ESET PROTECT

Příručka pro nasazení virtuální appliance

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

ESET PROTECT byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte https://www.eset.cz.

Technická podpora: https://servis.eset.cz

REV. 2024-04-12

ESET PROTECT Virtuální appliance

ESET PROTECT virtuální appliance (ESET PROTECT VA) je určena pro uživatele, kteří chtějí ESET PROTECT provozovat ve virtualizovaném prostředí. ESET PROTECT virtuální appliance představuje nejjednodušší a nejrychlejší způsob pro zprovoznění ESET PROTECT ve vaší síti (rychlejší než instalace prostřednictvím all-in-one balíčku nebo po jednotlivých komponentých).

ESET PROTECT virtuální appliance je připravena pro nasazení do většiny virtuálních prostředí. Podporuje nativní/bare-metal hypervizory (VMware vSphere/ESXi a Microsoft Hyper-V), stejně tak hostované hypervizory běžící na desktopovém operačním systému (VMware Workstation, VMware Player, Oracle VirtualBox). Pro více informací přejděte do kapitoly podporované hypervizory.

V této uživatelské příručce naleznete informace týkající se nasazení a správy ESET PROTECT virtuální appliance, včetně:

- Konzole pro správu ESET PROTECT virtuální appliance – jednoduché **textové grafické rozhraní** (TUI) s hlavním menu. Při využití textových příkazů dostupných v rozhraních budete pouze vyzváni na zadání požadovaných hodnot. Proto ESET PROTECT virtuální appliance dokáží používat a spravovat uživatelé, kteří nemají pokročilé znalosti a zkušenosti s operačním systémem CentOS 7 nebo jiných linuxových distribucí. Mezi důležitější funkce dostupné v tomto rozhraní patří:
    - Nastavení statické IP adresy – pokud DHCP server nepřiřadil ESET PROTECT VA IP adresu, provedete to ručně pomocí tohoto skriptu.
    - Migrace databáze – tuto funkci využijete při aktualizaci nebo migraci ESET PROTECT VA.
    - Zálohování a obnovení ESET PROTECT databáze – tyto funkce jsou důležité v rámci strategie obnovení při ztrátě dat a využijete je v případě problémů s ESET PROTECT VA.
    - Tovární nastavení – tímto skriptem vrátíte konfiguraci virtuální appliance do výchozího stavu, ve kterém je po čerstvém nasazení. To využijete v případě, kdy jste narazili na problémy při běhu virtuálního stroje s ESET PROTECT. Pro zabránění ztráty dat mějte připravenou zálohu databáze.
- Webmin – rozhraní pro správu – webové rozhraní třetí strany, které usnadňuje správu operačního systému Linux. Prostřednictvím intuitivního rozhraní dostupného z webového prohlížeče vám budete schopni vzdáleně spravovat ESET PROTECT virtuální appliance. V této příručce naleznete popsány nejdůležitější moduly Webminu.

O této nápovědě

V této **příručce k nasazení virtuální appliance** najdete instrukce k nasazení a konfiguraci ESET PROTECT Virtual Appliance (ESET PROTECT VA). Tento průvodce je určen pro všechny, kteří chtějí nasadit, spravovat a aktualizovat ESET PROTECT VA.

Z důvodu zachování konzistence a zabránění nejasnostem vychází použitá terminologie v této příručce z názvosloví ESET PROTECT. Používáme rovněž jednotnou sadu symbolů na zvýraznění částí kapitol, které jsou zvlášť důležité, případně by neměli uniknout vaší pozornosti.

i Poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.

Tato akce vyžaduje vaši pozornost a neměli byste ji ignorovat. Obvykle obsahuje nekritické, ale však důležité informace.

Kritická informace, které byste měli věnovat pozornost. Upozornění jsou umístěna tak, aby vás včas varovala a zároveň vám pomohla vyvarovat se chybám, které by mohly mít negativní následky. Prosím, důkladně si přečtěte text ohraničený tímto označením, protože se týká velmi citlivých systémových nastavení nebo upozorňuje na možná rizika.

Příklad popisující uživatelský scénář, který doplní danou kapitolu. Příklady používáme pro vysvětlení složitějších témat.

Konvence	Význam
Tučné písmo	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.
Kurzíva	Zástupné znaky pro informace, které máte zadat. Například název souboru nebo cesta k souboru znamená, že máte zadat skutečnou cestu nebo název souboru.
`Courier New`	Příklady kódů nebo příkazů.
Hypertextový odkaz	Poskytuje rychlý přístup do odkazovaných kapitol nebo externích zdrojů. Hypertextové odkazy jsou zvýrazněny modře, mohou být podtržené.
%ProgramFiles%	Systémová složka operačního systému Windows, do které se standardně instalují programy a další součásti systému.

- Online příručka je primárním zdrojem nápovědy. V případě funkčního připojení k internetu se automaticky zobrazí nejnovější verze online příručky. V navigační části online verze příručky k ESET PROTECT naleznete navigaci do jejích jednotlivých částí: Instalace/Aktualizace, Administrace, Nasazení VA a SMB příručka.
- Související informace tak naleznete jednoduchým procházením této struktury stránek. Pro nalezení požadovaných informací můžete využít vyhledávací pole v horní části.

Po otevření uživatelské příručky z navigační lišty umístěné v horní části budou výsledky vyhledávání omezeny na obsah dané příručky. Například, otevřete-li administrační část příručky, ve výsledcích vyhledávání nebudou témata z instalační/aktualizační příručky ani nápovědy pro nasazení VA.

- V Databázi znalostí naleznete odpovědi na nejčastější dotazy stejně jako doporučené řešení mnoha situací. Články pravidelně aktualizujeme a připravujeme návody na řešení aktuálních situací.
- ESET fórum představuje jednoduchý způsob, jak ESET uživatelé mohou požádat o radu a pomoci ostatním. Můžete sem umístit váš problém nebo dotaz týkající se produktu ESET.
- Váš názor/zpětnou vazbu na konkrétní kapitolu příručky odešlete následujícím způsobem: V dolní části stránky klikněte na odkaz **Byla pro vás tato informace užitečná?**

Předpoklady

Před nasazením ESET PROTECT virtuální appliance je nutné splnit níže uvedené předpoklady:

- Musíte používat podporovaný hypervizor.
- Pokud používáte VMware Workstation/Player nebo Oracle VirtualBox, musíte jej provozovat na podporovaném operačním systému.

- Ujistěte, že se synchronizuje čas mezi hostem a hostovaným operačním systémem.

- V BIOSu hostitelského systému musíte mít aktivní technologii **VT**. V závislosti na výrobci základní desky se funkce může jmenovat VT, Vanderpool Technology, Virtualization Technology, VMX nebo Virtual Machine Extensions. Toto nastavení zpravidla naleznete v BIOSu v sekci bezpečnost (security). Umístění tohoto nastavení závisí na výrobci vašeho systému.

- Síťový adaptér nastavte do režimu **Bridged** nebo **NAT**. V průběhu prvotní konfigurace ESET PROTECT VA můžete zadat podrobné informace o síti stejně jako doméně, které jsou potřebné pro úspěšný běh úlohy synchronizace statické skupiny.

- Pokud máte síťový adaptér nakonfigurovaný do režimu **NAT**, aby byl virtuální stroj s ESET PROTECT dostupný z internetu, musíte mít správně nastaven port forwarding. Potřebné porty jsou zobrazeny na úvodní obrazovce ESET PROTECT VA po dokončení prvotní konfigurace.

- ESET PROTECT virtuální appliance podporuje pouze IPv4 prostředí. Podporu IPv6 můžete nakonfigurovat ručně, ale tento scénář není podporován.

Doporučujeme vytvořit snapshot nově nasazené, nakonfigurované a domény připojení ESET PROTECT virtuální appliance. Rovněž doporučujeme vytvořit snapshot před tím, než začnete nasazovat ESET Management Agenty na koncové stanice.

- Při nasazení ESET PROTECT a ESET PROTECT MDM VAgentHost jsou vyžadovány certifikáty. Před jejich instalací již musíte mít funkční ESET PROTECT Server, abyste mohli vygenerovat certifikáty, které jsou používány pro šifrování komunikace mezi jednotlivými komponentami ESET PROTECT infrastruktury.

Doporučená konfigurace

V závislosti na velikosti vaší sítě a počtu klientů, kteří se budou k ESET PROTECT virtuální appliance připojovat, vezměte v potaz minimální a doporučenou konfiguraci virtuálního stroje.

Následující hodnoty platí pro virtuální appliance ESET PROTECT Server and ESET PROTECT MDM:

Počet klientů	Počet jader	Velikost RAM	Ostatní požadavky
méně než 5000 klientů	4	4 GB	Thick provisioned disk, ručně upravte paměťový limit MySQL.
více než 5000 klientů	8	8 GB	V závislosti na počtu klientů navyšte systémové prostředky virtuálního stroje ESET PROTECT, abyste předešli výkonovým problémům.

Pokud plánujete spravovat více než 5.000 klientů, doporučujeme ESET PROTECT Server/MDM nainstalovat na fyzický stroj (Microsoft Windows Server + Microsoft SQL Server).

Podporované hypervizory

ESET PROTECT Virtuální appliance (*protect_appliance.ova* je založena na virtuálním hardwaru typu `vmx-07`.

Virtuální appliance podporuje výhradně níže uvedené hypervizory. V jiným hypervizorech ji budete provozovat na vlastní riziko.

Hypervisor	Verze	ESET PROTECT Server Appliance	ESET PROTECT MDM Appliance
VMware vSphere/ESXi	6.5 a novější	✔	✔
VMware Workstation	9 a novější	✔	✔
VMware Player	7 a novější	✔	✔
Microsoft Hyper-V	Server 2012, 2012 R2, 2016, 2019	✔	✔
Oracle VirtualBox	6.0 a novější	✔	✔
Citrix	7.0 a novější	✔	✔

Pro přiřazení IP adresy ESET PROTECT VA doporučujeme využít DHCP server. IP adresa je nezbytná pro konfiguraci ESET PROTECT VA prostřednictvím webového rozhraní. Pokud ve své síti nemáte DHCP server, přiřaďte virtuální appliance statickou IP adresu ručně.

Implementace a údržba ESET PROTECT VA

Úspěšné zprovoznění ESET PROTECT virtuální appliance se skládá z následujících kroků:

1. Nasazení ESET PROTECT Appliance – nejprve je nutné *OVA* soubor ESET PROTECT virtuální appliance naimportovat do vašeho hypervizoru.

2. Konfigurace ESET PROTECT – následně prostřednictvím webového průvodce proveďte prvotní konfiguraci virtuální appliance. V průběhu konfigurace si vyberte typ appliance a vyplňte potřebná nastavení pro běh vámi vybrané ESET PROTECT virtuální appliance.

Veškeré další akce budete provádět prostřednictvím textového grafického rozhraní, případně Webminu:

1. Konzole pro správu ESET PROTECT – grafická konzole pro provádění nejdůležitějších akcí jako je konfigurace sítě, zálohování databáze, změna hesel atp. Z této konzole se můžete také dostat do systémového terminálu.

2. Webmin webové rozhraní – webové rozhraní třetí strany, prostřednictvím kterého můžete snadno spravovat operační systém CentOS, na kterém běží ESET PROTECT VA.

Zpracovány máme scénáře pro aktualizaci, migraci a disaster recovery:

Aktualizace a migrace ESET PROTECT – v této kapitole naleznete informace týkající se procesu aktualizace ESET PROTECT virtuální appliance na nejnovější verzi. Stejné kroky je možné použít také při migraci na jinou ESET PROTECT virtuální appliance.

Disaster recovery – tyto kroky využijte v případě, kdy ESET PROTECT VA nefunguje a není ji možné opravit, nebo není možné obnovit poškozenou instanci ESET PROTECT.

Stažení ESET PROTECT virtuální appliance

ESET PROTECT Virtual Appliance distribuujeme jako OVA soubor (Open Virtualization Appliance). Dostupná je ke stažení na webových stránkách společnosti ESET. Appliance nabízíme jako soubor protect_appliance.ova.

Pokud plánujete virtuální appliance provozovat v prostředí Microsoft Hyper-V, stáhněte si místo *OVA*

souborupro tect_appliance.vhd.zip.

- *protect_appliance.ova* – obsahuje několik typů ESET PROTECT appliance. Typ appliance si vyberete až po nasazení tohoto souboru. K dispozici jsou následující typy appliance:

  - **ESET PROTECT Server** – virtuální počítač, na kterém běží ESET PROTECT Server. Dále obsahuje Rogue Detection Sensor.

  - **ESET PROTECT MDM** – virtuální počítač, na kterém běží komponenta pro správu mobilních zařízení. Pokud nechcete do internetu vypublikovat celý ESET PROTECT Server, můžete pro správu mobilních zařízení z internetu zpřístupnit pouze ESET PROTECT MDM.

OVA soubor je šablona s operačním systémem CentOS 7. Pro nasazení *OVA* souboru ESET PROTECT VA postupujte podle kroků v závislosti na vámi používaném hypervizoru. Při použití `protect_appliance.ova` se můžete rozhodnout, jaký typ ESET PROTECT virtuální appliance chcete nasadit. Po vybrání typu appliance můžete začít prostřednictvím webového rozhraní s konfigurací ESET PROTECT VA. Po nasazení *OVA* souboru si vyberte typ appliance a proveďte její konfiguraci. virtuální appliance máte hotový virtuální počítač s ESET PROTECT, případně jeho komponentami.

Před tím, než se pustíte do nasazení, se ujistěte, že splňujete všechny předpoklady.

Po úspěšné nasazení a dokončení prvotní konfigurace se můžete k ESET PROTECT serveru připojit prostřednictvím ESET PROTECT Web Console a ESET PROTECT začít používat.

> ESET nabízí ESET PROTECT virtuální appliance, nicméně neposkytuje technickou podporu k použitému operačnímu systému a není zodpovědný za jeho údržbu ani jeho částí. ESET PROTECT virtuální appliance je navržena tak, aby její nasazení a používání bylo co nejjednodušší a je založena na veřejně dostupném operačním systému, který obsahuje komponenty třetích stran. Správa a aktualizace těchto komponent je výhradně na administrátorovi ESET PROTECT VA. Operační systém doporučujeme pravidelně aktualizovat, aby se zabránilo bezpečnostním problémům.

Hesla na ESET PROTECT virtuální appliance

V ESET PROTECT virtuální appliance se používá několik odlišných uživatelských účtů. Jejich vysvětlení naleznete v níže uvedené tabulce:

Typ účtu	Výchozí heslo	Popis a použití
Uživatel root operačního systému (CentOS)	`eraadmin`	Pod tímto uživatelem se přihlašujete do ESET PROTECT virtuální appliance. Pod tímto uživatelem si můžete otevřít konzoli pro správu ESET PROTECT VA a přihlásit se do Webmin webového rozhraní. Tento uživatel může rovněž provést Factory reset nebo použít funkci Pull database from other server. Obvykle je toto heslo ve virtuální appliance označováno jako **VM password**.
Databázový uživatel root (MySQL)	`eraadmin`	Jedná se o účet s oprávněním root pro přístup k MySQL databázovému serveru. Pod tímto uživatelem budete provádět zálohu nebo obnovení databáze. Obvykle je toto heslo ve virtuální appliance označováno jako **database root password**.

Typ účtu	Výchozí heslo	Popis a použití
Administrátor ESET PROTECT Web Console	definované v průběhu konfigurace ESET PROTECT	Jedná se o důležité heslo, prostřednictvím kterého se přihlásíte do ESET PROTECT Web Console.

Výchozí heslo se změní v průběhu konfigurace ESET PROTECT. Vámi definované heslo v průběhu konfigurace ESET PROTECT VA se použije pro všechny výše uvedené uživatelské účty. Nicméně, pro každý uživatelský účet si můžete následně nastavit unikátní heslo. Nakolik je bezpečnější používat odlišná hesla, jejich správa může být komplikovanější. Z tohoto důvodu doporučujeme osvojit si efektivní způsob správy více hesel používaných na ESET PROTECT VA.

Po nasazení ESET PROTECT virtuální appliance je heslo pro všechny výše uvedené účty společné: `eraadmin`. Ke změně hesel dojde až při prvotní konfiguraci appliance.

V případě, že zapomenete heslo k některému z výše uvedených účtů, můžete si je změnit prostřednictvím konzole pro správu. Případně přejděte do kapitoly Zapomněl jsem heslo pro přístup do ESET PROTECT VA, co mám dělat.

Proces nasazení ESET PROTECT virtuální appliance

Vyberte si vámi používaný hypervizor a postupujte podle dalších kroků pro nasazení appliance:

- vSphere
- VMware Workstation/Player
- Microsoft Hyper-V
- Oracle VirtualBox
- Citrix

vSphere

Nasazení ESET PROTECT VA prostřednictvím vSphere klienta

1. Připojte se prostřednictvím vSphere klienta k vCenter nebo přímo k ESXi serveru.

2. Pokud používáte vSphere Client, v hlavním menu aplikace klikněte na **File** > **Deploy OVF Template**. V případě vSphere Web Client klikněte na **Actions** > **Deploy OVF Template**.

3. Klikněte na tlačítko **Browse** a vyberte soubor *protect_appliance.ova* stažený z webových stránek společnosti ESET a klikněte na **Open**.

Nepodporované verze VMware ESXi neakceptují SHA-256 certifikáty. Pokud se vám v průběhu importování ESET PROTECT VA 9.1 zobrazí chyba související s certifikátem, bude nutné z *.ova* balíčku odstranit certifikát (*.cert* soubor). Následně bude možné v nasazení pokračovat.

4. V dialogovém okně OVF Template Details klikněte na tlačítko **Next**.

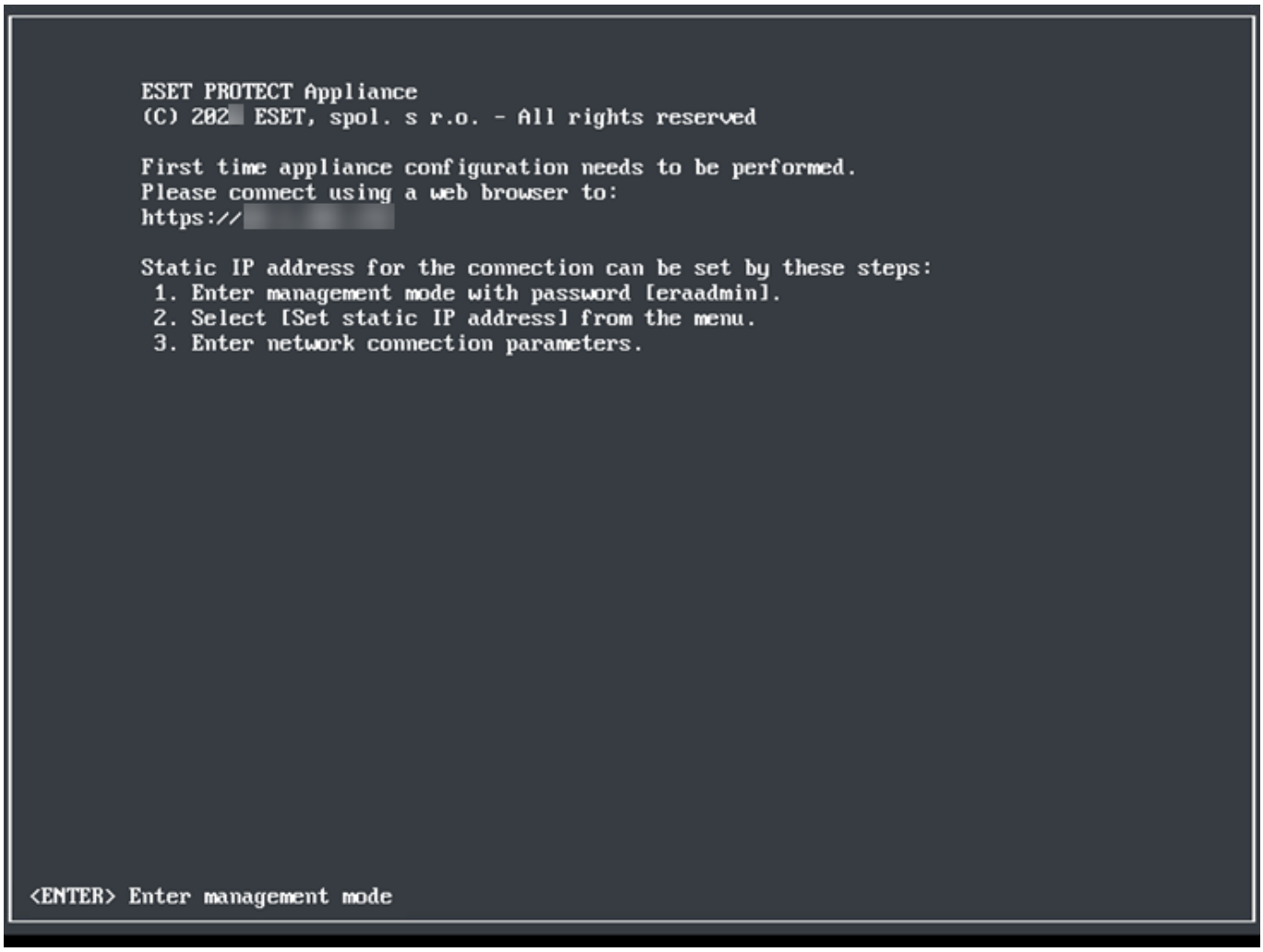
5. Přečtěte si a odsouhlaste licenční ujednání s koncovým uživatelem (EULA).

6. Dále postupujte podle instrukcí na obrazovce a vyplňte následující informace týkající se nového virtuálního počítače:

- **Name and Location** – zadejte název nově vytvářené šablony a umístění, kam chcete virtuální počítače uložit.
- **Host / Cluster** – vyberte hosta nebo cluster, na kterém šablona poběží.
- **Resource Pool** – vyberte resource pool, do které chcete šablonu nasadit.
- **Storage** – vyberte umístění, kam chcete uložit soubory virtuálního počítače.
- **Disk Format** – vyberte formát disku, který chcete použít.
- **Network Mapping** – vyberte síť, do které chcete virtuální stroj připojit. Ujistěte se, že jste vybrali síť, ve kterém je vytvořen IP pool.

7. Po kliknutí na tlačítko **Next** se zobrazí souhrn konfigurace a kliknutím na tlačítko **Finish** spustíte proces vytvoření virtuálního stroje. Na základě vámi definované konfigurace se nyní vytvoří virtuální počítač.

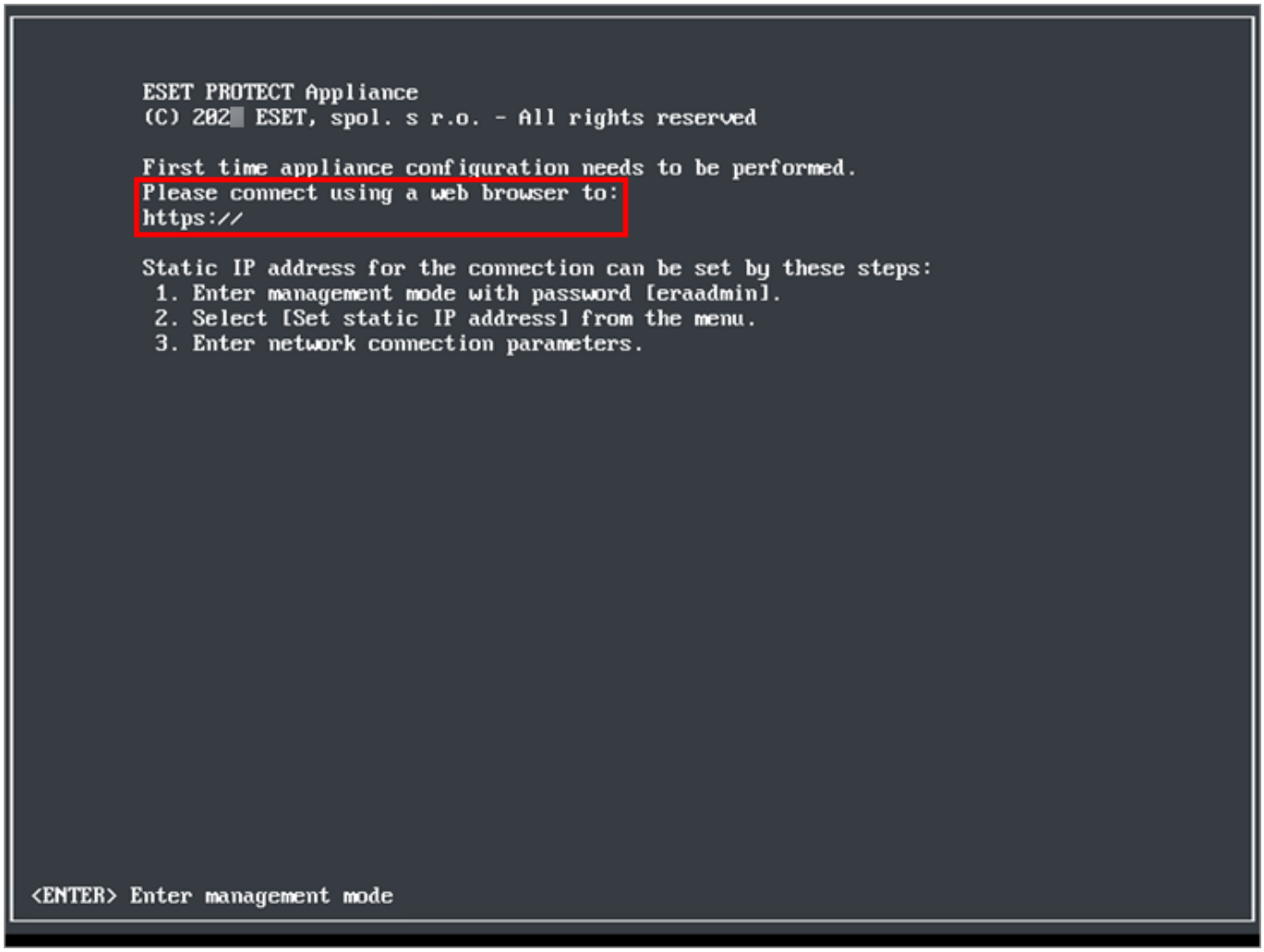
8. Po úspěšném vytvoření ESET PROTECT virtuálního stroje jej můžete zapnout. Při prvotním spuštění se zobrazí následující obrazovka:



Otevřete si webový prohlížeč a do adresního řádku zadejte IP adresu nově nasazené ESET PROTECT appliance. IP adresa je uvedena na obrazovce virtuálního počítače (viz obrázek výše). Konkrétně v sekci "**First time appliance configuration needs to be performed. Please connect using a web browser to:** *https://[IP address]*".

Následně přejděte ke konfiguraci appliance prostřednictvím webového rozhraní.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně. To provedete prostřednictvím konzole pro správu DHCP VA. V případě, že virtuální stroj nemá přiřazenou IP adresu, na obrazovce uvidíte URL bez IP adresy.
Pokud i přesto, že máte v síti DHCP server, nedošlo k přiřazení adresy, ujistěte se, že máte v daném síťovém rozsahu volnou IP adresu.



Doporučujeme nastavit vCenter Roles and Permissions ve VMware tak, aby ostatní uživatelé neměnili přístup k ESET PROTECT virtuálnímu stroji. Tím zabráníte neoprávněným zásahům do konfigurace ESET PROTECT virtuálního stroje. Uživatelé ESET PROTECT zpravidla nepotřebují přístup k samotnému virtuálnímu stroji. Přístup k ESET PROTECT přidělíte jednotlivým uživatelům prostřednictvím sad oprávnění definovaných v ESET PROTECT Web Console.

VMware Workstation/Player

Nasazení ESET PROTECT VA do VMware Workstation/Player

Doporučujeme vždy používat nejnovější verzi VMware Player. Síťový adaptér nastavte do režimu **Bridged** nebo **NAT**.

Aby byl virtuální stroj s ESET PROTECT dostupný z internetu, musíte mít správně nastaven port forwarding.

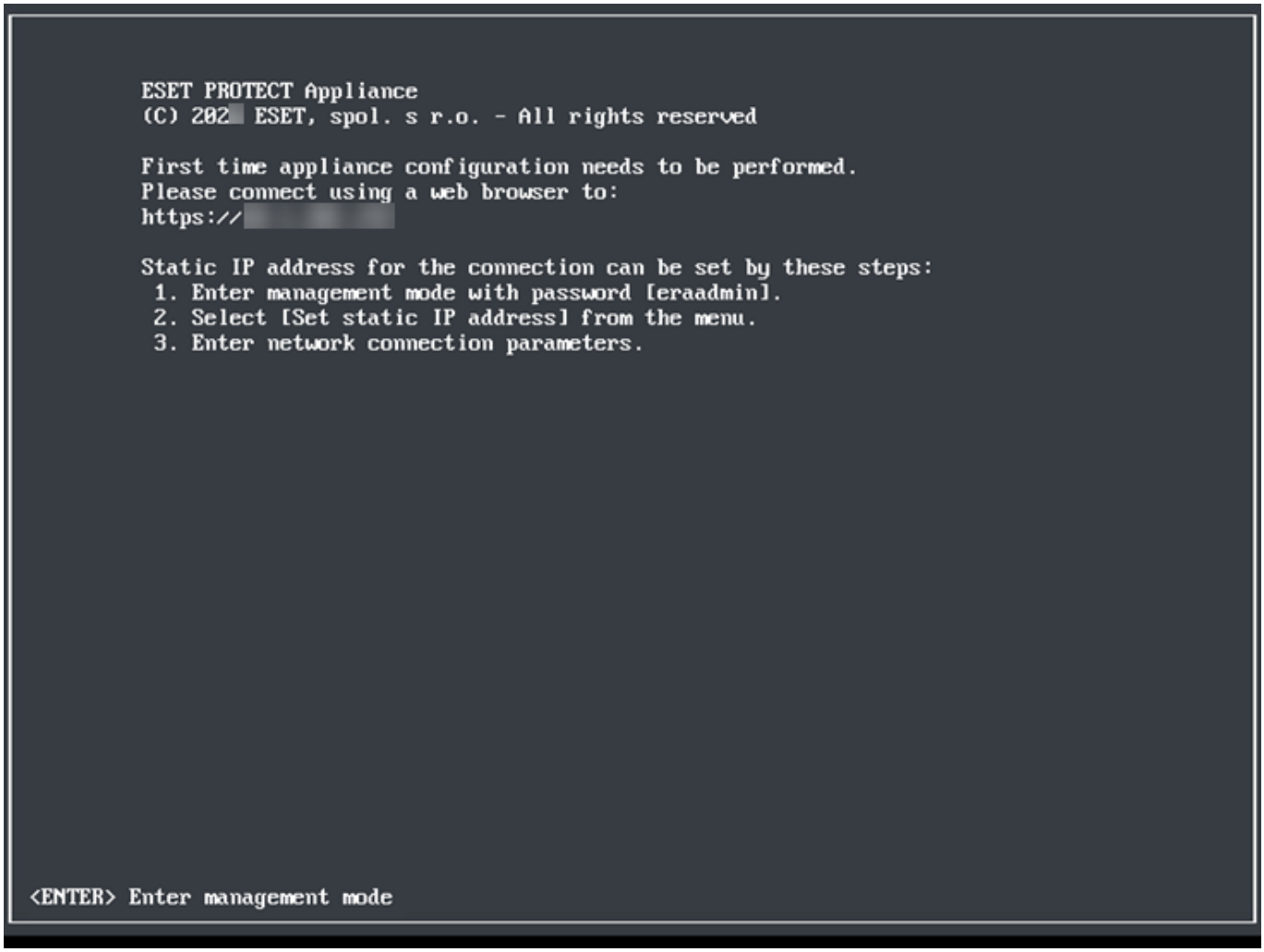
1. V hlavním okně klikněte na **File** > **Deploy OVF Template**.

2. Vyberte soubor *protect_appliance.ova* stažený z webových stránek společnosti ESET a klikněte na **Open**.

3. Zadejte název nového virtuálního stroje, případně vyberte složku, do které chcete stroj uložit, a klikněte na tlačítko **Importovat**.

