně 41

Postup odinstalace v prostředí Dockeru

Pokud chcete odinstalovat konzolu Identity Console nasazenou jako kontejner Dockeru, postupujte takto:

- 1 Zastavte kontejner konzoly Identity Console:

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

- 2 Spuštěním následujícího příkazu odeberte kontejner Dockeru s konzolou Identity Console:

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

- 3 Spuštěním následujícího příkazu odeberte bitovou kopii Dockeru:

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

- 4 Odeberte svazek Dockeru:

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

POZNÁMKA: Když svazek odeberete, odeberou se ze serveru související data.

Postup odinstalace samostatné konzoly Identity Console (bez Dockeru)

Pokud chcete odinstalovat samostatně nasazenou konzolu Identity Console, postupujte takto:

- 1 Na počítači, kde je konzola Identity Console nainstalována, přejděte do adresáře `/usr/bin`.

- 2 Spusťte následující příkaz:

```
./identityconsoleUninstall
```

- 3 Konzole Identity Console se úspěšně odinstaluje.

POZNÁMKA: Když je na počítači nainstalována služba eDirectory nebo jiný produkt NetIQ, musí uživatel ručně odinstalovat *nici* a *openssl*.