4. Přečtěte si a odsouhlaste licenční ujednání s koncovým uživatelem (EULA).

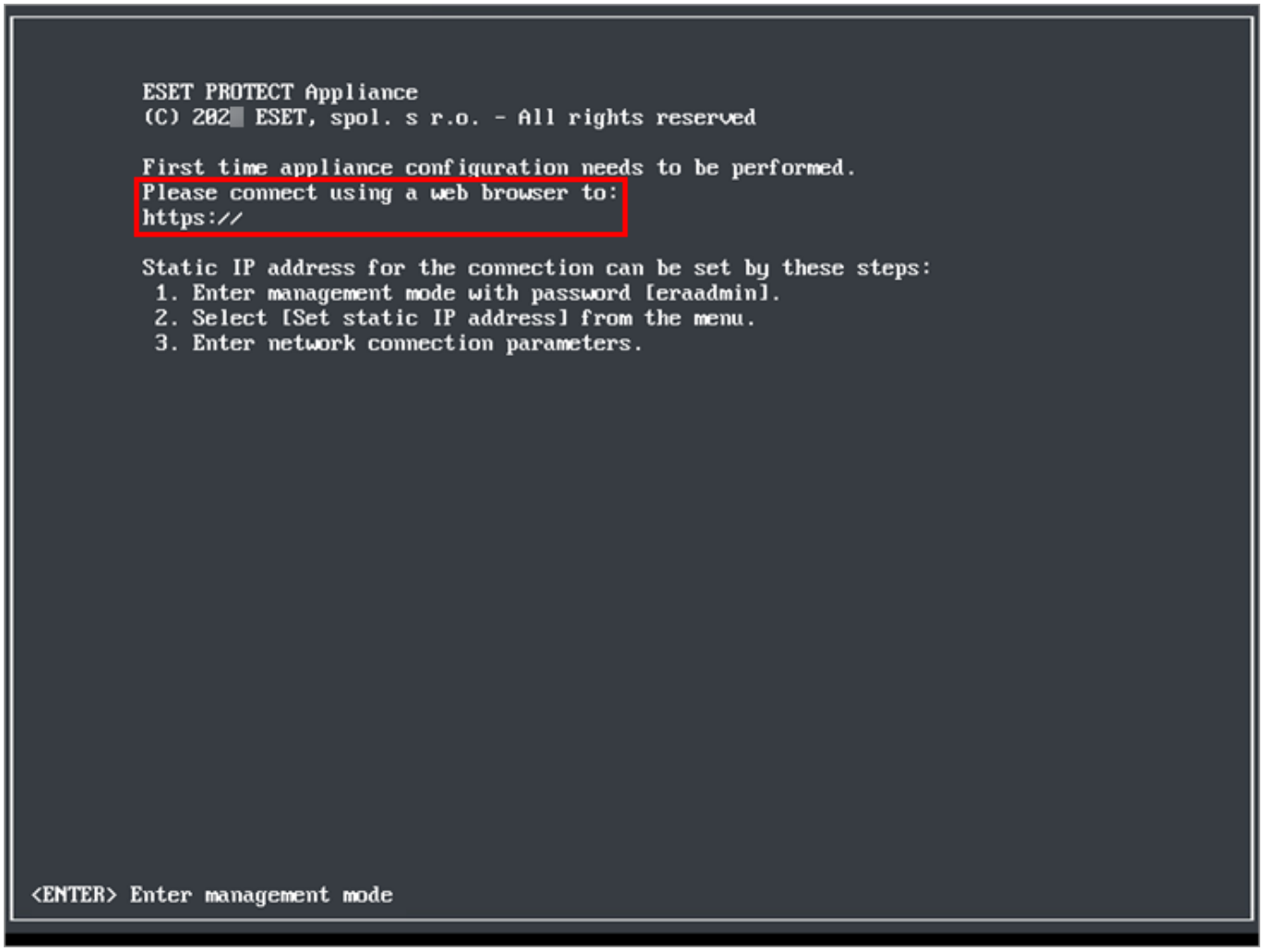
5. Po úspěšném vytvoření virtuálního stroje jej můžete zapnout. Při prvotním spuštění se zobrazí následující obrazovka:



Otevřete si webový prohlížeč a do adresního řádku zadejte IP adresu nově nasazené ESET PROTECT appliance. IP adresa je uvedena na obrazovce virtuálního počítače (viz obrázek výše). Konkrétně v sekci "**First time appliance configuration needs to be performed. Please connect using a web browser to:** *https://[IP address]*".

Následně přejděte ke konfiguraci appliance prostřednictvím webového rozhraní.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně. To provedete prostřednictvím konzole pro správu DHCP VA. V případě, že virtuální stroj nemá přiřazenou IP adresu, na obrazovce uvidíte URL bez IP adresy.
Pokud i přesto, že máte v síti DHCP server, nedošlo k přiřazení adresy, ujistěte se, že máte v daném síťovém rozsahu volnou IP adresu.



Microsoft Hyper-V

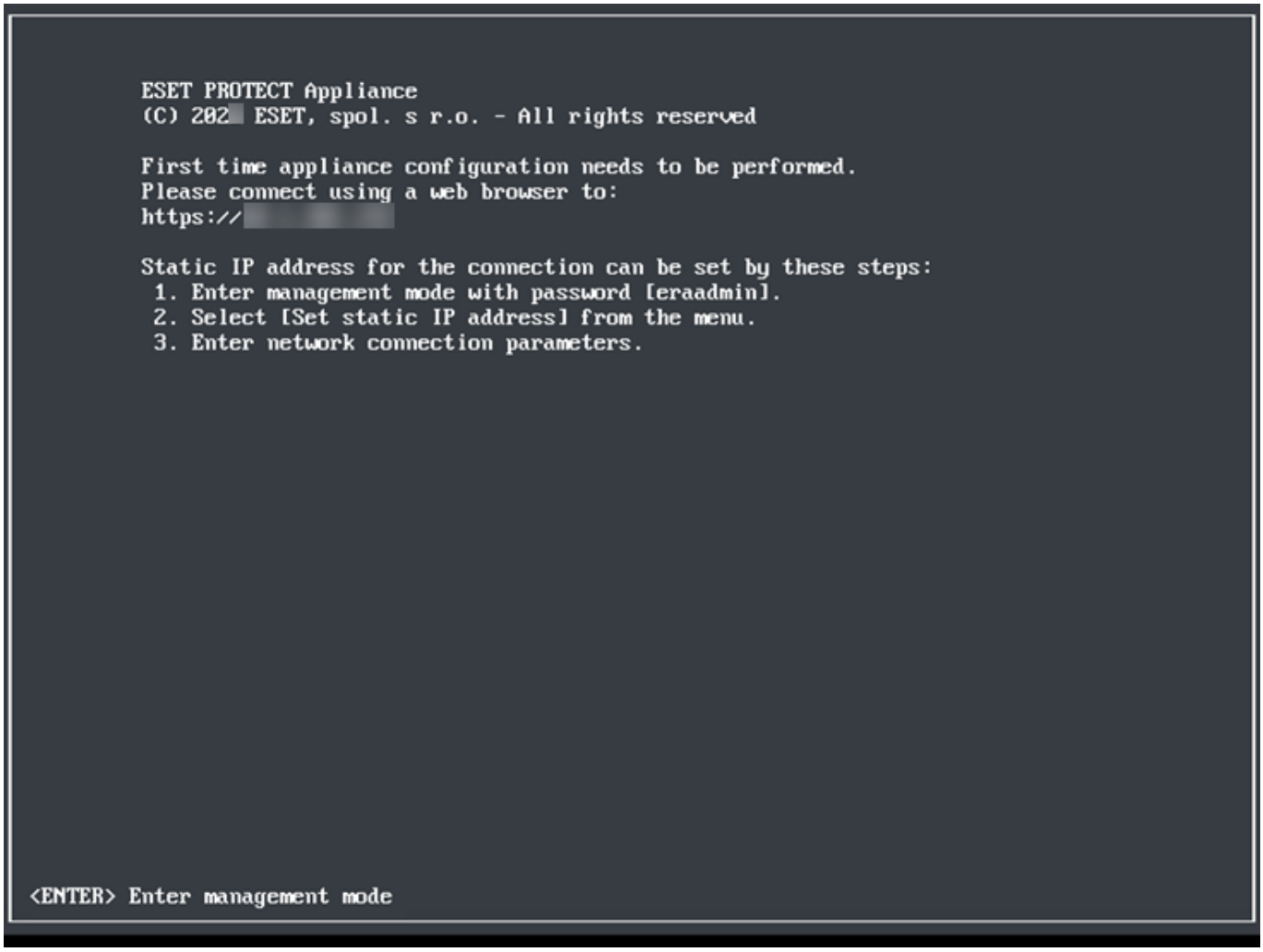
Nasazení ESET PROTECT VA do Microsoft Hyper-V

1. Rozbalte soubor `protect_appliance.vhd.zip` stažený z webových stránek společnosti ESET (například prostřednictvím 7-Zip).

2. Spusťte správce technologie Hyper-V a připojte se k požadovanému Hyper-V serveru.

3. Vytvořte **nový** virtuální stroj jako generaci 1. Přiřaďte mu alespoň 4 jádra a 4 GB RAM a jako disk použijte stažený .vhd soubor.

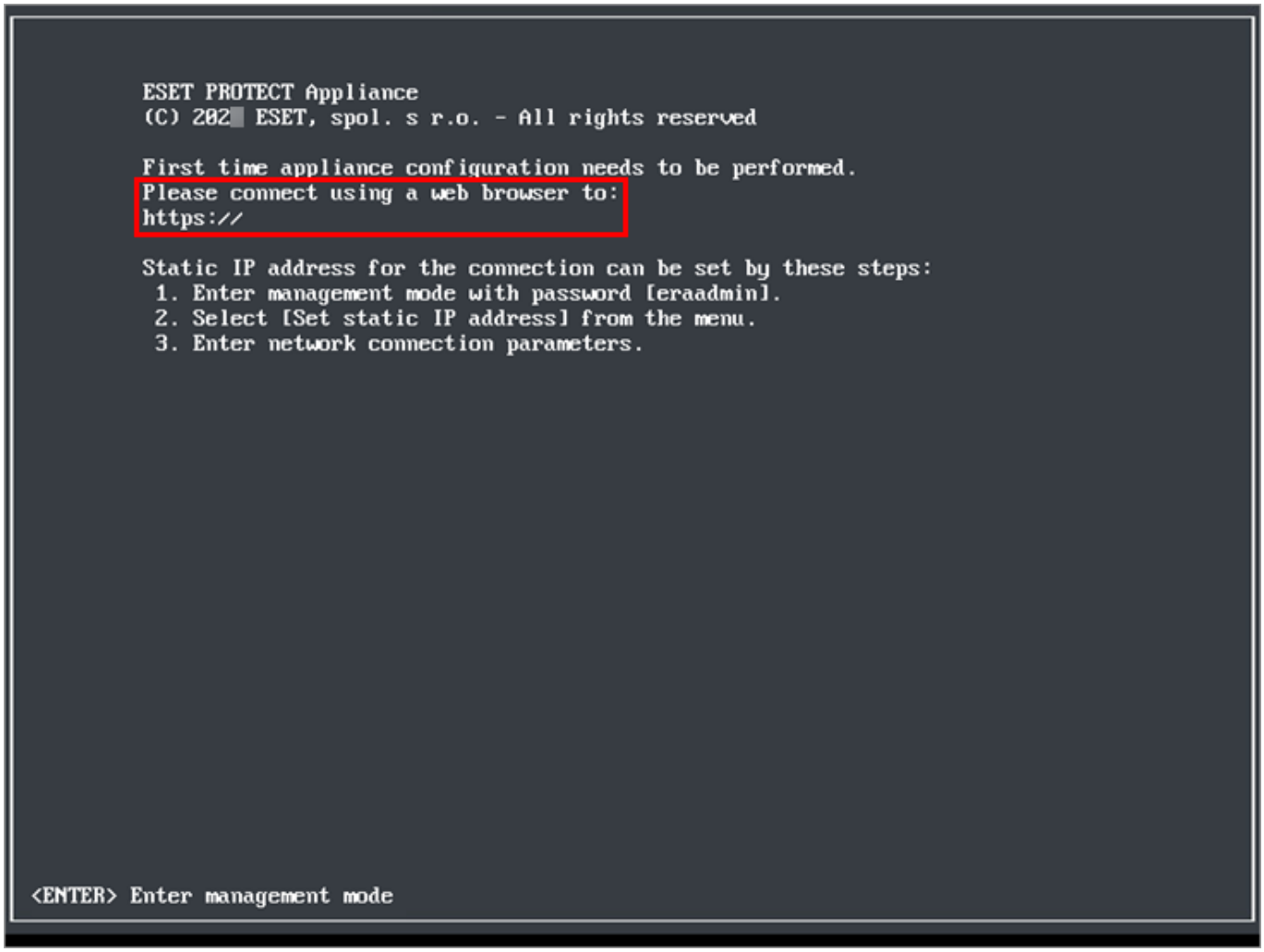
4. Po úspěšném vytvoření virtuálního stroje jej můžete zapnout. Při prvotním spuštění se zobrazí následující obrazovka:



Otevřete si webový prohlížeč a do adresního řádku zadejte IP adresu nově nasazené ESET PROTECT appliance. IP adresa je uvedena na obrazovce virtuálního počítače (viz obrázek výše). Konkrétně v sekci "**First time appliance configuration needs to be performed. Please connect using a web browser to:** *https://[IP address]*".

Následně přejděte ke konfiguraci appliance prostřednictvím webového rozhraní.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně. To provedete prostřednictvím konzole pro správu DHCP VA. V případě, že virtuální stroj nemá přiřazenou IP adresu, na obrazovce uvidíte URL bez IP adresy.
Pokud i přesto, že máte v síti DHCP server, nedošlo k přiřazení adresy, ujistěte se, že máte v daném síťovém rozsahu volnou IP adresu.



Oracle VirtualBox

Nasazení ESET PROTECT VA do VirtualBox

Doporučujeme vždy používat nejnovější verzi VirtualBox. Síťový adaptér nastavte do režimu **Bridged** nebo **NAT**.

Aby byl virtuální stroj s ESET PROTECT dostupný z internetu, musíte mít správně nastaven port forwarding.

1. V hlavním okně klikněte na **File** a vyberte možnost **Import Appliance**.

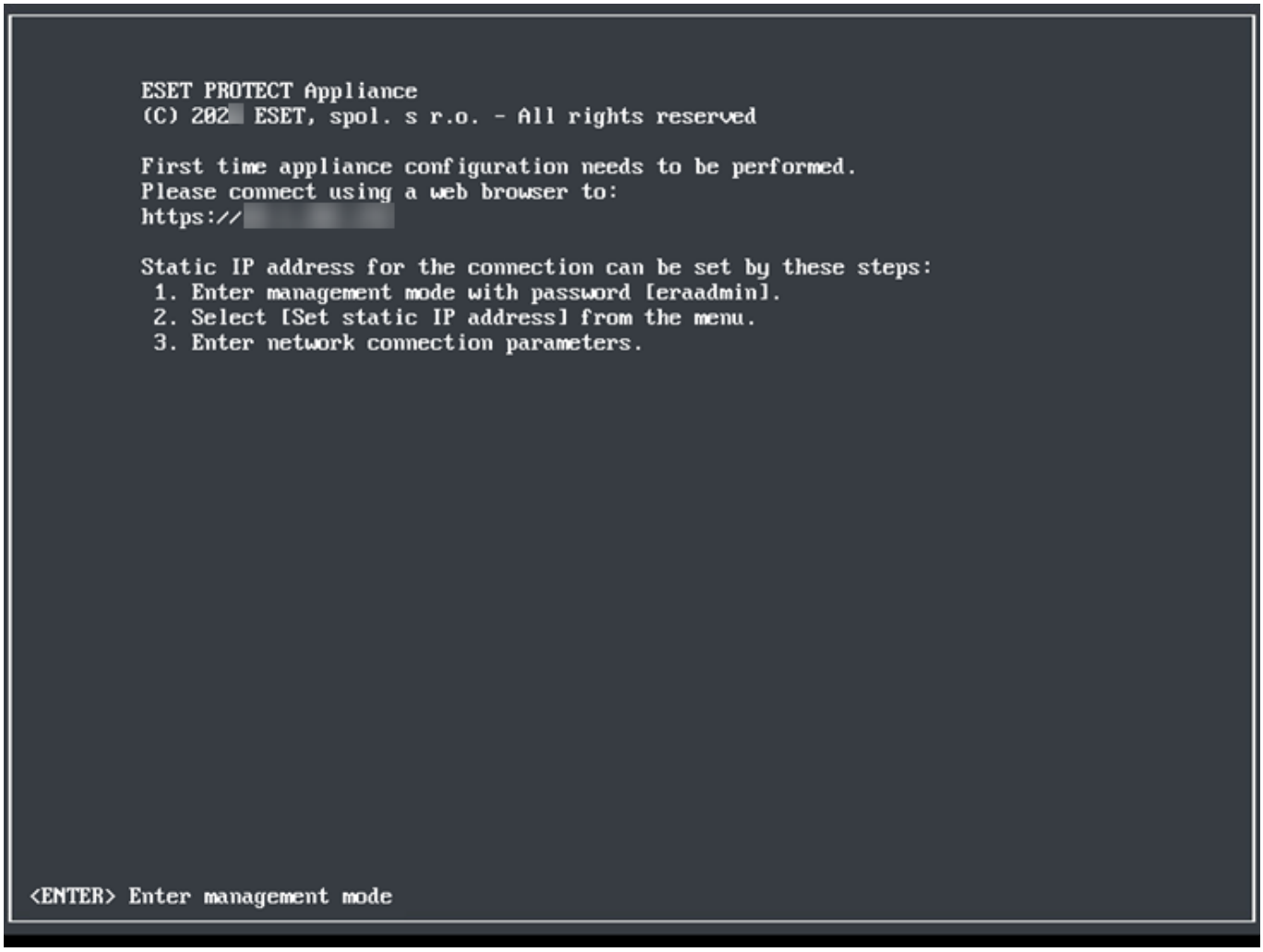
2. Klikněte na tlačítko **Browse** a vyberte soubor *protect_appliance.ova* stažený z webových stránek společnosti ESET a klikněte na **Open**.

3. Klikněte na tlačítko **Next**.

4. Prohlédněte si souhrnné nastavení virtuálního stroje a klikněte na tlačítko **Import**.

5. Přečtěte si a odsouhlaste licenční ujednání s koncovým uživatelem (EULA).

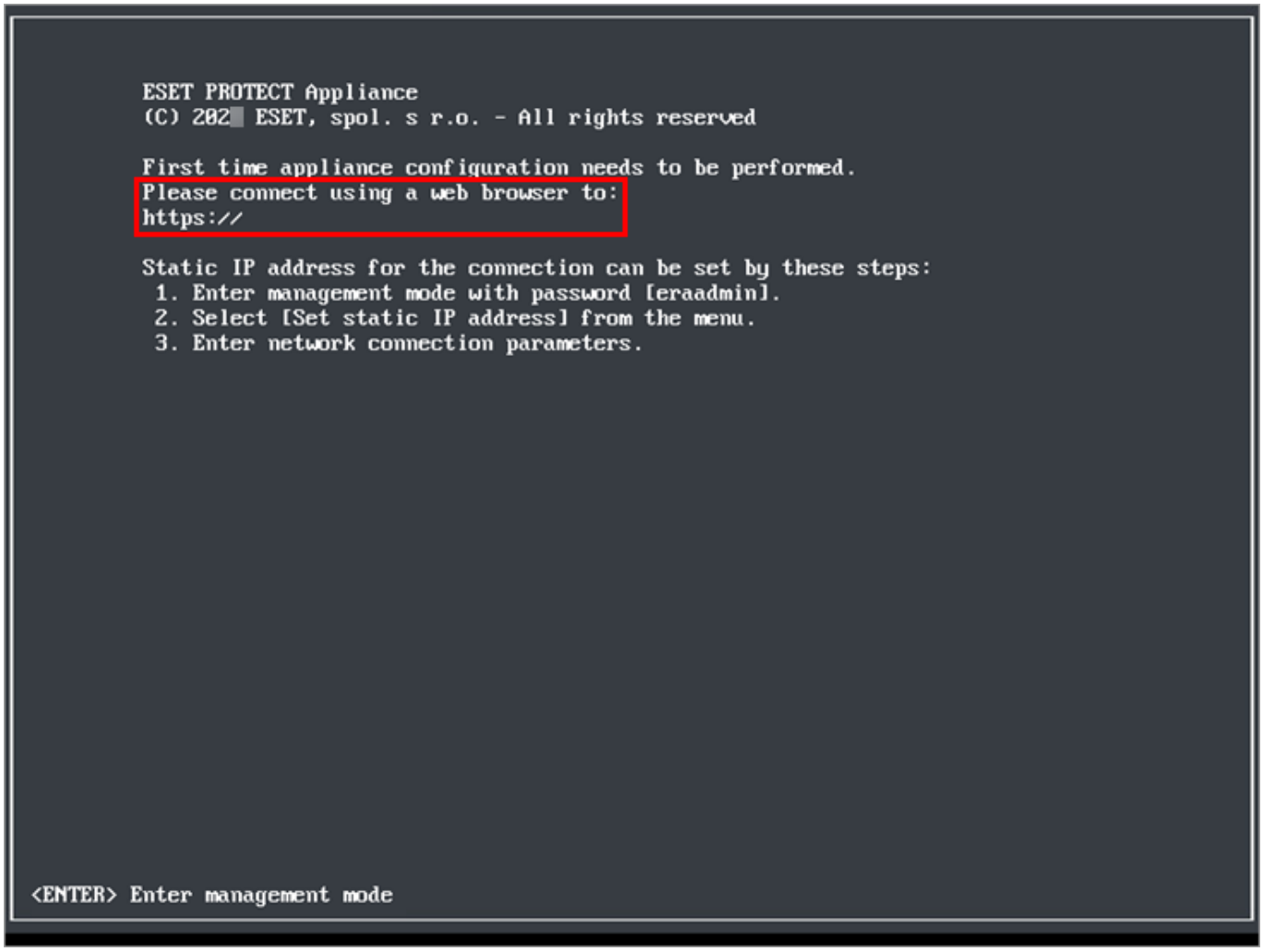
6. Po úspěšném vytvoření ESET PROTECT virtuálního stroje jej můžete zapnout. Při prvotním spuštění se zobrazí následující obrazovka:



Otevřete si webový prohlížeč a do adresního řádku zadejte IP adresu nově nasazené ESET PROTECT appliance. IP adresa je uvedena na obrazovce virtuálního počítače (viz obrázek výše). Konkrétně v sekci "**First time appliance configuration needs to be performed. Please connect using a web browser to:** *https://[IP address]*".

Následně přejděte ke konfiguraci appliance prostřednictvím webového rozhraní.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně. To provedete prostřednictvím konzole pro správu DHCP VA. V případě, že virtuální stroj nemá přiřazenou IP adresu, na obrazovce uvidíte URL bez IP adresy.
Pokud i přesto, že máte v síti DHCP server, nedošlo k přiřazení adresy, ujistěte se, že máte v daném síťovém rozsahu volnou IP adresu.



Citrix

Nasazení ESET PROTECT VA do Citrix prostředí

Předpoklady

- Ve vašem Citrix prostředí musí být dostupná IPv4 síť. ESET PROTECT VA nepodporuje IPv6.
- Připravený *.ovf* soubor na stroji, ze kterého budete nasazovat ESET PROTECT VA.
- Oprávnění Pool Admin pro importování *OVF/OVA* balíčku.
- Dostatek volného místo přiřazeného uživateli, který provádí nasazení; alespoň 100 GB.

Proces nasazení

1.V hlavním okně klikněte na **File** > **Import**.

2.Klikněte na tlačítko **Browse** a vyberte soubor *protect_appliance.ova* stažený z webových stránek společnosti ESET a klikněte na **Next**.

3.Zaškrtněte možnost **I accept the End User License Agreements** a pokračujte kliknutím na tlačítko **Next**.

4.Vyberte pool nebo standalone server, na který chcete umístit ESET PROTECT VA a klikněte na tlačítko **Next**.

5.Umístěte importovaný virtuální disk do storage repository a pokračujte kliknutím na tlačítko **Next**.

6.Pomocí možnosti **Target Network** namapujte virtuální síťové rozhraní a klikněte na tlačítko **Next**.

7.Volitelně ověřte digitální podpis stažené appliance a pokračujte kliknutím na tlačítko **Next**.

8.Vyberte možnost **Don't use Operating System Fixup** a klikněte na tlačítko **Next**.

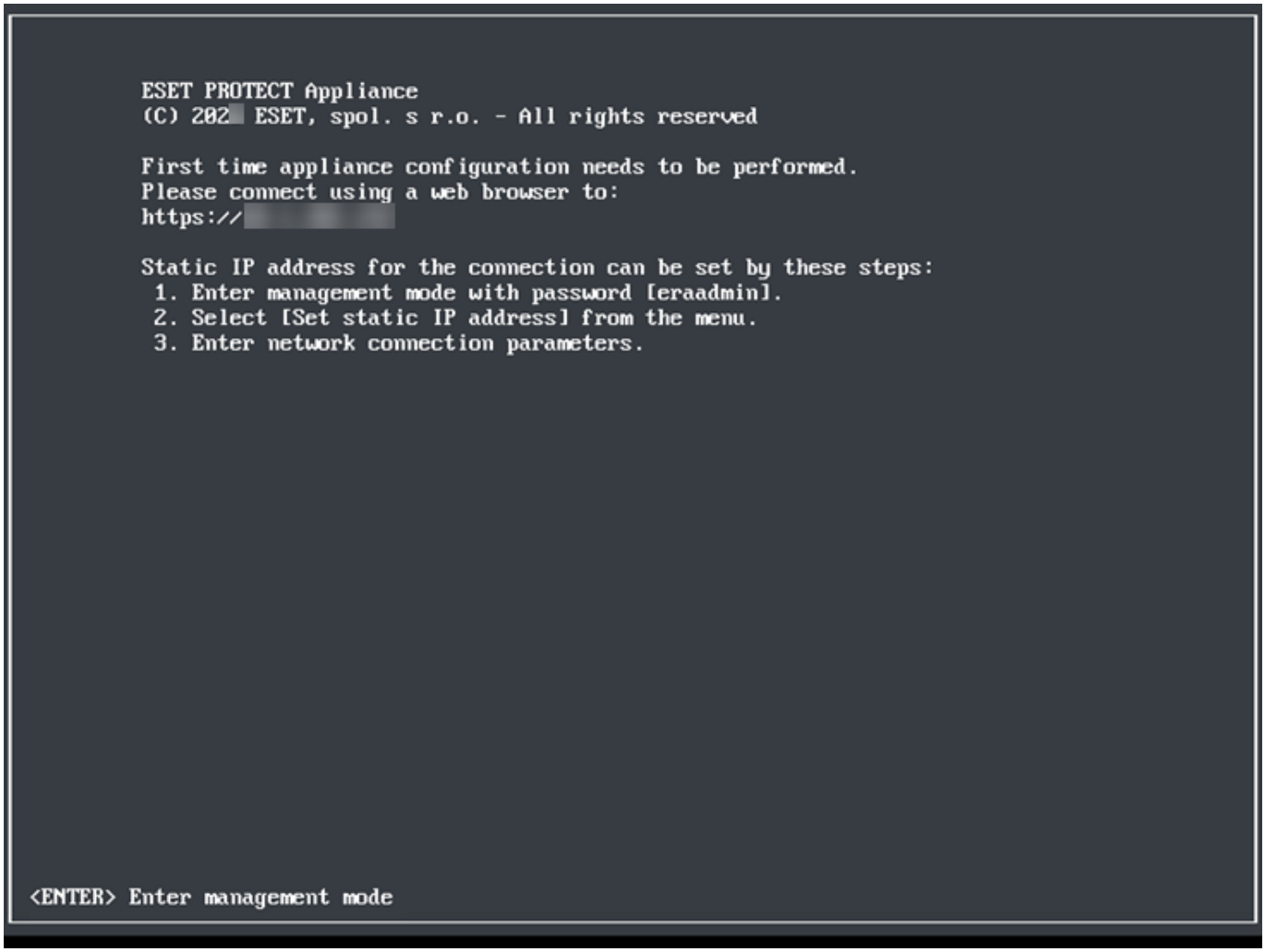
9.Dále vyberte síť (stejnou jako v kroku 6), do které se dočasně nainstalujte ESET PROTECT VA a použije se pro import, a pokračujte kliknutím na tlačítko **Next**.

10. Zkontrolujte nastavení a klikněte na tlačítko **Finish**.

Nasazení může chvíli trvat, během něhož se může Citrix server jevit jako nečinný. Nepřerušujte proces nasazení.

Více informací o nasazení *OVF/OVA* naleznete v dokumentaci společnosti Oracle.

Po úspěšném vytvoření virtuálního stroje jej můžete zapnout. Při prvotním spuštění se zobrazí následující obrazovka:

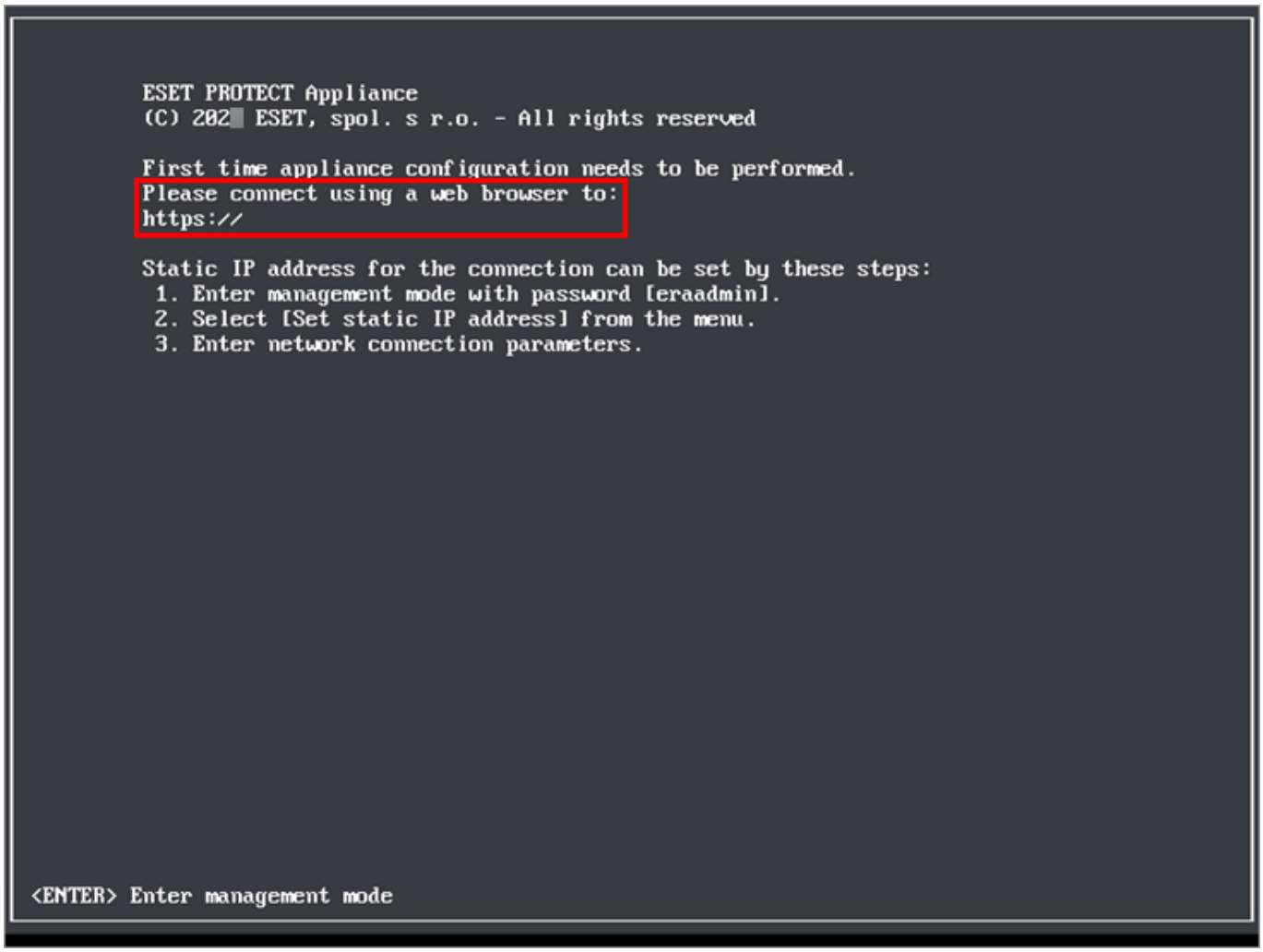


Otevřete si webový prohlížeč a do adresního řádku zadejte IP adresu nově nasazené ESET PROTECT appliance. IP adresa je uvedena na obrazovce virtuálního počítače (viz obrázek výše). Konkrétně v sekci "**First time appliance**

configuration needs to be performed. Please connect using a web browser to: *https://[IP address]"*.

Následně přejděte ke konfiguraci appliance prostřednictvím webového rozhraní.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně. To provedete prostřednictvím konzole pro správu DHCP VA. V případě, že virtuální stroj nemá přiřazenou IP adresu, na obrazovce uvidíte URL bez IP adresy.
Pokud i přesto, že máte v síti DHCP server, nedošlo k přiřazení adresy, ujistěte se, že máte v daném síťovém rozsahu volnou IP adresu.



Prvotní konfigurace ESET PROTECT virtuální appliance

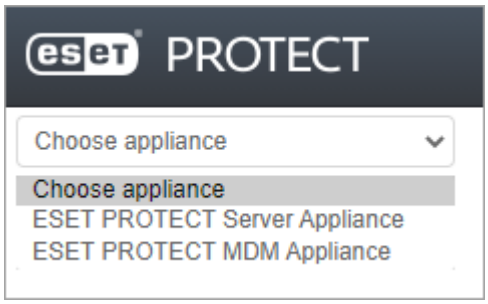
ESET PROTECT Virtual Appliance (ESET PROTECT VA) můžete pohodlně nakonfigurovat prostřednictvím webového rozhraní. Abyste mohli provést prvotní konfiguraci ESET PROTECT VA prostřednictvím webového rozhraní, je potřeba aby DHCP server přiřadil virtuálnímu počítači IP adresu.

Pokud ve své síti nemáte DHCP server, přiřaďte ESET PROTECT virtuální appliance statickou IP adresu ručně.

Po nasazení ESET PROTECT virtuální appliance si **vyberte typ appliance**, kterou chcete provozovat. Výběr a konfiguraci ESET PROTECT VA provedete následně prostřednictvím webového prohlížeče. Dále postupuje podle toto, zda chcete konfigurovat:

- ESET PROTECT Server Appliance

- ESET PROTECT MDM Appliance



ESET PROTECT Server Appliance

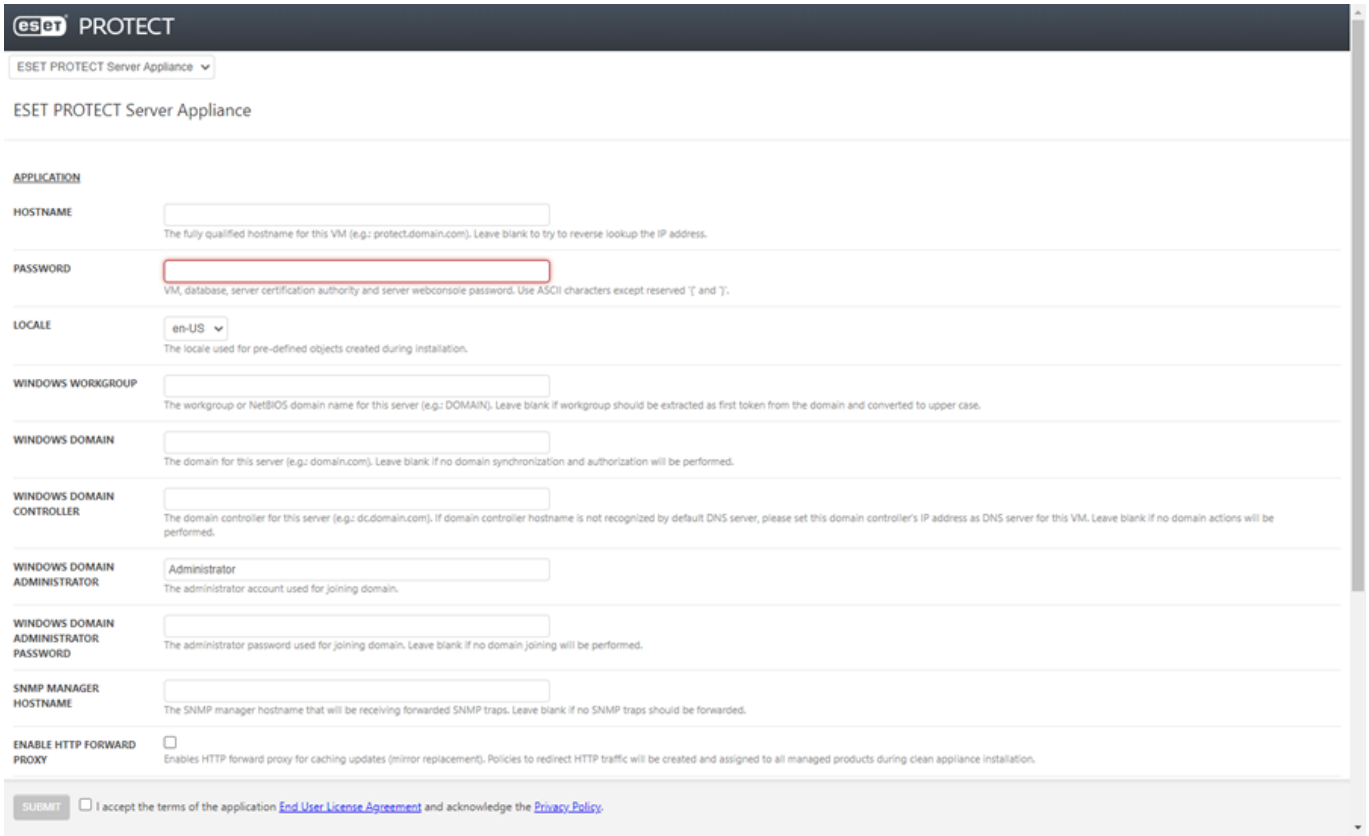
V této kapitole uvádíme postup konfigurace Virtual Appliance jako ESET PROTECT server. Konfigurační stránka je rozdělena na dvě části **Application** a **Networking properties**. Abyste mohli pokračovat dále, je nutné vyplnit všechny povinné parametry označené červeně. V případě potřeby vyplňte rovněž volitelné parametry.

Tato ESET PROTECT virtuální appliance vytvoří virtuální počítač, na kterém poběží ESET PROTECT server. Vhodná je pro SMB i enterprise prostředí.

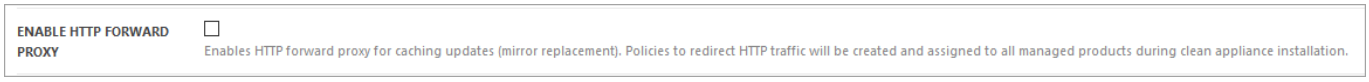
Povinné položky pro konfiguraci ESET PROTECT server appliance:

- **Password** – jedná se o důležité heslo. Nastaví se jako heslo uživatele root v operačním systému CentOS, použije se jako heslo pro přístup do ESET PROTECT databáze, bude jej mít výchozí účet Administrator v ESET PROTECT Web Console a ESET PROTECT certifikační autorita bude opatřena tímto heslem.

Výchozí uživatelský účet pro přístup do Web Console je **Administrator**.



Sice to není nutné, ale doporučujeme vyplnit také nepovinné parametry. Například můžete vyplnit informace o připojení do domény. Tím si ušetříte čas při ruční konfiguraci v budoucnu, protože tato dato jsou vyžadována například při synchronizaci.



Zobrazení většího obrázku

Dále můžete aktivovat Apache HTTP Proxy, komponentu která dokáže do cache ukládat aktualizační a instalační balíčky. Pro její aktivaci vyberte možnost **Enable HTTP forward proxy**. Následně dojde k vytvoření odpovídajících politik (s názvem **Používat HTTP Proxy** a jejich přiřazení nejnadřazenější statické skupině **Všechna zařízení** pro následující produkty:

- ESET Endpoint pro Windows
- ESET Endpoint pro macOS (OS X) a Linux
- ESET Management Agent
- ESET File Security for Windows Server (6+)
- ESET Server Security pro Windows (8+)
- ESET Shared Local Cache

- Vytvořená politika ovlivní nastavení produkty tak, aby se připojoval k internetu prostřednictvím této proxy. V konfiguraci se jako proxy server použije lokální IP adresa ESET PROTECT serveru a port 3128. Autentifikace je vypnutá. V případě potřeby můžete toto nastavení zkopírovat a použít jej také pro další produkty.
- Pomocí této komponenty snížíte vytížení do internetu, protože Apache HTTP Proxy bude do cache ukládat data stahovaná produkty ESET. Instalaci této komponenty **doporučujeme** již ve chvíli, kdy budete prostřednictvím ESET PROTECT ve své síti spravovat alespoň 37 stanic.
- Apache HTTP Proxy můžete nainstalovat kdykoli později. Potřebné kroky naleznete ve FAQ k ESET PROTECT virtuální appliance.

Konfigurace sítě

Pro konfiguraci síťového adaptéru odrolujte stránku a vyplňte pole: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. Všechna pole jsou volitelná.

Připojení ESET PROTECT virtuální appliance do domény

ESET PROTECT virtuální appliance můžete připojit do domény již v průběhu prvotní konfigurace. Pro použití ESET PROTECT VA v doméně je nutné vyplnit níže uvedená nastavení:

Windows workgroup – pracovní skupina nebo NETBIOS jméno domény, například DOMAIN.

Windows domain – název domény, například *domain.com*.

Windows domain controller – název doménového řadiče. Zadejte plně kvalitifikované jméno (FQDN)

doménového řadiče.

Windows domain administrator – uživatelský účet, pod kterým se provede přidání stroje do domény.

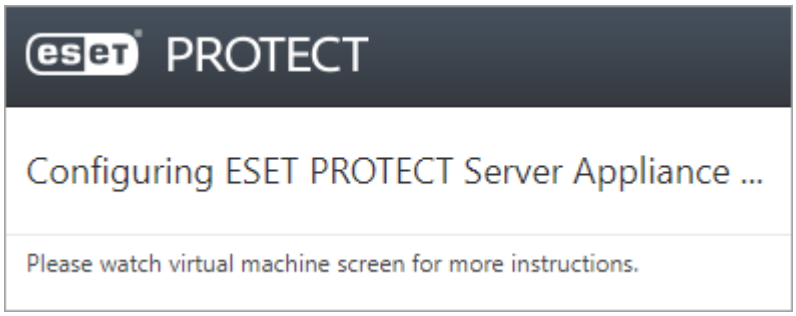
Windows domain administrator password – heslo k výše uvedenému uživatelskému účtu.

DNS1 – IP adresa DNS serveru. Ve většině případů shodný s adresou doménového řadiče.

Zkontrolujte vámi zadané parametry. Ujistěte se, že jste veškeré parametry nastavili správně. Později je již nebude možné jednoduše změnt.

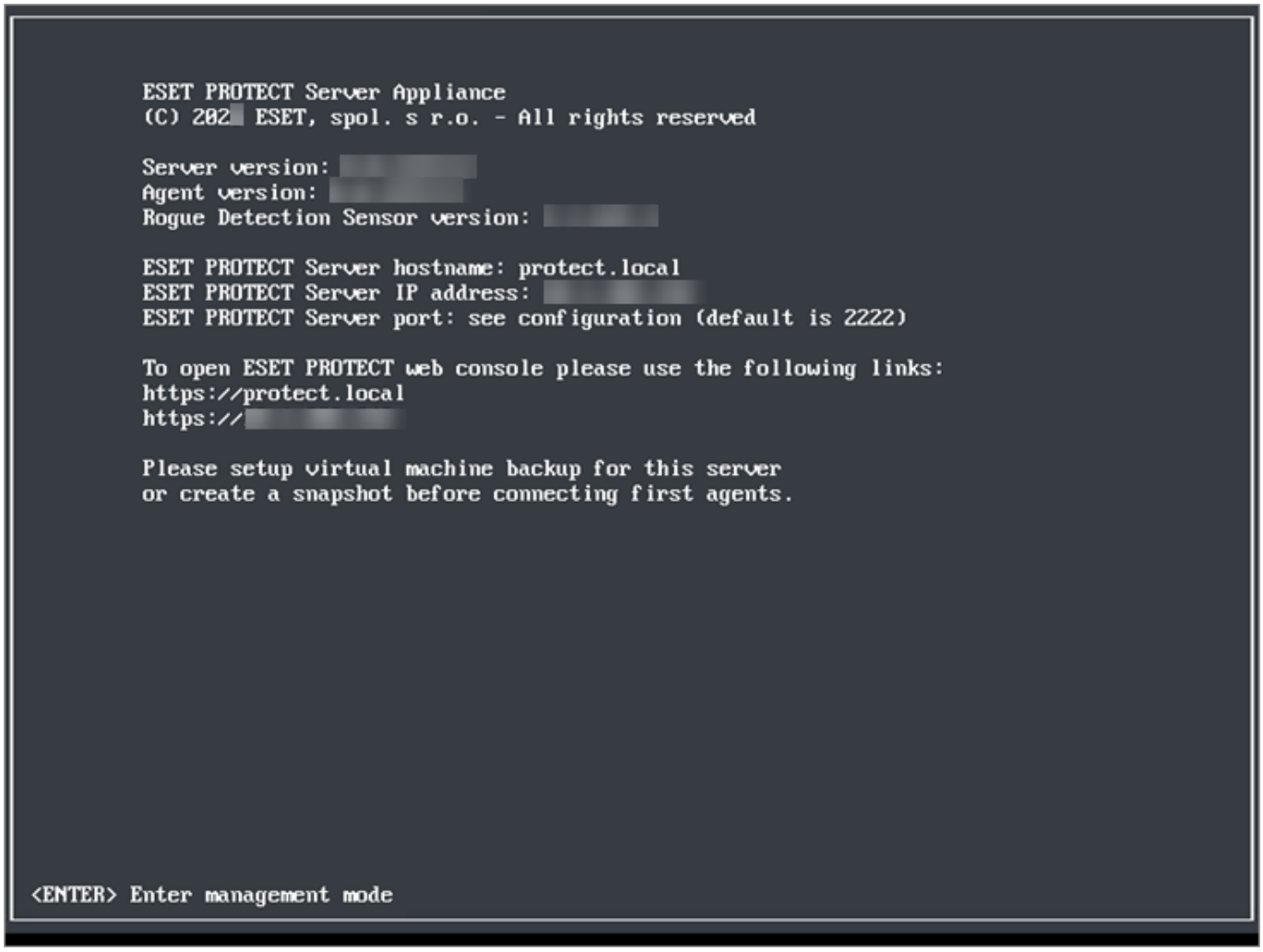
Zaškrtněte možnost **Souhlasím s licenčním ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

Akci dokončete kliknutím na tlačítko **Submit**. Následně se zobrazí tato informace:



Tuto stránku neaktualizuje. Prohlížeč nebo záložku s touto stránku zavřete a vraťte se zpět do konzole ESET PROTECT VA.

Po restartování a automatickém nakonfigurování ESET PROTECT Virtual Appliance se zobrazí konzole s podrobnými informace. Na úvodní obrazovce jsou uvedeny informace o verzích ESET PROTECT komponent stejně jako název server serveru, IP adresa a port. Naleznete zde také adresu, na níž je dostupná ESET PROTECT Web Console, ve formátu *https://[hostname] and https://[IP address]*.



Před připojením prvních ESET Management Agentů doporučujeme vytvořit snapshot virtuálního stroje.

Do internetového prohlížeče zadejte adresu (výše uvednou) na níž je dostupná ESET PROTECT Web Console a přihlaste se. Mějte na paměti, že uvedený název serveru a IP adresa uvedená na obrázku je pouze ilustrační, a ve vašem prostředí bude odlišná. Po přihlášení již můžete ESET PROTECT začít používat.

Po prvním přihlášení do ESET PROTECT Web Console doporučujeme spustit klientskou úlohu pro aktualizaci operačního systému na server, kde běží ESET PROTECT.

ESET PROTECT MDM Appliance

V této kapitole uvádíme postup konfigurace ESET PROTECT MDM Appliance. Konfigurační stránka je rozdělena na dvě části: **Application** a **Networking properties**. Abyste mohli pokračovat dále, je nutné vyplnit všechny povinné parametry označené červeně. V případě potřeby vyplňte rovněž volitelné parametry.

Tato ESET PROTECT virtuální appliance vytvoří virtuální počítač, na kterém poběží ESET PROTECT MDM. Vhodná je pro SMB i enteprise prostředí.

Před tím, než začnete konfigurovat ESET PROTECT MDM Appliance, si vytvořte ve Web Console certifikát pro Mobile Device Connector, který se bude používat pro připojení k ESET PROTECT Serveru. Pokud si jej předem nevytvoříte, při asistované instalaci se v průběhu nasazení VA vygeneruje automaticky, ale jeho parametry nemusí odpovídat vašim potřebám.

ESET PROTECT MDM můžete nakonfigurovat dvěma způsoby:

1.**Asistovaná instalace (vyžaduje přímé spojení do ESMC Web Console)**

Povinné položky pro konfiguraci ESET PROTECT MDM Appliance:

- **Password** – Jedná se o důležité heslo, prostřednictvím kterého se přihlásíte do konzole pro správu ESET PROTECT VA a databáze.

- **ESET PROTECT Server Hostname** - zadejte název nebo IP adresu ESET PROTECT Serveru, ke kterému se má ESET PROTECT MDM připojit.

- **ESET PROTECT Server Port** – port, který se použije pro komunikaci s ESET PROTECT serverem (standardně 2222). Pokud jste si jej změnili, zadejte vámi definovaný.

- **Web Console Port** – port, který se použije pro komunikaci s Web Console (standardně 2223). Pokud jste si jej změnili, zadejte vámi definovaný.

- **Web Console password** – zadejte heslok uživatelskému účtu, který má přístup do konzole ESET PROTECT Web Console a alespoň oprávnění pro asistovanou instalaci (použít můžete výchozí účet Administrator).

- Volitelně můžete vyplnit pole **Webconsole Hostname**. Jedná se o název serveru, na kterém běží Web Console. Pokud ponecháte pole prázdné, použije se automaticky hodnota zadaná do pole **ESET PROTECT Server Hostname**.

- **MDM Hostname** – zadejte FQDN nebo IP adresu (musí odpovídat MDC certifikátu vytvořeném v ESET PROTECT Web Console).

2.**Ruční konfigurace (vyžaduje předem exportované certifikáty z Web Console)**

Povinné položky pro konfiguraci ESET PROTECT MDM Appliance:

- **Password** – Jedná se o důležité heslo, prostřednictvím kterého se přihlásíte do konzole pro správu ESET PROTECT VA a databáze.

- **ESET PROTECT Server Hostname** - zadejte název nebo IP adresu ESET PROTECT Serveru, ke kterému se má ESET PROTECT MDM připojit.

- **ESET PROTECT Server Port** – port, který se použije pro komunikaci s ESET PROTECT serverem (standardně 2222). Pokud jste si jej změnili, zadejte vámi definovaný.

- **Web Console Port** – port, který se použije pro komunikaci s Web Console (standardně 2223). Pokud jste si jej změnili, zadejte vámi definovaný.

- **Certification authority Base64** – zadejte exportovaný veřejný klíč certifikační autority v Base64 formátu. Pro více informací přejděte do kapitoly ESET PROTECT certifikáty

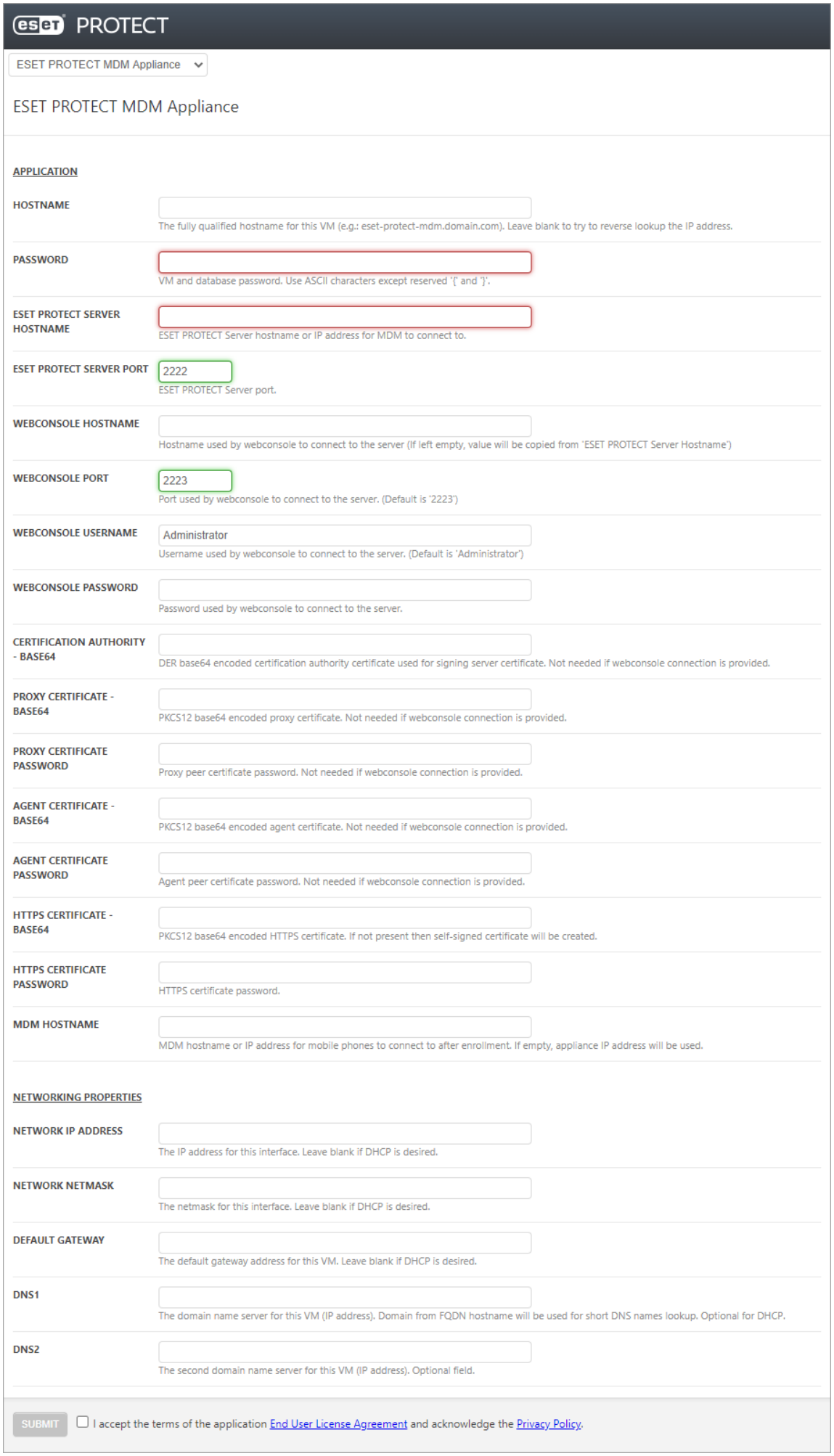
- **Proxy Certificate Base64** – zadejte exportovaný certifikát proxy v Base64 formátu. Pro více informací přejděte do kapitoly ESET PROTECT certifikáty Pro ověření komunikace mezi ESET PROTECT Serverem a MDM je využíván Proxy certifikát.

- **Agent Certificate Base64** – zadejte exportovaný certifikát agenta v Base64 formátu. Pro více informací přejděte do kapitoly ESET PROTECT certifikáty

- **MDM Hostname** – zadejte FQDN nebo IP adresu (musí odpovídat MDC certifikátu vytvořeném v ESET PROTECT Web Console).

Konfigurace sítě

Pro konfiguraci síťového adaptéru odrolujte stránku a vyplňte pole: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. Všechna pole jsou volitelná.


PROTECT
ESET PROTECT MDM Appliance
ESET PROTECT MDM Appliance
APPLICATION
HOSTNAME
The fully qualified hostname for this VM (e.g.: eset-protect-mdm.domain.com). Leave blank to try to reverse lookup the IP address.
PASSWORD
VM and database password. Use ASCII characters except reserved '{' and '}'.
ESET PROTECT SERVER HOSTNAME
ESET PROTECT Server hostname or IP address for MDM to connect to.
ESET PROTECT SERVER PORT
2222
ESET PROTECT Server port.
WEBCONSOLE HOSTNAME
Hostname used by webconsole to connect to the server (If left empty, value will be copied from 'ESET PROTECT Server Hostname')
WEBCONSOLE PORT
2223
Port used by webconsole to connect to the server. (Default is '2223')
WEBCONSOLE USERNAME
Administrator
Username used by webconsole to connect to the server. (Default is 'Administrator')
WEBCONSOLE PASSWORD
Password used by webconsole to connect to the server.
CERTIFICATION AUTHORITY - BASE64
DER base64 encoded certification authority certificate used for signing server certificate. Not needed if webconsole connection is provided.
PROXY CERTIFICATE - BASE64
PKCS12 base64 encoded proxy certificate. Not needed if webconsole connection is provided.
PROXY CERTIFICATE PASSWORD
Proxy peer certificate password. Not needed if webconsole connection is provided.
AGENT CERTIFICATE - BASE64
PKCS12 base64 encoded agent certificate. Not needed if webconsole connection is provided.
AGENT CERTIFICATE PASSWORD
Agent peer certificate password. Not needed if webconsole connection is provided.
HTTPS CERTIFICATE - BASE64
PKCS12 base64 encoded HTTPS certificate. If not present then self-signed certificate will be created.
HTTPS CERTIFICATE PASSWORD
HTTPS certificate password.
MDM HOSTNAME
MDM hostname or IP address for mobile phones to connect to after enrollment. If empty, appliance IP address will be used.
NETWORKING PROPERTIES
NETWORK IP ADDRESS
The IP address for this interface. Leave blank if DHCP is desired.
NETWORK NETMASK
The netmask for this interface. Leave blank if DHCP is desired.
DEFAULT GATEWAY
The default gateway address for this VM. Leave blank if DHCP is desired.
DNS1
The domain name server for this VM (IP address). Domain from FQDN hostname will be used for short DNS names lookup. Optional for DHCP.
DNS2
The second domain name server for this VM (IP address). Optional field.
SUBMIT
I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy.

Zkontrolujte vámi zadané parametry. Ujistěte se, že jste veškeré parametry nastavili správně. Později již nebude možné jednoduše je změnit.

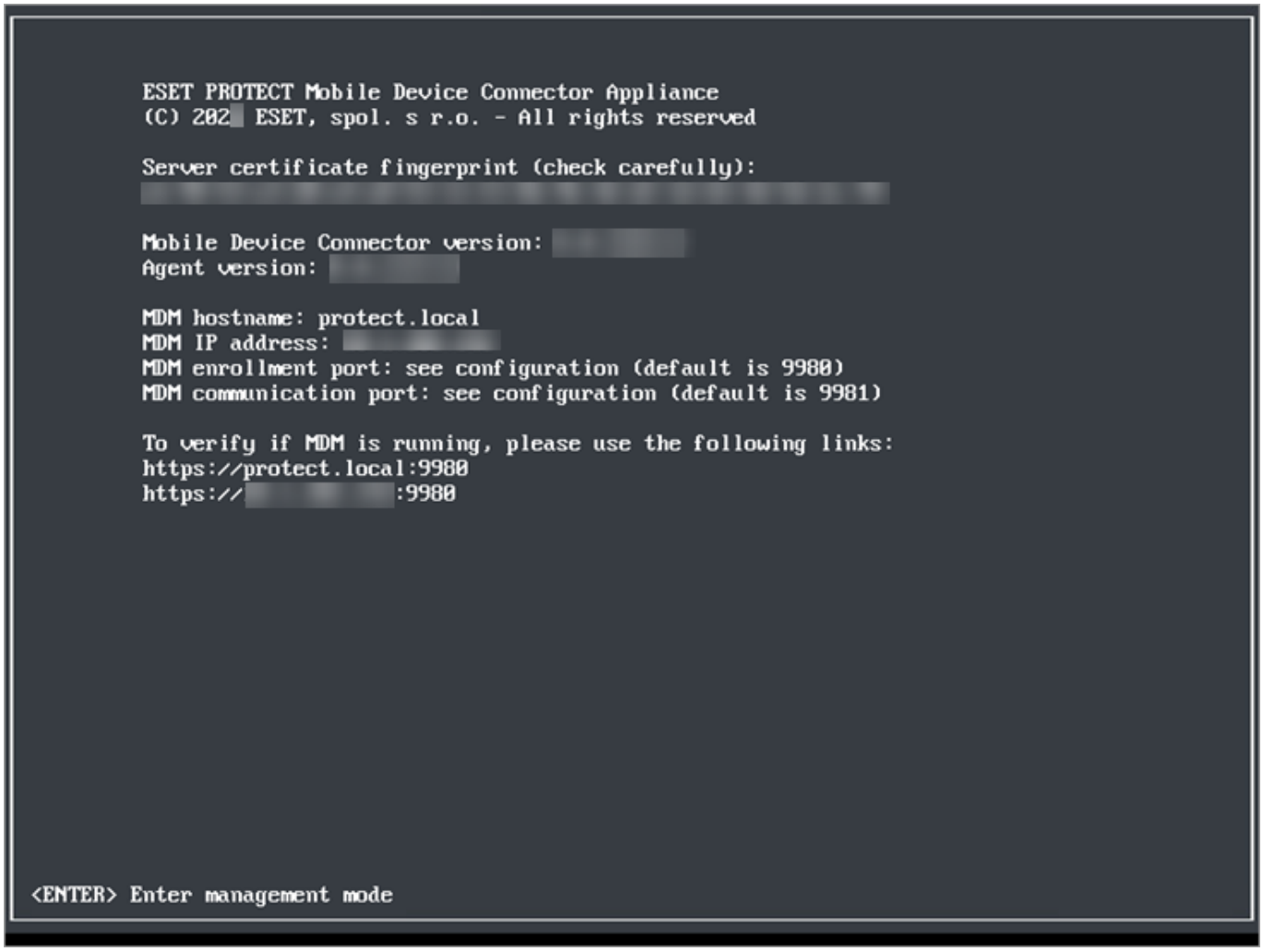
Zaškrtněte možnost **Souhlasím s licenčním ujednáním koncového uživatele a beru na vědomí zásady ochrany osobních údajů**. Jednotlivé dokumenty naleznete na našich webových stránkách v sekci Licenční ujednání s koncovým uživatelem (EULA), Podmínky použití a Zásady ochrany osobních údajů pro produkty ESET.

Po provedení změn klikněte na tlačítko **Submit**.

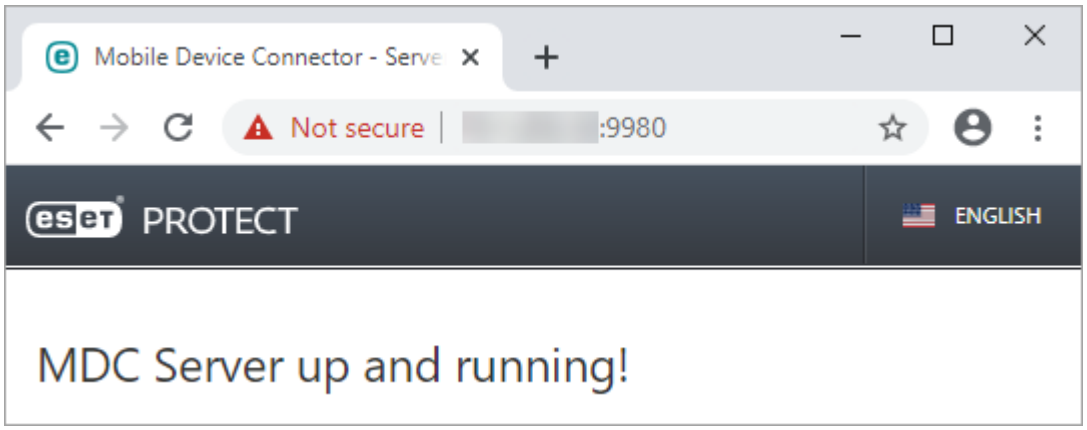
Následně se **zobrazí** tato informace:

Tuto stránku neaktualizuje. Prohlížeč nebo záložku s touto stránku zavřete a vraťte se zpět do konzole ESET PROTECT VA.

Po restartování a automatickém nakonfigurování ESET PROTECT Virtual Appliance se zobrazí konzole s podrobnými informace o MDM. Na úvodní obrazovce jsou uvedeny informace o verzích ESET PROTECT komponent stejně jako název ESET PROTECT MDM, IP adresa a port. Naleznete zde také registrační adresu ve formátu *https://[nazev_serveru]:9980 a https://[IP_adresa]:9980*.



Pro ověření funkčnosti komponenty Mobile Device Connector zadejte do internetového prohlížeče výše uvedenou registrační adresu. Mějte na paměti, že uvedený název serveru a IP adresa uvedená na obrázku je pouze ilustrační, a ve vašem prostředí bude odlišná. Pokud bylo nasazení úspěšné, zobrazí se následující informace:



Konzole pro správu ESET PROTECT virtuální appliance

Po úspěšném nasazení ESET PROTECT VA si otevřete okno virtuálního počítače. Na obrazovce virtuálního stroje jsou zobrazeny základní informace o ESET PROTECT VA a jejím stavu, jako je název počítače, jeho IP adresa a bližší informace o nainstalovaných ESET PROTECT komponentách. Stisknutím klávesy **Enter** se z této obrazovky můžete přepnout do **konzole pro správu ESET PROTECT virtuální appliance**. Pro vstup do režimu správy zadejte heslo, které jste si nastavili v průběhu konfigurace ESET PROTECT a dvakrát potvrďte stisknutím klávesy **Enter**. Pokud jste

zatím heslo pro přístup do ESET PROTECT VA nenastavovali, pro vstup do režimu správy použijte výchozí heslo `eraadmin`.

Po přihlášení do konzole pro správu ESET PROTECT VA máte k dispozici tyto možnosti:

- Set Static IP address
- Enable/Disable remote access
- Backup database
- Restore database
- Reset after snapshot revert
- Pull database from other server
- Změna hesla do virtuálního stroje
- Change database password
- Rejoin domain
- Configure domain
- Factory reset

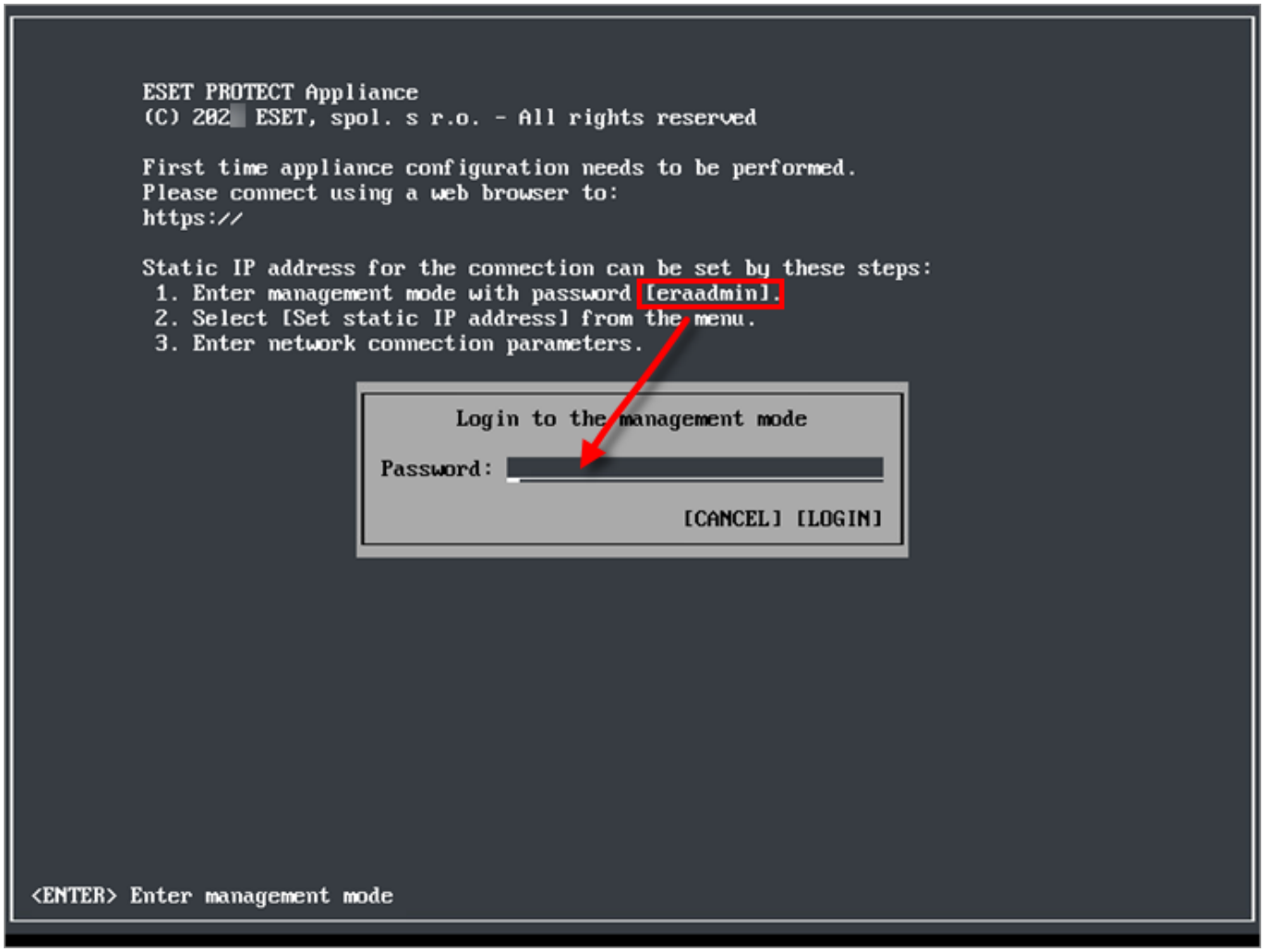
> Dostupnost jednotlivých možností závisí na použitém typu ESET PROTECT virtuální appliance a fázi jejího nasazení.

- **Restart system** – pomocí této možnosti restartujete ESET PROTECT VA.
- **Shut down system** – pomocí této možnosti vypnete ESET PROTECT VA.
- **Lock screen** – pomocí této možnosti uzamknete počítač a **zabráníte ostatním osobám v používání** ESET PROTECT virtuální appliance a přístupu k jejím souborům. Uzamknout obrazovku můžete také stisknutím klávesy **Esc**. Tímto opustíte režim správy a vrátíte se zpět na hlavní obrazovku ESET PROTECT VA.
- **Exit to Terminal** – pomocí této možnosti se přepnete do terminálu operačního systému. Tímto opustíte režim správy ESET PROTECT VA a zobrazí se terminál. Pro návrat na hlavní obrazovku ESET PROTECT VA zadejte příkaz `exit`, případně `logout`, a potvrďte klávesou **Enter**.

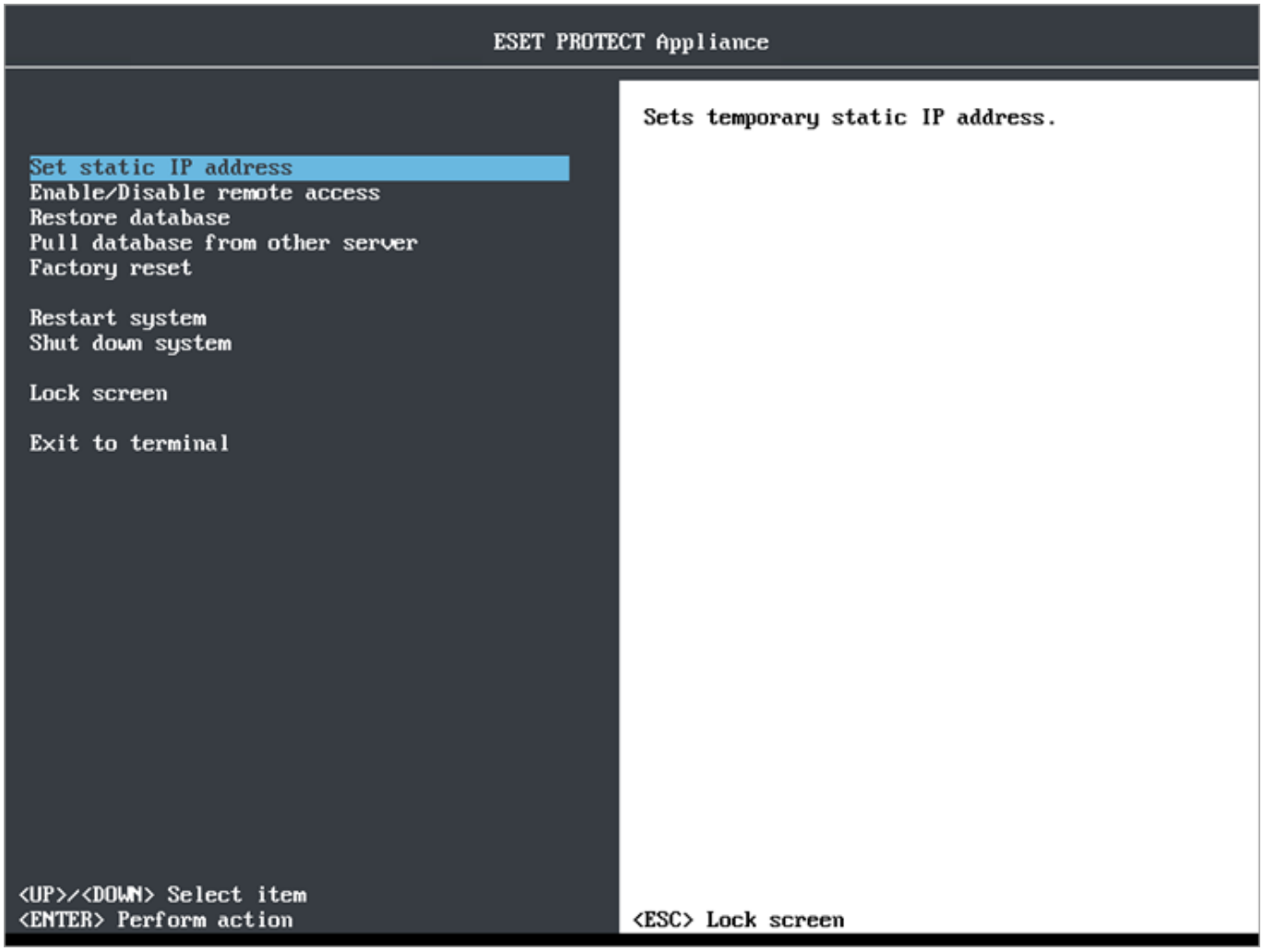
Nastavení statické IP adresy

Pokud ESET PROTECT VA nepřiřadil IP adresu váš DHCP server, je nutné ji nastavit ručně. Pro ruční nastavení IP adresy postupujte podle níže uvedených kroků:

1. Na úvodní obrazovce virtuální appliance stiskněte klávesu **Enter** a přejděte do **režimu správy**. Zadejte heslo `eraadmin` a potvrďte jej **dvojitým** stisknutím klávesy **Enter**.



2. Pomocí šipek vyberte z dostupných možností **Set static IP address** a potvrďte stisknutím klávesy **Enter**.



3. Zobrazí se interaktivní průvodce konfigurací síťového adaptéru, který vás vyzve k zadání:
   - IP adresy
   - Masky sítě
   - Brány
   - Adresy DNS serveru

> Parametry sítě zadávejte v IPv4 formátu. Příklad: `192.168.1.10` (IP adresa), `255.255.255.0` (maska). Mějte na paměti, že i po správné konfiguraci síťového adaptéru **nebude** ESET PROTECT VA odpovídat na ping.

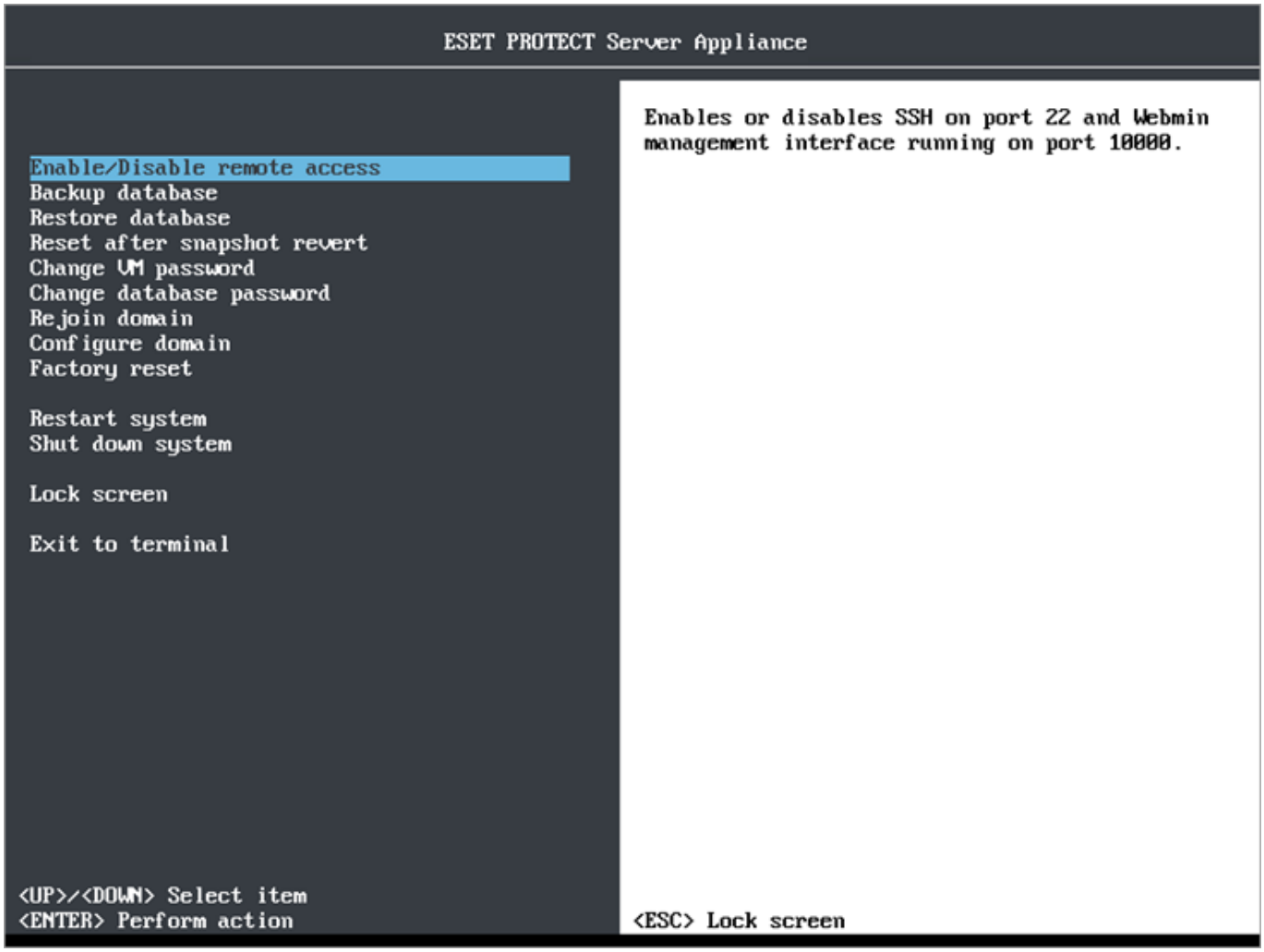
4. Pokračujte stisknutím klávesy **Enter** nebo pomocí kombinace kláves **Ctrl+C zůstaňte v terminálu**.

ESET PROTECT virtuální appliance má jeden síťový adaptér, ale v případě potřeby **můžete přidat další**. Nicméně tato funkce vždy konfiguruje rozhraní `eth0`.

Zapnutí/vypnutí vzdáleného přístupu

Abyste mohli k virtuální appliance přistupovat vzdáleně (prostřednictvím (Webmin webového rozhraní a SSH), je nutné tuto službu nejprve povolit.

Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Enable/Disable remote access** a potvrďte stisknutím klávesy **Enter**.

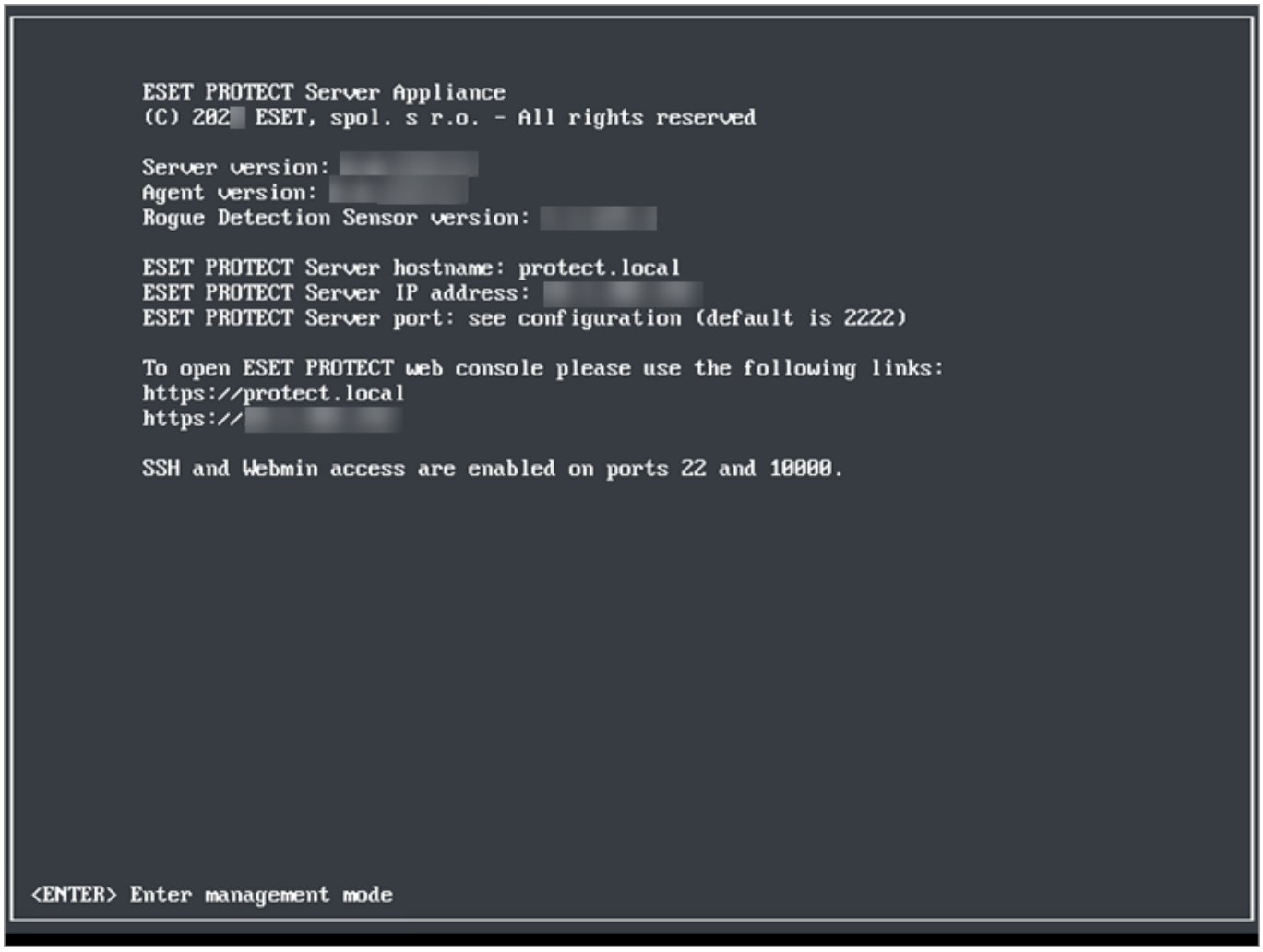


Nyní můžete:

- Používat Webmin – více informací naleznete v kapitole Webmin – rozhraní pro správu. Webové rozhraní je dostupné prostřednictvím protokolu HTTPS a běží na portu 10000. Pro přístup k Webmin webovému rozhraní zadejte do internetového prohlížeče adresu společně s portem číslo 10000 ve formátu *https://<host name or IP address>:10000* (například *https://10.10.11.16:10000* nebo *https://protect.local:10000*).

- Vzdáleně se připojit prostřednictvím SSH na portu 22 (vyžadováno pro použití funkce na migraci databáze.

Níže uvádíme příklad obrazovky konzole ESET PROTECT virtuální appliance se zapnutým vzdáleným přístupem.



Dále se podívejte do kapitoly SSH: řešení problémů.

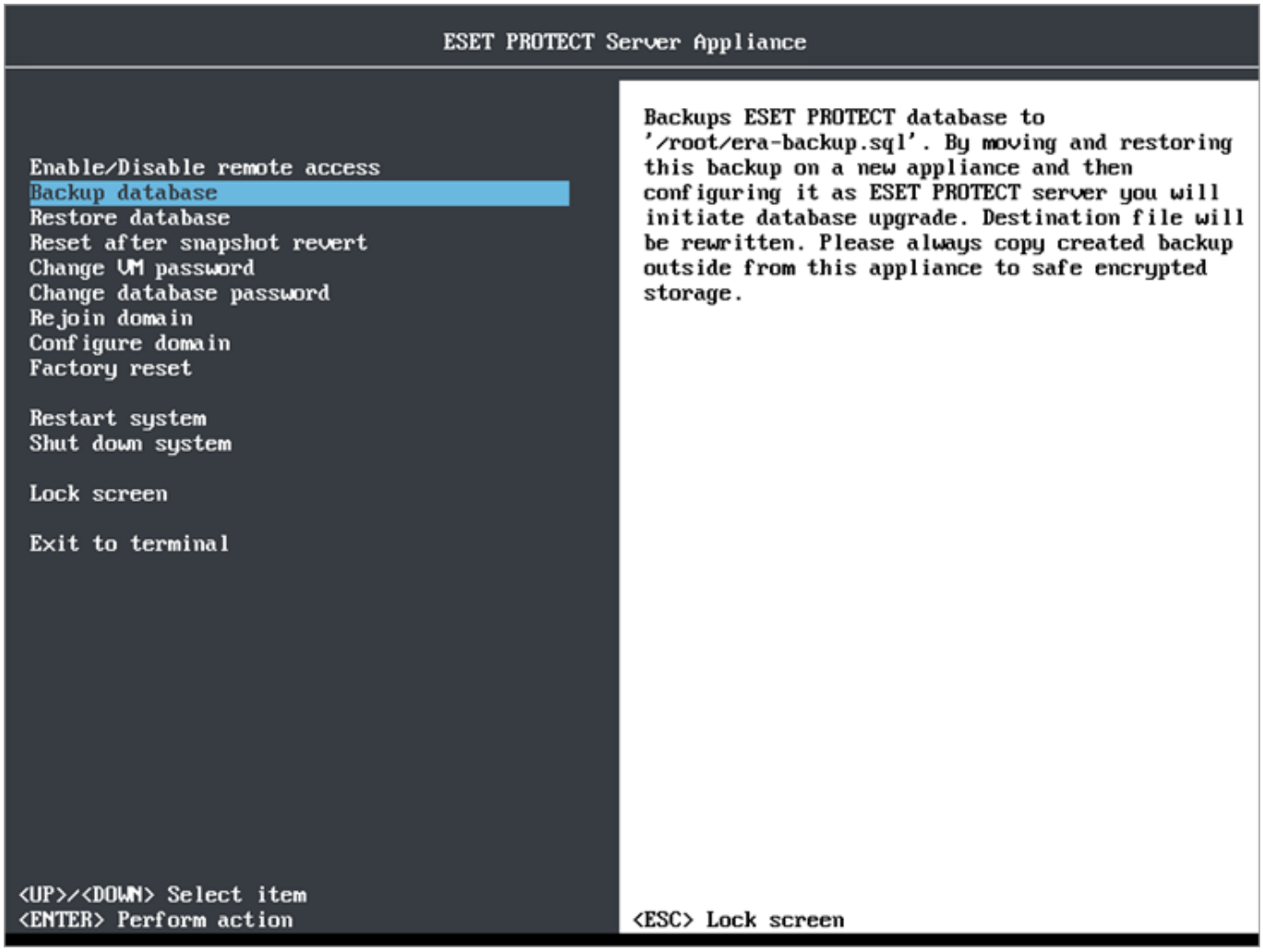
Záloha databáze

Zálohování představuje nezbytnou součást pro zabránění ztráty dat (disaster recovery). Pomocí této funkce (**Backup database**) vytvoříte zálohu **ESET PROTECT** databáze. MySQL soubor s názvem *era-backup.sql* se vytvoří do složky *root*.

Alternativu k zálohování databáze představují snapshoty celého virtuálního stroje. Tím si zachováte celou ESET PROTECT virtuální appliance, včetně veškerého nastavení společně s ESET PROTECT databází. Při návratu ke staršímu snapshotu nezapomeňte spustit úlohu pro Reset po obnovení snapshotu, čímž vynutíte synchronizaci dat.

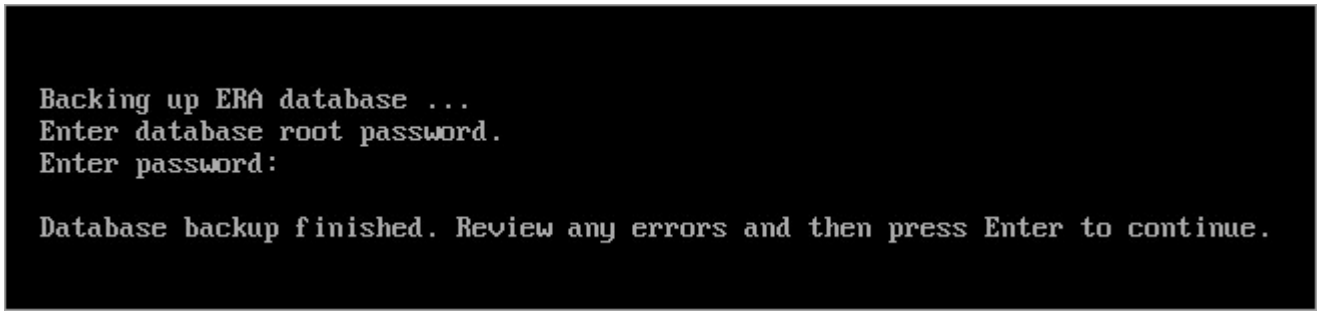
ESET PROTECT databázi doporučujeme pravidelně zálohovat a zálohu ukládat na externí úložiště. Pokud by došlo k problémům a ztrátě dat, budete mít k dispozici kopii ESET PROTECT databáze – uloženou mimo ESET PROTECT virtuální appliance. Například v případě poškození ESET PROTECT VA nebo jejím smazání. Pokud budete mít aktuální zálohu ESET PROTECT databáze, budete schopni ESET PROTECT virtuální appliance obnovit do stavu před nehodou. Pro více informací přejděte do kapitoly Disaster recovery ESET PROTECT virtuální appliance

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Backup database** a potvrďte stisknutím klávesy **Enter**.



2. Před zahájením zálohování budete vyzváni k zadání vašeho databazového root hesla.

Pokud si nepamatujete heslo databázového uživatele root, můžete si jej změnit. Následně spusťte zálohování znovu.



V závislosti na velikosti databáze může tato operace chvíli trvat.
V průběhu zálohování databáze dojde k zastavení služby ESET PROTECT, aby byla zajištěna konzistence dat.

Vždy zkontrolujte, zda není na obrazovce nějaké chybové hlášení. V případě výskytu chyby nelze považovat zálohování za úspěšné. V takovém případě zkuste **zálohu databáze spustit znovu**.

Vytvořenou zálohu databáze naleznete ve složce: */root/era-backup.sql*

Zálohu si stáhněte, například prostřednictvím Webmin File manager, a uložte na bezpečné místo.

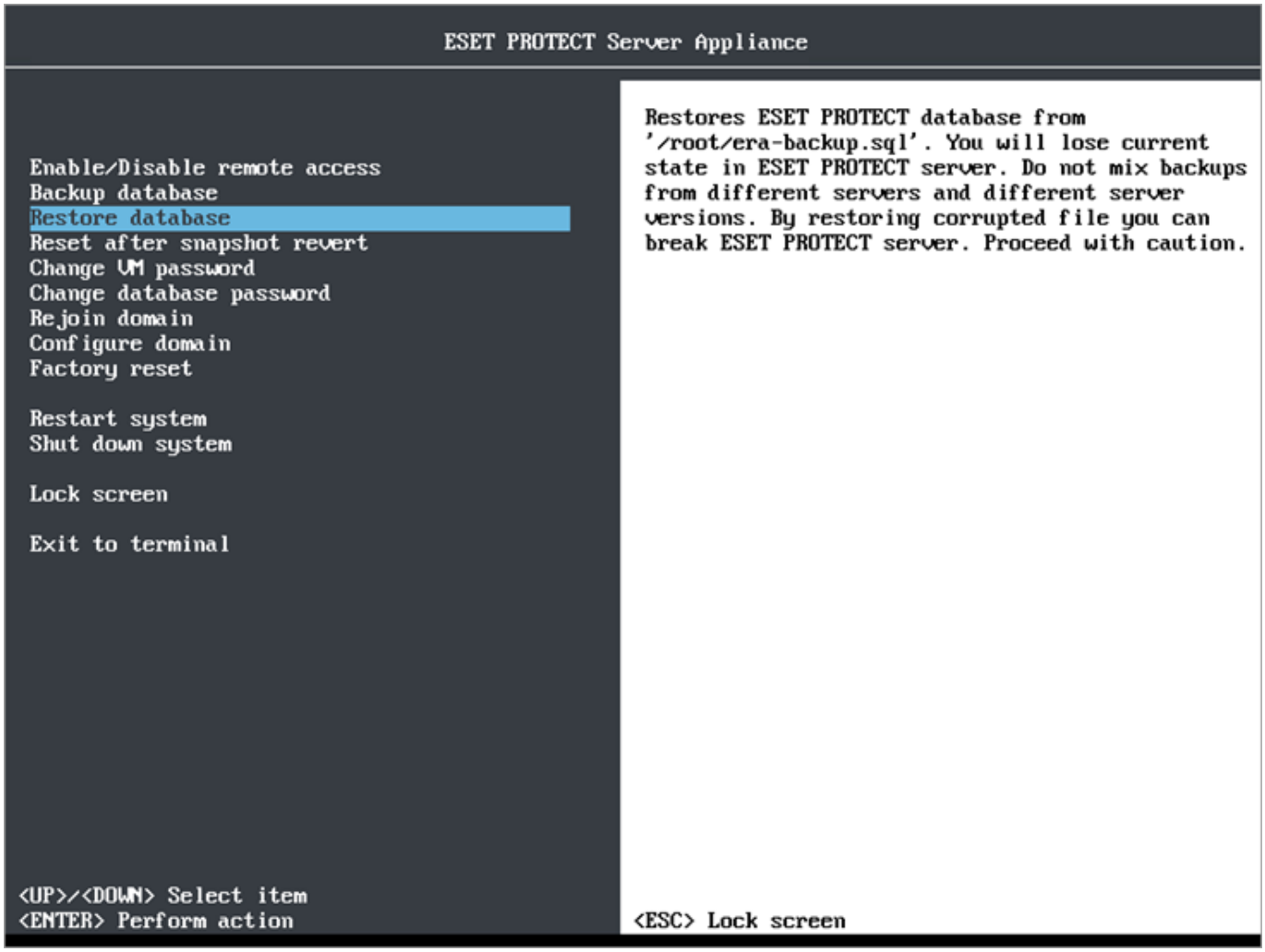
Obnovení databáze

Pomocí této funkce nahradíte aktuálně používanou databázi verzí ze zálohy.

Před obnovením databáze doporučujeme vytvořit snapshot virtuálního stroj nebo zálohu stávající databáze. V případě komplikací se snadno vrátíte k předchozímu stavu.

Pro **obnovení databáze** postupujte podle níže uvedených kroků:

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Restore database** a potvrďte stisknutím klávesy **Enter**.



Nahrajte dump databáze (*era-backup.sql*), kterou chcete obnovit, do složky *root*. To můžete provést například prostřednictvím Webmin File manager. Mějte na paměti, že dojde k přepsání cílového souboru *era-backup.sql*. Tento krok přeskočte, pokud se již ve složce *root* nachází soubor *era-backup.sql*, který chcete obnovit.

V žádném případě nepoužívejte při obnovení databázi z jiného serveru a jiné verze. Vždy obnovujte databázi (soubor *era-backup.sql*) na stejnou ESET PROTECT VA, na níž jste provedli její zálohu. Výjimkou je situace, kdy máte čistou, ještě nenakonfigurovanou ESET PROTECT virtuální appliance.

2. Při obnovení databáze budete vyzváni k zadání **hesla databázového uživatele root**. Pokud obnovujete na

čistou ESET PROTECT virtuální appliance, nebudete vyzváni k zadání hesla.

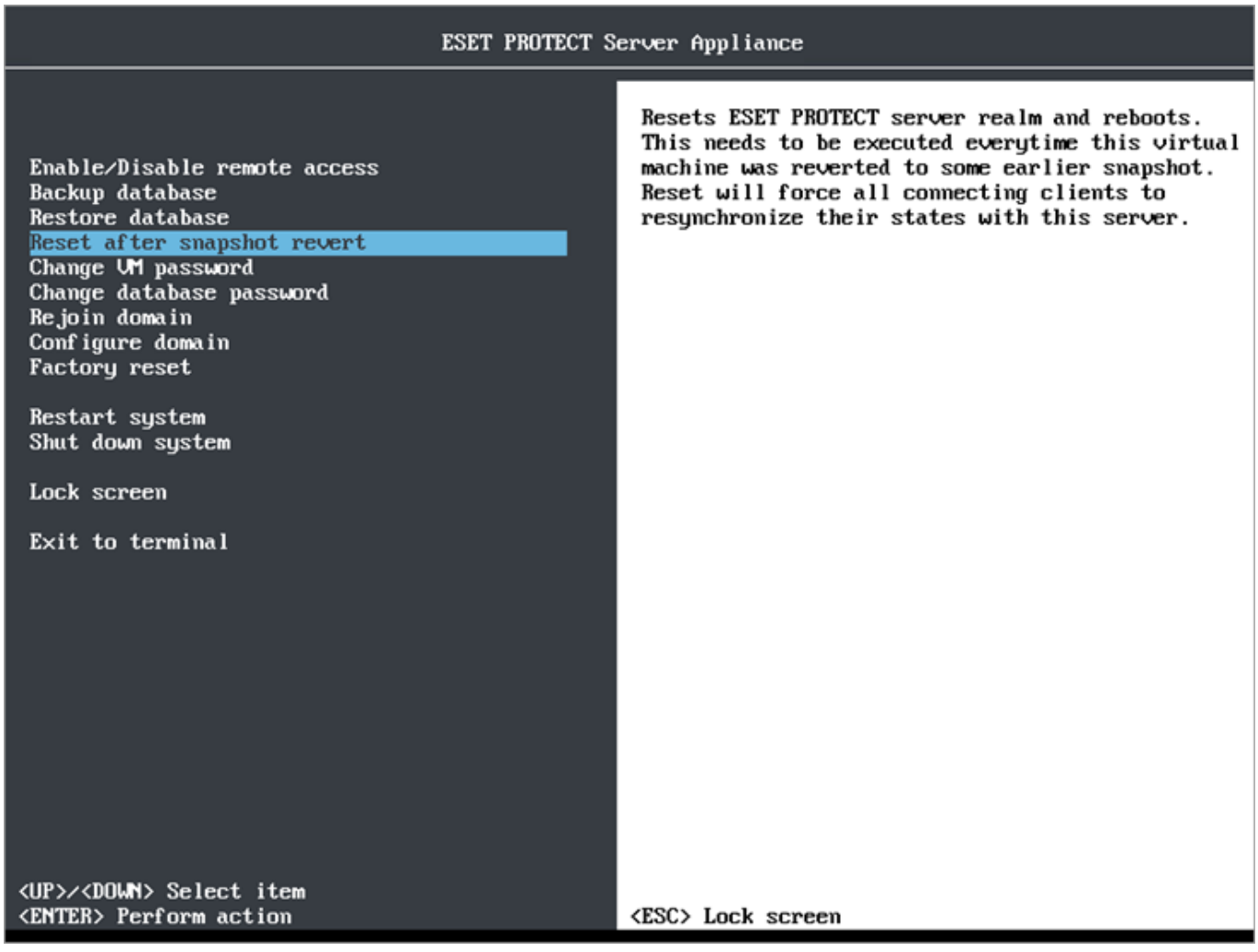
V závislosti na velikosti databáze může tato operace chvíli trvat.

Vždy zkontrolujte, zda není na obrazovce nějaké chybové hlášení. V případě výskytu chyby nelze považovat obnovení za úspěšné. V takovém případě zkuste **obnovení databáze** spustit znovu.

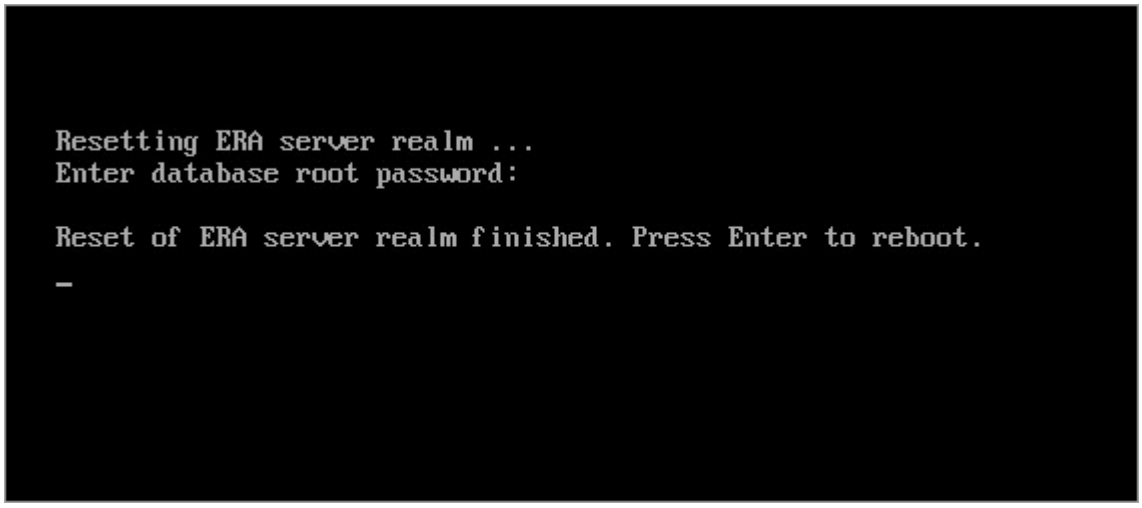
Reset po obnovení snapshotu

Kdykoli obnovíte snapshot virtuálního zařízení do jeho dřívějšího stavu, je nutné spustit funkci **Reset after snapshot revert** k vynucení synchronizace stavů všech klientů se serverem.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Reset after snapshot revert** a potvrďte stisknutím klávesy **Enter**.



2. Předtím, než dojde k resetování **ESET PROTECT Server realm**, budete vyzváni k zadání databazového root hesla.



Migrace databáze ze starého serveru

Pomocí této funkce můžete přemigrovat obsah ESET PROTECT databáze ze staré virtuální appliance do nové. Tato funkce podporuje migraci pouze ESET PROTECT serveru, nikoli jiných komponent jako je MDM. Využít ji můžete také pro aktualizaci ESMC nebo starší ESET PROTECT virtuální appliance na nejnovější verzi nebo migraci stávající ESET PROTECT VA.

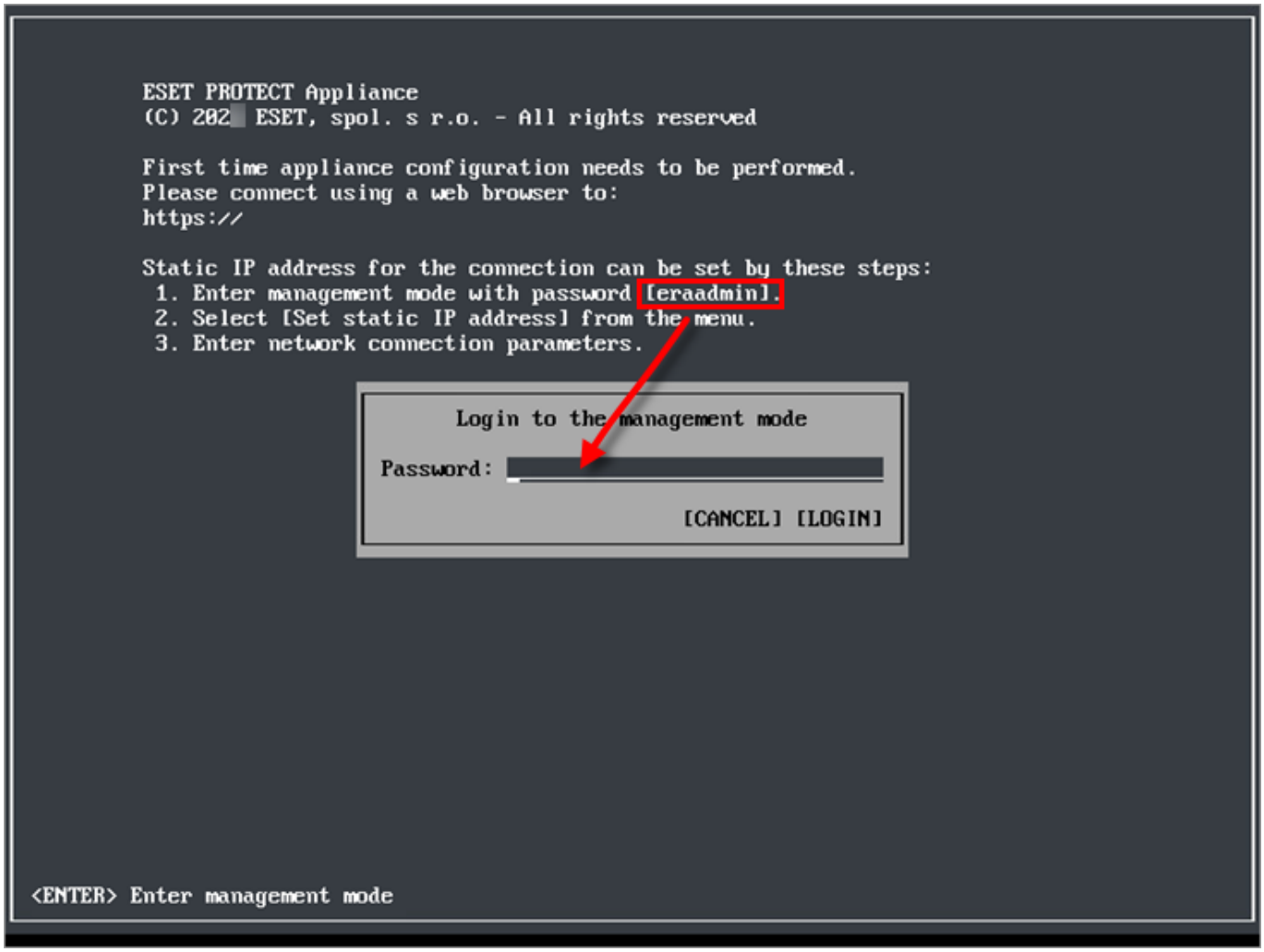
Pokud jste prováděli migraci, ponechte v chodu původní ESET PROTECT virtuální appliance a prostřednictvím ní nasměrujte agenty na nový server. V opačném případě by se agenti stále snažili připojovat ke staré ESET PROTECT VA.
Ujistěte se. že máte na původní ESET PROTECT VA povolen SSH přístup.
Databázi je možné přemigrovat pouze v případě, kdy na nové virtuální appliance běží ESET PROTECT Server ve stejné nebo novější verzi. V průběhu migrace dojde k aktualizaci struktury databáze, proto není možné migrovat na starší verzi. Přenesení databáze patří mezi jeden ze dvou způsobů, jak můžete aktualizovat svou VA.

Pro migraci databáze postupujte podle níže uvedených kroků:

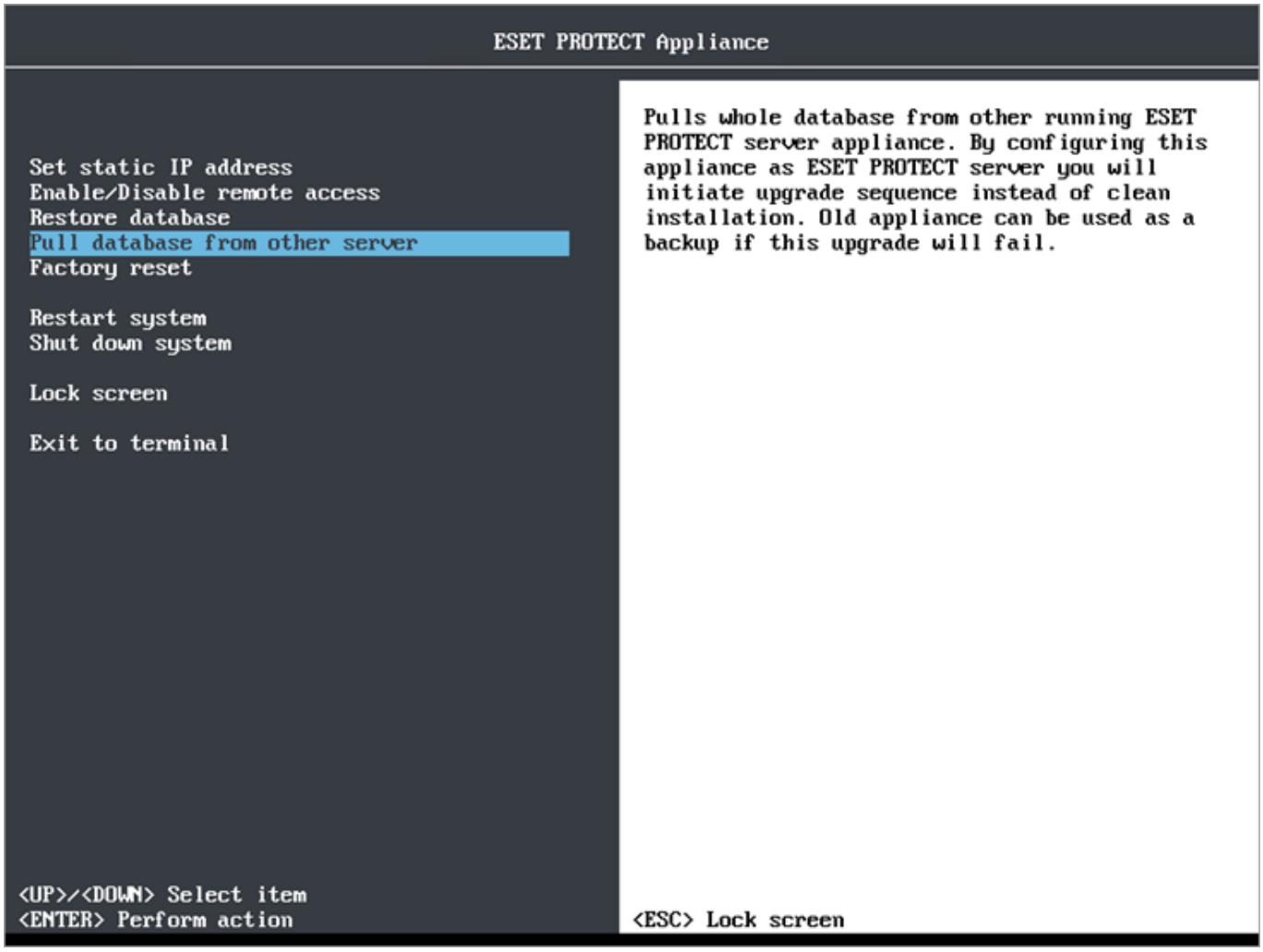
1. Nasaďte novou ESET PROTECT VA, ale zatím ji nekonfigurujte.

2. Na úvodní obrazovce nové ESET PROTECT virtuální appliance stiskněte klávesu **Enter** a přejděte do **režimu správy**.

3. Zadejte heslo `eraadmin` a potvrďte jej **dvojitým** stisknutím klávesy **Enter**.



4. Pomocí šipek vyberte z dostupných možností **Pull database from other server** a potvrďte stisknutím klávesy **Enter**.



5. Zadejte **heslo databázového uživatele root** pro přístup k databázi na původní ESET PROTECT VA, ze které chcete databázi importovat. Pokud jste heslo neměnili, je stejné jako heslo pro přístup do původní ESET PROTECT VA.

6. **Enter connection to remote ESET PROTECT VA (SSH)** – zadejte heslo uživatele `root` a název/IP adresu ESET PROTECT virtuální appliance ve formátu: `root@IPaddress` or `root@hostname`

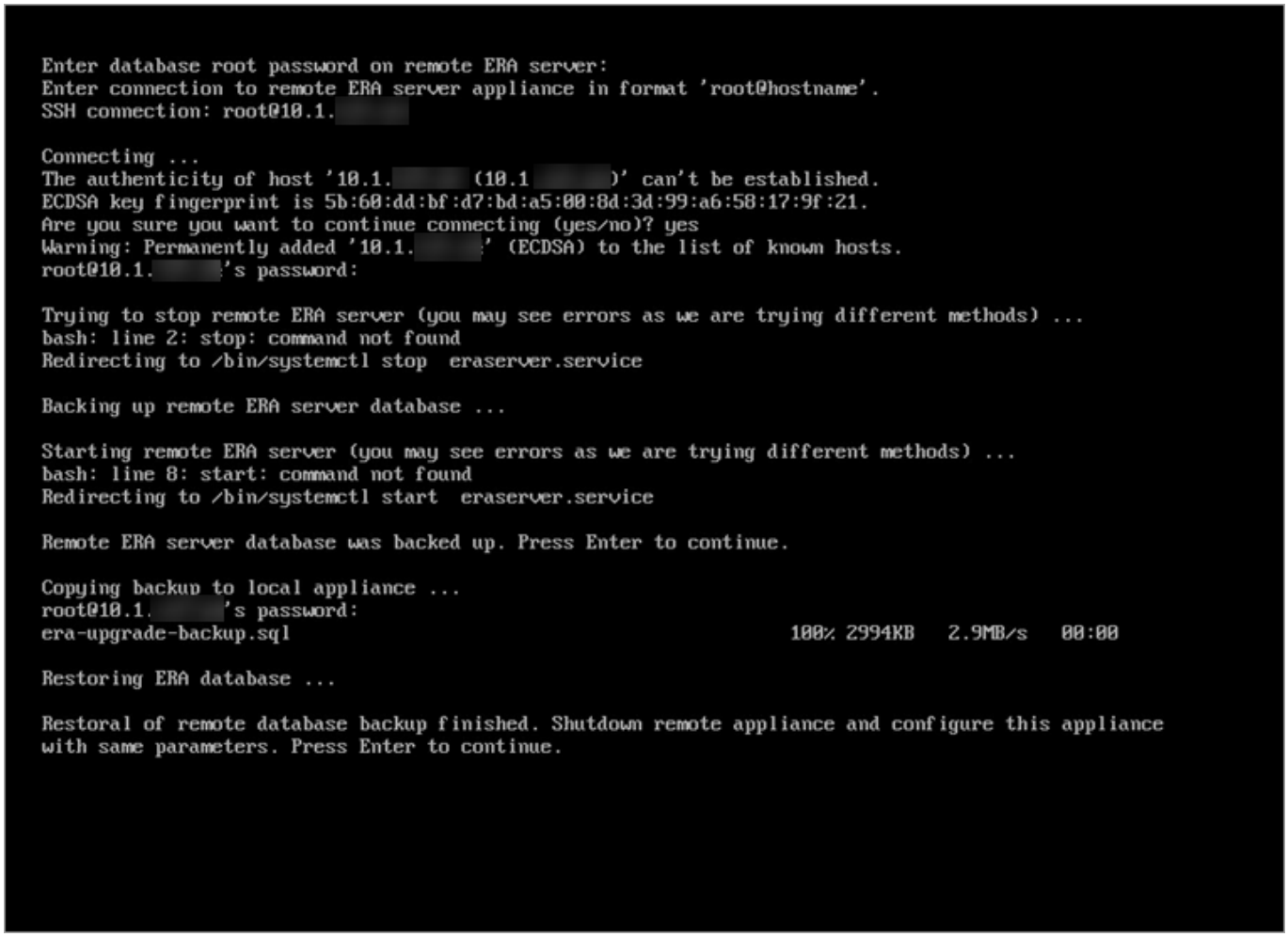
7. V případě, že budete vyzváni k ověření (**The authenticity of host**), zadejte `yes`. V opačném případě tento krok ignorujte.

8. Zadejte **heslo pro přístup k virtuálnímu stroji** původní ESET PROTECT virtuální appliance a stiskněte klávesu **Enter**. Po dokončení se zobrazí informace **Remote ERA Server database was backed up**.

i V závislosti na velikosti databáze může tato operace chvíli trvat.

9. Znovu zadejte **heslo pro přístup k virtuálnímu stroji** původní ESET PROTECT virtuální appliance. V případě velkých databází můžete být k tomuto kroku vyzváni opakovaně.

10. Vyčkejte na obnovení databáze.



11. Pokud provádíte aktualizaci: Po úspěšném přenesení ESET PROTECT databáze původní ESET PROTECT VA vypněte.

- Smažte ji ale až ve chvíli, kdy si budete jisti, že nová ESET PROTECT virtuální appliance funguje správně.
- Důrazně nedoporučujeme pro odinstalaci starého ESET PROTECT VA Serveru používat odinstalační skript.

Tím dojde zároveň k odasociování (odstranění) všech licencí z nového ESET PROTECT serveru (jeho databáze). Pro zabránění vzniku této situace smažte před odinstalovám databázi starého ESET PROTECT serveru (příkazem `DROP DATABASE`).

12. Nakonfigurujte novou appliance:

- **Aktualizace** – v tomto případě nastavte ESET PROTECT virtuální appliance stejně jako původní.
- **Migrace** – pokud jste přesouvali ESET PROTECT VA do jiné sítě, upravte konfiguraci domény (viz kapitolu připojení do domény a opětovné připojení do domény), případně síťového adaptéru.

Ujistěte se, že máte dostupná všechny data, všichni klienti se připojují k novému serveru a ESET PROTECT VA se chová stejně jako předchozí,

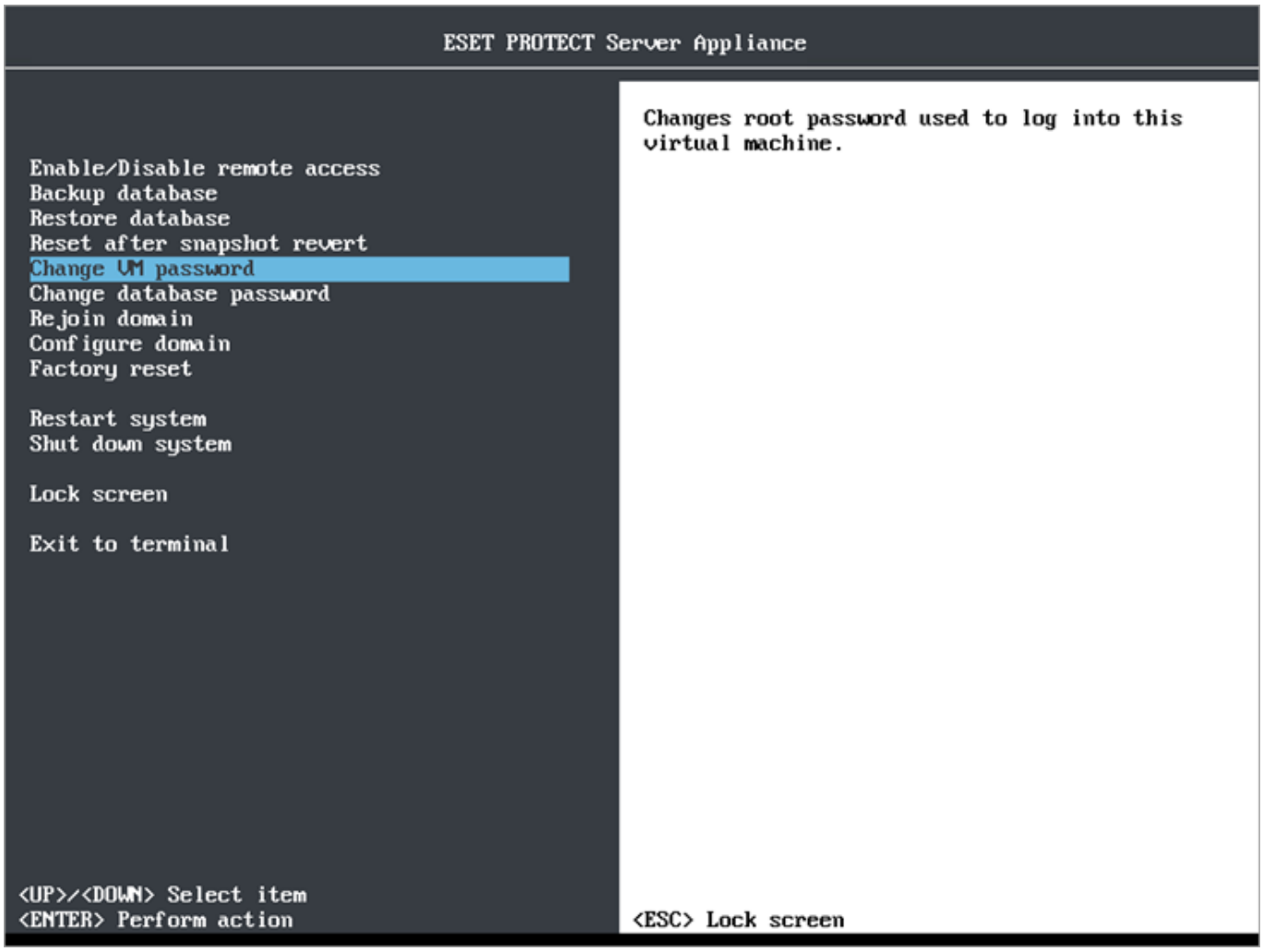
Změna hesla do virtuálního stroje

Heslo do virtuálního stroje se používá pro přihlášení do nasazené ESET PROTECT virtuální appliance. Pokud chcete změnit heslo do virtuálního stroje nebo nechcete více zabezpečit váš virtuální počítač, doporučujeme používat silná hesla a pravidelně je měnit.

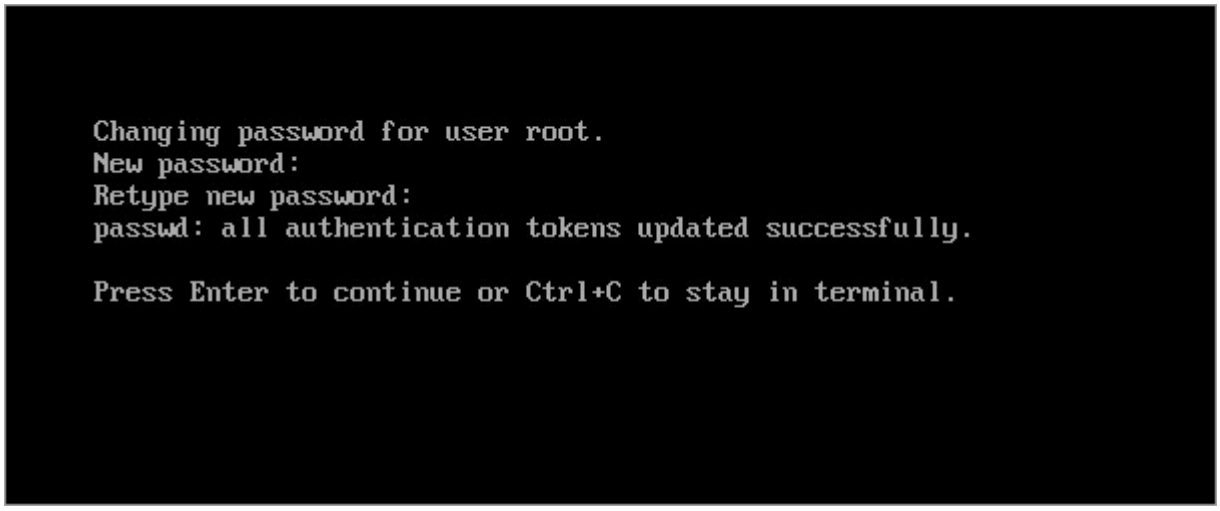
Pomocí těchto kroků změníte pouze heslo pro přístup do virtuální appliance. Heslo pro přístup do ESET PROTECT Web Console a heslo databázového uživatele root zůstane beze změny. Více informací naleznete v kapitole hesla na ESET PROTECT virtuální appliance.

Pokud jste heslo zapomněli, přejděte do kapitoly Zapomněl jsem heslo pro přístup do ESET PROTECT VA, co mám dělat.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu **Enter**, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Change VM password** a potvrďte stisknutím klávesy **Enter**.



2. Do prázdného pole zadejte vaše **Nové heslo**, stiskněte klávesu **Enter** a zadejte jej **znovu** pro potvrzení.

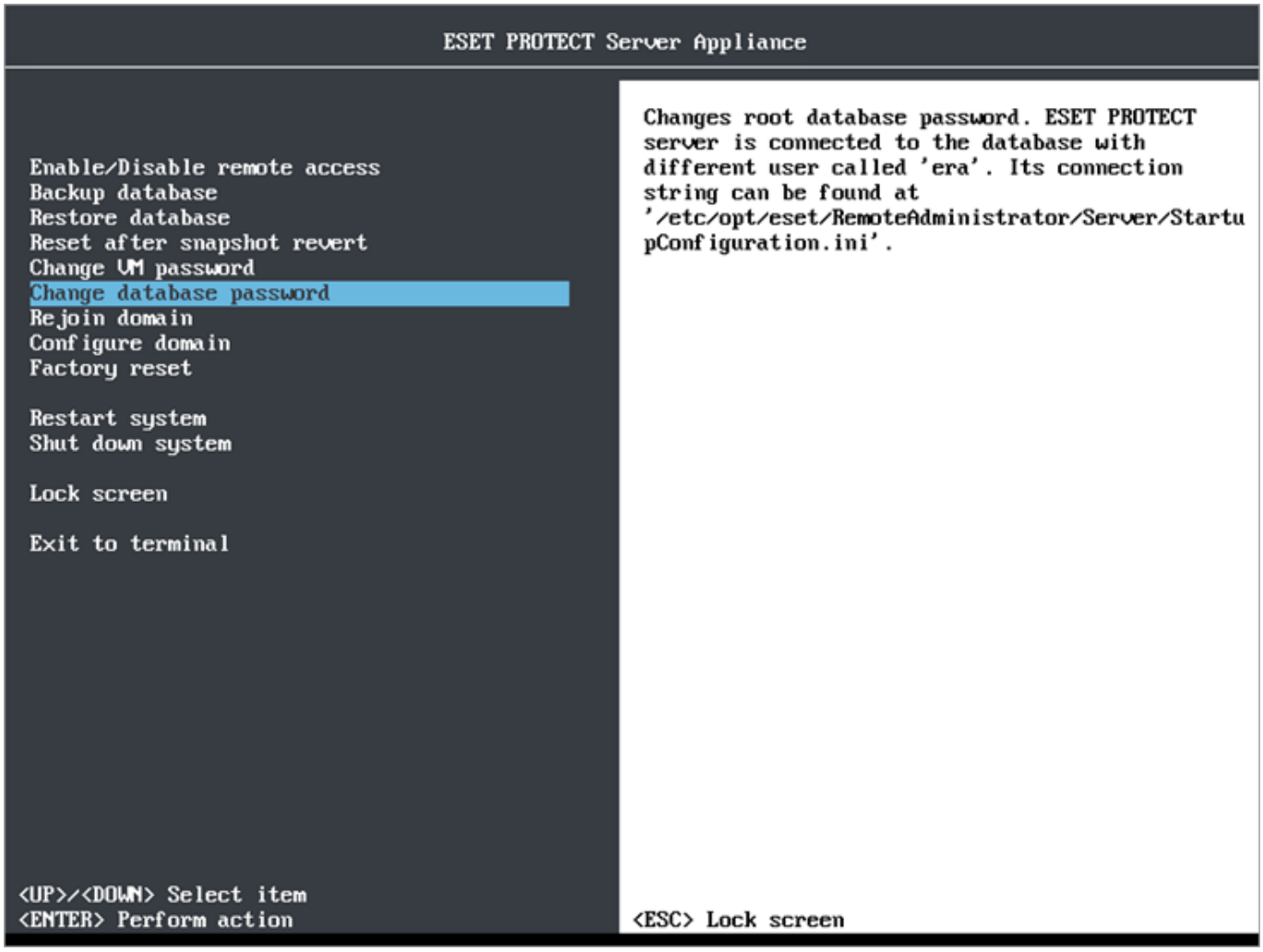


Po úspěšné změně hesla se zobrazí informace all authentication tokes updated successfully. Při příštím přihlášení již použijte **nové heslo**.

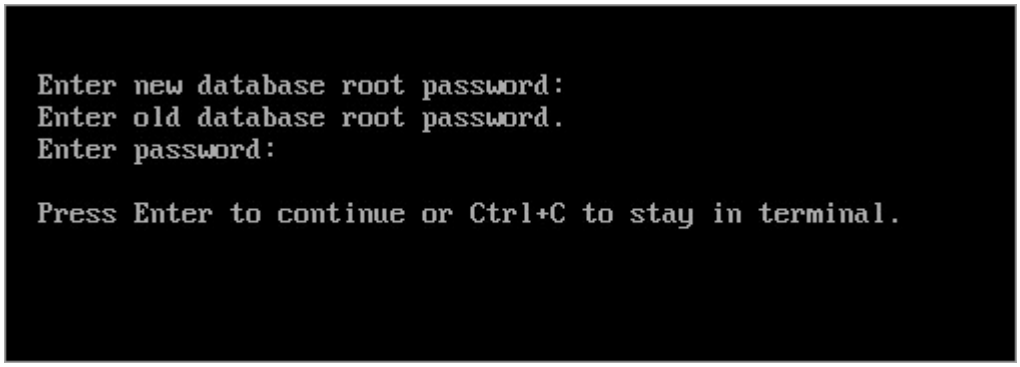
Change database password

Prostřednictvím hesla databázového uživatele `root` získáte úplný přístup k MySQL databázovému serveru. MySQL uživatel `root` má úplnou kontrolu pouze nad MySQL serverem.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu **Enter**, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Change database password** a potvrďte stisknutím klávesy **Enter**.



2. Po zobrazení výzvy **Enter old database root password** zadejte heslo, které jste zadali v průběhu konfigurace ESET PROTECT virtuální appliance. Pokud jste jej měnili samostatně, může být odlišné od hesla k **virtuálnímu stroji** (VM).



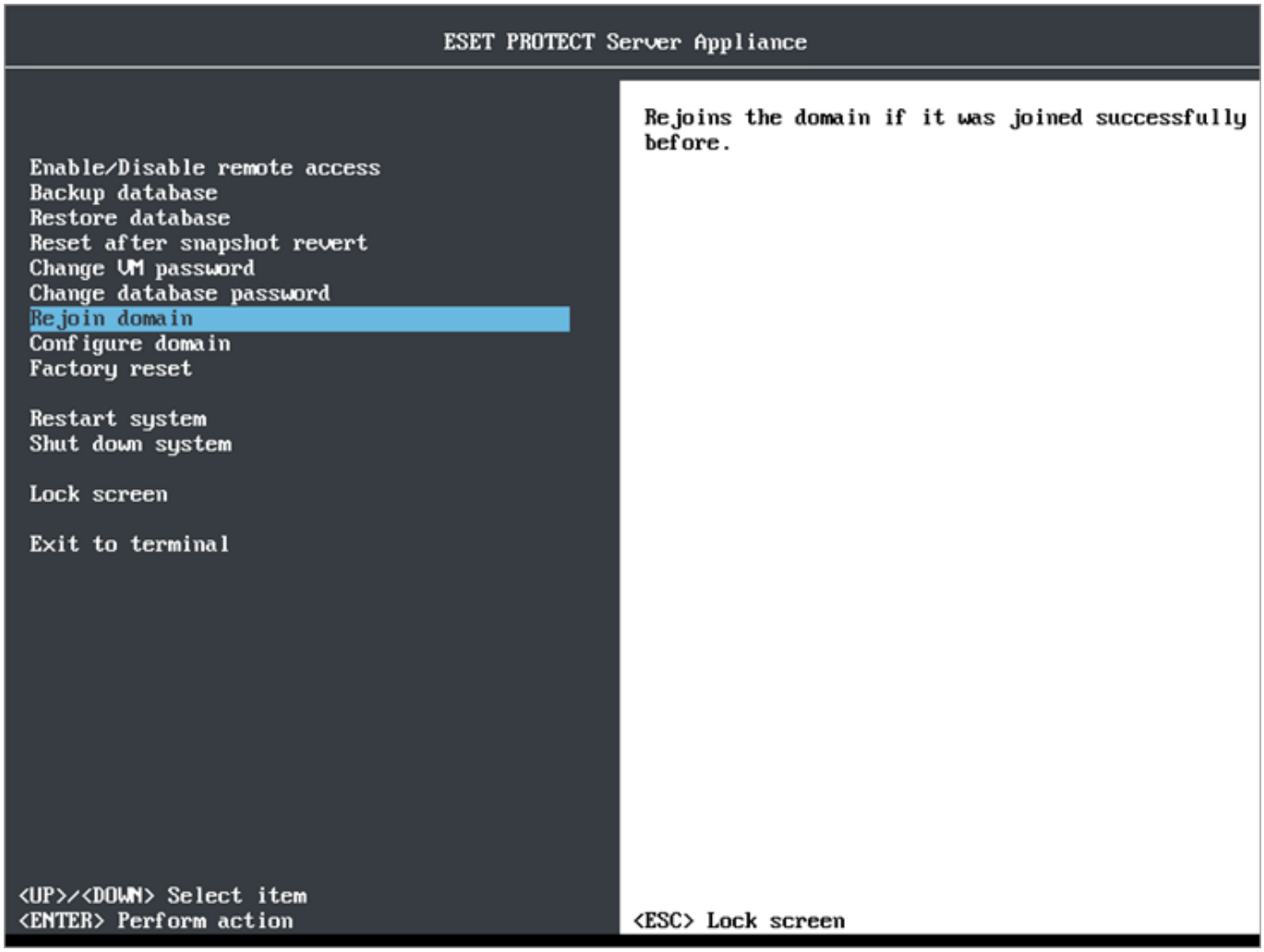
Heslo bylo úspěšně změněno.

Opětovné připojení do domény

Pokud došlo k porušení důvěry nebo pozorujete jiné potíže týkající se Active Directory, pomocí této možnosti můžete virtuální stroj znovu připojit do domény.

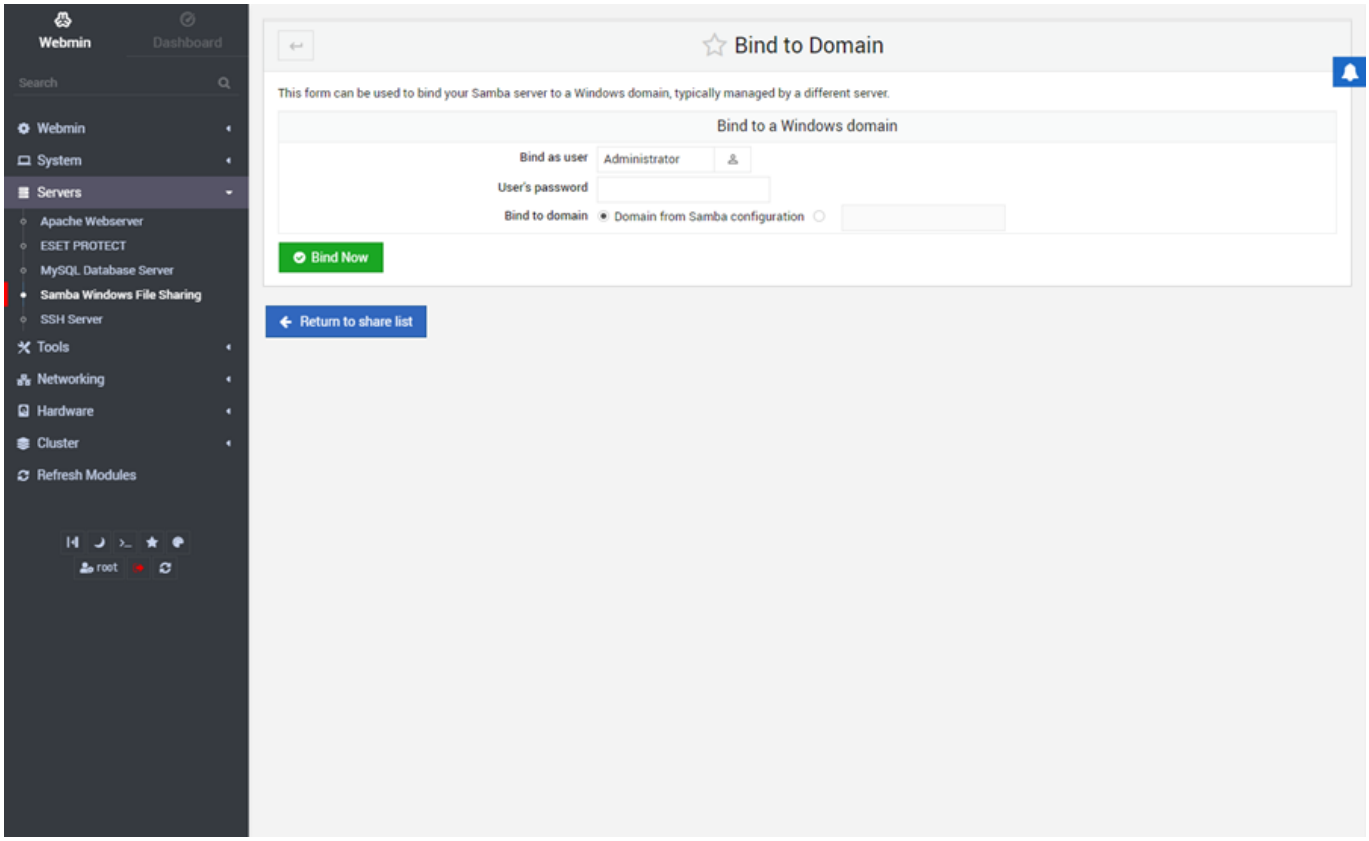
Pro použití této funkce je nezbytné správně nakonfigurovat připojení do domény.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Rejoin domain** a potvrďte stisknutím klávesy **Enter**.



2. Zadejte uživatelské jméno a heslo doménového uživatele, který má oprávnění přidávat počítače do domény.

Pokud nemáte zkušenosti se systémem Linux a terminálem, můžete parametry Samba Windows File Sharing konfigurovat prostřednictvím Webminu a funkce **Bind to Domain**.



Configure domain

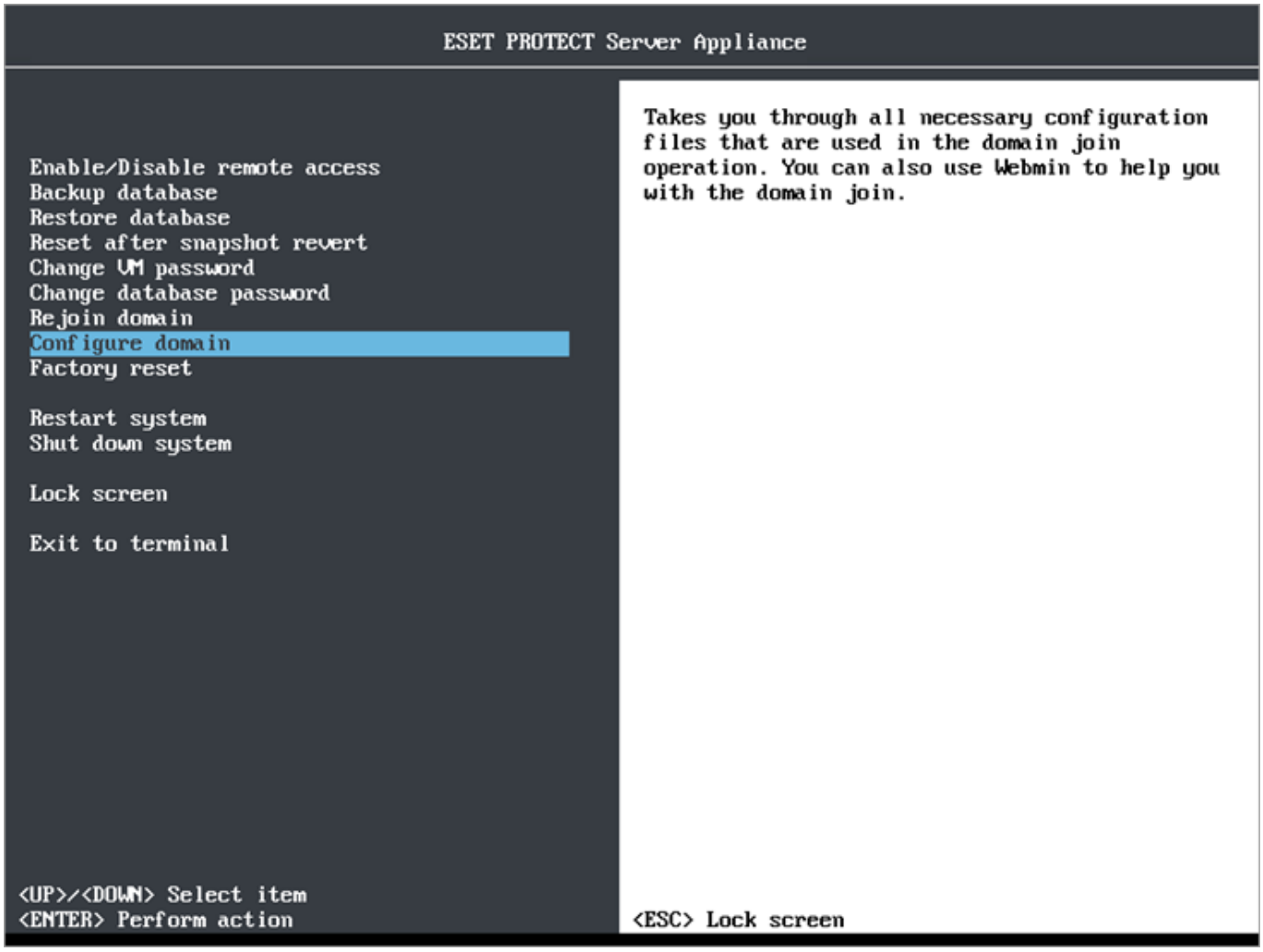
Připojení do domény obvykle selže z důvodu nesprávné konfigurace souborů dostupných v ESET PROTECT VA. Funkce **Configure Domain** vás provede konfigurační potřebných souborů, ve kterých definujte své prostředí. Nakonfigurovat je nutné níže uvedené soubory:

Název souboru	Popis
/etc/hosts	Soubor Hosts by měl obsahovat název a IP adresu vašeho doménového řadiče.
/etc/krb5.conf	Konfigurační soubor Kerberos musí být správně nakonfigurován. Pro ověření správné konfigurace použijte příkaz `kinit <user-from-domain>`.
/etc/ntp.conf	Do konfiguračního souboru NTP byste měli přidat záznam pro pravidelnou synchronizaci času vůči doménovému řadiči.
/etc/samba/smb.conf	Konfigurační soubor Samba musí být správně nakonfigurován.

Tyto soubory se v systému již nachází a je potřeba do nich doplnit pouze správné údaje jako je název domény, DNS server, informace o doménovém řadiči atp.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu **Enter**, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Configure domain** a potvrďte stisknutím klávesy **Enter**.

> Tento pokročilý postup je určen výhradně pro zkušené administrátory.



2. Stiskněte klávesu **Enter** a upravte první konfigurační soubor.

3. Pomocí kláves **CTRL + X** ukončete textový editor. Změny uložte stisknutím klávesy **Y**. Pokud nechcete změny uložit stiskněte klávesu **N**. V případě, že jste neprovedli v souboru žádné změny, textový editor se ukončí. Pokud chcete v souboru provést další změny, místo kláves **Ctrl + X** stiskněte **CTRL + C** pro přerušení operace a návrat zpět do textového editoru. Vzorové příklady konfigurace naleznete v Databázi znalostí.

> Více informací o připojení virtuální appliance do domény naleznete v souboru */root/help-with-domain.txt*. Pro jeho zobrazení můžete na ESET PROTECT VA využít Webmin File manager. Alternativně si jej otevřete v textovém editoru příkazem `nano help-with-domain.txt`.
> Pokud nemáte zkušenosti se systémem Linux a terminálem, můžete parametry pro připojení do domény (Kerberos, NTP nebo nastavení sítě) konfigurovat prostřednictvím Webminu a funkce Samba Windows File Sharing.

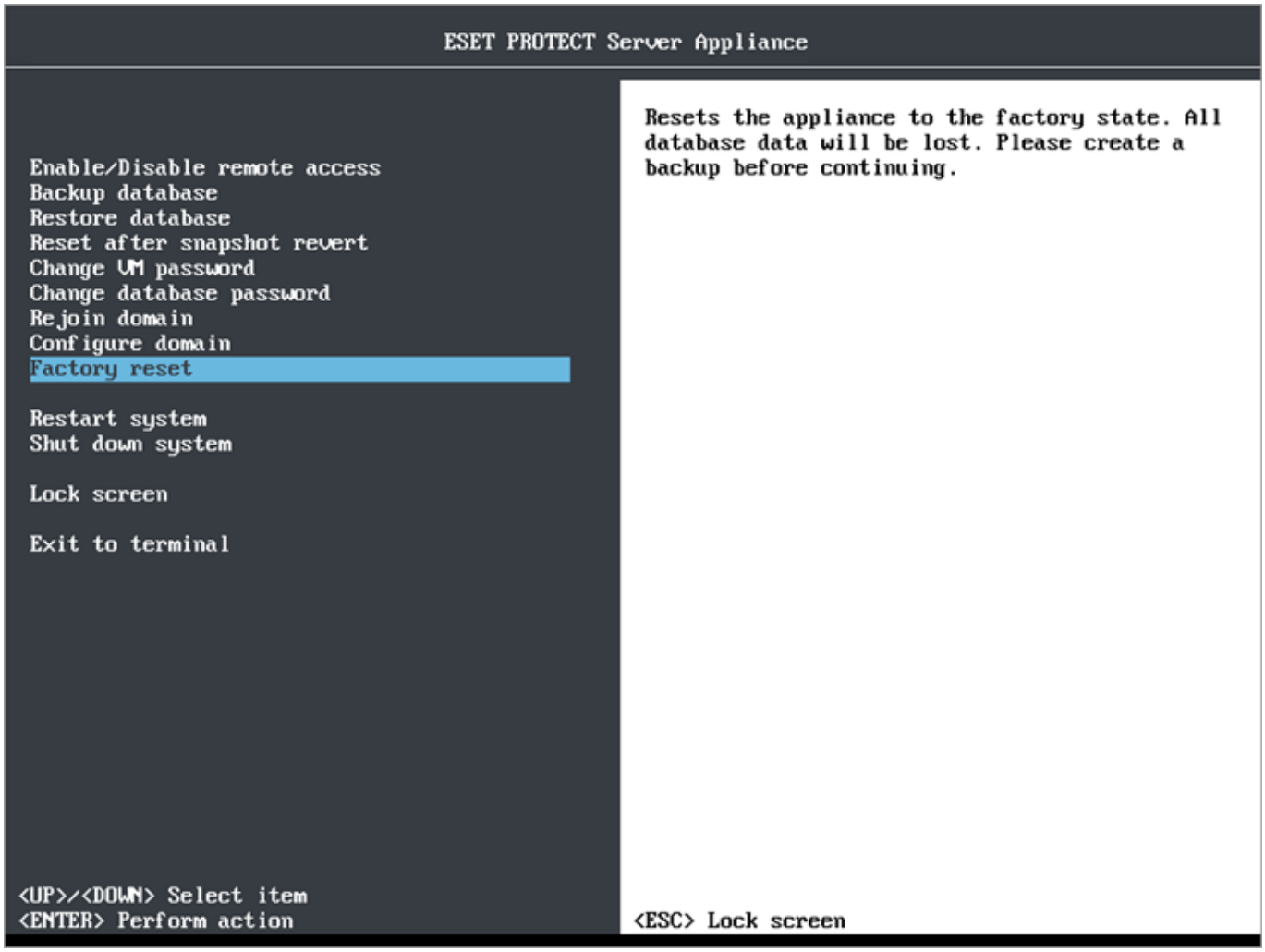
4. Po dokončení konfigurace vyberte možnost **Rejoin domain** a zadejte údaje administrátora (uživatelské jméno a heslo) pro připojení appliance do domény.

Factory reset

Pokud chcete vrátit ESET PROTECT virtuální appliance do **výchozího stavu**, v jakém byla po nasazení a nastavit si ji znovu, můžete k tomu použít právě tuto úlohu. Po jejím spuštění dojde k odstranění všech ESET PROTECT komponent včetně databáze a souvisejících nastavení.

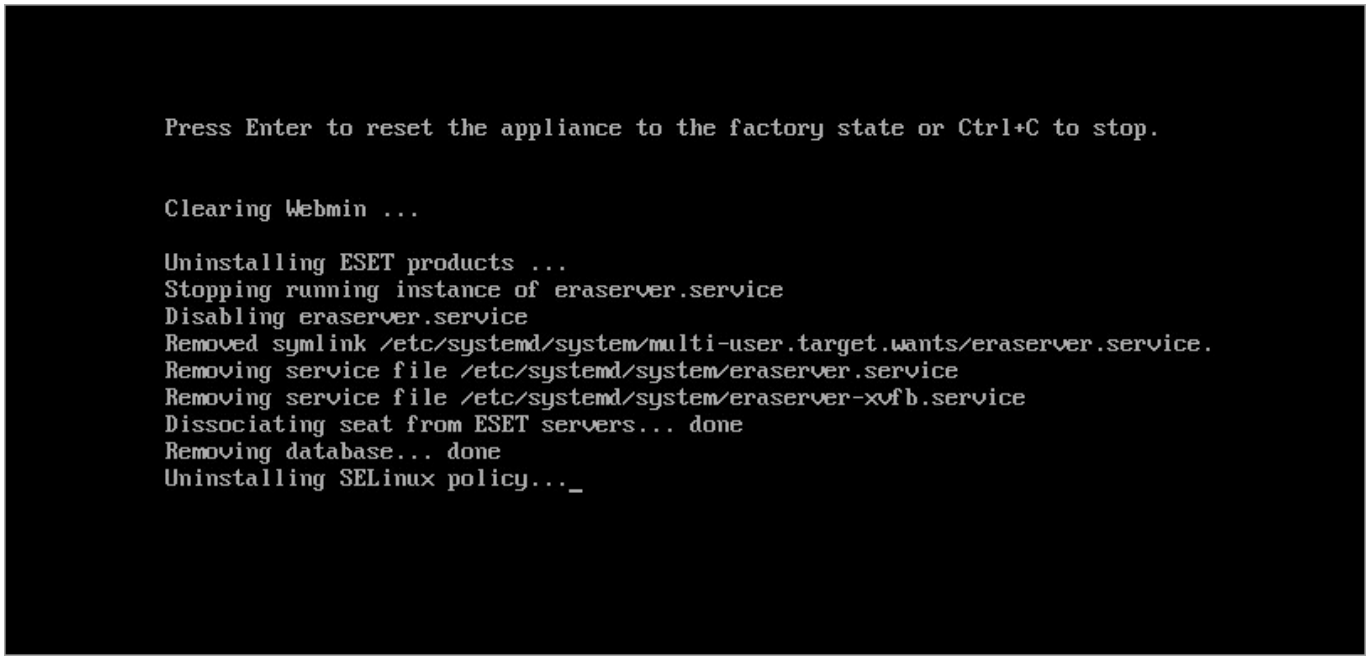
Před obnovením do **továrního nastavení** doporučujeme provést zálohu ESET PROTECT databáze. V průběhu obnovení dojde k zahození databáze.
Na **výchozí hodnoty** se obnoví pouze hodnoty, které jste změnili prostřednictvím prvotní konfigurace ESET PROTECT VA, ostatní nastavení zůstanou beze změny. V ojedinělých případech se obnovení do **továrního nastavení** nemusí zdařit. V takovém případě doporučujeme nasadit novou ESET PROTECT virtuální appliance. Dále pokračujte kroky z kapitoly aktualizace a migrace nebo disaster recovery.

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Factory reset** a potvrďte stisknutím klávesy **Enter**.



2. Potvrďte stisknutím klávesy **Enter** a **vyčkejte na provedení všech akcí**. Pokud jste se rozhodli, že nechcete obnovit nastavení ESET PROTECT VA, stále se můžete pomocí kláves **CTRL + C** vrátit zpět.

Stisknutí kláves **CTRL + C** v průběhu procesu obnovení **může vést k poškození** virtuální appliance.



Pokud se na obrazovce zobrazí chyby, zkuste appliance **obnovit znovu** do továrního nastavení. V případě, že obnovení appliance do **továrního nastavení** nepomůže, doporučujeme nasadit novou appliance a dále postupuje podle kroků uvedených v kapitole aktualizace a migrace nebo disaster recovery.

Při obnovení **továrního nastavení** dojde k:

- resetování nastavení sítě, obnovení hesel a názvu stroje
- deaktivování Webminu, smazání konfiguračních souborů, balíčků a systémových protokolů
- odstranění všech dat z ESET PROTECT databáze
- obnovení hesla databázového uživatele ESET PROTECT

Po restartování ESET PROTECT virtuální appliance bude v původním stavu, jako po čerstvém nasazení, a připravena ke konfiguraci.

Vámi provedené změny a nastavení nesouvisející s ESET PROTECT zůstanou beze změny.

Webmin – rozhraní pro správu

Webmin je webové rozhraní třetí strany, prostřednictvím kterého můžete snadno spravovat operační systém CentOS, na kterém běží virtuální appliance. Webmin je určen pro uživatele, kteří mají základní zkušenosti s operačním systémem Linux, ale nejsou obeznámeni s komplexností správy systému. Prostřednictvím webového rozhraní můžete tyto úlohy snadno provádět a automaticky za vás aktualizujte potřebné konfigurační soubory. Díky tomu se stává správa systému mnohem snadnější.

- Webmin si můžete, stejně jako Web Console, zobrazit z jakéhokoli zařízení v síti a disponuje internetovým prohlížečem. Jeho používání prostřednictvím sítě je jednodušší než používání lokálních aplikací s grafických rozhraním.
- Aktuální verze Webminu je možné používat pro komerční i nekomerční použití zcela zdarma. Podrobnější informace naleznete na webových stránkách Webmin.

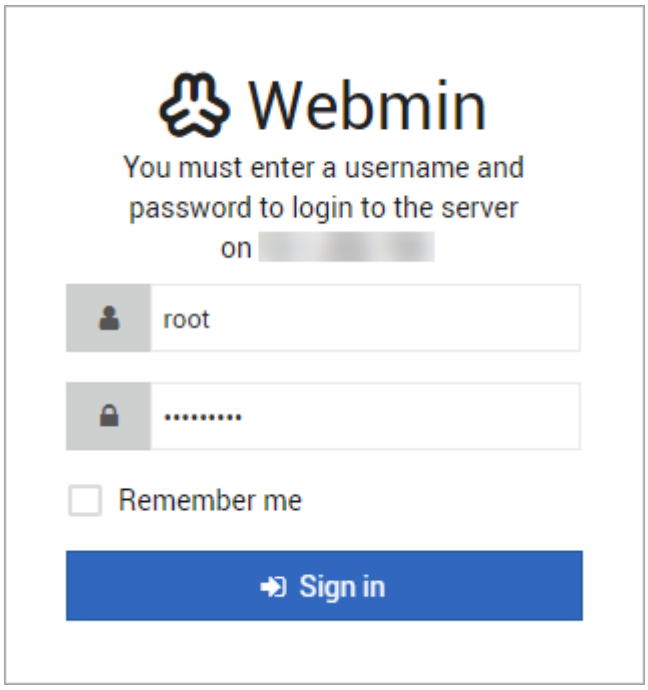
Webmin je součástí ESET PROTECT virtuální appliance. Pokud jej chcete používat, nejprve je nutné jej aktivovat. Webmin běží na HTTPS a portu 10000. Po jeho aktivování se na ESET PROTECT úvodní obrazovce virtuální appliance zobrazí informace, že je aktivní a na jaké IP adrese je dostupný.

Přístup k Weminu:

Pro přístup k Webmin webovému rozhraní zadejte do internetového prohlížeče název/IP adresu ESET PROTECT VA a port 10000. Adresa by měla být ve formátu: *https://<host name or IP address>:10000*.
Příklad:*https://10.1.119.162:10000* nebo *https://esmcva:10000.*

Zadejte přihlašovací údaje:

- uživatelské jméno: **root**
- výchozí heslo je **eraadmin**. Pokud jste si v průběhu prvotní konfigurace ESET PROTECT VA nastavili vlastní, zadejte své heslo.



Po úspěšném přihlášení se zobrazí Webmin nástěnka.

Nástěnka

Po přihlášení do Webminu se zobrazí **nástěnka**, na níž jsou uvedeny základní systémové informace o vaší ESET PROTECT virtuální appliance. Mezi dostupnými údaji na název stroje, operační systém, doba běhu, využití paměti atp. V dolní části se mohou zobrazit upozornění, která mohou vyžadovat vaši interakci. Například, pokud je dostupný aktualizace Webminu, provedete ji přímo z oznámení kliknutím na tlačítko **Upgrade Webmin Now**. Webmin doporučujeme pravidelně aktualizovat. Po dokončení aktualizace se zobrazí informace **Webmin install complete**.

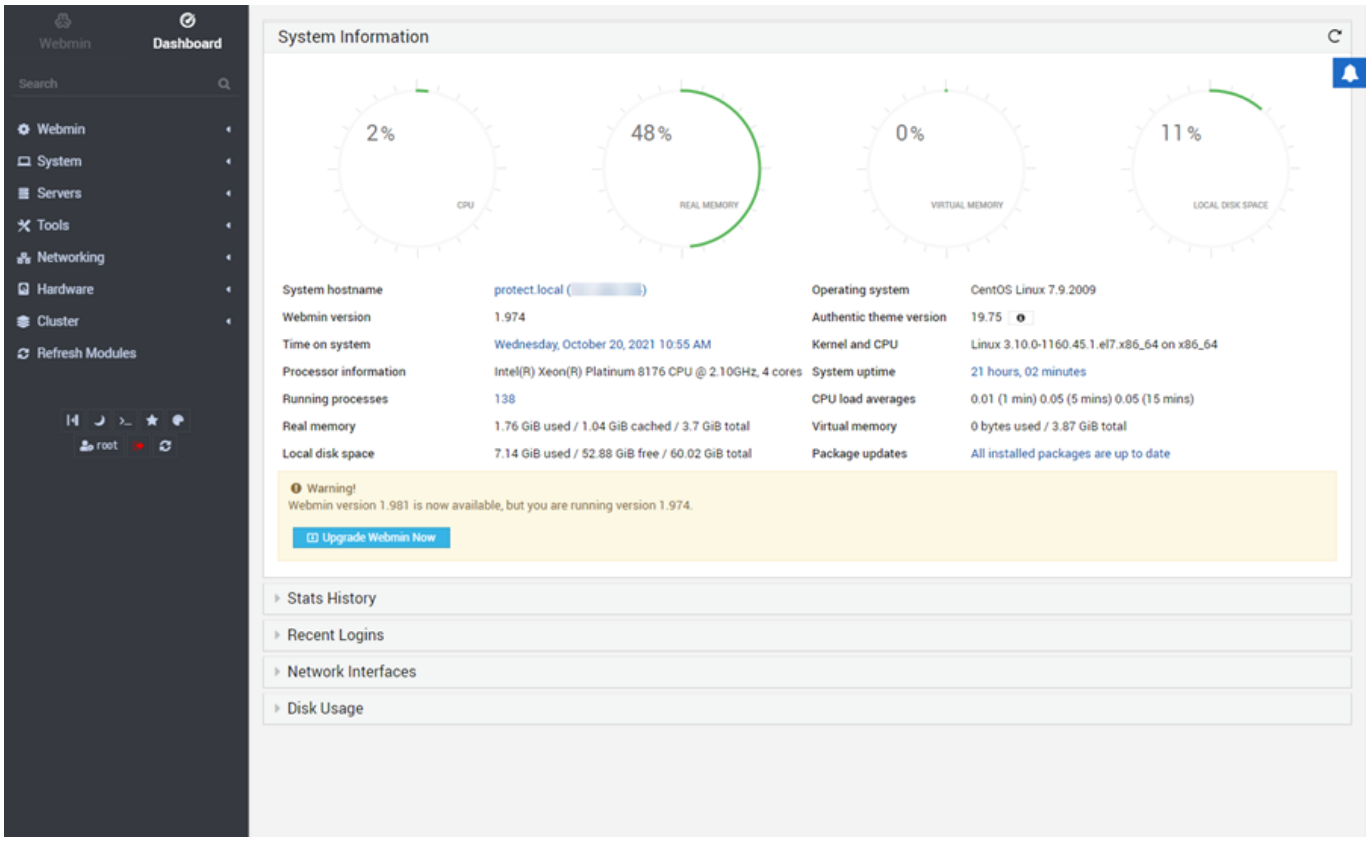
V hlavním menu jsou dostupné tyto moduly: **Webmin**, **System**, **Servers**, **Tools**, **Networking**, **Hardware** a **Cluster**. Pro více informací o jednotlivých modulech se podívejte do dokumentace Webminu.

Webmin automaticky detekuje konfiguraci virtuální appliance a zobrazuje vždy relevantní moduly.

Pro správu ESET PROTECT virtuální appliance budete ve většině případů potřebovat tyto moduly:

- System
- Servers
- Nástroje
- Networking

Mějte na paměti, že Webmin běží s úplnými právy uživatele **root**. To znamená, že prostřednictvím webového rozhraní můžete měnit/vytvářet soubory a spouštět libovolné příkazy a skripty. Při neopatrném použití můžete nechtěně smazat důležité soubory a znefunkčnit virtuální stroj. Z tohoto důvodu buďte při používání Webminu opatrní. Pokud budete provádět potenciálně nebezpečné akce, Webmin vás na to upozorní. Přesto doporučujeme provádět pouze akce, u kterých jste si jisti, co děláte.



Oznámení – vás může upozornit například na dostupnost nové verze. Tato informace a všechny další se zobrazí v dolní části nástěnky.

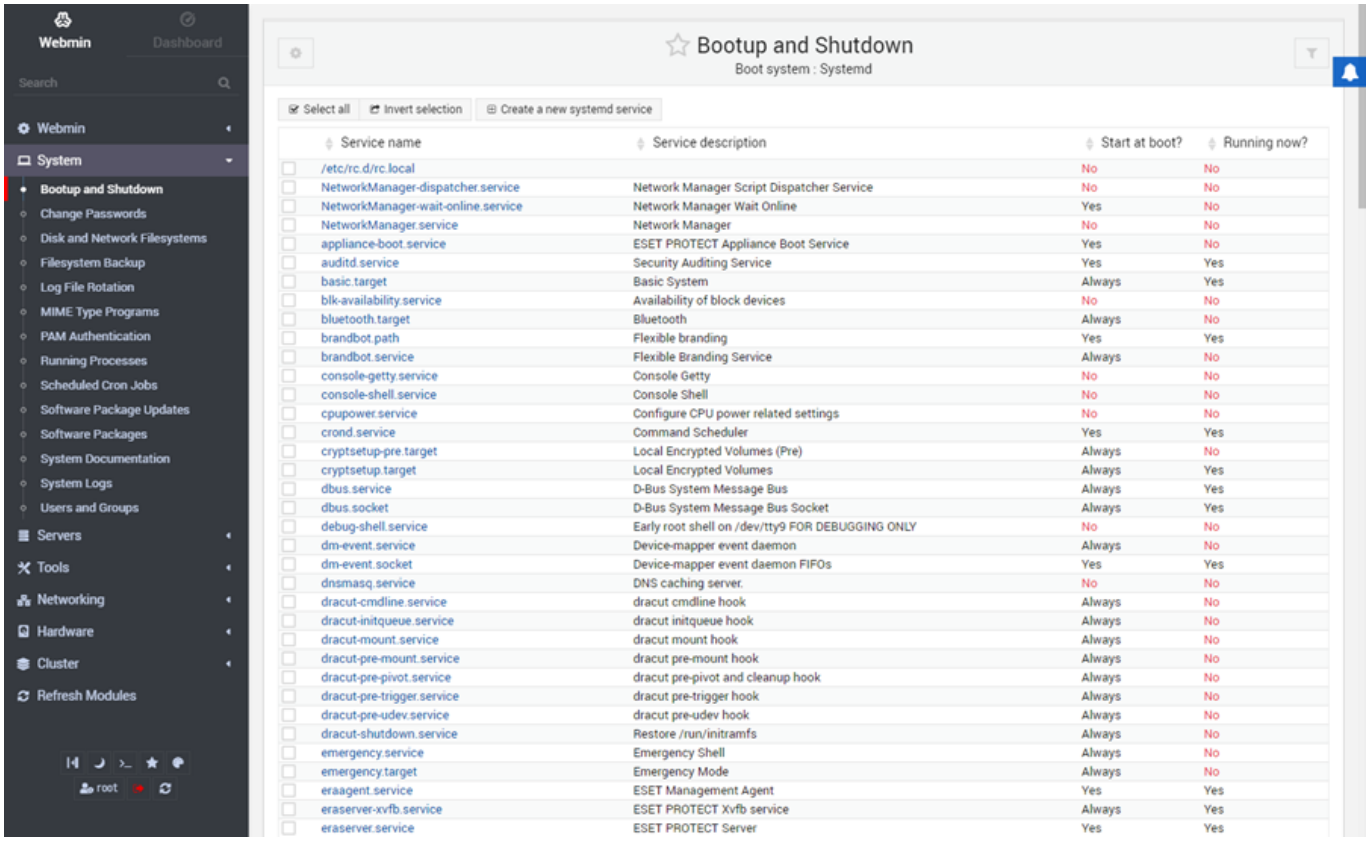
Odhlášení – pro odhlášení klikněte v levém menu na tlačítko s ikonou  .

System

V této části můžete konfigurovat některé moduly **systému**:

Bootup and Shutdown – prostřednictvím tohoto modulu můžete spravovat služby, modifikovat je, spustit/zastavit/restartovat služby jednotlivě nebo hromadně. Vytvářet a upravovat můžete rovněž skripty spouštěné při startu nebo vypínání systému. V dolní části stránky se nachází tlačítka pro **restart** nebo **vypnutí**

virtuálního počítače s ESET PROTECT.



Change Passwords – v této části můžete změnit hesla jednotlivých uživatelů operačního systému.

> Tuto možnost nepoužívejte, pokud chcete změnit heslo pro přístup do virtuálního stroje, případně heslo databázového uživatele. K tomuto účelu využijte v konzole pro správu ESET PROTECT možnost Change VM password nebo Change database password.

Running Processes – prostřednictvím tohoto Webmin modulu si můžete spravovat všechny běžící procesy. Běžící procesy v systému si můžete zobrazit, ukončit je, změnit jejich prioritu, případně spustit další.

Software Package Updates – tento modul zobrazuje seznam dostupných aktualizací a přímo z něj můžete aktualizovat vybrané/všechny balíčky.

System Logs – v této části si můžete zobrazit systémové protokoly a případně zde můžete změnit umístění pro ukládání protokolů.

Servers

V této části můžete konfigurovat některé **serverové** moduly:

Apache Webserver – jedná se o jeden z nejkomplexnější a nejužitečnější modul, pomocí nějž můžete konfigurovat většinu funkční webového serveru Apache. Využít jej můžete jako HTTP Server pro distribuci instalačních balíčků nebo aktualizací. Nezapomeňte však následně ve firewallu povolit potřebné porty.

> Nejedná se o stejný webový server, který pohání ESET PROTECT Web Console. Tento Apache můžete použít pro vlastní potřebu a libovolně si jej konfigurovat.

ESET PROTECT – prostřednictvím tohoto modulu můžete **spustit diagnostický nástroj**, **resetovat administrátorské**

heslo pro přístup do ESET PROTECT, **vyměnit certifikát** ESET PROTECT serveru a **importovat certifikační autoritu**, **vyměnit certifikát ESET Management Agenta** a **certifikační autoritu**, **opravit detaily připojení ESET Management Agent** nebo **upravit konfiguraci webového serveru Apache Tomcat (soubor server.xml)** z důvodu změny HTTPS certifikátu nebo šifrovacích algortimů.

MySQL Database Server – pomocí tohoto nástroje můžete konfigurovat databázový server, spravovat obsah databáze a měnit hesla uživatelům.

> Tento modul nepoužívejte k zálohování nebo obnově ESET PROTECT databáze. K danému účelu využijte konzoli pro správu ESET PROTECT VA. Více informací naleznete v kapitole zálohování databáze.

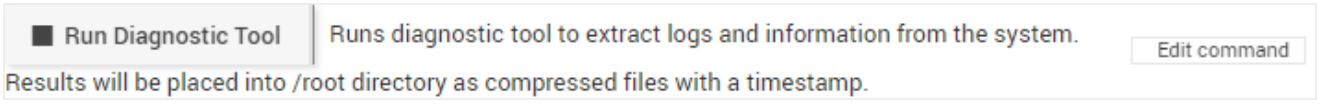
Samba Windows File Sharing – v této části můžete definovat složky, které mají být sdílené s Windows stanicemi prostřednictvím SMB (Server Message Block) protokolu. Aby sdílení fungovalo, je nutné na ESET PROTECT VA nakonfigurovat Sambu. Zároveň můžete v této části nakonfigurovat připojení appliance do domény. Pokud jste aktivovali Sambu, nezapomeňte potřebné porty povolit ve firewallu.

SSH Server – v této části můžete detailně nastavit SSH/OpenSSH server a předpokládá, že máte základní uživatelské znalosti o klientských programech. Konfigurovat zde můžete SSH server a samotné uživatele.

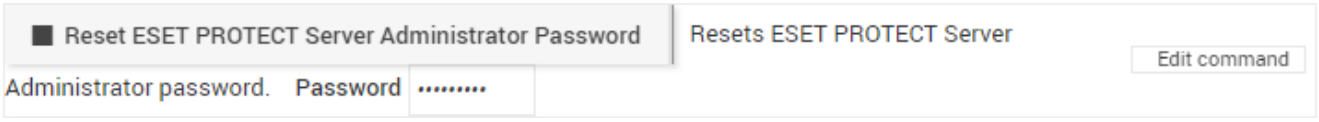
ESET PROTECT

Prostřednictvím modulu ESET PROTECT můžete **provádět předdefinované příkazy** určené k opravě/výměně ESET PROTECT certifikátů, spuštění diagnostického nástroje nebo resetování hesla pro přístup do ESET PROTECT Web Console.

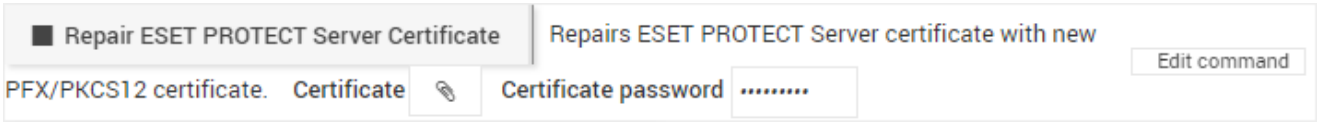
Run Diagnostic Tool – po kliknutí na toto tlačítko se spustí diagnostický nástroj a sesbírá informace ze systému. V průběhu sběru dat se exportují protokoly ESET PROTECT Serveru a ESET Management Agenta. Výsledný *.zip* archiv naleznete ve složce root a stáhnout si jej můžete například pomocí nástroje File Manager.



Reset ESET PROTECT Server Administrator Password – pokud jste zapomněli heslo pro přístup do ESET PROTECT Web Console nebo jen chcete heslo resetovat, zadejte do zobrazeného pole nové heslo a potvrďte kliknutím na tlačítko.



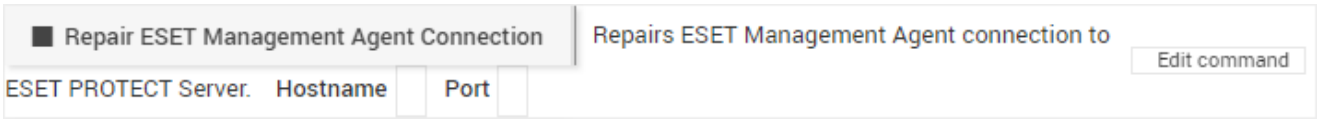
Repair ESET PROTECT Server Certificate – pomocí této možnosti můžete do ESET PROTECT Serveru nahrát nový certifikát ve formátu PFX/PKCS12. Klikněte na ikonu **sponky** a vyberte certifikát pro ESET PROTECT server (ve formátu PFX PKCS12) a klikněte na tlačítko **Otevřít**. Zadejte heslo k certifikátu ESET PROTECT serveru a potvrďte stisknutím tlačítka.



Repair ESET PROTECT **Server Certification Authority** – pomocí této možnosti můžete do ESET PROTECT Serveru **importovat** certifikační autoritu ve formátu DER. Klikněte na ikonu **sponky** a vyberte veřejný klíč certifikáty

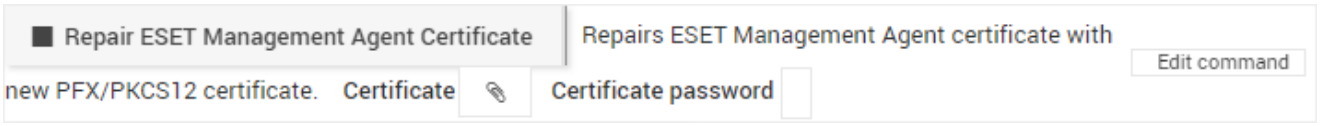
autority (ve formátu *.der*) a klikněte na tlačítko **Otevřít**.

Repair ESET Management Agent Connection – tuto možnost využijte pro opravení spojení ESET Management Agenta s ESET PROTECT serverem. Zadejte **název/IP adresu** ESET PROTECT serveru a **port**, ke kterému se má připojovat, a potvrďte kliknutím na tlačítko.

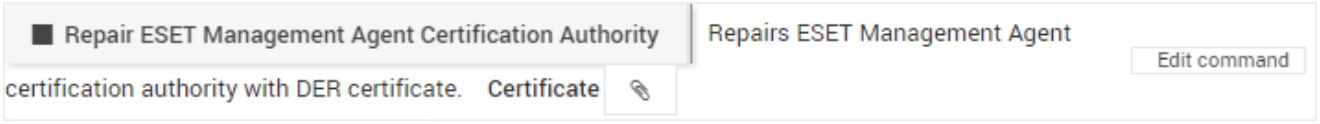


Repair ESET Management **Agent Certificate** – pomocí této možnosti **vyměníte** PFX/PKCS12 certifikát ESET Management Agenta. Klikněte na ikonu **sponky** a vyberte certifikát pro ESET Management agenta (ve formátu *PFX PKCS12*) a klikněte na tlačítko **Otevřít**. Zadejte heslo k certifikátu ESET Management agenta a potvrďte stisknutím tlačítka.

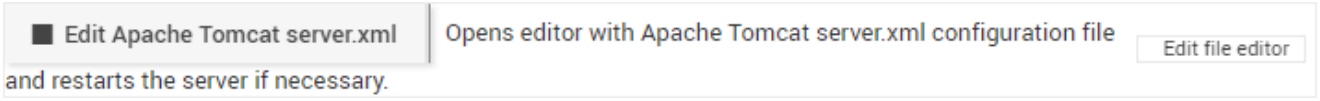
V hesle certifikátu není možné použít následující znaky: " \ neboť mohou způsobit chybu při inicializaci agenta.



Repair ESET Management **Agent Certification Authority** – pomocí této možnosti **vyměníte** veřejný klíč (DER soubor) **certifikační autority**, který používá ESET Management Agent. Klikněte na ikonu **sponky** a vyberte veřejný klíč certifikáty autority (ve formátu *.der*) a klikněte na tlačítko **Otevřít**.



Edit Apache Tomcat server.xml – pomocí této možnosti můžete upravit konfigurační soubor server.xml webového serveru Apache Tomcat. Například z důvodu změny HTTPS certifikátu nebo šifrovacích algoritmů. Po kliknutí na tlačítko se v textovém editoru otevřete soubor `/etc/tomcat/server.xml`. Po provedení změn klikněte na tlačítko **Save**. Pokud je to potřeba, dojde k automatickému restartování služby. V případě, že nechcete provést žádné změny, klikněte na tlačítko **Return to commands**.



Nástroje

V této části naleznete několik odlišných modulů. Mezi nejužitečnější patří:

File Manager – pomocí tohoto webového správce můžete pohodlně pracovat se soubory uloženými ve virtuální appliance. Při prvním otevření File manager (známého též jako **Filemin**) se standardně načte obsah složky /root na ESET PROTECT VA. Nicméně složka se může lišit v závislosti na tom, pod jakým uživatelem se přihlásíte.

• Pro pohyb mezi složkami jednoduše klikněte na název složky, případně její ikonu. V levé horní části Filemin okna se zobrazuje aktuální složka. Pro zobrazení jejího obsahu klikněte na libovolnou část cesty.

• Filemin dokáže vyhledávat soubory. Pro vyhledávání klikněte na panelu nástrojů (v pravém horním rohu) na **Tools** a vyberte možnost **Search**. Do pole **Search query** zadejte šablonu, podle níž chcete vyhledávat.

• Pro stažení souboru z ESET PROTECT VA do svého počítače prostřednictvím webového prohlížeče klikněte na jeho název nebo ikonu.

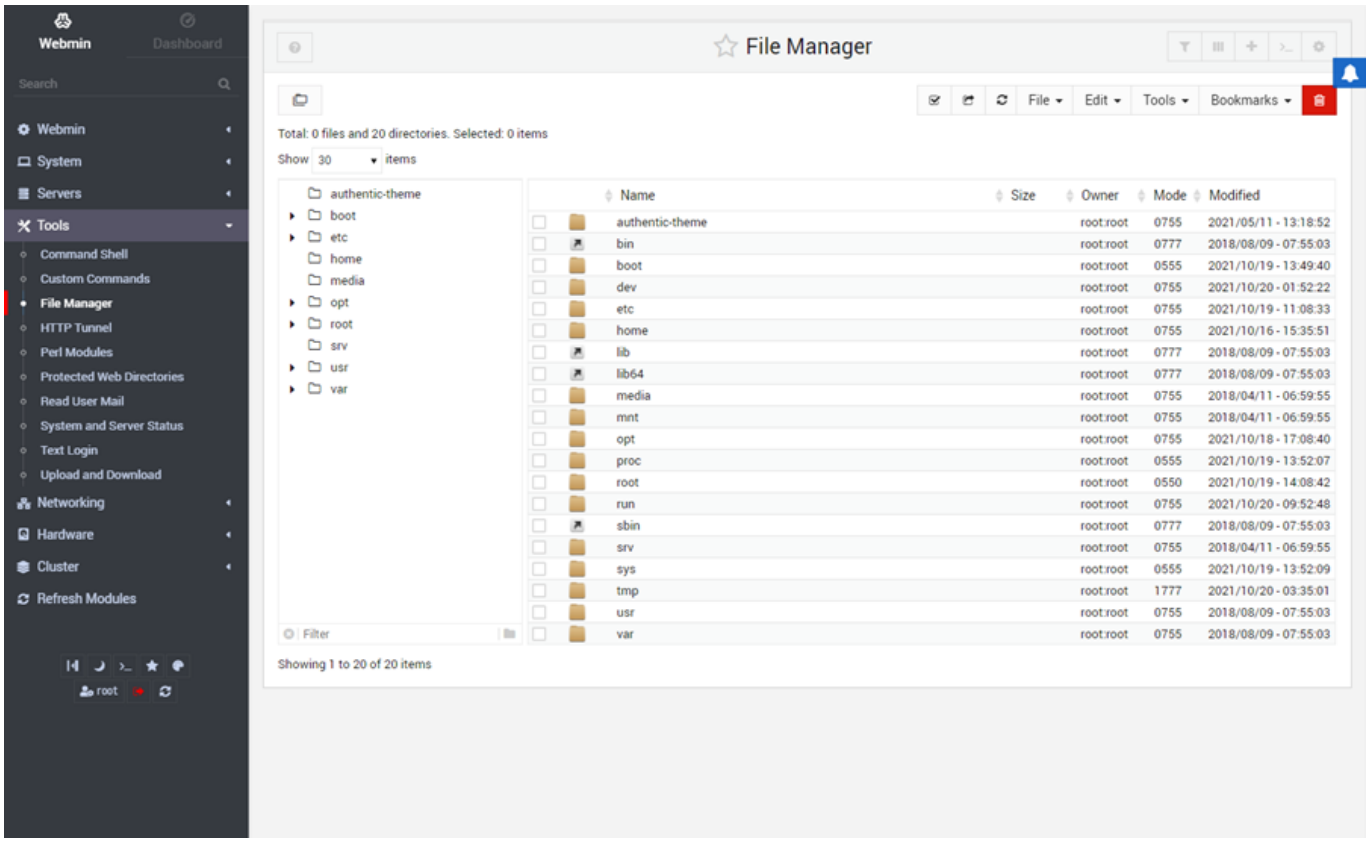
• Pokud chcete do virtuální appliance z vašeho počítače nahrát soubor prostřednictvím webového prohlížeče, klikněte na **File** > **Upload to current folder**. V zobrazeném dialogovém okně vyberte soubory, které chcete nahrát. Více souborů najednou můžete nahrát po kliknutí na tlačítko **Upload Files**. Soubory se nahrají do aktuální složky. Po dokončení nahrávání dojde k aktualizování seznamu a v seznamu se zobrazí vámi nahrané soubory.

• Soubor si můžete stáhnout též vzdáleně. Pro získání odkazu klikněte na **File** a vybrat možnost **Get from URL**.

• Pro zobrazení libovolného souboru a jeho úpravu souboru klikněte na možnost **Edit icon** ve sloupci **Actions**.

• Nový prázdný soubor vytvoříte kliknutím na **File** a vybrání možnosti **Create new file**. Následně zadejte název nového souboru.

• Pro přejmenování souboru nebo složky klikněte pravým tlačítkem na soubor/složku a z kontextového menu vyberte možnost **Přejmenovat**.



Upload and download – jedná se o další užitečný modul Webminu z kategorie **Tools**. Prostřednictvím něj můžete provádět níže uvedené akce se soubory:

• **Download from web** – zadejte URL souborů, které chcete do ESET PROTECT VA stáhnout a následně definujte složku pro uložení souborů.

• **Upload to server** – klikněte na ikonu sponky a vyberte soubory ze svého počítače, které chcete nahrát. Současně můžete vybrat nejvýše 4 soubory. Následně definujte složku, do níž chcete soubory nahrát.

• **Download from server** – do pole **File to download** zadejte cestu k souboru, který chcete z ESET PROTECT virtuální appliance stáhnout prostřednictvím prohlížeče do svého počítače. Pro zahájení stahování klikněte na tlačítko **Download**. Mějte na paměti, že zároveň můžete stahovat pouze jeden soubor.

Networking

Ve většině případů nebude nutné provádět změnu v síťovém adaptéru, nicméně provést to můžete v sekci **Networking**. V této sekci máte přístup k následujícím modulům:

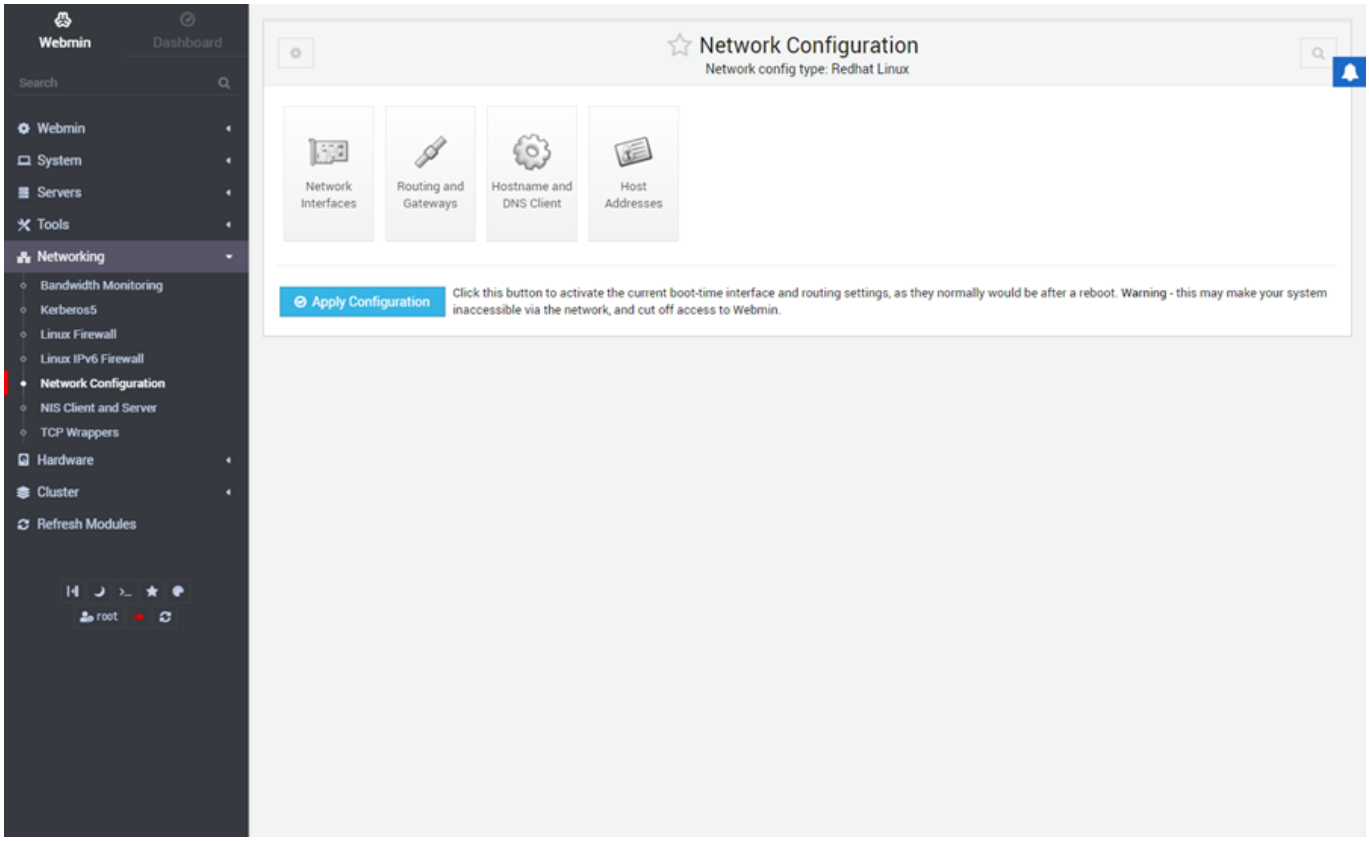
Kerberos5 configuration – správně nastavený Kerberos je důležitý pro vytvoření ověřovacího ticketu do Active Directory. Pokud budete mít vše nastaveno správně, můžete použít skript na Opětovné připojení do domény virtuální appliance do domény.

Linux Firewall – firewall založený na IPtables. V případě potřeby můžete povolit další porty přidáním dalších nebo úpravou stávajících pravidel.

Network configuration – v této části nakonfigurujete všechna síťová rozhraní (přiřadíte jim IP adresy), host soubor atp.

Změny se po dokončení konfigurace projeví až po stisknutí tlačítka **Apply Configuration**.

Tato část je určena výhradně zkušeným uživatelům. Nesprávnou změnou síťové konfigurace můžete odpojit od sítě a Webmin již nebude dostupný. V každém případě můžete virtuální stroj dále konfigurovat prostřednictvím terminálu, který spustíte pomocí konzole pro správu ESET PROTECT.



ESET PROTECT certifikáty

Certifikáty budete potřebovat ve chvíli, kdy si jako typ ESET PROTECT virtuální appliance vyberete MDM.

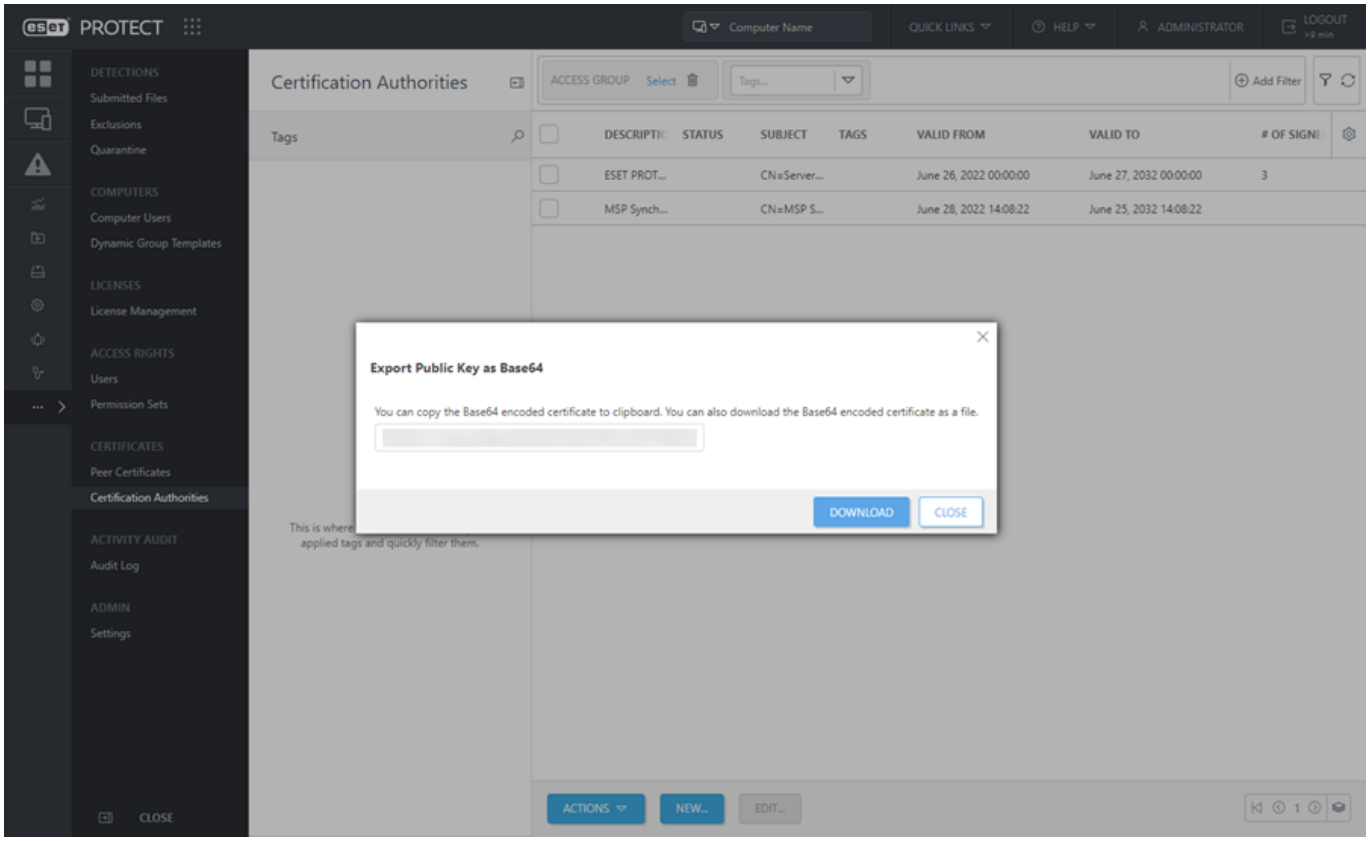
Certifikáty jednotlivých ESET PROTECT komponenty jsou dostupné ve Web Console.

Pro získání certifikátu v Base64 formátu:

1. V hlavním menu Web Console přejděte do sekce **Další** > **Klientské certifikáty**.

2. Klikněte na požadovaný certifikát a z kontextového menu vyberte možnost Exportovat jako Base64. Certifikát si můžete zkopírovat nebo stáhnout jako .txt soubor.

Stejným způsobem si můžete stáhnout certifikáty pro všechny komponenty infrastruktury i certifikační autoritu.



Pro exportování certifikátů musí mít uživatel oprávnění **Použít** u položky **Certifikáty**. Více informací naleznete v kapitole seznam oprávnění.

Aktualizace/migrace ESET PROTECT virtuální appliance

Pro aktualizaci nebo migraci své virtuální appliance můžete využít níže uvedení kroky:

- **Aktualizace** – proces, při kterém se nainstaluje novější verzie ESET PROTECT komponent.
- **Migrace** – proces, při kterém se přesune obsah ESET PROTECT VA na jinou instanci ve stejné verzi.
- **Migrace a aktualizace** – proces, při kterém se přesune obsah ESET PROTECT VA na jinou instanci ve vyšší verzi.

Ve ESET PROTECT virtuální appliance od verze 8.1 je ve výchozím nastavení aktivní rozšířené zabezpečení. Pokud používáte ESMC nebo ESET PROTECT virtuální appliance 8.0 a máte rozšířené zabezpečení deaktivované, pro přechodu na ESET PROTECT virtuální appliance 8.1 a novější zůstane rozšířené zabezpečení vypnuté.

Před aktualizací/migrací

Před zahájením migrace nebo aktualizace ESMC/ESET PROTECT proveďte zálohu databáze, exportujte veřejný klíč certifikační autority a klientské certifikáty.

Migrace databáze vs Aktualizace součástí

Svou virtuální appliance můžete aktualizovat dvěma způsoby:

- Přemigrováním databáze – tímto aktualizujete celou appliance (včetně operačního systému), nejen samotný ESET PROTECT server. Jedná se o složitější proces, který vyžaduje v průběhu migrace dvě souběžně běžící appliance. Tento postup je doporučen při aktualizaci mezi hlavními verzemi nebo při řešení problémů.

- Aktualizace prostřednictvím klientské úlohy spuštěné z webové konzole – jedná se o jednodušší proces, který nevyžaduje přístup k appliance, pouze k Web Console. Tento postup doporučujeme při aktualizaci na minoritní verzi nebo při aplikování hotfixů.

Proces aktualizace a migrace (doporučený způsob aktualizace)

Podle níže uvedených kroků přemigrujete a aktualizujete ESET PROTECT virtuální appliance.

1. Stáhněte si z webových stránek společnosti ESET aktuální verzi *protect_appliance.ova*, resp. `protect_appliance.vhd.zip` v případě Microsoft Hyper-V.

2. Nasaďte novou ESET PROTECT VA. Projděte si kroky pro nasazení ESET PROTECT. Zatím novou ESET PROTECT VA **nekonfigurujte**.

3. Přemigrujte databázi ze staré VA. Pro více informací přejděte do kapitoly Migrace databáze ze starého serveru.

Prozatím původní VA server neodinstalovávejte/nemažte.

4. Dokončete konfiguraci ESET PROTECT VA prostřednictvím webového rozhraní.

5. Ujistěte se, že se nová virtuální appliance chová stejně, jako předchozí:ESET PROTECT

   - Pokud má nová ESET PROTECT VA **odlišnou IP adresu**:

     a) Na starém ESET PROTECT serveru vytvořte politiku pro ESET_MNG agenta, prostřednictvím které jej přesunete na nový server a přiřaďte ji všem zařízením (ideálně nejnadřazenější skupině Všechna zařízení).

     b) Vyčkejte, až si všichni ESET Management agenti politiku převezmou.

     c) Ujistěte se, že se všechny stanice připojují k nové ESET PROTECT VA.

     d) Nyní můžete původní VA vypnout a zahodit.

Důrazně nedoporučujeme pro odinstalaci starého ESET PROTECT VA Serveru používat odinstalační skript. Tím dojde zároveň k odasociování (odstranění) všech licencí z nového ESET PROTECT serveru (jeho databáze). Pro zabránění vzniku této situace smažte před odinstalovám databázi starého ESET PROTECT serveru (příkazem `DROP DATABASE`).

   - Pokud má nová ESET PROTECT VA **stejnou IP adresu**:

Ujistěte se, že nový ESET PROTECT Server má stejné síťové nastavení (IP adresu, FQDN, název serveru, DNS SRV záznam) jako původní. Pokud používáte hostname, stačí změnit záznam na DNS serveru.

a)Vypněte původní VA.

b)Zapněte novou ESET PROTECT VA.

c)Ujistěte se, že se všechny stanice připojují k nové ESET PROTECT VA.

d)Nyní můžete původní VA vypnout a zahodit.

Důrazně nedoporučujeme pro odinstalaci starého ESET PROTECT VA Serveru používat odinstalační skript. Tím dojde zároveň k odasociování (odstranění) všech licencí z nového ESET PROTECT serveru (jeho databáze). Pro zabránění vzniku této situace smažte před odinstalovám databázi starého ESET PROTECT serveru (příkazem `DROP DATABASE`).

6.Aktualizujte několik ESET Management agentů prostřednictvím klientské úlohy na ESET PROTECTaktualizaci součástí infrastruktury.

7.Pokud se agenti po provedení aktualizace připojují, aktualizujte zbytek infrastruktury.

Proces aktualizace (alternativní způsob aktualizace)

Aktualizováním ESMC nebo starší verze ESET PROTECT nedojde k aktualizaci softwaru dostupného na virtuální appliance (operačního systému, balíčků vyžadovaných pro správnou funkci ESET PROTECT serveru). Z tohoto důvodu doporučujeme po dokončení aktualizace provést migraci na novou appliance.

Aktualizujte komponenty na VA prostřednictvím klientské úlohy na Aktualizaci součástí.

1.Nejprve aktualizujte ESET PROTECT server.

2.Aktualizujte několik ESET Management agentů.

3.Pokud se agenti po provedení aktualizace připojují, aktualizujte zbytek infrastruktury.

Disaster recovery ESET PROTECT virtuální appliance

V případě, že přestal virtuální stroj fungovat a nejde spustit, došlo k jeho poškození nebo jste nedopatřením smazali stroj z úložiště, pomocí následujících kroků můžete ESET PROTECT komponentu uvést do původního stavu bez toho, aniž byste přišli o data.

Abyste mohli obnovit ESET PROTECT virtuální appliance do původního funkčního stavu, musíte mít zálohu databáze.

1. **Stáhněte** si z webových stránek společnosti ESET aktuální verzi *protect_appliance.ova*, resp. `protect_appliance.vhd.zip` v případě Microsoft Hyper-V. Získáte tak zároveň nejnovější verzi ESET PROTECT VA.

2. **Nasaďte novou ESET PROTECT VA**, ale zatím ji nekonfigurujte. Projděte si kroky pro nasazení ESET PROTECT.

3. **Aktivujte Webmin**, abyste mohli nahrát MySQL soubor se zálohou databáze. Více informací naleznete v

kapitole Zapnutí/vypnutí vzdáleného přístupu.

4. Obnovte databázi z nahraného souboru. Více informací naleznete v kapitole **Obnovení databáze**.

5. **Nakonfigurujte** čerstvě nasazenou ESET PROTECT VA s obnovenou databází tak, jako původní VA. Více informací naleznete v kapitole Konfiguraci ESET PROTECT virtuální appliance.

Řešení problémů

V této kapitole uvádíme seznam souborů, do kterých byste se měli podívat v případě, kdy řešíte nějaký problém související s ESET PROTECT VA. Diagnostické protokoly si mohou rovněž vyžádat specialisté technické podpory. K analýze můžete zaslat následující soubory:

Protokol	Umístění	Popis
Konfigurace ESET PROTECT VA	*/root/appliance-configuration-log.txt*	Pokud proces nasazení ESET PROTECT VA selhal, virtuální počítač nerestartujte a podívejte se do tohoto protokolu.
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log* */var/log/eset/RogueDetectionSensor/RDSensorInstaller.log*	Instalační protokol ESET PROTECT Serveru. Protokoly dalších ESET PROTECT komponent naleznete ve stejném umístění. Pouze se liší název složky v závislosti na komponentě.
Trace log ESET PROTECT serveru Trace log ESET Management agenta	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/Agent/*	Zkontrolujte trace protokoly daných komponent: *trace.log* *status.html* *last-error.html* Trace logy dalších ESET PROTECT komponent naleznete ve stejném umístění. Pouze se liší název složky v závislosti na komponentě.
Apache HTTP Proxy	*/opt/apache/logs/* */var/log/httpd*	Cesta k protokolu ve starší verzi ESET PROTECT VA. Cesta k protokolu v novější verzi ESET PROTECT VA.
Dumpy ESET PROTECT serveru	*/var/opt/eset/RemoteAdministrator/Server/Dumps/*	
Výstup diagnostického nástroje ESET PROTECT serveru nebo ESET Management agenta	*/root/RemoteAdministratorAgentDiagnostic.zip*	Pokud pozorujete na své ESET PROTECT VA problémy, můžete spustit **diagnostický nástroj**. Podrobné informace naleznete ve Webmin modulu ESET PROTECT.

Pokud služba agenta nebo serveru padá a nejste schopni změnit úroveň protokolování prostřednictvím Web Console, trace protokolování aktivujete vytvořením prázdného souboru v odpovídající složce:

Pro agenta použijte příkaz:

```
touch /var/log/eset/RemoteAdministrator/Agent/traceAll
```

Pro server použijte příkaz:

```
touch /var/log/eset/RemoteAdministrator/Server/traceAll
```

Výše uvedené soubory můžete z virtuální appliance získat například prostřednictvím Webminu.

Pokud vám koncové stanice hlásí chybu **Servery služby EPNS nejsou dosažitelné**, přejděte do kapitoly řešení problémů.

FAQ: ESET PROTECT virtuální appliance

V této kapitole naleznete odpovědi na nejčastější dotazy týkající se virtuální appliance. Kliknutím na název kapitoly si zobrazíte instrukce pro vyřešení problému:

- Jak zjistím, jakou verzi ESET PROTECT komponent používám?
- Jak povolit ping na ESET PROTECT VA?
- Je nutné do ESET PROTECT VA instalovat další komponenty?
- Jak ručně aktivovat Apache HTTP Proxy na ESET PROTECT VA?
- Jak nastavit LDAP pro povolení synchronizace statické skupiny v ESET PROTECT VA?
- Konfigurace LDAPS pro připojení k doméně
- Zapomněl jsem heslo pro přístup do ESET PROTECT VA, co mám dělat?
- Jak změnit connection string pro připojení do ESET PROTECT databáze?
- Jak nastavit Hyper-V Server pro RD Sensor?
- Jak změnit porty, které používá ESET PROTECT?
- Jak zvýšit paměťový limit MySQL serveru?
- Mám problém s ESET PROTECT běžícím na Hyper-V Server 2012 R2
- Jak zvýšit výkon Oracle VirtualBox?
- Jak zprovoznit příkaz YUM, pokud jsem za Proxy?
- Jak aktualizovat operační systém na ESET PROTECT VA?

- Jak trvale vypnout SELinux?
- Jak restartovat konzoli pro správu?
- Jak využít Proxy pro směrování komunikace agentů?
- Jak povolit vzdálený přístup prostřednictvím SSH?

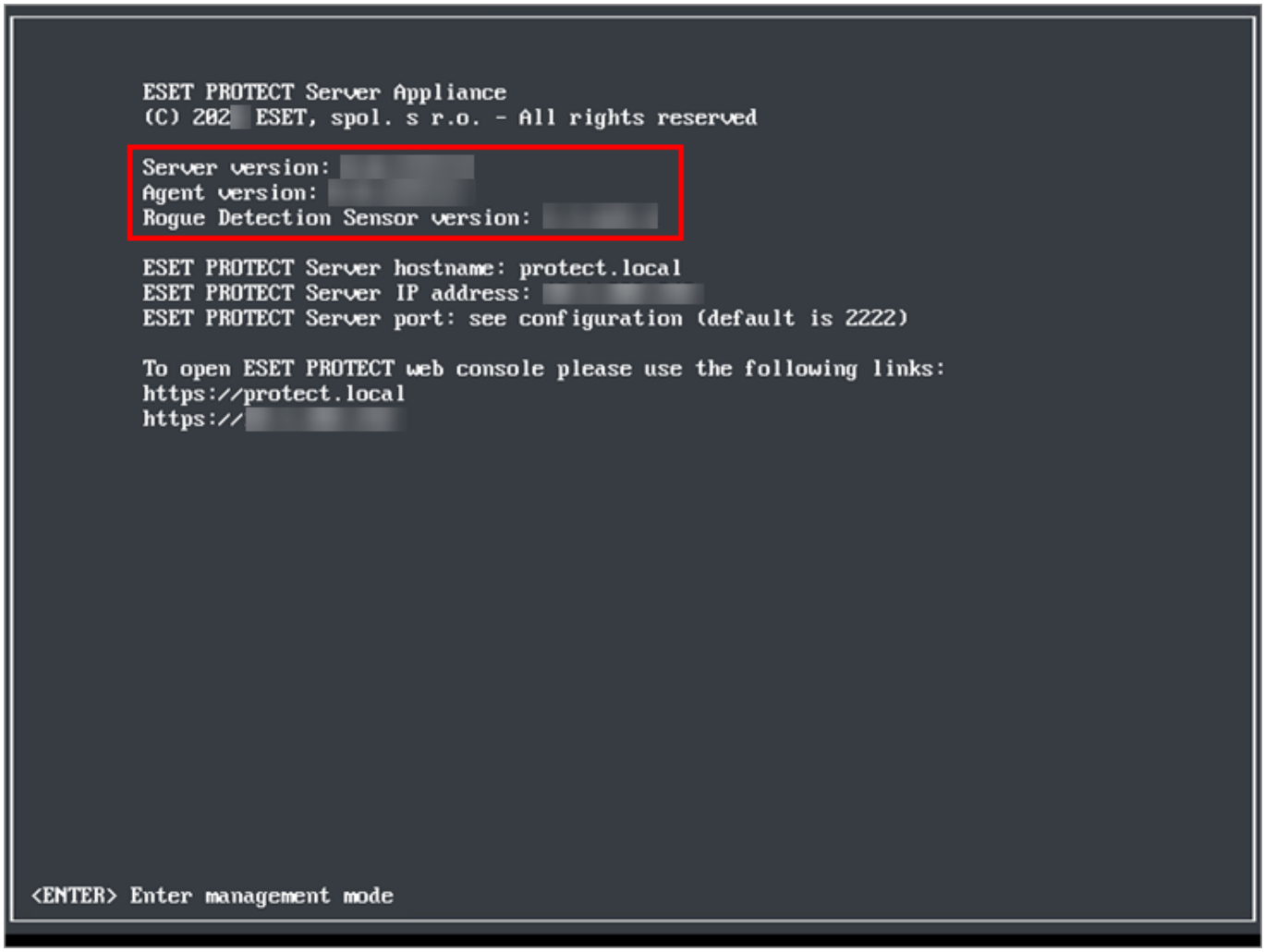
Pokud jste řešení svého problému nenalezli v této kapitole, zkuste v dalších částech příručky k ESET PROTECT vyhledat klíčová slova nebo fráze, která vystihuje váš problém.

Pokud v nápovědě nenajdete odpověď na otázku či řešení problému, prohledejte Databázi znalostí.

V případě potřeby se můžete obrátit na specialisty technické podpory. Odkaz na kontaktní formulář naleznete v ESET PROTECT Web Console v sekci **Nápověda**, kdy vyberte možnost **Kontaktovat technickou podporu**.

Jak zjistím, jakou verzi ESET PROTECT komponent používám?

Seznam všech nainstalovaných ESET PROTECT komponent včetně verze naleznete na úvodní obrazovce ESET PROTECT virtuální appliance. Zobrazené informace se aktualizují vždy při restartu appliance. Případně se přepněte do režimu pro správy (Enter management mode), vyberte možnost **Exit to terminal**, opusťte terminál a vraťte se zpět.



Jak povolit ping na ESET PROTECT VA?

Na ESET PROTECT virtuální appliance není ve výchozí konfiguraci povolen ping. Pro jeho povolení si otevřete terminál, případně se přihlaste prostřednictvím SSH jako uživatel root.

Před tím, než začnete, si nejprve příkazem `hostnamectl` zjistěte verzi operačního systému CentOS. Následně postupujte podle níže uvedených kroků, v závislosti na verzi systému.

Prostup pro virtuální appliance s operačním systémem CentOS 7

1. Přidejte pravidlo do iptables příkazem:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

2. Uložte konfiguraci iptables příkazem:

```
service iptables save
```

Nyní bude ESET PROTECT virtuální appliance odpovídat na příkaz ping z počítačů nacházejících se ve stejném síťovém rozsahu.

Je nutné do ESET PROTECT VA instalovat další komponenty?

Ne, ESET PROTECT virtuální appliance je samostatný hotový produkt. Nasadíte jej a nakonfigurujete. Jedná se o nejjednodušší a nejrychlejší cestu pro zprovoznění ESET PROTECT, pokud používáte podporovaný hypervizor.

Jak ručně aktivovat Apache HTTP Proxy na ESET PROTECT virtuální appliance?

Tato komponenta dokáže do cache ukládat aktualizace detekční jádra, instalační balíčky a informace z ESET LiveGrid®. Pokud jste neaktivovali Apache HTTP Proxy při prvotní konfiguraci virtuální appliance, otevřete si terminál a v závislosti na používaném operačním systému spusťte jako uživatel root následující příkazy:

i
- Umístění `apachectl` a `htcacheclean` se může lišit v závislosti na použitém operačním systému. Před spuštěním skriptu si zkontrolujte, zda se v dané složce skutečně binárky nacházejí.
- Parametr `/var/cache/httpd/proxy` definuje složku, do níž se ukládá cache. Její umístění je definováno v konfiguračním souboru `/etc/httpd/conf.d/proxy.conf` v sekci `CacheRoot`.

Prostup pro virtuální appliance s operačním systémem CentOS 7

1. `systemctl enable httpd`
2. `sudo mkdir -p /etc/systemd/system/httpd.service.requires`
3. `sudo ln -s /usr/lib/systemd/system/htcacheclean.service`

```
/etc/systemd/system/httpd.service.requires
```

4. `systemctl start httpd`

5. `htcacheclean -d60 -t -i -p/var/cache/httpd/proxy -l10000M`

> **i** Parametry pro údržbu cache si můžete přizpůsobit: `-d` definuje interval čištění v minutách, `-p` definuje cestu ke složce s cache, `-t` vymaže všechny prázdné složky, `-i` inteligentně smaže pouze nezměněnou cache, `-l` definuje limit pro velikost cache.

6. Pro povolení portu 3128 ve firewallu:

a) `iptables -A INPUT -p tcp --dport 3128 -j ACCEPT`

b) `ip6tables -A INPUT -p tcp --dport 3128 -j ACCEPT`

c) `service iptables save`

d) `service ip6tables save`

7. Následně si vytvořte odpovídající politiku pro všechny ESET produkty / součásti ESET PROTECT infrastruktury tak, aby komunikace těchto komponent procházela do internetu prostřednictvím Apache HTTP Proxy. Ujistěte se, že v konfiguraci Apache máte v sekci ProxyMatch uveden název serveru. Pro více informací přejděte do Databáze znalostí (část **II. Configure policy settings for client computers**).

Řešení problémů

Pokud vám koncové stanice hlásí chybu **Servery služby EPNS nejsou dosažitelné**, pomocí následujících kroků deaktivujte časový limit připojení:

1. Vytvořte konfigurační soubor *reqtimeout.conf*:
`sudo touch /etc/httpd/conf.d/reqtimeout.conf`

2. V textovém editoru si otevřete vytvořený konfigurační soubor:
`nano /etc/httpd/conf.d/reqtimeout.conf`

3. Vložte do něj následující nastavení:
`RequestReadTimeout header=0 body=0`

4. Uložte a zavřete konfigurační soubor.
Stiskněte klávesy CTRL+X > dále **Y** > potvrďte klávesou **Enter**

5. V textovém editoru si otevřete soubor *httpd.conf*:
`nano /etc/httpd/conf/httpd.conf`

6. Na konec souboru přidejte níže uvedené řádky:
`IncludeOptional conf.d/reqtimeout.conf`

7. Uložte a zavřete konfigurační soubor.
Stiskněte klávesy CTRL+X > dále **Y** > potvrďte klávesou **Enter**

8. Restartujte službu Apache HTTP Proxy:

```
systemctl restart httpd
```

Jak nastavit LDAP pro povolení synchronizace statické skupiny v ESET PROTECT VA?

Pokud se připojení do domény nezdaří, obvykle je to v důsledku nesprávné konfigurace ESET PROTECT VA. Pro více informací si přejděte do Databáze znalostí.

Konfigurace LDAPS pro připojení k doméně

ESET PROTECT Server instalovaný na Windows používaná pro připojení k Active Directory (AD) šifrovaný LDAPS (LDAP over SSL) protokol.

Podle následujících kroků nakonfigurujte ESET PROTECT virtuální appliance tak, aby se dokázala připojit k Active Directory prostřednictvím LDAPS.

Předpoklady

- Nastavte LDAPS na doménovém řadiči – ujistěte se, že máte exportovaný veřejný klíč DC certifikační autority.
- Ujistěte se, že máte na své ESET PROTECT VA správně nakonfigurován Kerberos.

Aktivace LDAPS na ESET PROTECT VA

1. Otevřete si hlavní obrazovku ESET PROTECT VA.
2. Stiskněte klávesu Enter. Pro vstup do režimu správy zadejte heslo, které jste si nastavili v průběhu konfigurace ESET PROTECT a **dvakrát** potvrďte stisknutím klávesy **Enter**.
3. Pomocí šipek vyberte z dostupných možností **Exit to Terminal** a potvrďte stisknutím klávesy **Enter**.
4. Zastavte službu ESET PROTECT server.

```
systemctl stop eraserver
```

5. Zadejte následující příkaz:

```
nano /etc/systemd/system/eraserver.service
```

6. Do sekce **[Service]** přidejte řádek:

```
Environment="ESMC_ENABLE_LDAPS=1"
```

7. Po dokončení úprav souboru stiskněte klávesy **Ctrl + X** a změny uložte stisknutím klávesy **Y**. Stisknutím klávesy **Enter** editor ukončete.

8. Následujícím příkazem znovu načtěte konfiguraci:

```
systemctl deamon-reload
```

9. Spusťte službu ESET PROTECT server.

```
systemctl start eraserver
```

10. Zkopírujte soubor s certifikátem, který jste vygenerovali na doménovém řadiči, do následujícího umístění na ESET PROTECT VA:

```
/etc/pki/ca-trust/source/anchors/
```

11. Spusťte následující příkaz:

```
update-ca-trust
```

Zapomněl jsem heslo pro přístup do ESET PROTECT VA, co mám dělat?

Nastartujte virtuální počítač ESET PROTECT VA v tzv. Single-User režimu. Postup naleznete v dokumentaci k operačnímu systému CentOS 7. V terminálu režimu Single-User si změňte heslo pomocí příkazu `passwd`.

Pokud se obdržíte chybové hlášení `"passwd: Authentication token manipulation error"`, postupujte podle kroků při řešení problémů.

Jak změnit connection string pro připojení do ESET PROTECT databáze?

Connection string pro připojení do ESET PROTECT databáze můžete změnit v souboru `StartupConfiguration.ini`.

Pro jeho změnu postupujte na ESET PROTECT VA podle níže uvedených kroků:

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu **Enter**, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Exit to terminal** a potvrďte stisknutím klávesy **Enter**.

2. Konfigurační soubor si otevřete v textovém editoru příkazem:

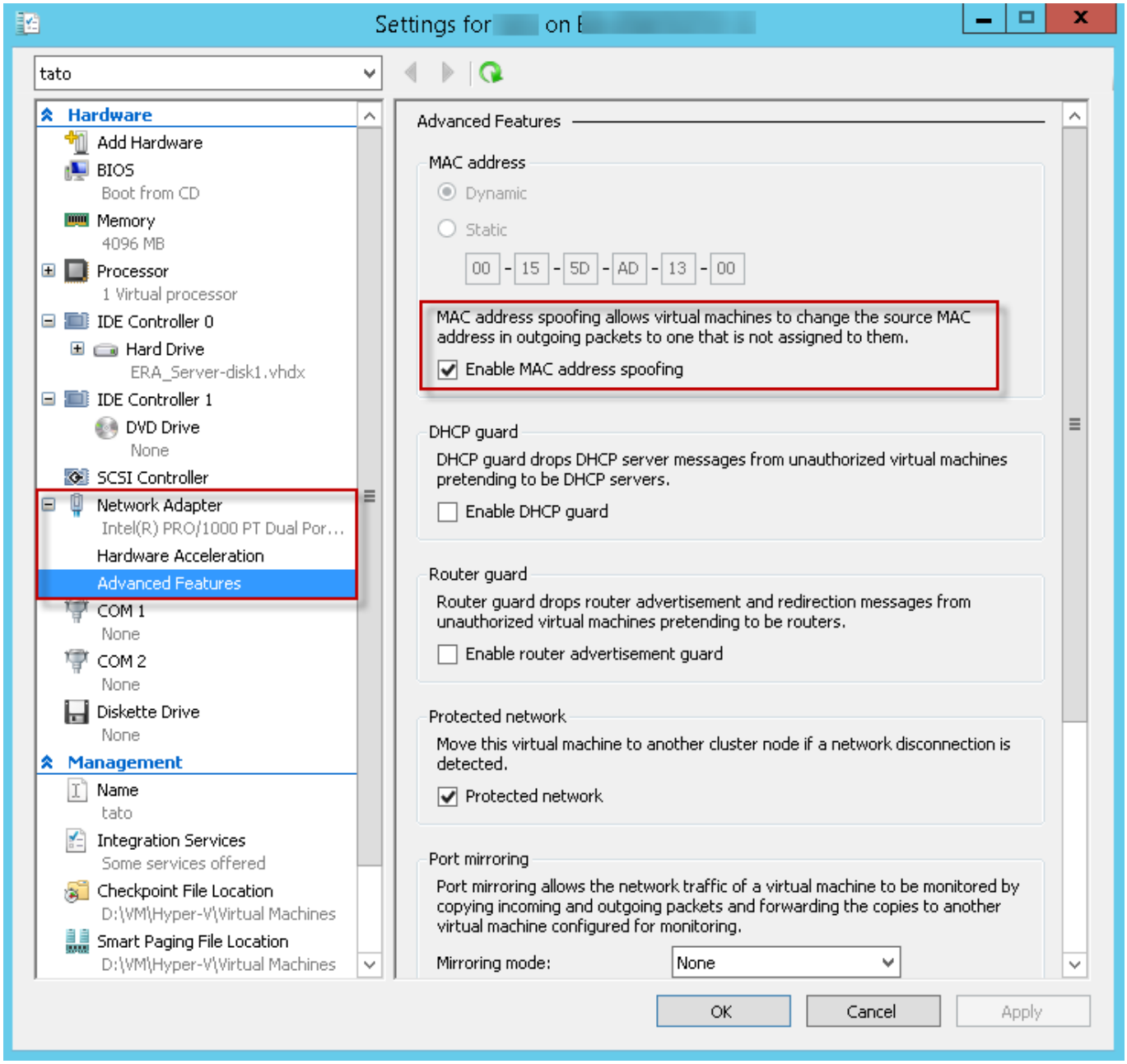
```
nano /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

3. Upravte connection string pro připojení do ESET PROTECT databáze.

4. Po dokončení úprav souboru stiskněte klávesy `Ctrl+X` a změny uložte stisknutím klávesy `y`.

Jak nastavit Hyper-V Server pro RD Sensor

Ujistěte se, že spoofing MAC adresy je v nastavení vašeho Hyper-V povolen (viz níže).



Jak změnit porty, které používá ESET PROTECT?

Podle níže uvedených kroků můžete změnit port, na kterém běží webová konzole, případně porty, které používá pro komunikaci ESET PROTECT server s jednotlivými komponentami.

Port ESET PROTECT Web Console (standardně 8443)

1.Otevřete si Webmin.

2.Přejděte do sekce **Servers** > **ESET PROTECT** a klikněte na **Edit Apache Tomcat server.xml**.

3.Upravte řádek `<Connector port="8443"` tak, aby obsahoval vámi požadované číslo portu, a klikněte

na **Save and Close**.

4.V textovém editoru si otevřete soubor *EraWebServerConfig.properties*:

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

5.Upravte řádek `server_port=` tak, aby obsahoval vámi požadované číslo portu, a uložte změny.

6.Restartujte službu webového serveru: `systemctl restart tomcat`

Porty ESET PROTECT serveru (standardně 2222, 2223) – v hlavním menu ESET PROTECT Web Console přejděte do sekce **Další** > **Nastavení**. V sekci **Připojení** proveďte potřebné změny.

> Při změně portů je potřeba odpovídajícím způsobem modifikovat nastavení firewallu. To můžete provést například prostřednictvím Webminu, kdy v sekci **Networking** > **Linux Firewall** změňte čísla portů u existujících pravidel. Případně si vytvořte nová pravidla.

Jak zvýšit paměťový limit MySQL serveru?

Pro zvýšení paměťového limitu MySQL serveru postupujte podle následujících kroků:

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu **Enter**, zadejte heslo a potvrďte opětovným stisknutím klávesy Enter. Pomocí **šipek** vyberte z dostupných možností Exit to Terminal a potvrďte stisknutím klávesy **Enter**.

2. Konfigurační soubor si otevřete v textovém editoru příkazem:
`nano /etc/my.cnf`

3. Najděte řádek `innodb_buffer_pool_size = 1024M` a hodnotu zvyšte na 1/2 dostupné RAM. `1024` znamená 1024 MB.

4. Pomocí kláves `CTRL + X` ukončete textový editor a stiskem klávesy `y` uložte změny.

5. Restartujte virtuální appliance pomocí možnosti **Restartujte system** dostupné v **konzole pro správu**.

Mám problém s ESET PROTECT běžícím na Hyper-V Server 2012 R2

Po přihlášení do ESET PROTECT Web Console se zobrazí chyba "Unable to handle Kernel NULL pointer dereference at (null)".

Pro vyřešení problému **deaktivujte dynamické přiřazování paměti** v nastavení virtuálního stroje.

Jak zvýšit výkon Oracle VirtualBox?

V **Nastavení** lze změnit počet procesorů pro ESET PROTECT Virtuální appliance. V nastavení virtuálního stroje přejděte na záložku **Systém** > **Procesor**. Snižte počet procesorů VA. Máte-li například 4 fyzická jádra, přiřaďte virtuální appliance pouze 2 jádra.

Jak zprovoznit příkaz YUM, pokud jsem za Proxy serverem?

Pokud ve své síti používáte pro přístup k internetu proxy server a chcete aby vám na virtuální appliance fungoval příkaz `yum`, je nutné odpovídajícím způsobem upravit jeho konfiguraci.

Pro konfiguraci `yum` postupujte podle níže uvedených kroků:

1. Pro přechod do režimu správy stiskněte na úvodní obrazovce virtuální appliance klávesu Enter, zadejte heslo a potvrďte opětovným stisknutím klávesy **Enter**. Pomocí šipek vyberte z dostupných možností **Exit** to Terminal a potvrďte stisknutím klávesy **Enter**.

2. Konfigurační soubor si otevřete v textovém editoru příkazem:
```
nano /etc/yum.conf
```

3. Do konfiguračního souboru přidejte řádek s informací o nadřazené proxy. Příklad:
```
proxy=http://proxysvr.yourdom.com:3128
```

4. Pokud proxy vyžaduje autentifikaci uživatelským jménem a heslem, definujte je. Příklad:
```
proxy=http://proxysvr.yourdom.com:3128
proxy_username=YourProxyUsername
proxy_password=YourProxyPassword
```

5. Po dokončení úprav souboru stiskněte klávesy `Ctrl + X` a změny uložte stisknutím klávesy `y`.

> Mějte na paměti, že všechny informace uložené v souboru `/etc/yum.conf` jsou v čitelné podobě. Jinými slovy, uživatelské jméno a heslo si může přečíst jakýkoli uživatel. Z tohoto důvodu doporučujeme použít unikátní heslo.

Více informací naleznete v dokumentaci společnosti Oracle.

Jak aktualizovat operační systém na ESET PROTECT VA?

V případě, že se vám v ESET PROTECT Web Console zobrazí u zařízení, na kterém běží ESET PROTECT Server, hláška **Operační systém není aktualizovaný**, je nutné aktualizovat operační systém na ESET PROTECT virtuální appliance. K provedení této akce využijte klientskou úlohu Aktualizace operačního systému, která je dostupná v Web Console.ESET PROTECT Po úspěšném provedení aktualizace uvedené hlášení zmizí.

> Při aktualizování operačního systému prostřednictvím Webminu, z terminálu nebo pomocí nástrojů třetích stran, nemusí hlášení zmizet. Pro korektní reportování stavu **aktualizací operačního systému** doporučujeme využívat klientskou úlohu v ESET PROTECT Web Console.

Jak trvale vypnout SELinux?

SELinux je ve virtuální appliance standardně zapnutý. Pro jeho vypnutí postupujte podle níže uvedených kroků:

1. V Konzole pro správu vyberte možnost **Exit to Terminal**.

2. Spusťte příkaz:
`nano /etc/selinux/config`

3. Změňte řádek:
`SELINUX=permisive`
na
`SELINUX=disabled`

4. Stisknutím kláves CTRL + X uložte změny a zavřete textový editor.

5. Pro použití nového nastavení restartujte počítač příkazem:
`reboot`

Jak restartovat konzoli pro správu?

Grafické rozhraní virtuální appliance je možné restartovat bez nutnosti restartování celého virtuálního stroje. Obnovením grafického rozhraní aktualizujete zobrazovaná data v konzoli. To se může hodit v případě, kdy jste provedli změnu v konfiguraci, ale na úvodní obrazovce se zatím změny neaktualizovaly.

1. V Konzole pro správu vyberte možnost **Exit to Terminal**.

2. Spusťte příkaz:
`./appliance-gui restart`

Jak využít Proxy pro směrování komunikace agentů?

Pro směrování komunikace ESET Management Agentů na ESET PROTECT Server je možné využít Apache HTTP Proxy. Pro instalaci Apache HTTP Proxy se podívejte do instalační příručky popisující kroky na linuxu.

Jak povolit vzdálený přístup prostřednictvím SSH?

Pro povolení SSH na ESET PROTECT VA (nebo ESMC VA) přejděte do kapitoly Zapnutí/vypnutí vzdáleného přístupu

Řešení problémů

Otevřete si terminál a spusťte následující příkazy:

- `sudo systemctl sshd status` – ověřte, zda služba SSH běží. Pokud neběží spusťte ji příkazem: `sudo systemctl start sshd`

• `sudo iptables -S` - pokud je port 22 otevřen, jako výstup příkazu uvidíte záznam: `-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`. Pro přidání portu 22 do iptables použijte příkaz: `sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel”) Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob

instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro fungování Softwaru a pro jeho aktualizaci a upgrade. Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace"), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti", které jsou k dispozici na webu https://go.eset.com/eol_business. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

DODATEK K DOHODĚ

Zasílání infiltrací a informací Poskytovateli. Na zasílání informací poskytovateli se vztahují následující dodatečná ustanovení:

Tento Software obsahuje funkce, které slouží ke shromažďování informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, informací o operacích a funkcích Softwaru a informací o spravovaných zařízeních (dále jen "Informace") a jejich odeslání Poskytovateli. Informace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) týkající se spravovaných zařízení. Po aktivaci této funkce Softwaru mohou být Informace shromažďovány a zpracovávány Poskytovatelem v souladu se Zásadami ochrany osobních údajů a příslušnými právními předpisy.

Software vyžaduje, aby byla na spravovaném počítači nainstalována komponenta, která umožňuje přenos informací mezi spravovaným počítačem a softwarem pro vzdálenou správu. Informace, které jsou předmětem přenosu, obsahují data o správě, jako jsou informace o hardwaru a softwaru na spravovaném počítači, a pokyny pro správu ze softwaru pro vzdálenou správu. Další obsah dat přenášených ze spravovaného počítače je určen nastavením softwaru nainstalovaného ve spravovaném počítači. Obsah pokynů ze softwaru pro správu je určen nastavením softwaru pro vzdálenou správu.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Zásady ochrany osobních údajů

Společnost ESET spol. s r.o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsaná v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. 31333532 jako „Správce údajů“ (dále jen „ESET“ nebo „My“) chce postupovat transparentně, pokud jde o zpracování osobních údajů a soukromí našich zákazníků. Abychom dosáhli tohoto cíle, zveřejňujeme zde tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků ("Koncový uživatel" nebo "Vy") o následujících tématech:

- Zpracování osobních údajů

- Důvěrnost údajů,
- Práva subjektu údajů.

Zpracování osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v Licenčním ujednáním s koncovým uživatelem ("EULA"), ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané ve smlouvě EULA a dokumentaci k produktu, například služby aktualizace/upgradu, ESET LiveGrid®, ochranu proti zneužití dat, podporu atd. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Pro účely správy bezpečnostních produktů ESET jsou vyžadovány a lokálně ukládány různé informace, například ID licence a jméno, název produktu, informace o licenci, informace o aktivaci a vypršení platnosti či informace o hardwaru a softwaru týkající se spravovaného počítače s nainstalovaným bezpečnostním produktem ESET. Kvůli usnadnění správy a dohledu nad funkcemi a službami jsou shromažďovány a uchovávány záznamy týkající se aktivit spravovaných bezpečnostních produktů ESET a spravovaných zařízení. Tyto záznamy nejsou automaticky odesílány společnosti ESET.
- Informace o procesu instalace a vašem počítači, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako jsou údaje o hardwaru, ID instalace, výpisy chyb, ID licencí, IP adresa, MAC adresa a nastavení konfigurace produktu, které může zahrnovat také spravovaná zařízení.
- Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb.
- Na webu https://my.eset.com je potřeba vytvořit účet, pomocí něhož tato funkce aktivuje sběr dat v případě odcizení počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory, jako jsou například vygenerované soubory protokolů.
- Údaje o využívání naší služby jsou na konci relace zcela anonymizovány. Po ukončení relace nejsou ukládány žádné osobní údaje, na jejichž základě by vás bylo možné identifikovat.

Důvěrnost údajů

ESET je společnost s celosvětovou působností. Informace, které společnost ESET zpracovává, mohou být přenášeny k přidruženým subjektům nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb, podpora nebo fakturace. Na základě vaší polohy a služeb, které si zvolíte, může být potřeba přenést vaše údaje do země, kde neplatí rozhodnutí Evropské komise o odpovídající ochraně. I v takovém případě každý přenos informací podléhá právním předpisům o ochraně údajů a probíhá pouze v případě potřeby. Bez výjimky musí být stanoveny standardní smluvní doložky, závazná firemní pravidla nebo jiná vhodná ochrana.

Děláme vše pro to, aby nedocházelo k uchovávání dat delší dobu, než je nezbytné k poskytování služeb podle smlouvy EULA. Naše doba uchovávání může trvat déle než platnost vaší licence, a to z toho důvodu, abychom vám poskytli čas pro snadné a pohodlné obnovení. Minimalizované a pseudonymizované statistiky a další data ze služby ESET LiveGrid® mohou být dále zpracovávány pro statistické účely.

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost,

integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat dozorčí orgány i subjekty údajů. Jako subjekt údajů máte právo podat stížnost u dozorčího orgánu.

Práva subjektu údajů

Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Za podmínek stanovených příslušnými zákony o ochraně údajů máte jako subjekt údajů nárok na následující práva:

- právo požádat společnosti ESET o přístup k vašim osobním údajům,
- právo na opravu vašich osobních údajů, pokud jsou nepřesné (máte také právo na doplnění neúplných osobních údajů),
- právo požadovat vymazání vašich osobních údajů,
- právo požadovat omezení zpracování vašich osobních údajů,
- právo podat námitky proti zpracování,
- právo podat stížnost, stejně tak
- právo na přenositelnost dat.

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Vedoucí pracovník ochrany osobních údajů
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk