ESET PROTECT

Príručka nasadenia virtuálneho zariadenia

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r. o.

ESET PROTECT bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukovaná žiadnym prostriedkom ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti ESET, spol. s r. o.

ESET, spol. s r. o. si vyhradzuje právo zmeny programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 19.3.2023

1 Virtuálne zariadenie ESET PROTECT 1
1.1 O tejto príručke 1
1.2 Požiadavky 2
1.2 Odporúčané systémové konfigurácie 3
2 Podporované nástroje Hypervisor 4
3 Fázy implementácie a údržba virtuálneho zariadenia ESET PROTECT 4
4 Stiahnutie virtuálneho zariadenia ESET PROTECT 5
5 Heslá pre virtuálne zariadenie ESET PROTECT 5
6 Nasadenie virtuálneho zariadenia ESET PROTECT 6
6.1 vSphere 6
6.2 VMware Workstation/Player 9
6.3 Microsoft Hyper-V 11
6.4 Oracle VirtualBox 13
6.5 Citrix 15
7 Konfigurácia virtuálneho zariadenia ESET PROTECT 17
7.1 Zariadenie ESET PROTECT Server 18
7.2 Zariadenie ESET PROTECT MDM 21
8 Konzola na správu virtuálneho zariadenia ESET PROTECT 26
8.1 Nastavenie statickej IP adresy 27
8.2 Povolenie/zakázanie vzdialeného prístupu 30
8.3 Zálohovanie databázy 31
8.4 Obnovenie databázy 33
8.5 Vykonanie obnovy po vrátení zmien k snímke 34
8.6 Migrácia databázy z iného servera 35
8.7 Zmena hesla pre virtuálny počítač 39
8.8 Zmena hesla pre databázu 40
8.9 Opätovné pripojenie k doméne 41
8.10 Nastavenie domény 43
8.11 Obnovenie pôvodných nastavení 44
9 Rozhranie na správu Webmin 46
9.1 Riadiaci panel 47
9.2 Systém 49
9.3 Servery 50
9.3 ESET PROTECT 50
9.4 Nástroje 52
9.5 Networking 53
10 ESET PROTECT certifikáty 54
11 ESET PROTECT VA aktualizácia/migrácia 55
12 Obnova virtuálneho zariadenia ESET PROTECT po nehode 57
13 Riešenie problémov 58
14 Najčastejšie otázky o virtuálnom zariadení ESET PROTECT 59
14.1 Ako zistiť, ktoré súčasti produktu ESET PROTECT sú nainštalované? 60
14.2 Ako povoliť ping na virtuálnom zariadení ESET PROTECT? 61
14.3 Potrebujem do svojho virtuálneho zariadenia ESET PROTECT pridať ďalšie súčasti? 62
14.4 Ako povoliť Apache HTTP Proxy na virtuálnom zariadení ESET PROTECT po počiatočnej konfigurácii? 62
14.5 Ako nastaviť LDAP pre povolenie synchronizácie statických skupín na virtuálnom zariadení ESET PROTECT? 63
14.6 Konfigurácia pripojenia LDAPS k doméne 63
14.7 Ako obnoviť zabudnuté heslo pre virtuálne zariadenie ESET PROTECT? 65

14.8 Ako zmeniť reťazec pripojenia pre databázu ESET PROTECT? 65
14.9 Ako nastaviť Hyper-V Server pre RD Sensor? 65
14.10 Ako zmeniť číslo portu pre virtuálne zariadenie ESET PROTECT? 66
14.11 Ako zvýšiť veľkosť pamäte pre MySQL Server? 67
14.12 Mám problém s nástrojom ESET PROTECT bežiacom na Hyper-V Serveri 2012 R2. 67
14.13 Ako zlepšiť výkon nástroja Oracle VirtualBox? 67
14.14 Ako povoliť príkaz YUM, ak používam HTTP proxy server? 68
14.15 Ako aktualizovať operačný systém na počítači, na ktorom je nainštalovaný ESET PROTECT VA Server? 68
14.16 Ako natrvalo vypnúť SELinux? 69
14.17 Ako reštartovať konzolu na správu virtuálneho zariadenia? 69
14.18 Ako použiť Proxy na pripájanie agentov? 69
14.19 Ako povoliť SSH? 69
15 Licenčná dohoda s koncovým používateľom 70
16 Zásady ochrany osobných údajov 77

Virtuálne zariadenie ESET PROTECT

Virtuálne zariadenie ESET PROTECT (ESET PROTECT VA) je dostupné pre používateľov, ktorí chcú spúšťať ESET PROTECT vo virtualizovanom prostredí. Virtuálne zariadenie ESET PROTECT zjednodušuje nasadenie nástroja ESET PROTECT a je rýchlejšie ako all-in-one inštalátor alebo inštalácia súčastí.

Virtuálne zariadenie ESET PROTECT môže byť nasadené vo väčšine virtuálnych prostredí. Podporuje natívne aj čisté (bez systému) nástroje hypervisor (VMware vSphere/ESXi a Microsoft Hyper-V), ako aj hostiteľské nástroje hypervisor, ktoré sa často používajú na operačných systémoch určených pre stolové počítače (VMware Workstation, VMware Player a Oracle VirtualBox). Úplný zoznam nájdete v kapitole Podporované nástroje Hypervisor.

Táto príručka podrobne vysvetľuje postup nasadzovania a spravovania ESET PROTECT VA vrátane jeho nových funkcií:

- Konzola na správu virtuálneho zariadenia ESET PROTECT – jednoduché **textové používateľské rozhranie** (TUI) s hlavným menu. Toto rozhranie vám pomôže s textovými príkazmi zobrazením výzvy na zadanie potrebných hodnôt. ESET PROTECT VA dokážu bez problémov používať a spravovať aj používatelia, ktorí nemajú pokročilé skúsenosti s prácou v CentOS 7 alebo iných Linuxových operačných systémoch. Medzi najdôležitejšie funkcie dostupné v tomto rozhraní patria:
    - Set static IP address – manuálne nastavenie statickej IP adresy v prípade, že vaše ESET PROTECT VA nemá DHCP serverom priradenú žiadnu IP adresu.
    - Pull database from other server – pre prípad, že potrebujete aktualizovať alebo migrovať svoje ESET PROTECT VA.
    - Backup and restore of ESET PROTECT database – tieto funkcie sú dôležité pre váš plán obnovy v prípade straty dát a sú k dispozícii v prípade problémov s ESET PROTECT VA.
    - Factory reset – obnoví virtuálne zariadenie do pôvodného stavu, v akom sa nachádza po čerstvom nasadení. Túto funkciu môžete použiť v prípade problémov s ESET PROTECT VA. Aby ste sa vyhli strate dát, majte vždy vytvorenú zálohu databázy.
- Rozhranie na správu Webmin – webové rozhranie tretej strany, ktoré zjednodušuje správu Linuxového systému. Umožňuje vám spravovať ESET PROTECT VA vzdialene z vášho webového prehliadača pomocou intuitívneho rozhrania. Najdôležitejšie moduly rozhrania Webmin sú popísané v tomto dokumente.

O tejto príručke

Príručka nasadenia virtuálneho zariadenia (VA) obsahuje inštrukcie nasadenia a nakonfigurovania virtuálneho zariadenia ESET PROTECT (ESET PROTECT VA). Táto príručka je určená pre každého, kto chce nasadiť, spravovať a aktualizovať ESET PROTECT VA.

Pre zachovanie konzistentnosti, a aby sa zabránilo zámene, je terminológia použitá v tejto príručke založená na názvoch parametrov nástroja ESET PROTECT. Používame tiež sadu symbolov na zvýraznenie kapitol, ktoré sú obzvlášť dôležité alebo potrebné.

> Poznámky môžu poskytovať cenné informácie, ako napríklad špecifické funkcie alebo odkaz na súvisiacu kapitolu.

Takéto informácie si vyžadujú vašu pozornosť a neodporúča sa ich ignorovať. Zvyčajne ide o podstatné informácie, hoci nie sú mimoriadne závažné.

Upozornenia obsahujú mimoriadne dôležité informácie, pri ktorých by ste mali spozornieť. Upozornenia sú umiestnené tak, aby vás včas varovali a zároveň vám pomohli predísť chybám, ktoré by mohli mať negatívne následky. Prosím, dôkladne si prečítajte text ohraničený týmto označením, pretože sa týka vysoko citlivých systémových nastavení alebo upozorňuje na riziká.

Toto označenie obsahuje ukážkový príklad, ktorý priamo súvisí s informáciami v príslušnej kapitole. Príklady sa využívajú hlavne pri komplikovanejších kapitolách.

Konvencia	Význam
Tučné písmo	Pomenúva položky rozhrania, ako napr. polia a tlačidlá možností.
Kurzíva	Zástupné symboly pre údaje, ktoré máte poskytnúť. Napríklad, názov súboru alebo cesta znamená, že máte zadať konkrétnu cestu k súboru alebo názov súboru.
`Courier New`	Príklady kódov alebo príkazov.
Hypertextové prepojenie	Poskytuje rýchly a jednoduchý prístup k súvisiacim prepojeným kapitolám alebo externým webovým lokalitám. Hypertextové prepojenia sú zvýraznené modrou farbou a môžu byť podčiarknuté.
%ProgramFiles%	Systémový adresár Windows, kde sú uložené programy systému Windows a ďalšie programy.

- Online pomocník je hlavným zdrojom pomocného obsahu. Pri pripojení na internet je zobrazovaná vždy najnovšia verzia Online pomocníka. Online pomocník pre produkt ESET PROTECT obsahuje štyri aktívne karty na vrchnej navigačnej hlavičke: Inštalácia/Aktualizácia, Administrácia, Nasadenie VA a Príručka pre malé a stredne veľké podniky.
- Táto príručka je rozdelená na niekoľko kapitol a podkapitol. Konkrétne informácie môžete nájsť pomocou poľa určeného na vyhľadávanie v hornej časti.

Keď otvoríte používateľskú príručku z navigačného panela umiestneného vo vrchnej časti stránky, vyhľadávanie bude obmedzené len na obsah danej príručky. Napríklad, ak otvoríte časť Administrácia, kapitoly z časti Inštalácia/aktualizácia a Nasadenie VA nebudú zahrnuté do výsledkov vyhľadávania.

- Databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najrýchlejší nástroj na riešenie rozličných druhov problémov.
- ESET fórum poskytuje používateľom produktov spoločnosti ESET jednoduchý spôsob, ako získať pomoc a zároveň pomôcť iným. Môžete tam uverejniť akúkoľvek otázku alebo sa informovať o akomkoľvek probléme v súvislosti s produktmi spoločnosti ESET.
- Môžete odoslať vaše hodnotenie alebo poskytnúť spätnú väzbu na konkrétnu kapitolu pomocníka: Kliknite na odkaz **Zanechajte nám spätnú väzbu** nachádzajúci sa pod stránkou pomocníka.

Požiadavky

Pred nasadením virtuálneho zariadenia ESET PROTECT (PRODUCT VA) je potrebné splniť nasledujúce požiadavky:

- Musíte použiť podporovaný nástroj hypervisor.

- Uistite sa, že je podporovaný hosťovský operačný systém (ak je použitý hostiteľský hypervisor, ako napríklad VMware Workstation/Player alebo Oracle VirtualBox).

- Uistite sa, že nastavenia systémových hodín medzi hostiteľským a hosťovským operačným systémom sú zosynchronizované.

- **VT musí byť povolené** v nastaveniach systému BIOS hostiteľského systému. Táto funkcia môže byť pomenovaná rôzne: VT, Vanderpool Technology, Virtualization Technology, VMX, alebo Virtual Machine Extensions. Toto nastavenie sa zvyčajne nachádza na bezpečnostnej obrazovke systému BIOS. Umiestnenie tohto nastavenia závisí od dodávateľa systému.

- Uistite sa, že sieťový adaptér je na vašom virtuálnom počítači nastavený ako **Bridged** (prípadne **NAT**). Počas konfigurácie ESET PROTECT VA môžete upresniť sieťové nastavenia vrátane podrobností o doméne, aby sa úloha Synchronizácia statickej skupiny spustila správne.

- Ak používate režim **NAT**, presmerovanie portov musí byť nastavené na vašom virtuálnom počítači, aby bol ESET PROTECT dostupný zo siete. Porty, pre ktoré je potrebné nastaviť presmerovanie, sú zobrazené v okne konzoly ESET PROTECT VA po jeho úspešnom nasadení a nastavení.

- ESET PROTECT VA podporuje len prostredia IPv4. Hoci je možné manuálne nakonfigurovať prostredie IPv6, protokol IPv6 nie je podporovaný.

Odporúčame vám vytvoriť snapshot (snímku) nasadeného a nastaveného ESET PROTECT VA a synchronizovať ho s Active Directory. Odporúčame tiež vytvoriť snapshot pred nasadením ESET Management Agenta na klientske počítače.

- Pri nasadení ESET PROTECT sú potrebné certifikáty ESET PROTECT MDM. Na vygenerovanie týchto certifikátov, ktoré šifrujú komunikáciu medzi súčasťami ESET PROTECT, musíte mať spustenú inštanciu ESET PROTECT Servera.

Odporúčané systémové konfigurácie

V závislosti od veľkosti vašej infraštruktúry, konkrétne od počtu klientov spravovaných virtuálnym zariadením ESET PROTECT, je potrebné vziať na vedomie minimálnu a odporúčanú konfiguráciu virtuálneho počítača.

Nasledujúce veľkosti sa vzťahujú na ESET PROTECT Server a ESET PROTECT MDM virtuálne zariadenie:

Počet klientov	Počet jadier	Veľkosť RAM	Iné
menej ako 5000 klientov	4	4 GB	Thick provisioned disk, manuálne zmeňte konfiguráciu pre zvýšenie veľkosti pamäte pre MySQL.
viac ako 5000 klientov	8	8 GB	Proporčne zvýšte počet dostupných prostriedkov pre vaše ESET PROTECT VA, aby sa predišlo problémom s výkonom.

Ak plánujete mať viac ako 5 000 spravovaných klientov, dôrazne odporúčame nainštalovať ESET PROTECT Server/MDM na fyzický počítač so systémom Microsoft Windows Server s Microsoft SQL Serverom.

Podporované nástroje Hypervisor

Virtuálne zariadenie ESET PROTECT (VA) (*protect_appliance.ova*) je založené na virtuálnom hardvéri typu `vmx-07`.

Virtuálne zariadenie je podporované len na uvedených nástrojoch Hypervisor. Používanie virtuálneho zariadenia na iných nástrojoch Hypervisor je na vlastnú zodpovednosť.

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

Odporúčame, aby ste vo svojej sieti použili na pridelenie IP adresy svojmu virtuálnemu zariadeniu ESET PROTECT DHCP server. Táto IP adresa je potrebná pre prístup do konfiguračného webového rozhrania ESET PROTECT VA. Ak nemáte vo vašej sieti DHCP server, budete musieť nastaviť manuálnu IP adresu.

Fázy implementácie a údržba virtuálneho zariadenia ESET PROTECT

Implementácia virtuálneho zariadenia ESET PROTECT pozostáva z nasledujúcich hlavných fáz, ktoré sú potrebné pre úspešné nasadenie a konfiguráciu:

1. Proces nasadenia zariadenia ESET PROTECT – nasadenie súboru *OVA* virtuálneho zariadenia ESET PROTECT na váš nástroj Hypervisor.

2. Konfigurácia virtuálneho zariadenia ESET PROTECT – konfigurácia po nasadení, vykonávaná prostredníctvom webového rozhrania ESET PROTECT VA. Časť konfigurácia vám umožňuje výber typu zariadenia a zadanie špecifických údajov a vlastností, ktoré sú potrebné pre správne fungovanie daného ESET PROTECT VA.

Ďalšie nastavenia a správa sú vykonávané pomocou TUI (textové používateľské rozhranie) a pomocou nástroja Webmin:

1. Konzola na správu virtuálneho zariadenia ESET PROTECT – umožňuje vám vykonávať operácie súvisiace s údržbou, ako napr. zálohovanie a obnova, zmena hesla, obnovenie pôvodných nastavení atď.

2. Rozhranie na správu Webmin – umožňuje jednoduché spravovanie vášho ESET PROTECT VA.

Aktualizácia, migrácia a postup obnovy po nehode:

Aktualizácia/migrácia ESET PROTECT VA – ak chcete aktualizovať ESET PROTECT VA na najnovšiu verziu, podrobné inštrukcie nájdete v tejto kapitole. Rovnaký postup platí aj pre migráciu vášho ESET PROTECT VA.

Obnova ESET PROTECT VA po nehode – postupujte podľa tejto časti v prípade, že ESET PROTECT VA prestalo fungovať a nie je možné odstrániť daný problém alebo neviete obnoviť poškodenú inštanciu ESET PROTECT VA.

Stiahnutie virtuálneho zariadenia ESET PROTECT

Virtuálne zariadenie ESET PROTECT poskytujeme ako súbor typu OVA (Open Virtualization Appliance). Je dostupné na webovej stránke spoločnosti ESET v časti Na stiahnutie. Zariadenie je k dispozícii ako protect_appliance.ova.

Ak chcete nasadiť vaše virtuálne zariadenie na Microsoft Hyper-V, použite `protect_appliance.vhd.zip` namiesto súboru *OVA*.

- *protect_appliance.ova* – obsahuje viacero typov ESET PROTECT zariadení. Nasaďte tento súbor a vyberte typ zariadenia, ktorý chcete spustiť. Máte na výber nasledujúce typy zariadení:
  - **ESET PROTECT Server** – ESET PROTECT Server, ktorý bude bežať na vyhradenom virtuálnom počítači. Obsahuje tiež nástroj Rogue Detection Sensor.
  - **ESET PROTECT MDM** – súčasť, ktorá je určená len na správu mobilných zariadení. Ak nechcete, aby bol na internete viditeľný celý váš ESET PROTECT Server, môžete na internete sprístupniť len ESET PROTECT MDM VM, vďaka čomu bude aj naďalej umožnená správa mobilných zariadení.

Súbor *OVA* je šablóna, ktorá obsahuje funkčný operačný systém CentOS 7. Pre nasadenie súboru *OVA* virtuálneho zariadenia ESET PROTECT postupujte podľa inštrukcií pre váš nástroj hypervisor. Pri použití súboru `protect_appliance.ova` si môžete vybrať, ktoré ESET PROTECT zariadenie má váš virtuálny počítač po nasadení spúšťať. Po vybratí typu virtuálneho zariadenia môžete začať s konfiguráciou virtuálneho zariadenia ESET PROTECT. Po nasadení súboru *OVA* vyberte typ zariadenia a upravte nastavenia vášho virtuálneho zariadenia. Virtuálne zariadenie je ucelené prostredie s nástrojom ESET PROTECT (alebo jednou z jeho súčastí).

Predtým, ako začnete s nasadením sa uistite, že všetky požiadavky sú splnené.

Po dokončení nasadenia a konfigurácie sa môžete pripojiť na ESET PROTECT Server pomocou rozhrania ESET PROTECT Web Console a začať používať ESET PROTECT.

> **i** Spoločnosť ESET poskytuje virtuálne zariadenia ESET PROTECT, nie je však zodpovedná za podporu alebo údržbu vašich operačných systémov alebo ich súčastí. Virtuálne zariadenia ESET PROTECT sú navrhnuté na zjednodušenie používania a nasadzovania, pričom používajú verejne dostupné operačné systémy obsahujúce súčasti, ktoré neboli vyvinuté spoločnosťou ESET. Spravovanie a aktualizácia týchto súčastí je zodpovednosťou používateľa virtuálneho zariadenia ESET PROTECT. Odporúčame pravidelne aktualizovať operačný systém, aby sa predišlo bezpečnostným problémom.

Heslá pre virtuálne zariadenie ESET PROTECT

Virtuálne zariadenie ESET PROTECT používa niekoľko odlišných používateľských účtov. Nasledujúca tabuľka vysvetľuje jednotlivé typy účtov:

Typ účtu	Prednastavené heslo	Popis a použitie
Operačný systém (CentOS) root	`eraadmin`	Toto je účet, pomocou ktorého sa môžete prihlásiť do svojho ESET PROTECT VA. Poskytuje vám prístup do konzoly na správu virtuálneho zariadenia ESET PROTECT a rozhrania na správu Webmin. Umožňuje vám obnoviť továrenské nastavenia pomocou funkcie Factory reset alebo vykonať akciu Pull database from other server (načítanie obsahu databázy z iného servera). Zvyčajne budete vyzvaný na zadanie vášho **hesla pre virtuálny počítač**.
Databáza (MySQL) root	`eraadmin`	Toto je root účet pre MySQL databázový server. Umožňuje vám vykonávať databázové operácie, ako napr. Backup (zálohovanie) alebo Restore (obnova) databázy. Zvyčajne budete vyzvaný na zadanie vášho root **hesla databázy**.
Správca ESET PROTECT Web Console	špecifikované počas konfigurácie ESET PROTECT VA	Toto heslo je dôležité, pretože vám umožňuje prístup do rozhrania ESET PROTECT Web Console.

Prednastavené heslo je možné zmeniť počas konfigurácie virtuálneho zariadenia ESET PROTECT. Všetky účty uvedené vyššie budú mať rovnaké heslo, ktoré ste špecifikovali počas konfigurácie ESET PROTECT VA. Avšak, pre každý účet môže byť nastavené iné heslo. Je bezpečnejšie používať odlišné heslá, hoci používanie viacerých hesiel môže byť komplikovanejšie. Z tohto dôvodu odporúčame nájsť si efektívny spôsob spravovania rôznych hesiel pre ESET PROTECT VA, aby nenastal zmätok.

> **i** Keď nasadíte ESET PROTECT VA, ktoré ešte nie je nakonfigurované, bude používať rovnaké heslo `eraadmin` pre všetky horeuvedené účty, až kým nebude zmenené v rámci konfigurácie virtuálneho zariadenia ESET PROTECT.

V prípade, že zabudnete heslo pre ktorýkoľvek zo spomínaných účtov, pozrite si kapitolu Ako obnoviť zabudnuté heslo pre ESET PROTECT VA.

Nasadenie virtuálneho zariadenia ESET PROTECT

Kliknite na typ nástroja Hypervisor, ktorý budete používať a zobrazia sa príslušné inštrukcie nasadenia:

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

vSphere

Nasadenie virtuálneho zriadenia ESET PROTECT pomocou vSphere klienta

1. Pripojte sa na vCenter Server pomocou vSphere klienta alebo priamo na ESXi server.

2. Ak používate vSphere klienta, kliknite na **File** > **Deploy OVF Template**. V prípade vSphere webového klienta kliknite na **Actions** > **Deploy OVF Template**.

3. Kliknite na **Browse**, vyhľadajte súbor *protect_appliance.ova*, ktorý ste stiahli z webovej stránky ESET.com a kliknite na **Open**.

Nepodporované verzie VMware ESXi neakceptujú certifikáty SHA-256. Ak sa vám počas importu balíka *.ova* pre ESET PROTECT VA 9.1 zobrazí chyba súvisiaca s certifikátom, bude potrebné odstrániť súbor *.cert* z balíka *.ova* a následne pokračovať s nasadením.

4. Kliknite na **Next** v okne podrobností šablóny OVF (OVF Template Details).

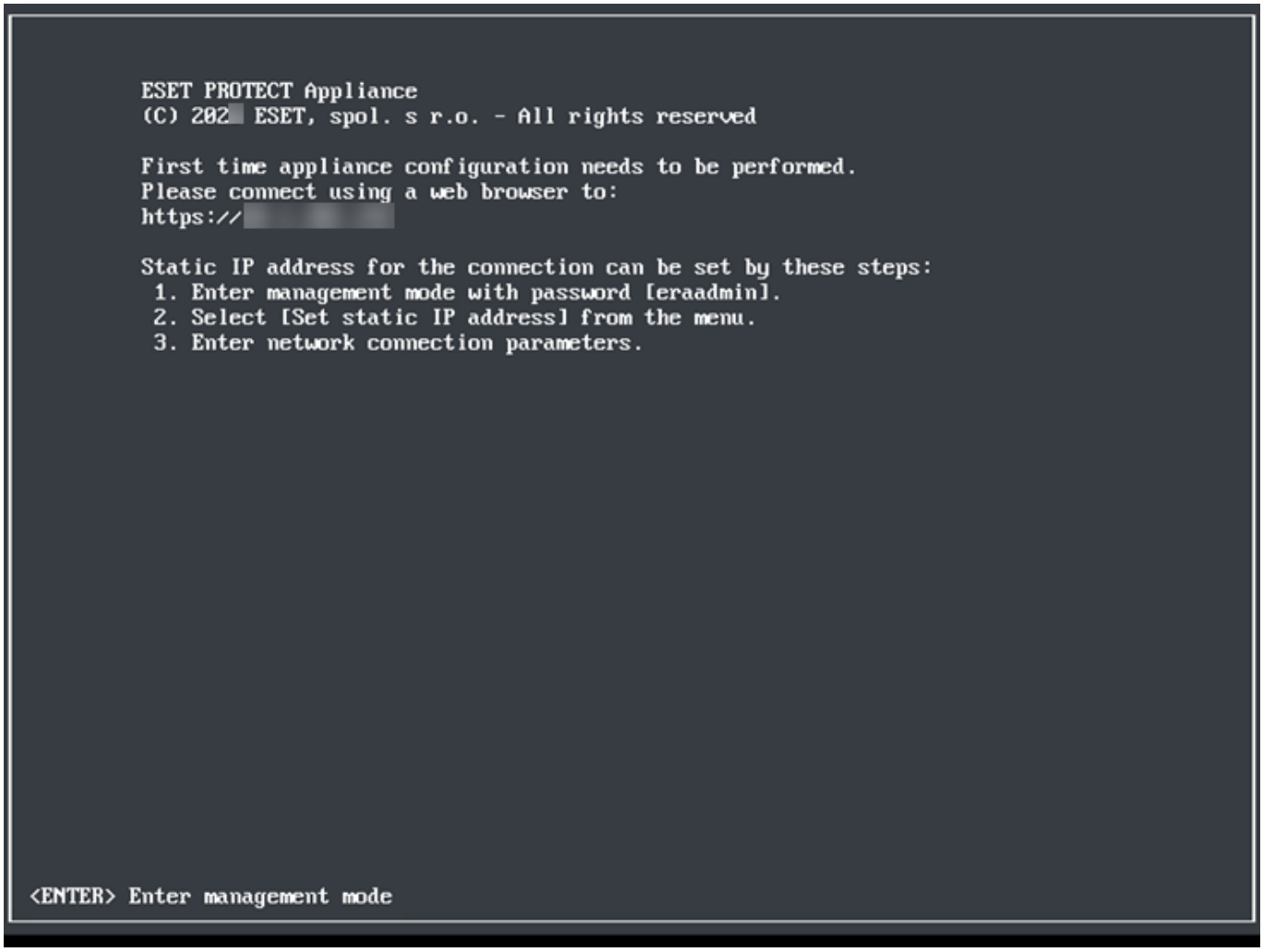
5. Prečítajte si Licenčnú zmluvu koncového používateľa (EULA) a potvrďte ju, ak s ňou súhlasíte.

6. Pre dokončenie inštalácie postupujte podľa pokynov na obrazovke a zadajte nasledujúce informácie o vašom virtuálnom kliente:

- **Name and Location** – zadajte názov pre nasadenú šablónu a umiestnenie, kde sú uložené súbory virtuálneho počítača.
- **Host / Cluster** – vyberte hostiteľa alebo klaster, na ktorom chcete spustiť šablónu.
- **Resource Pool** – vyberte fond prostriedkov, v rámci ktorého chcete nasadiť šablónu.
- **Storage** – vyberte umiestnenie, kde sa budú ukladať súbory virtuálneho počítača.
- **Disk Format** – vyberte formát, ktorý budú používať virtuálne disky.
- **Network Mapping** – vyberte sieť, ktorú bude používať virtuálny počítač. Uistite sa, že ste vybrali sieť virtuálneho počítača združenú s fondom IP, ktorý ste vytvorili.

7. Kliknite na **Next**, skontrolujte súhrn nasadenia a kliknite na **Finish**. Následne bude automaticky vytvorený virtuálny počítač s nastaveniami, ktoré ste definovali.

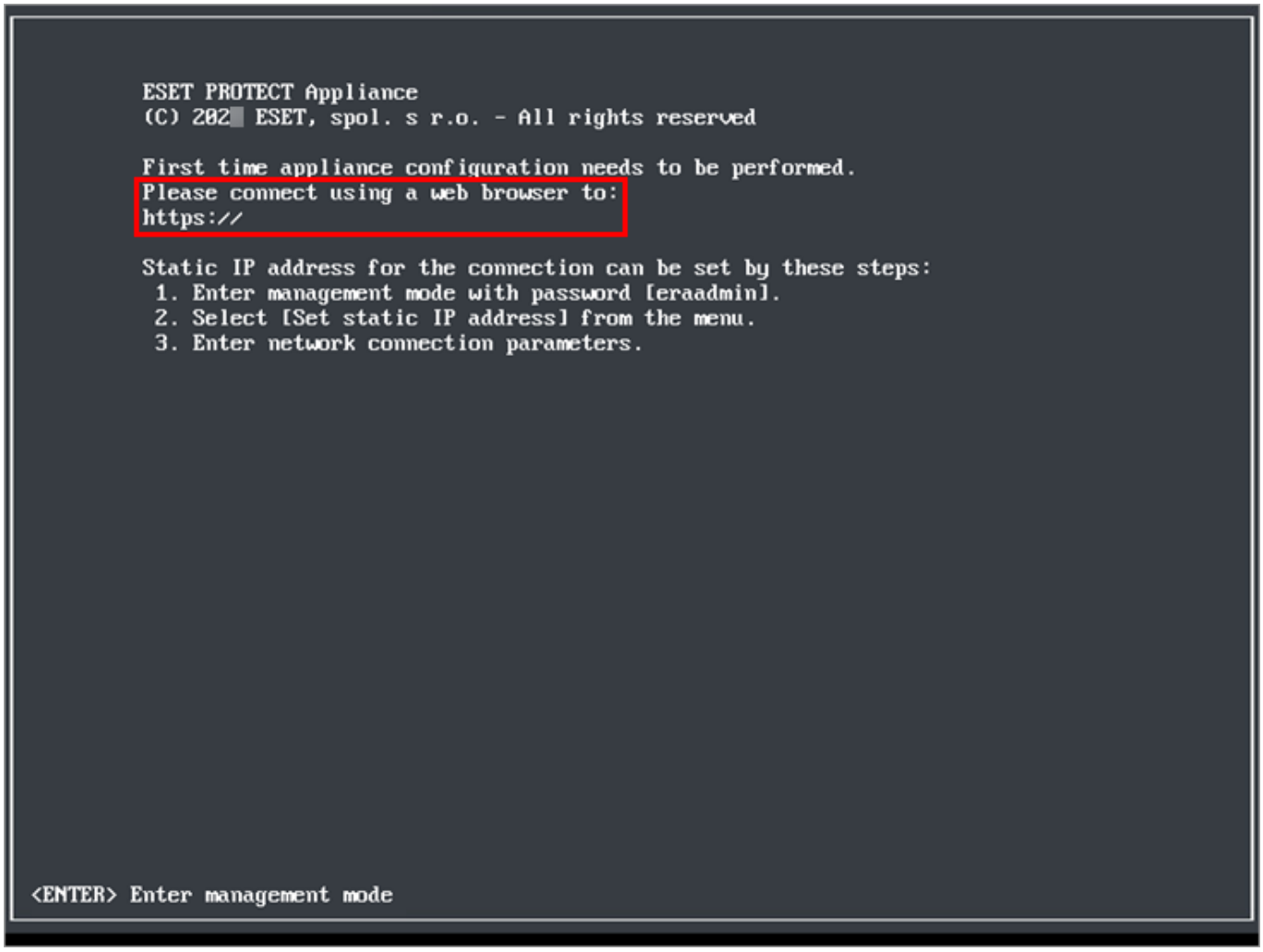
8. Po úspešnom nasadení virtuálneho zariadenia ESET PROTECT ho môžete spustiť. Zobrazia sa nasledujúce informácie:



Otvore svoj webový prehliadač a zadajte IP adresu svojho nasadeného ESET PROTECT zariadenia do poľa s adresou. IP adresa je uvedená v okne konzoly (zobrazené nižšie). Zobrazí sa hlásenie „**First time appliance configuration needs to be performed. Je potrebné vykonať prvú konfiguráciu zariadenia. Pripojte sa pomocou webového prehliadača na** *https://[IP address]*".

Ďalším krokom je nastavenie vášho zariadenia pomocou webového rozhrania.

Ak nemáte vo svojej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu pomocou konzoly na správu. Ak nie je pridelená žiadna IP adresa, zobrazí sa nasledujúca informácia, pričom URL adresa nebude obsahovať IP adresu:
Ak nie je pridelená IP adresa, môže sa stať, že DHCP server nebude môcť prideliť novú. Uistite sa, že v podsieti, kde sa nachádza virtuálne zariadenie, sú dostupné voľné IP adresy.



Dôrazne odporúčame nastaviť vCenter roly a oprávnenia tak, aby používatelia VMware nemali prístup do virtuálneho počítača ESET PROTECT. Týmto sa zabráni tomu, aby mohli používatelia meniť nastavenia virtuálneho počítača ESET PROTECT. Nie je potrebné, aby používatelia nástroja ESET PROTECT vstupovali do virtuálneho počítača. Pre správu prístupu do nástroja ESET PROTECT použite Prístupové práva v ESET PROTECT Web Console.

VMware Workstation/Player

Nasadenie virtuálneho zriadenia ESET PROTECT pomocou nástroja VMware Workstation/Player

Odporúčame používať najnovšiu verziu nástroja VMware Player. Nastavte sieťový adaptér na vašom virtuálnom počítači na **Bridged** alebo **NAT**.

Presmerovanie portov musí byť na vašom virtuálnom počítači nastavené tak, aby bol produkt ESET PROTECT dostupný z internetu.

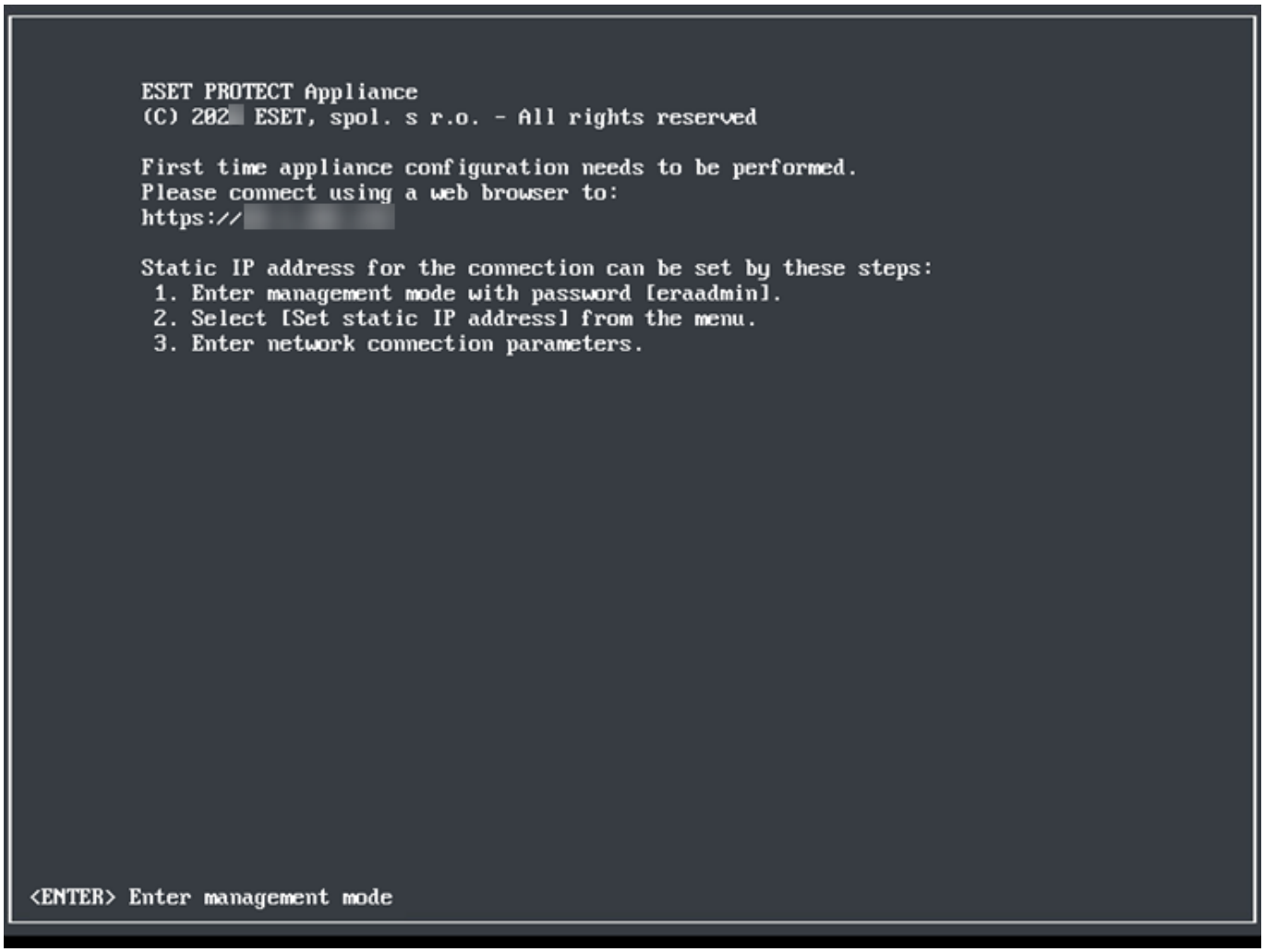
1. Zvoľte možnosť **File** > **Deploy OVF Template**.

2. Vyhľadajte súbor *protect_appliance.ova*, ktorý ste stiahli z webovej stránky spoločnosti ESET a kliknite na **Open**.

3. Zadajte názov a cestu pre nový virtuálny počítač a kliknite na **Import**.

4. Prečítajte si Licenčnú zmluvu koncového používateľa (EULA) a potvrďte ju, ak s ňou súhlasíte.

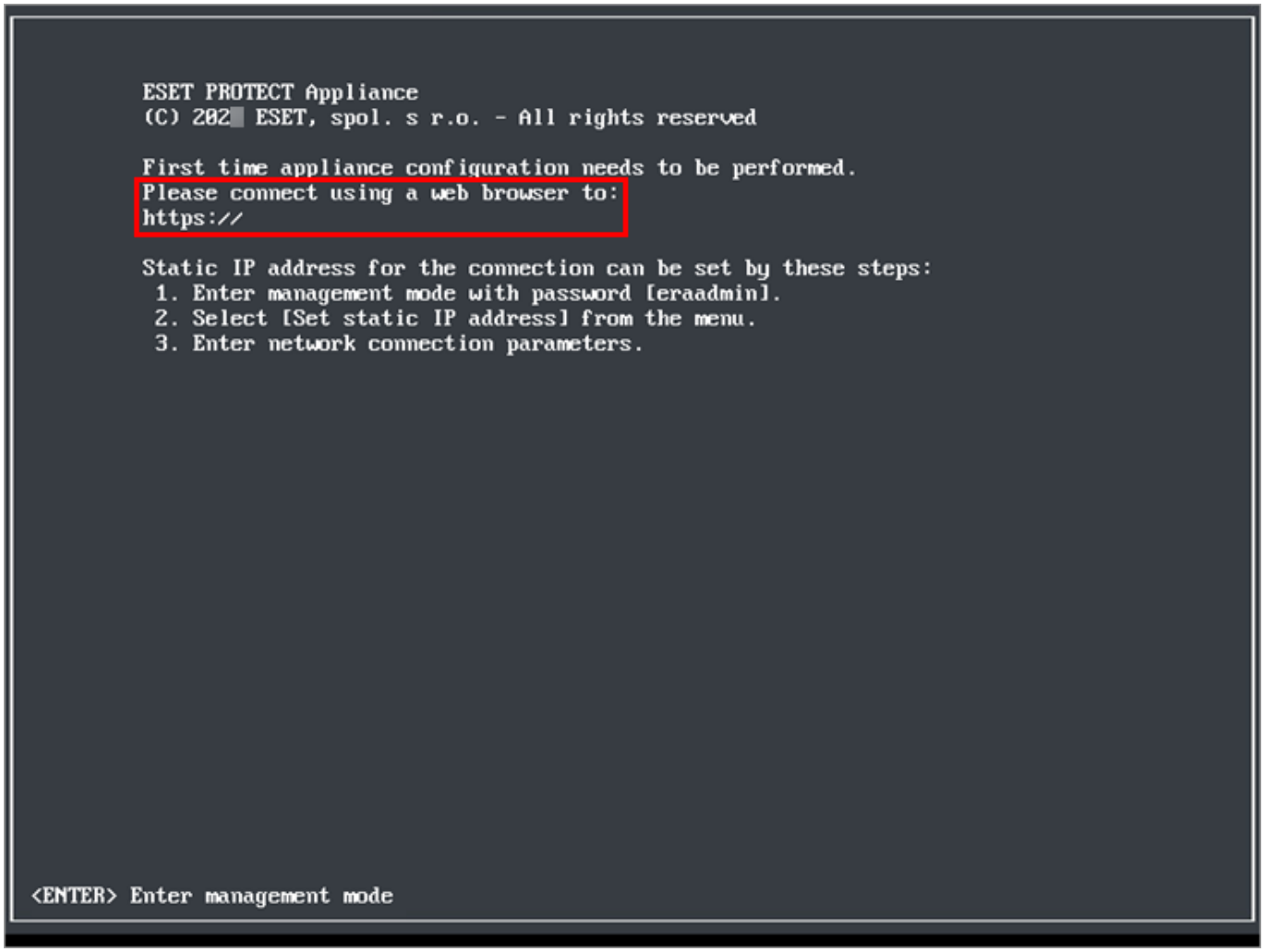
5. Po nasadení zariadenia ho môžete spustiť. Zobrazia sa nasledujúce informácie:



Otvore svoj webový prehliadač a zadajte IP adresu svojho nasadeného ESET PROTECT zariadenia do poľa s adresou. IP adresa je uvedená v okne konzoly (zobrazené nižšie). Zobrazí sa hlásenie „**First time appliance configuration needs to be performed. Je potrebné vykonať prvú konfiguráciu zariadenia. Pripojte sa pomocou webového prehliadača na** *https://[IP address]*".

Ďalším krokom je nastavenie vášho zariadenia pomocou webového rozhrania.

Ak nemáte vo svojej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu pomocou konzoly na správu. Ak nie je pridelená žiadna IP adresa, zobrazí sa nasledujúca informácia, pričom URL adresa nebude obsahovať IP adresu:
Ak nie je pridelená IP adresa, môže sa stať, že DHCP server nebude môcť prideliť novú. Uistite sa, že v podsieti, kde sa nachádza virtuálne zariadenie, sú dostupné voľné IP adresy.



Microsoft Hyper-V

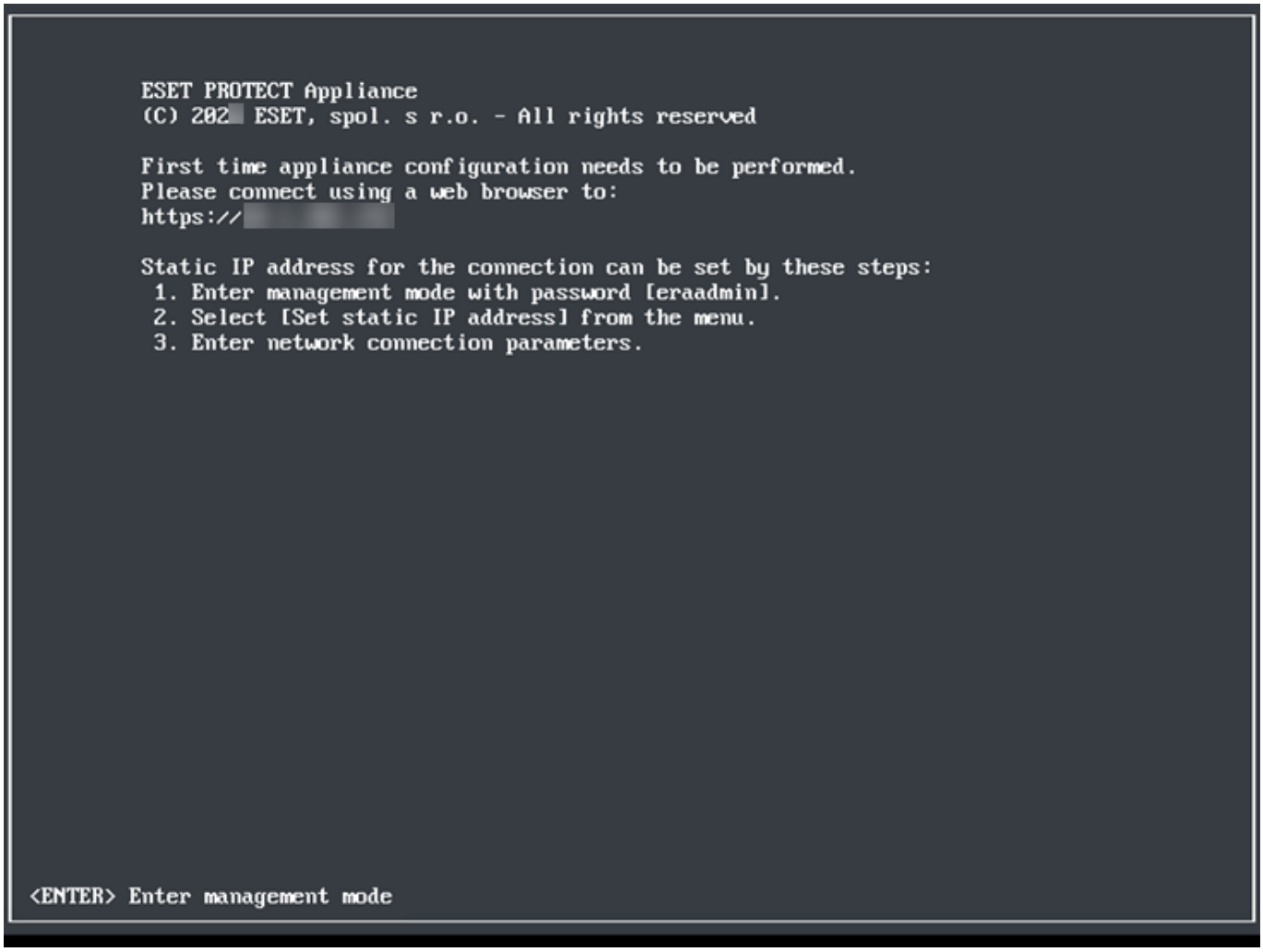
Nasadenie virtuálneho zriadenia ESET PROTECT pomocou nástroja Microsoft Hyper-V

1. Extrahujte súbor `protect_appliance.vhd.zip` (stiahnutý z webovej stránky spoločnosti ESET) napríklad pomocou nástroja Tar alebo 7-Zip.

2. Spustite Hyper-V manager a pripojte sa na príslušný Hyper-V.

3. Vytvorte **nový** virtuálny počítač (Generation 1), ktorý má aspoň 4 jadrá a 4 GB pamäte RAM.

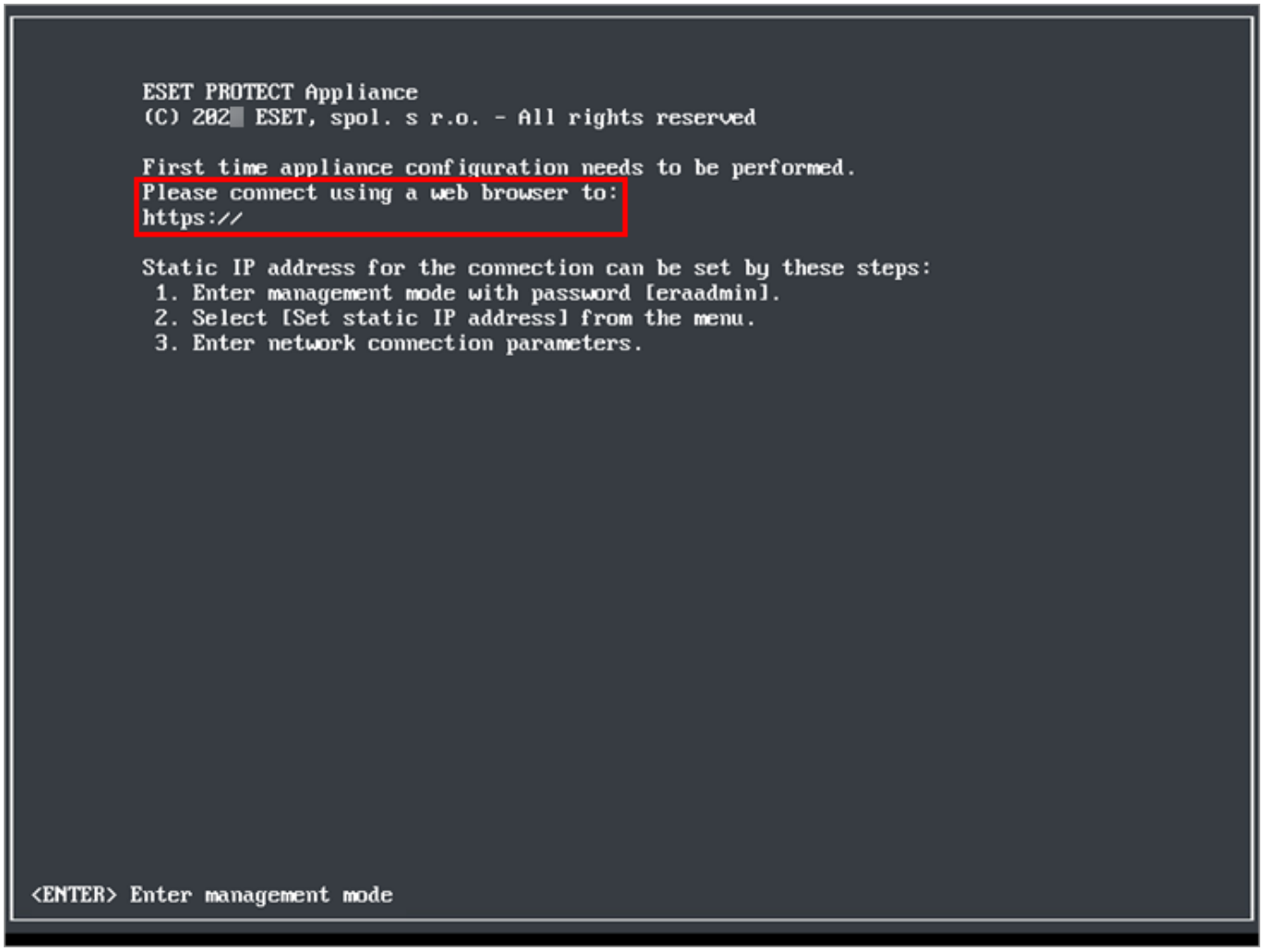
4. Po vytvorení virtuálneho počítača ho môžete spustiť. Zobrazia sa nasledujúce informácie:



Otvore svoj webový prehliadač a zadajte IP adresu svojho nasadeného ESET PROTECT zariadenia do poľa s adresou. IP adresa je uvedená v okne konzoly (zobrazené nižšie). Zobrazí sa hlásenie „**First time appliance configuration needs to be performed. Je potrebné vykonať prvú konfiguráciu zariadenia. Pripojte sa pomocou webového prehliadača na** *https://[IP address]*".

Ďalším krokom je nastavenie vášho zariadenia pomocou webového rozhrania.

Ak nemáte vo svojej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu pomocou konzoly na správu. Ak nie je pridelená žiadna IP adresa, zobrazí sa nasledujúca informácia, pričom URL adresa nebude obsahovať IP adresu:
Ak nie je pridelená IP adresa, môže sa stať, že DHCP server nebude môcť prideliť novú. Uistite sa, že v podsieti, kde sa nachádza virtuálne zariadenie, sú dostupné voľné IP adresy.



Oracle VirtualBox

Nasadenie virtuálneho zriadenia ESET PROTECT pomocou nástroja VirtualBox

Odporúčame používať najnovšiu verziu programu VirtualBox. Nastavte sieťový adaptér na svojom virtuálnom počítači na **Bridged**, prípadne na **NAT**.

> Presmerovanie portov musí byť na vašom virtuálnom počítači nastavené tak, aby bol produkt ESET PROTECT dostupný z internetu (ak je to potrebné).

1. Kliknite na **File** a vyberte možnosť **Import Appliance**.

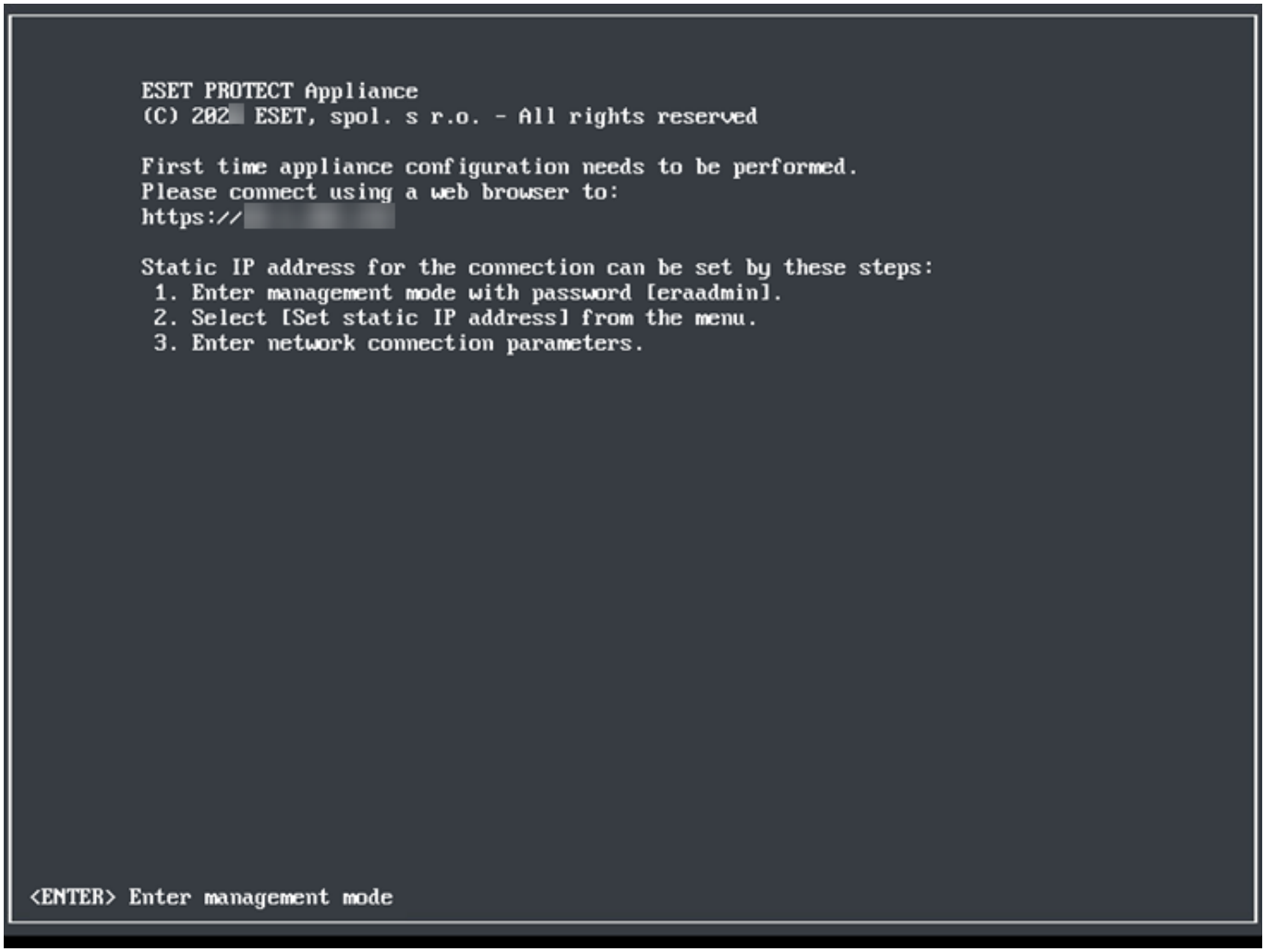
2. Kliknite na **Browse**, vyhľadajte súbor *protect_appliance.ova*, ktorý ste si stiahli z webovej stránky spoločnosti ESET, a kliknite na **Open**.

3. Kliknite na **Next**.

4. Skontrolujte nastavenia zariadenia a kliknite na **Import**.

5. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA), a ak s ňou súhlasíte, potvrďte ju.

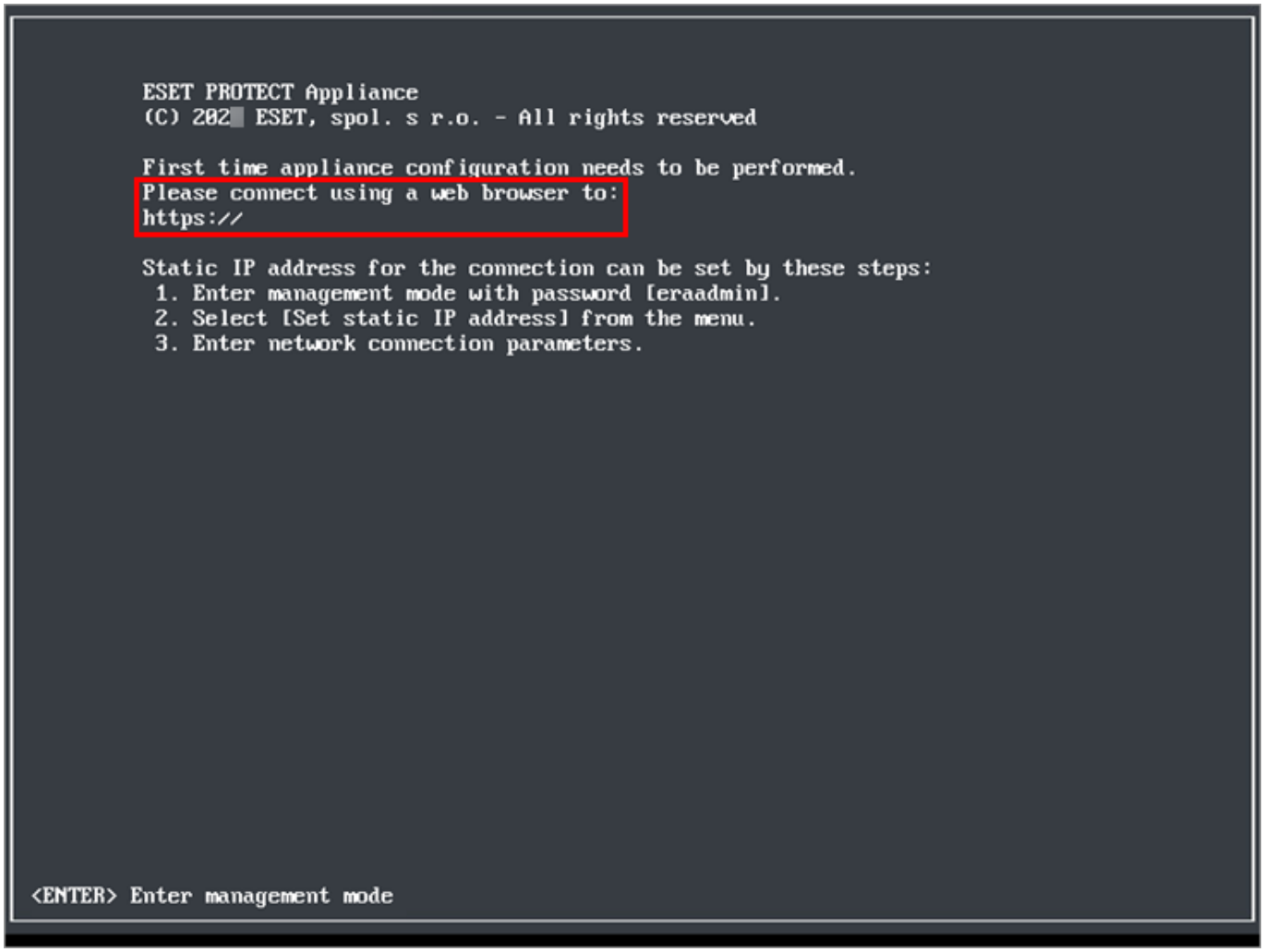
6. Po úspešnom nasadení virtuálneho zariadenia ESET PROTECT ho môžete spustiť. Zobrazia sa nasledujúce informácie:



Otvore svoj webový prehliadač a zadajte IP adresu svojho nasadeného ESET PROTECT zariadenia do poľa s adresou. IP adresa je uvedená v okne konzoly (zobrazené nižšie). Zobrazí sa hlásenie „**First time appliance configuration needs to be performed. Je potrebné vykonať prvú konfiguráciu zariadenia. Pripojte sa pomocou webového prehliadača na** *https://[IP address]*".

Ďalším krokom je nastavenie vášho zariadenia pomocou webového rozhrania.

Ak nemáte vo svojej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu pomocou konzoly na správu. Ak nie je pridelená žiadna IP adresa, zobrazí sa nasledujúca informácia, pričom URL adresa nebude obsahovať IP adresu:
Ak nie je pridelená IP adresa, môže sa stať, že DHCP server nebude môcť prideliť novú. Uistite sa, že v podsieti, kde sa nachádza virtuálne zariadenie, sú dostupné voľné IP adresy.



Citrix

Nasadenie ESET PROTECT VA v prostredí Citrix:

Požiadavky

- Vaša IPv4 sieť musí byť dostupná v prostredí Citrix. Protokol IPv6 nie je podporovaný virtuálnym zariadením ESET PROTECT.
- Súbor *.ovf* musí byť dostupný na počítači, kde budete nasadzovať ESET PROTECT VA.
- Na import balíka *OVF/OVA* sú potrebné povolenia správcu fondu (Pool Admin Permissions).
- Na účely nasadenia je potrebné mať dostatok ukladacieho priestoru, a to minimálne 100 GB.

Proces nasadenia:

1.Kliknite na **File** > **Import**.

2.Kliknite na **Browse**, vyhľadajte súbor *protect_appliance.ova*, ktorý ste si stiahli z webovej stránky spoločnosti ESET, a kliknite na **Next**.

3.Označte začiarkavacie políčko vedľa položky **I accept the End User License Agreements** a kliknite na **Next**.

4.Zvoľte fond (pool) alebo samostatný server, kde chcete umiestniť ESET PROTECT VA, a kliknite na **Next**.

5.Umiestnite importovaný virtuálny disk do ukladacieho repozitára a kliknite na **Next**.

6.Namapujte rozhrania virtuálnej siete výberom možnosti **Target Network** a kliknite na **Next**.

7.Vyberte možnosť overenia digitálneho podpisu (voliteľné) a kliknite na **Next**.

8.Zvoľte možnosť **Don't use Operating System Fixup** a kliknite na **Next**.

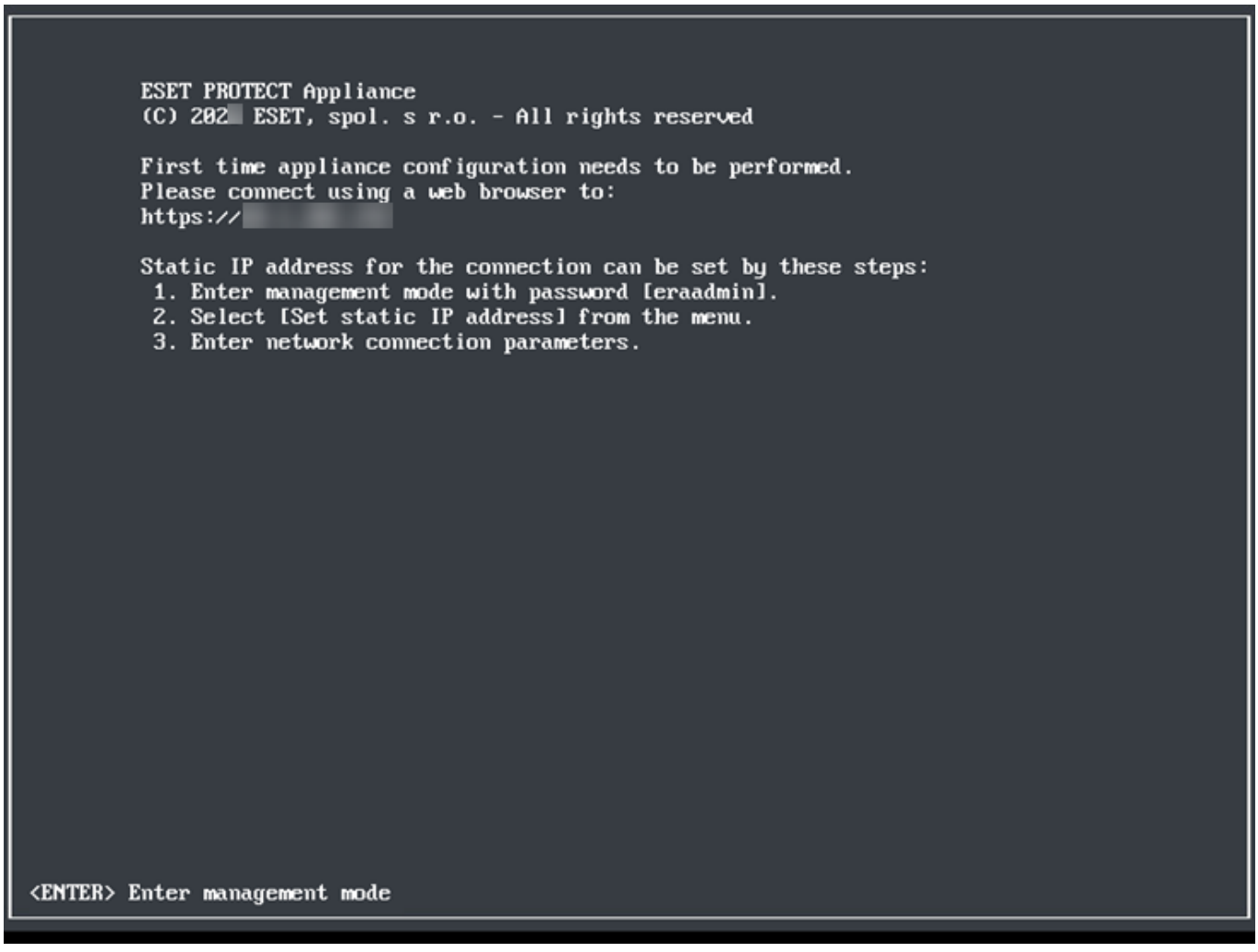
9.Vyberte sieť (rovnakú ako v kroku č. 6), kde nainštalujete dočasné ESET PROTECT VA, ktoré bude slúžiť na vykonanie importu, a kliknite na **Next**.

10. Skontrolujte nastavenia a kliknite na **Finish**.

Proces nasadenia môže chvíľu trvať, pričom Citrix server sa bude javiť ako nečinný. Neprerušujte tento proces.

Viac informácií o nasadení *OVF/OVA* nájdete v dokumentácii dodávateľa.

Po vytvorení virtuálneho počítača ho môžete spustiť. Zobrazia sa nasledujúce informácie:

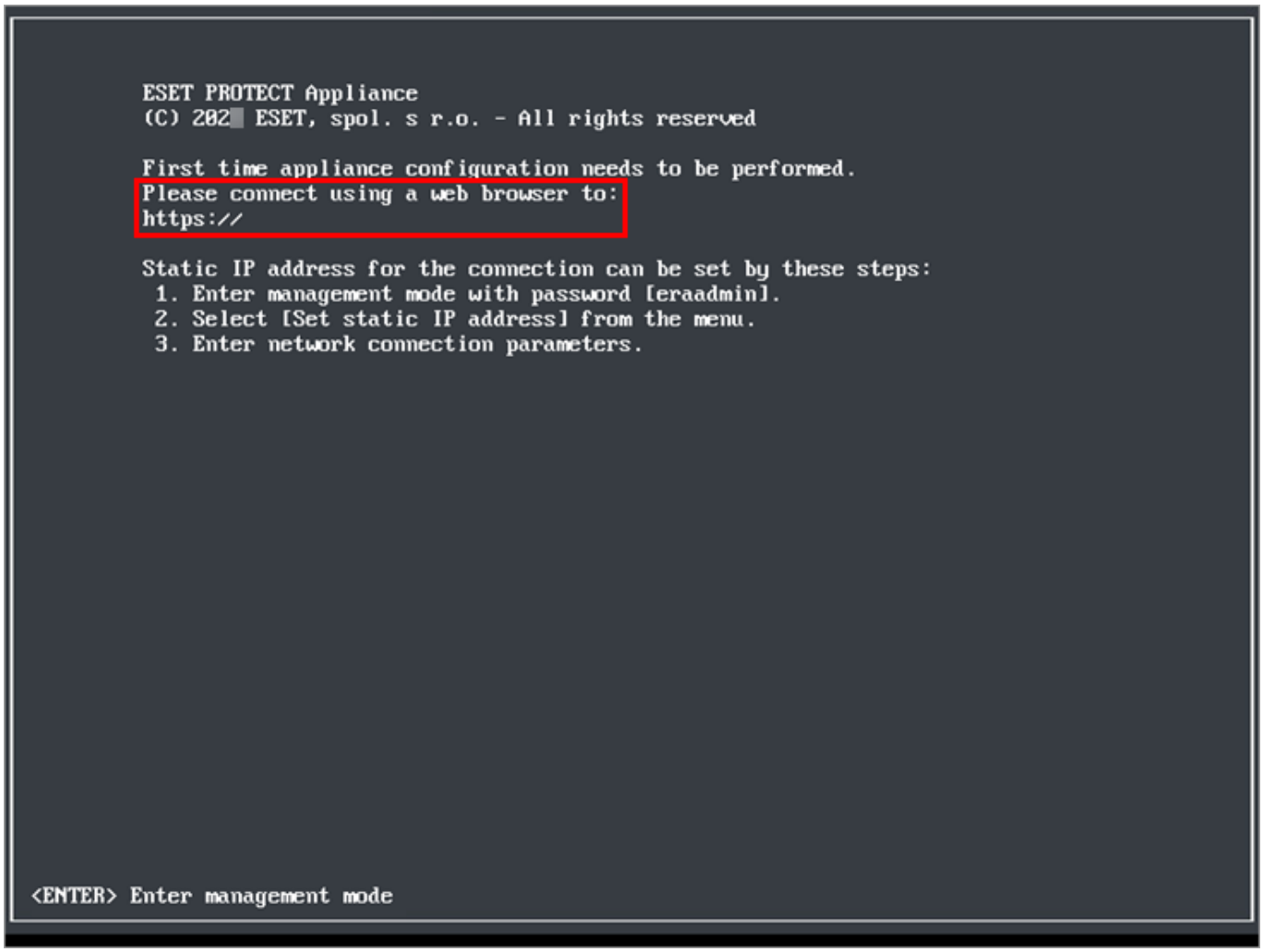


Otvore svoj webový prehliadač a zadajte IP adresu svojho nasadeného ESET PROTECT zariadenia do poľa s adresou. IP adresa je uvedená v okne konzoly (zobrazené nižšie). Zobrazí sa hlásenie „**First time appliance configuration needs to be performed. Je potrebné vykonať prvú konfiguráciu zariadenia. Pripojte sa pomocou**

webového prehliadača na *https://[IP address]*".

Ďalším krokom je nastavenie vášho zariadenia pomocou webového rozhrania.

Ak nemáte vo svojej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu pomocou konzoly na správu. Ak nie je pridelená žiadna IP adresa, zobrazí sa nasledujúca informácia, pričom URL adresa nebude obsahovať IP adresu:
Ak nie je pridelená IP adresa, môže sa stať, že DHCP server nebude môcť prideliť novú. Uistite sa, že v podsieti, kde sa nachádza virtuálne zariadenie, sú dostupné voľné IP adresy.



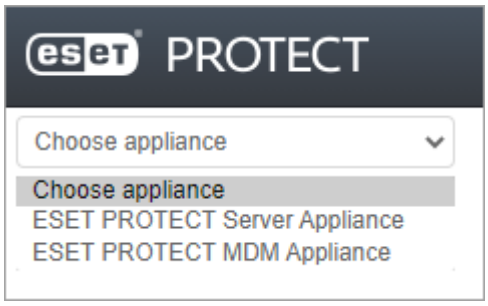
Konfigurácia virtuálneho zariadenia ESET PROTECT

Virtuálne zariadenie ESET PROTECT (ESET PROTECT VA) je možné jednoducho nastaviť pomocou webového rozhrania. Na použitie a prístup do webového rozhrania ESET PROTECT VA musíte mať vo vašej sieti DHCP server, aby malo ESET PROTECT VA automaticky pridelenú IP adresu.

Ak nemáte vo vašej sieti DHCP server, budete musieť pre ESET PROTECT VA nastaviť statickú IP adresu.

Po úspešnom nasadení virtuálneho počítača pre virtuálne zariadenie ESET PROTECT musíte vybrať **typ zariadenia ESET PROTECT**, ktorý chcete spustiť na virtuálnom počítači. Vo webovom prehliadači vyberte z roletového menu požadovaný typ zariadenia ESET PROTECT pre váš virtuálny počítač a nakonfigurujte ho. Kliknite na príslušný odkaz nižšie pre zobrazenie postupu konfigurácie pre váš typ zariadenia:

- Zariadenie ESET PROTECT Server
- Zariadenie ESET PROTECT MDM



Zariadenie ESET PROTECT Server

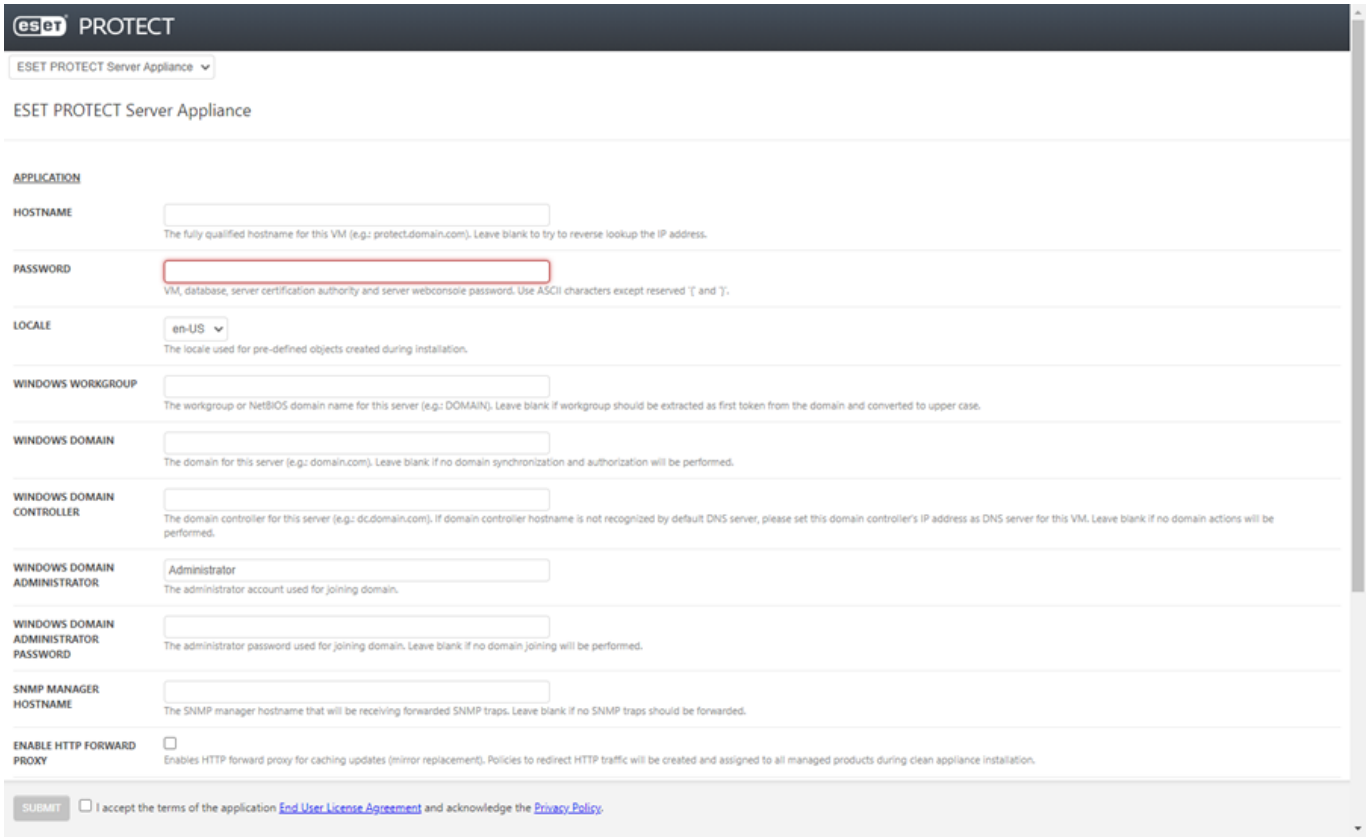
Toto je sekcia nastavení pre zariadenie ESET PROTECT Server. Pozostáva z 2 častí: **Application** a **Networking properties**. Vyplňte všetky povinné polia (označené červenou farbou). Ak je to potrebné, môžete tiež zadať voliteľné parametre.

Tento typ virtuálneho zariadenia ESET PROTECT spúšťa ESET PROTECT Server na vyhradenom virtuálnom počítači. Táto konfigurácia je odporúčaná pre menšie firmy aj pre veľké podnikové siete.

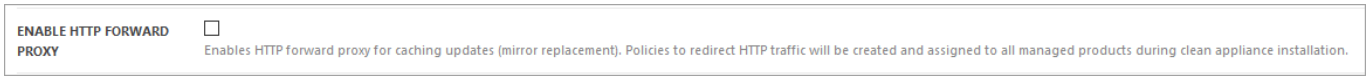
Povinné polia konfigurácie pre zariadenie ESET PROTECT Server:

- **Password** – toto heslo je dôležité, pretože bude použité vo virtuálnom počítači, databáze ESET PROTECT, certifikačnej autorite ESET PROTECT Servera a ESET PROTECT Web Console.

Predvolený používateľ Web Console je **Administrator**.



Hoci to nie je povinné, odporúčame zadať aj voliteľné parametre. Napríklad podrobnosti o doméne a doménovom radiči, prihlasovacie údaje pre účet správcu domény atď. Tieto parametre sú dôležité pre akcie na doméne, ako napr. synchronizácia.



Kliknite sem pre zväčšenie obrázku

Pre ukladanie aktualizácií do vyrovnávacej pamäte môžete povoliť Apache HTTP Proxy. Označte možnosť **Enable HTTP forward proxy** na inštaláciu Apache HTTP Proxy a vytvorenie a uplatnenie politík (pod názvom **Využitie HTTP proxy** a s uplatnením na skupinu **Všetko**) pre nasledujúce produkty:

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

- Vytvorená politika aktivuje HTTP Proxy pre príslušné produkty. Na základe predvolenej konfigurácie sa ako hostiteľ proxy nastaví lokálna IP adresa ESET PROTECT Servera a port 3128. Autentifikácia nebude aktívna. V prípade potreby môžete tieto nastavenia skopírovať do iných politík a použiť ich pre ďalšie produkty.

- Používanie HTTP Proxy môže zredukovať množstvo dát stiahnutých z internetu a zvýšiť rýchlosť sťahovania aktualizácií. Odporúčame označiť možnosť **Apache HTTP Proxy**, ak plánujete prostredníctvom nástroja ESET PROTECT spravovať viac ako 37 počítačov.

- Ak chcete, môžete Apache HTTP Proxy nainštalovať aj neskôr. Viac informácií nájdete v časti Najčastejšie otázky o virtuálnom zariadení ESET PROTECT.

Vlastnosti siete

Presuňte sa kurzorom myši smerom nadol, kde môžete nastaviť nasledujúce vlastnosti siete: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. Všetky polia sú voliteľné.

Pripojenie virtuálneho zariadenia ESET PROTECT k doméne

Počas počiatočnej konfigurácie môžete ESET PROTECT VA nakonfigurovať na spustenie v doméne. Nasledujúce nastavenia sú povinné pre použitie ESET PROTECT VA v rámci domény:

Windows workgroup – pracovná skupina alebo názov domény NETBIOS pre tento server, napr. DOMAIN.

Windows domain – doména pre tento server, napr. *domain.com*.

Windows domain controller – doménový radič pre tento server. Zadajte úplný názov domény (FQDN) pre doménový radič.

Windows domain administrator – účet použitý na pripojenie k doméne.

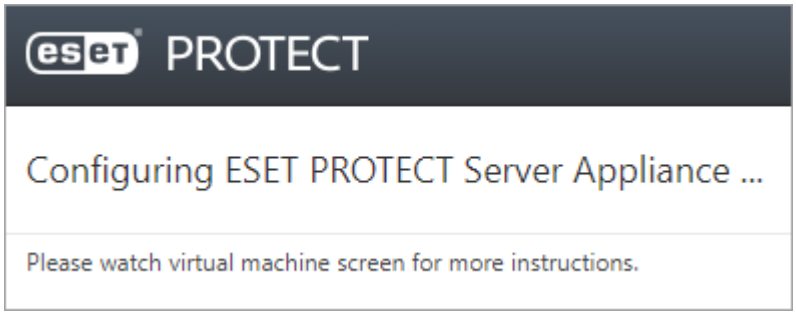
Windows domain administrator password – heslo správcu použité na pripojenie k doméne.

DNS1 – server DNS pre tento virtuálny počítač. Zadajte IP adresu doménového radiča.

Skontrolujte parametre konfigurácie. Uistite sa, že nastavenia sú správne, pretože dodatočné zmeny nie sú možné.

Označte možnosť **Súhlasím s podmienkami licenčnej dohody s koncovým používateľom a beriem na vedomie zásady ochrany osobných údajov**. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA), Podmienky používania a Zásady ochrany osobných údajov pre produkty ESET.

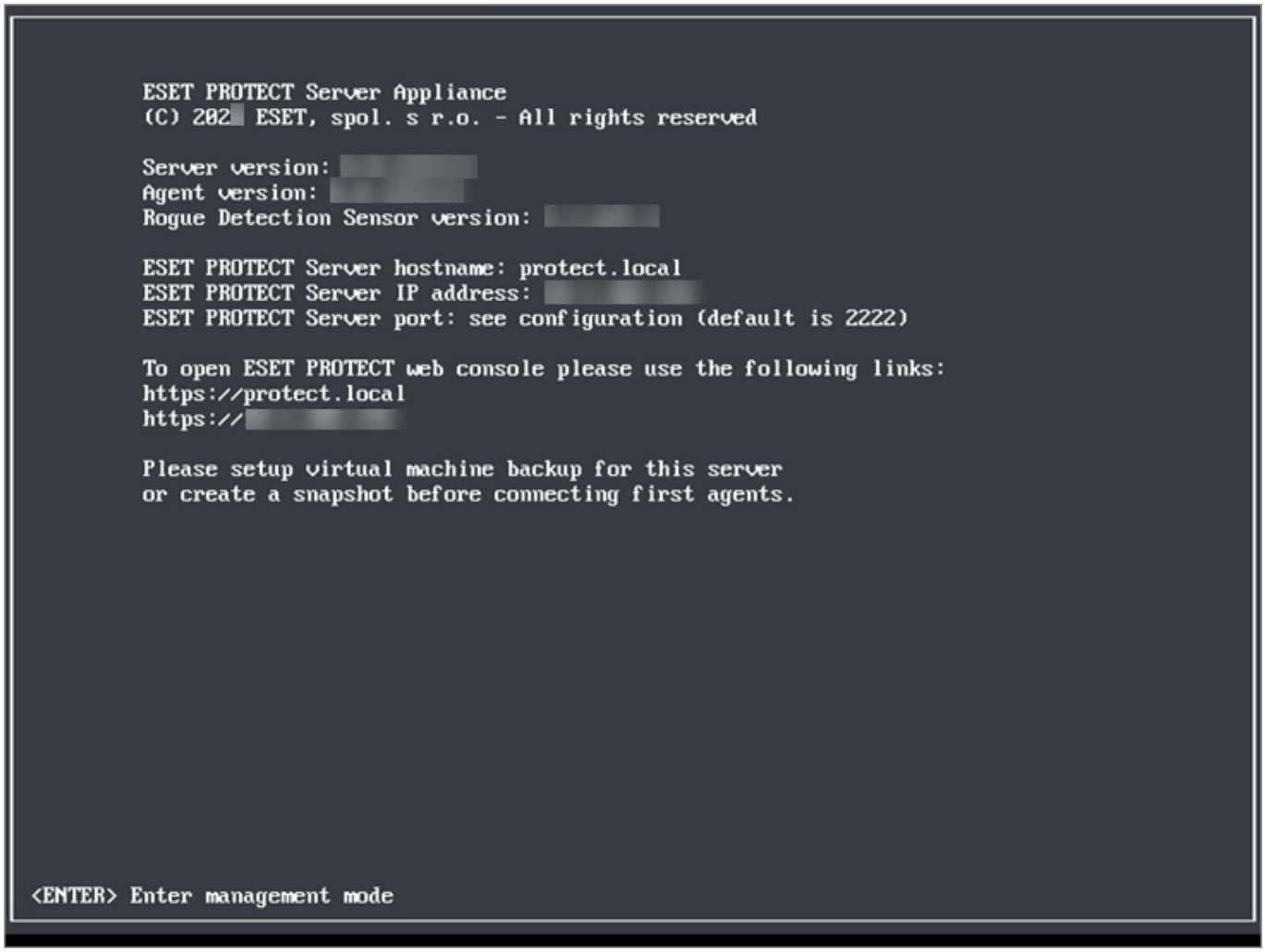
Po kliknutí na **Submit** sa zobrazí nasledujúca informácia:



Neobnovujte túto stránku vo vašom webovom prehliadači. Zatvorte kartu a prejdite do okna konzoly ESET PROTECT VA.

Okno konzoly virtuálneho zariadenia ESET PROTECT zobrazí informácie o stave. Zobrazia sa tiež verzie súčastí ESET

PROTECT, názov hostiteľa pre ESET PROTECT Server, IP adresa a číslo portu. Adresa ESET PROTECT Web Console bude zobrazená vo formáte *https:///[hostname] and https:///[IP address]*.



Odporúčame, aby ste si vytvorili snapshot (snímku) alebo zálohu virtuálneho počítača pred nasadením a pripojením prvých ESET Management Agentov.

Zadajte adresu pre ESET PROTECT Web Console (zobrazenú vyššie) do webového prehliadača a prihláste sa do rozhrania ESET PROTECT Web Console. Váš názov hostiteľa a IP adresa budú pravdepodobne odlišné, pretože názov hostiteľa a IP adresa uvedené na obrázku slúžia len ako príklad. Po prihlásení môžete začať používať ESET PROTECT.

Po prvom prihlásení do ESET PROTECT Web Console vám odporúčame spustiť klientsku úlohu Aktualizácia operačného systému na počítači, na ktorom je nainštalovaný ESET PROTECT.

Zariadenie ESET PROTECT MDM

Toto je sekcia nastavení pre zariadenie ESET PROTECT MDM. Konfigurácia pozostáva z 2 častí: **Application** a **Networking properties**. Vyplňte všetky povinné polia (označené červenou farbou). Ak je to potrebné, môžete tiež zadať voliteľné parametre.

Toto ESET PROTECT virtuálne zariadenie spúšťa ESET PROTECT MDM na vyhradenom virtuálnom počítači. Je vhodný pre podnikové siete, ale môže byť použitý aj pre malé firemné siete.

Predtým, ako začnete konfigurovať zariadenie ESET PROTECT MDM, si vytvorte certifikát pre Mobile Device Connector cez Web Console patriacu k ESET PROTECT Serveru, ku ktorému sa bude zariadenie ESET PROTECT MDM pripájať.

ESET PROTECT MDM je možné nakonfigurovať dvoma spôsobmi:

1.**Konfigurácia pomocou prihlasovacích údajov pre Web Console**

Povinné konfiguračné polia pre zariadenie ESET PROTECT MDM:

- **Password** – toto heslo je dôležité, pretože bude použité vo virtuálnom počítači a databáze ESET PROTECT.
- **ESET PROTECT Server Hostname** – zadajte názov hostiteľa alebo IP adresu ESET PROTECT Servera, aby sa mohlo ESET PROTECT MDM pripojiť na ESET PROTECT Server.
- **ESET PROTECT Server Port** – predvolený port ESET PROTECT Servera je 2222; ak používate iný port, zadajte svoje číslo portu.
- **Web Console Port** – predvolený port pre Web Console je 2223; ak používate iný port, zadajte svoje číslo portu.
- **Web Console password** – toto heslo je dôležité, pretože je potrebné pre prihlásenie sa do ESET PROTECT Web Console.
- Môžete prípadne zadať aj **Webconsole Hostname**. Tento názov hostiteľa je používaný nástrojom Web Console na pripojenie k serveru. Ak ponecháte príslušné pole prázdne, hodnota bude automaticky prevzatá z **ESET PROTECT Server Hostname**.
- **MDM názov hostiteľa** – zadajte FQDN alebo IP adresu (ako je uvedené v certifikáte MDC, ktorý ste vytvorili v ESET PROTECT Web Console).

2.**Konfigurácia pomocou využitia certifikátov**

Povinné konfiguračné polia pre zariadenie ESET PROTECT MDM:

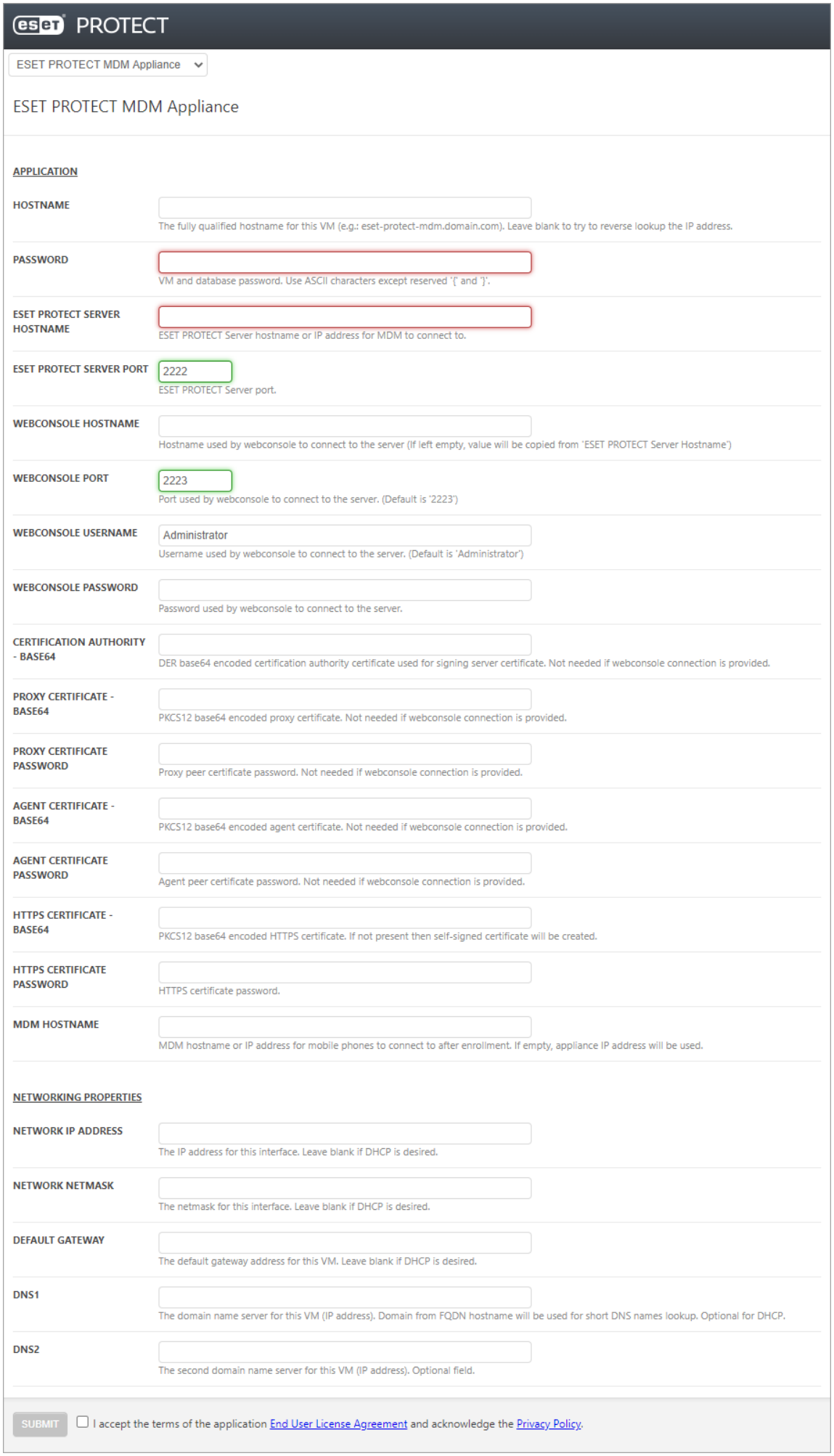
- **Password** – toto heslo je dôležité, pretože bude použité vo virtuálnom počítači a databáze ESET PROTECT.
- **ESET PROTECT Server Hostname** – zadajte názov hostiteľa alebo IP adresu ESET PROTECT Servera, aby sa mohlo ESET PROTECT MDM pripojiť na ESET PROTECT Server.
- **ESET PROTECT Server Port** – predvolený port ESET PROTECT Servera je 2222; ak používate iný port, zadajte svoje číslo portu.
- **Web Console Port** – predvolený port pre Web Console je 2223; ak používate iný port, zadajte svoje číslo portu.
- **Certification Authority Base64** – sem vložte certifikát certifikačnej autority vo formáte Base64. Viac informácií o získaní certifikátu nájdete v kapitole Certifikáty ESET PROTECT.
- **Proxy Certificate Base64** – sem vložte proxy certifikát vo formáte Base64. Viac informácií o získaní certifikátu nájdete v kapitole Certifikáty ESET PROTECT. Na overovanie komunikácie medzi ESET PROTECT Serverom a súčasťou MDM sa používa proxy certifikát.

- **Agent Certificate Base64** – sem vložte certifikát agenta vo formáte Base64. Viac informácií o získaní certifikátu nájdete v kapitole Certifikáty ESET PROTECT.

- **MDM názov hostiteľa** – zadajte FQDN alebo IP adresu (ako je uvedené v certifikáte MDC, ktorý ste vytvorili v ESET PROTECT Web Console).

Vlastnosti siete

Presuňte sa kurzorom myši smerom nadol, kde môžete nastaviť nasledujúce vlastnosti siete: **Network IP Address**, **Network Netmask**, **Default Gateway**, **DNS1**, **DNS2**. Všetky polia sú voliteľné.


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.

Skontrolujte parametre konfigurácie. Uistite sa, že nastavenia sú správne, pretože dodatočné zmeny nie sú možné.

Označte možnosť **Súhlasím s podmienkami licenčnej dohody s koncovým používateľom a beriem na vedomie zásady ochrany osobných údajov**. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA), Podmienky používania a Zásady ochrany osobných údajov pre produkty ESET.

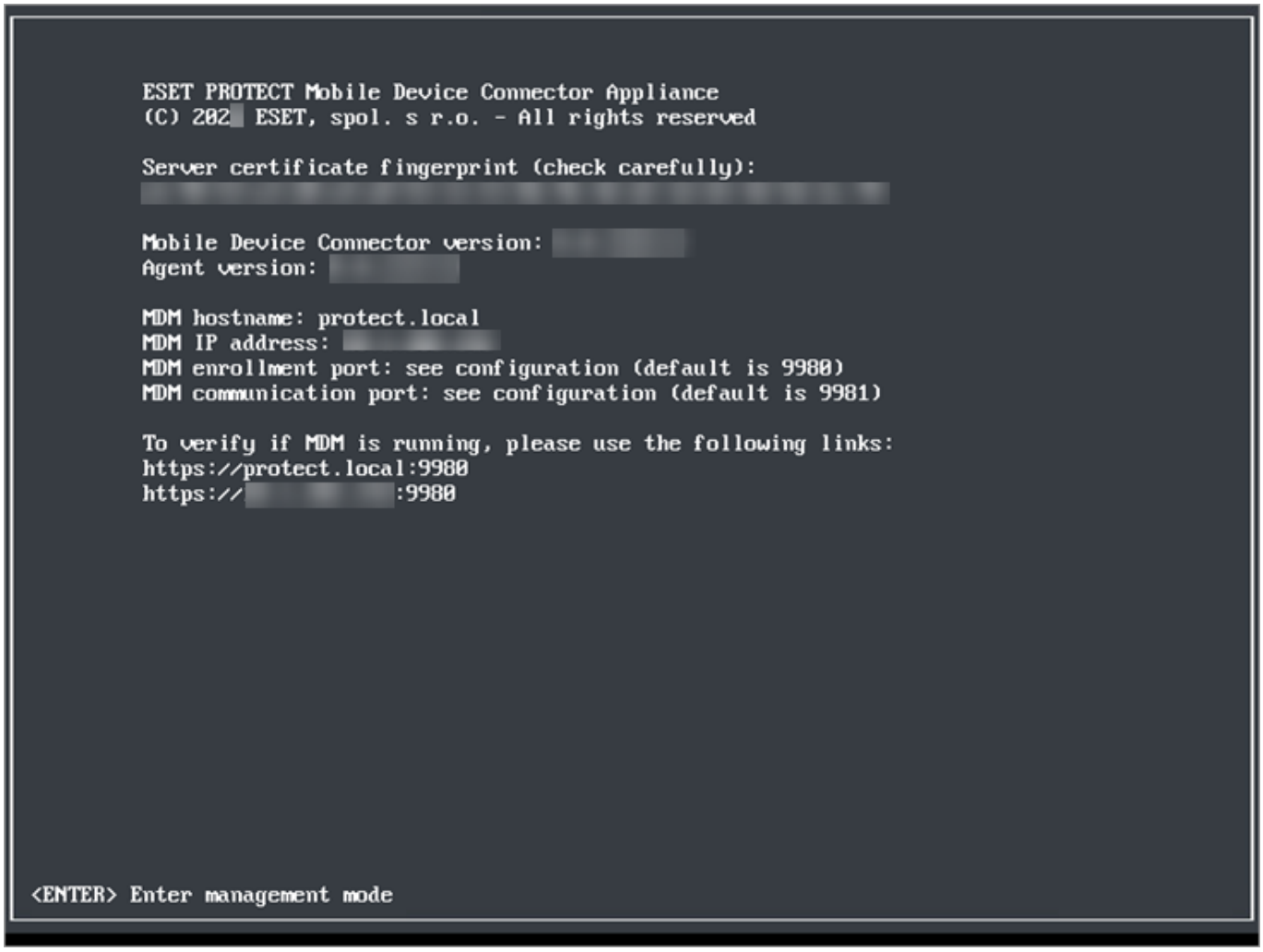
Kliknite na **Submit**, ak ste už skončili so zmenami.

Po kliknutí na **Submit** sa zobrazí nasledujúce oznámenie:

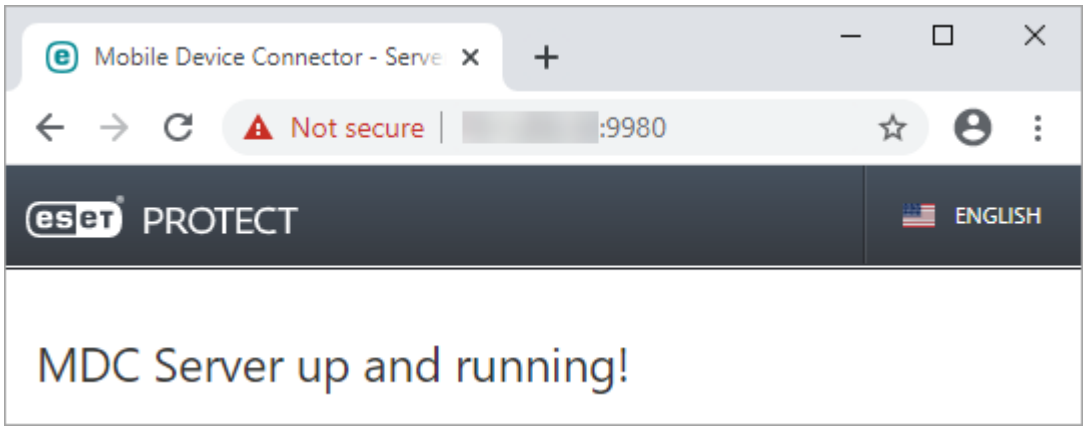


Neobnovujte túto stránku vo vašom webovom prehliadači. Zatvorte kartu a prejdite do okna konzoly ESET PROTECT VA.

Okno konzoly vášho virtuálneho zariadenia ESET PROTECT zobrazí informácie o stave zariadenia. Zobrazia sa verzie súčastí ESET PROTECT, ako aj názov hostiteľa pre ESET PROTECT MDM, IP adresa a číslo portu. Zobrazí sa aj adresa MDM registrácie vo formáte *https://[hostname]:9980 a https://[IP address]:9980*.



Zadajte adresu MDM registrácie (tak, ako je uvedené vyššie) do webového prehliadača pre potvrdenie správneho fungovania nástroja Mobile Device Connector. Váš názov hostiteľa a IP adresa budú pravdepodobne odlišné, pretože názov hostiteľa a IP adresa uvedené na obrázku slúžia len ako príklad. Ak bolo nasadenie úspešné, zobrazí sa nasledujúca správa:



Konzola na správu virtuálneho zariadenia ESET PROTECT

Po úspešnom nasadení ESET PROTECT VA otvorte terminálové okno virtuálneho počítača. Uvidíte obrazovku so základnými informáciami svojho ESET PROTECT VA, ako aj jeho stav. Toto je hlavná obrazovka ESET PROTECT VA.

Odtiaľto sa môžete prihlásiť do **konzoly na správu virtuálneho zariadenia ESET PROTECT** (tiež známa ako **režim správy**) stlačením tlačidla **Enter**. Pre vstup do režimu správy zadajte svoje heslo špecifikované počas konfigurácie ESET PROTECT VA a stlačte **Enter** dvakrát. Ak ste ešte ESET PROTECT VA nekonfigurovali, môžete na vstup do režimu správy použiť prednastavené heslo `eraadmin`.

Keď ste už prihlásený do konzoly na správu virtuálneho zariadenia ESET PROTECT, v rámci konfigurácie/správy sú dostupné tieto položky:

- Set Static IP address (Nastavenie statickej IP adresy)
- Enable/Disable remote access (Povolenie/zakázanie vzdialeného prístupu)
- Backup database (Zálohovanie databázy)
- Restore database (Obnovenie databázy)
- Reset after snapshot revert (Vykonanie obnovy po vrátení zmien k snímke)
- Pull database from other server (Načítanie obsahu databázy z iného servera)
- Change VM password (Zmena hesla pre virtuálny počítač)
- Change database password (Zmena hesla pre databázu)
- Rejoin domain (Opätovné pripojenie k doméne)
- Configure domain (Nastavenie domény)
- Factory reset (Obnovenie pôvodných nastavení)

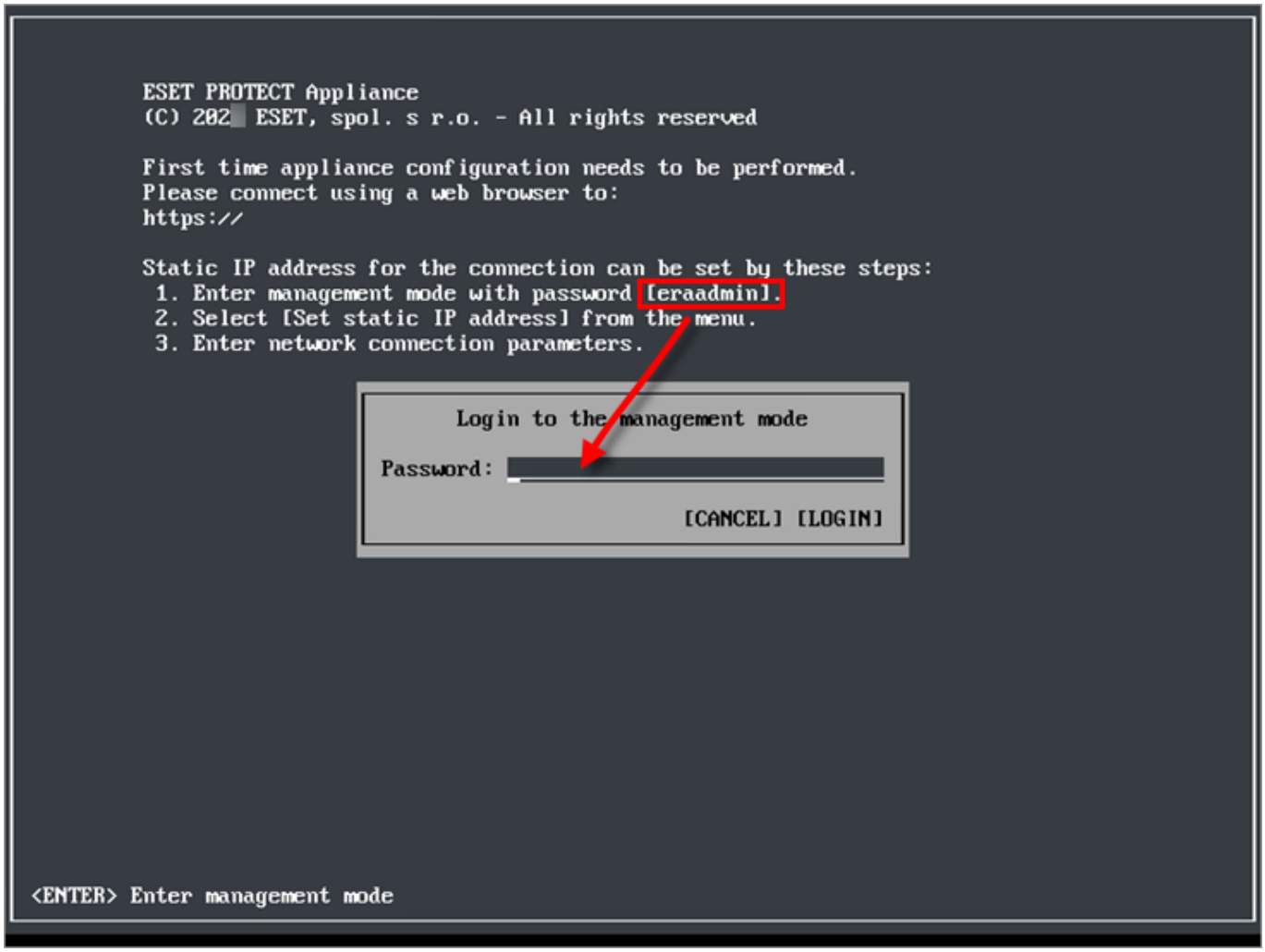
Dostupnosť položiek uvedených vyššie sa môže líšiť v závislosti od fázy implementácie ESET PROTECT VA a konfigurovaného typu zariadenia.

- **Restart system** – v prípade, že chcete reštartovať svoje ESET PROTECT VA.
- **Shut down system** – v prípade, že chcete vypnúť svoje ESET PROTECT VA.
- **Lock screen** – mali by ste uzamknúť obrazovku, aby ste zabránili ostatným ľudom používať vaše ESET PROTECT VA a pristupovať k jeho súborom. Uzamknúť obrazovku môžete aj pomocou tlačidla **Esc**, čo je ešte rýchlejšie. Režim správy sa ukončí a vy uvidíte hlavnú obrazovku ESET PROTECT VA.
- **Exit to terminal** – túto funkciu použite v prípade, že sa chcete dostať do terminálu operačného systému. Táto funkcia zatvorí konzolu na správu virtuálneho zariadenia ESET PROTECT a vstúpi do terminálu. Pre návrat z terminálu späť do hlavnej obrazovky ESET PROTECT VA napíšte `exit` a stlačte kláves **Enter** (môžete tiež použiť príkaz „`logout`“).

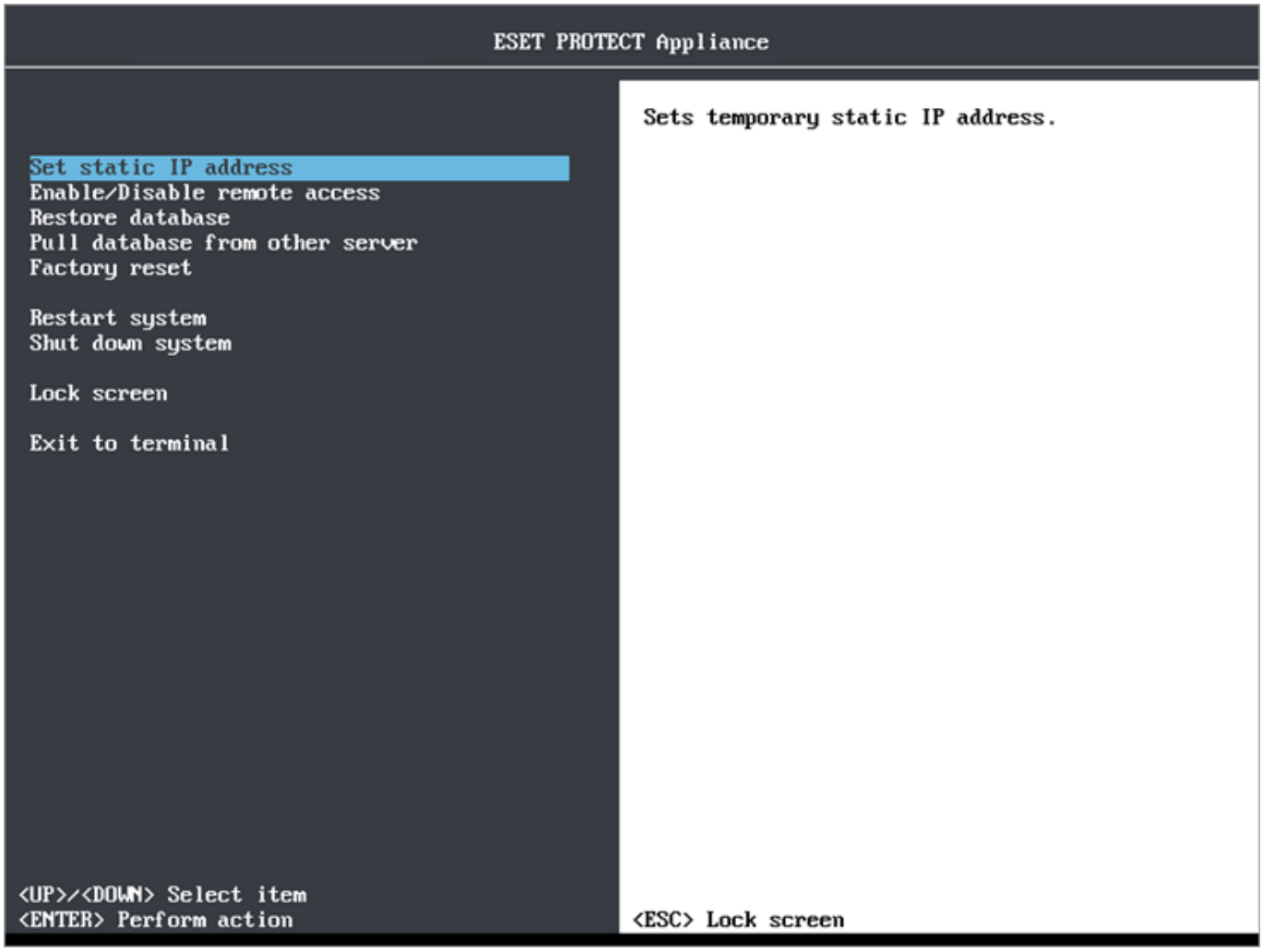
Nastavenie statickej IP adresy

V prípade, že vaše virtuálne zariadenie ESET PROTECT nemá pridelenú IP adresu pomocou DHCP servera, vyžaduje sa manuálne nastavenie. Postupujte podľa inštrukcií uvedených nižšie pre manuálne nastavenie statickej IP adresy:

1. Na hlavnej obrazovke konzoly virtuálneho počítača stlačte **Enter** pre vstúpenie do **režimu správy**. Napíšte `eraadmin` a dvakrát stlačte kláves **Enter** pre **prihlásenie**.



2. Zvoľte možnosť **Set static IP address** pomocou šípok a stlačte **Enter**.



3. Spustí sa interaktívny sprievodca sieťovým nastavením a bude od vás vyžadovať tieto nastavenia:
   - Static IP address (statická IP adresa)
   - Network mask (maska siete)
   - Gateway address (adresa brány)
   - DNS server address (adresa DNS servera)

> Sieťové parametre musia byť zadané v IPv4 formáte decimálnych čísel oddelených bodkou, napr. `192.168.1.10` (IP adresa) alebo `255.255.255.0` (maska siete).
> Dostupnosť (ping) počítača s ESET PROTECT VA **nie je** možné testovať ani v prípade, že sieť je nastavená správne.

4. Pre pokračovanie stlačte **Enter** alebo stlačte **Ctrl+C**, ak chcete **ostať** v termináli.

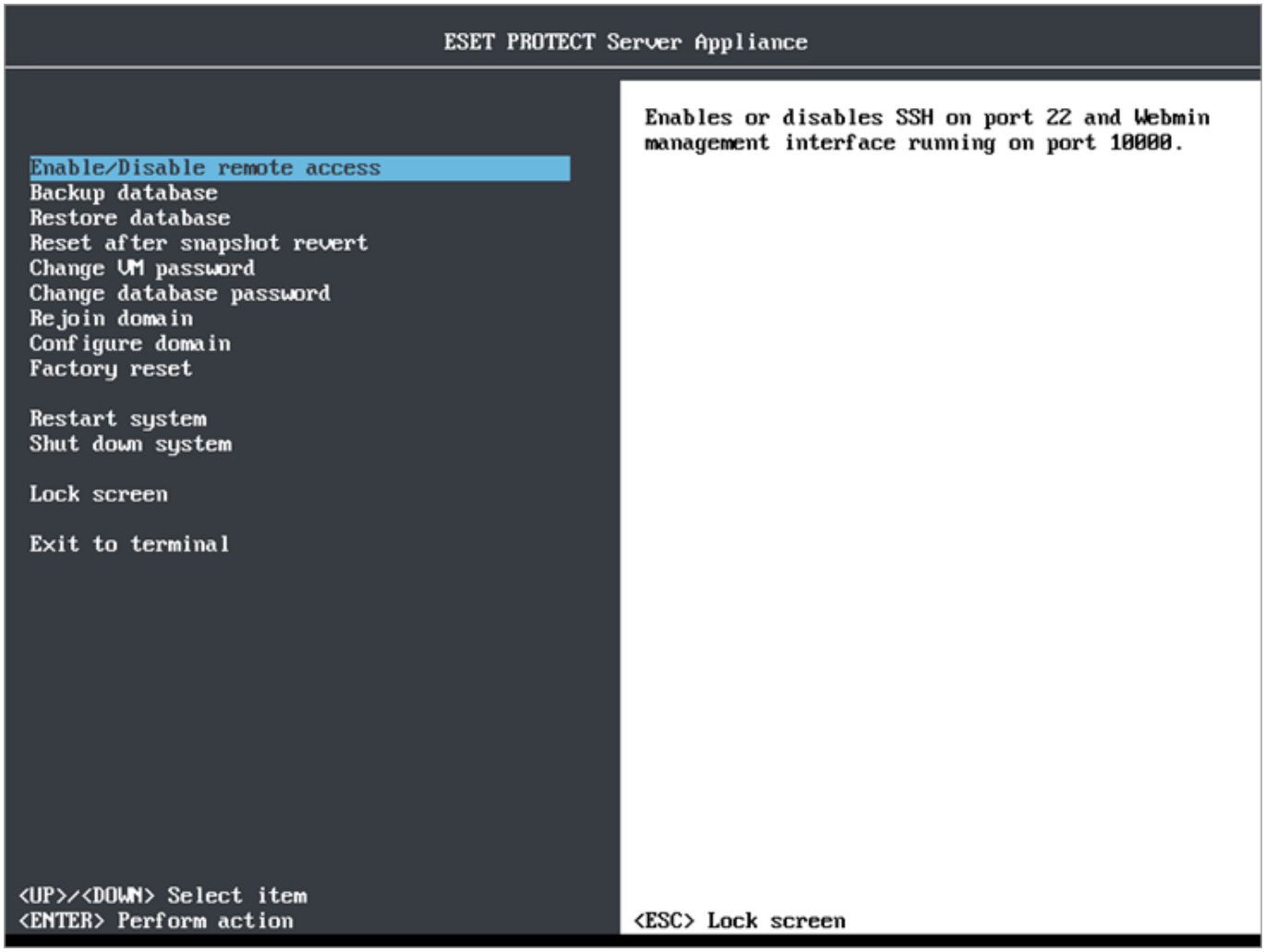
ESET PROTECT VA má štandardne jeden sieťový adaptér, ktorý je zvyčajne postačujúci, ale ak z určitých dôvodov pridáte viacero sieťových adaptérov, funkcia **Set static IP address** sa bude vzťahovať iba na `eth0` adaptér.

Enable/Disable remote access (Povolenie/zakázanie

vzdialeného prístupu)

Predtým, ako budete môcť používať vzdialený prístup (Rozhranie na správu Webmin a SSH), musíte ho najprv povoliť.

Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Enable/Disable remote access** a stlačte kláves **Enter**.

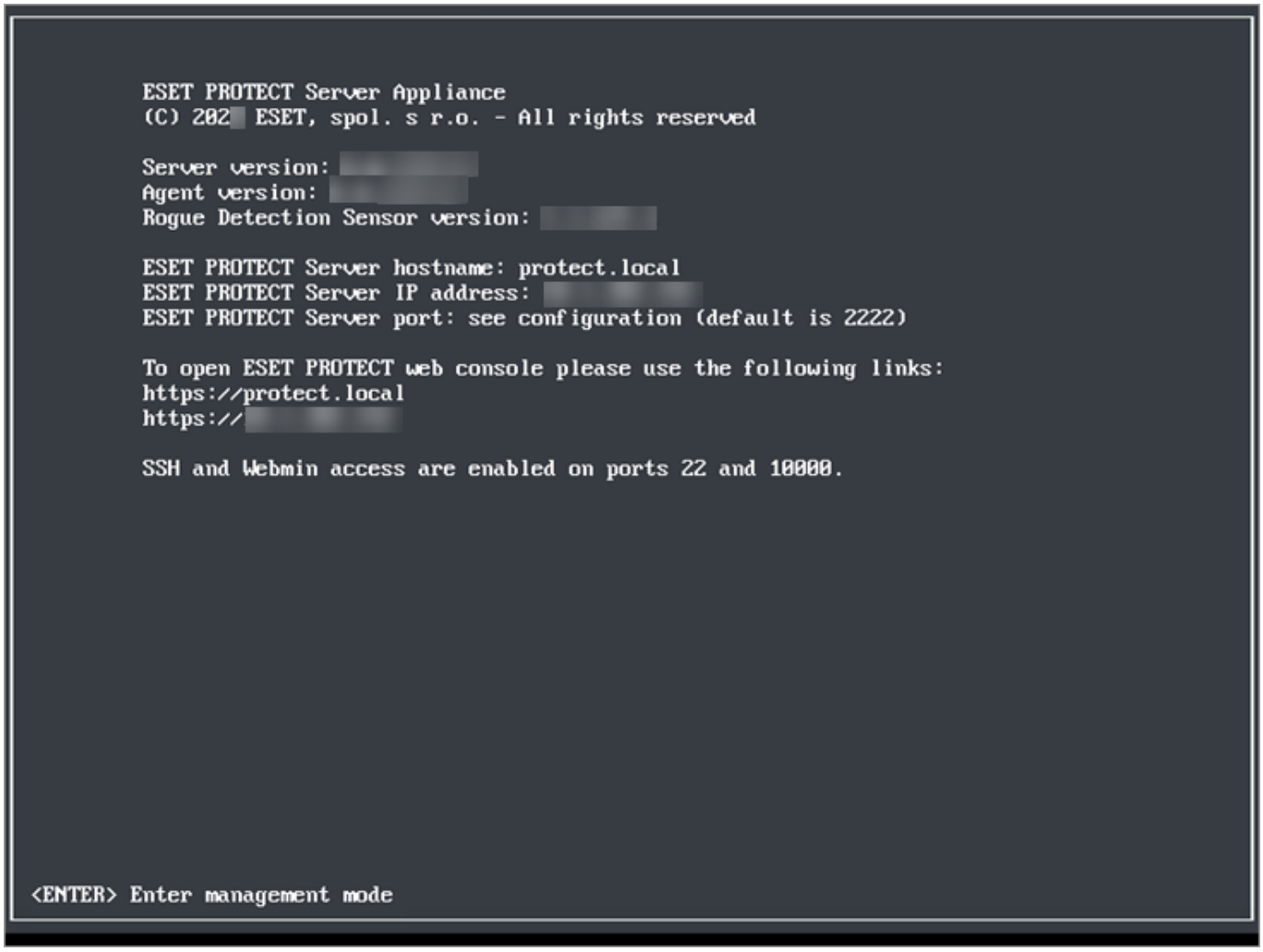


Teraz môžete použiť:

- Webmin – podrobnosti nájdete v kapitole Rozhranie na správu Webmin. Nástroj Webmin používa HTTPS a je spustený na porte 10000. Na prístup do rozhrania Webmin použite IP adresu uvedenú spolu s číslom portu 10000 vo formáte *https://<host name or IP address>:10000*, napr. *https://10.10.11.16:10000* alebo *https://protect.local:10000*.

- Vzdialený prístup cez SSH na porte 22 (toto je potrebné na umožnenie migrácie databázy).

Na hlavnej obrazovke konzoly na správu ESET PROTECT VA sa zobrazia nasledujúce informácie:



Riešenie problémov týkajúcich sa SSH

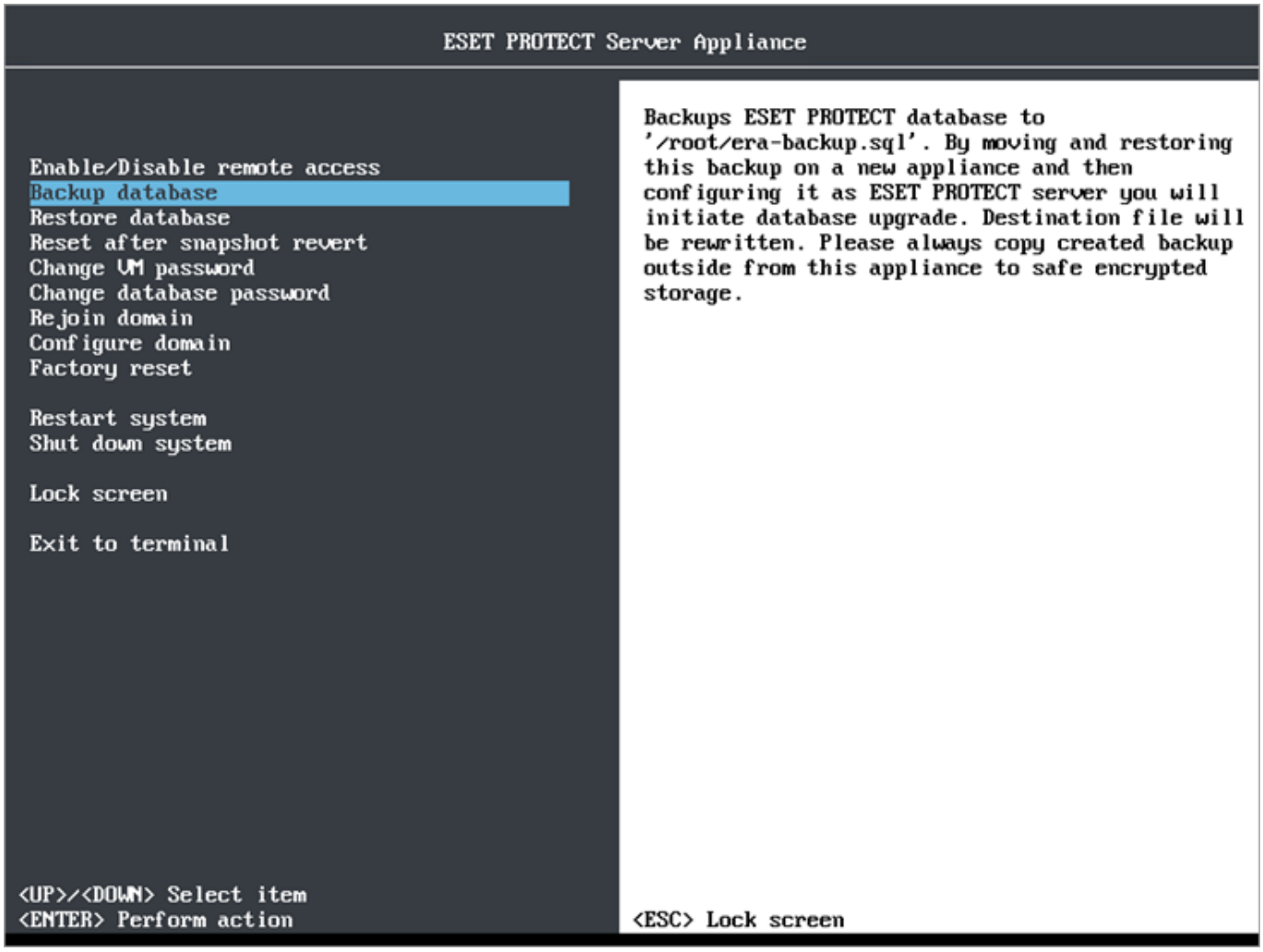
Zálohovanie databázy

Zálohovanie je nevyhnutnou súčasťou efektívneho plánu obnovy v prípade straty údajov. Pomocou funkcie **Backup database** môžete vašu **ESET PROTECT databázu** zálohovať a uložiť do záložného súboru MySQL *era-backup.sql*, ktorý sa nachádza v *root* priečinku.

Alternatívou zálohovania databázy je vytvorenie snímok (snapshots) virtuálneho počítača. Týmto spôsobom bude zachované celé ESET PROTECT VA, všetky jeho nastavenia, ako aj ESET PROTECT databáza. Ak však obnovíte snímku (snapshot) vášho virtuálneho počítača, budete musieť spustiť funkciu Reset after snapshot revert.

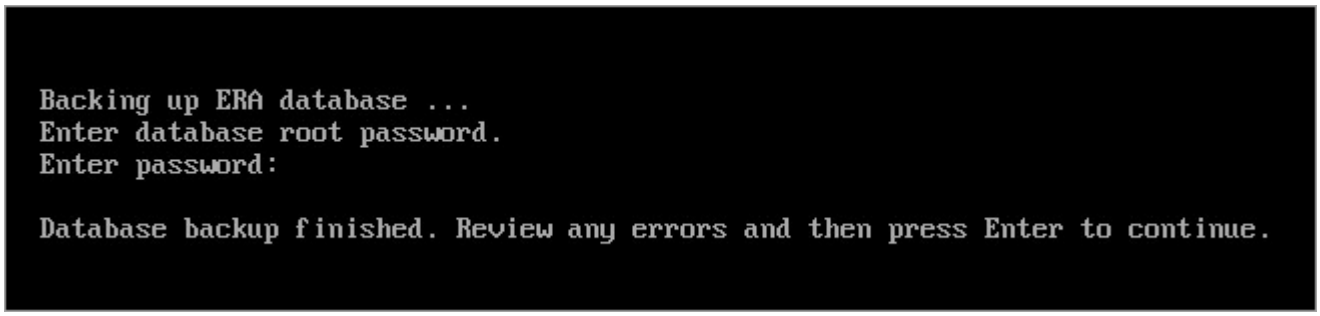
Odporúčame, aby ste vykonávali zálohu vašej ESET PROTECT databázy často a ukladali záložný súbor na externé úložisko. Toto je dôležité, pretože v prípade, že by došlo k problémom resp. strate údajov, budete mať kópiu celej ESET PROTECT databázy uloženú inde (nie lokálne na vašom ESET PROTECT VA). Príkladom môže byť poškodenie ESET PROTECT VA alebo jeho zmazanie. Ak ste nedávno vykonali zálohu ESET PROTECT databázy, budete môcť obnoviť ESET PROTECT VA do rovnakého stavu, v akom bolo tesne pred nehodou. Podrobný postup nájdete v časti Obnova ESET PROTECT VA po nehode.

1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Zvoľte možnosť **Backup database** pomocou šípok a stlačte kláves **Enter**.



2. Predtým, ako bude môcť byť vykonaná záloha databázy, vás systém vyzve, aby ste zadali root heslo databázy.

Ak si nepamätáte root heslo databázy, môžete ho zmeniť a znova spustiť zálohu databázy.



Tento proces môže trvať od niekoľkých sekúnd až po niekoľko hodín v závislosti od veľkosti vašej databázy. Počas zálohovania databázy sa služba ESET PROTECT Server zastaví, aby sa zachovala konzistentnosť dát.

Vždy skontrolujte, či sa na obrazovke nenachádzajú chybové hlásenia. Ak nájdete chybové hlásenia, zálohovanie databázy nebolo úspešné. Skúste **zálohu databázy** vykonať znova.

Zálohu databáz nájdete tu: */root/era-backup.sql*

Stiahnite si záložný súbor na bezpečné miesto pomocou nástroja Webmin File manager.

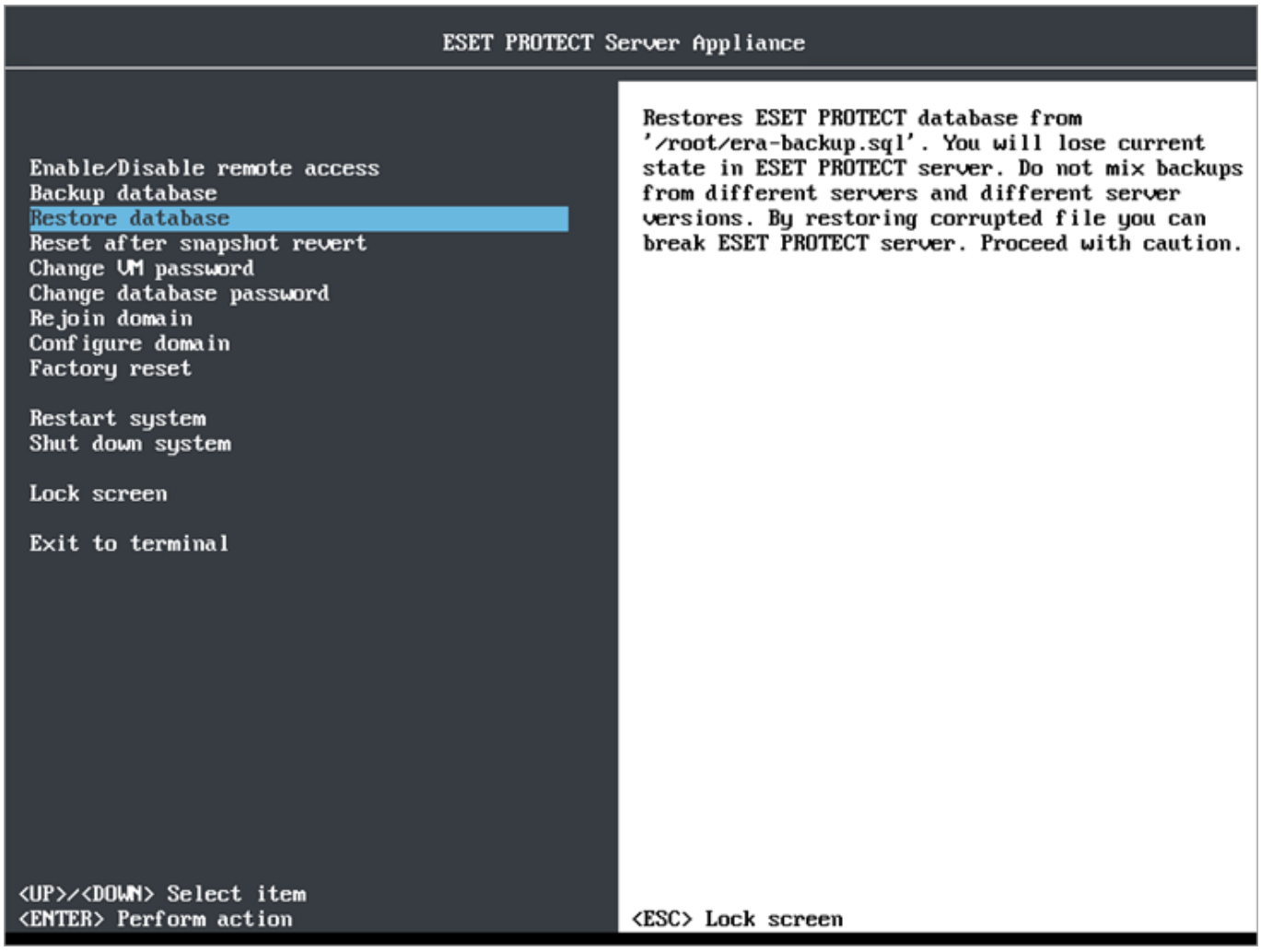
Restore database (Obnovenie databázy)

Táto funkcia nahradí vašu aktuálnu databázu zálohovanou databázou.

Odporúčame mať pripravený snapshot (snímku) virtuálneho počítača alebo zálohu aktuálnej databázy. Bude to slúžiť ako záložný plán pre prípad, že sa pri obnove vyskytnú problémy.

Pre vykonanie **obnovy databázy** postupujte podľa nasledujúcich inštrukcií:

1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Zvoľte možnosť **Restore database** pomocou **šípok** a stlačte kláves Enter.



Nahrajte váš záložný súbor *era-backup.sql*, ktorý chcete obnoviť, do *root* adresára pomocou nástroja Webmin File manager. Cieľový súbor *era-backup.sql* bude prepísaný. Vynechajte tento krok, ak chcete obnoviť súbor *era-backup.sql*, ktorý sa už nachádza v *root* adresári.

Nezamieňajte zálohy z rôznych serverov a rôznych serverových verzií. Použite iba súbor *era-backup.sql*, ktorý bol zálohovaný na rovnakom ESET PROTECT VA. Jedinou výnimkou, kedy môžete obnoviť databázu na iné ESET PROTECT VA, je prípad, keď je PRODUCT VA čerstvo nasadené a ešte na ňom nebola vykonaná konfigurácia.

2. Na začiatku procesu obnovenia databázy vás systém môže vyzvať, aby ste zadali **root heslo databázy**. Ak však obnovujete databázu na čerstvo nasadenom ESET PROTECT VA, ktoré ešte nebolo nakonfigurované,

nebude sa od vás vyžadovať heslo.



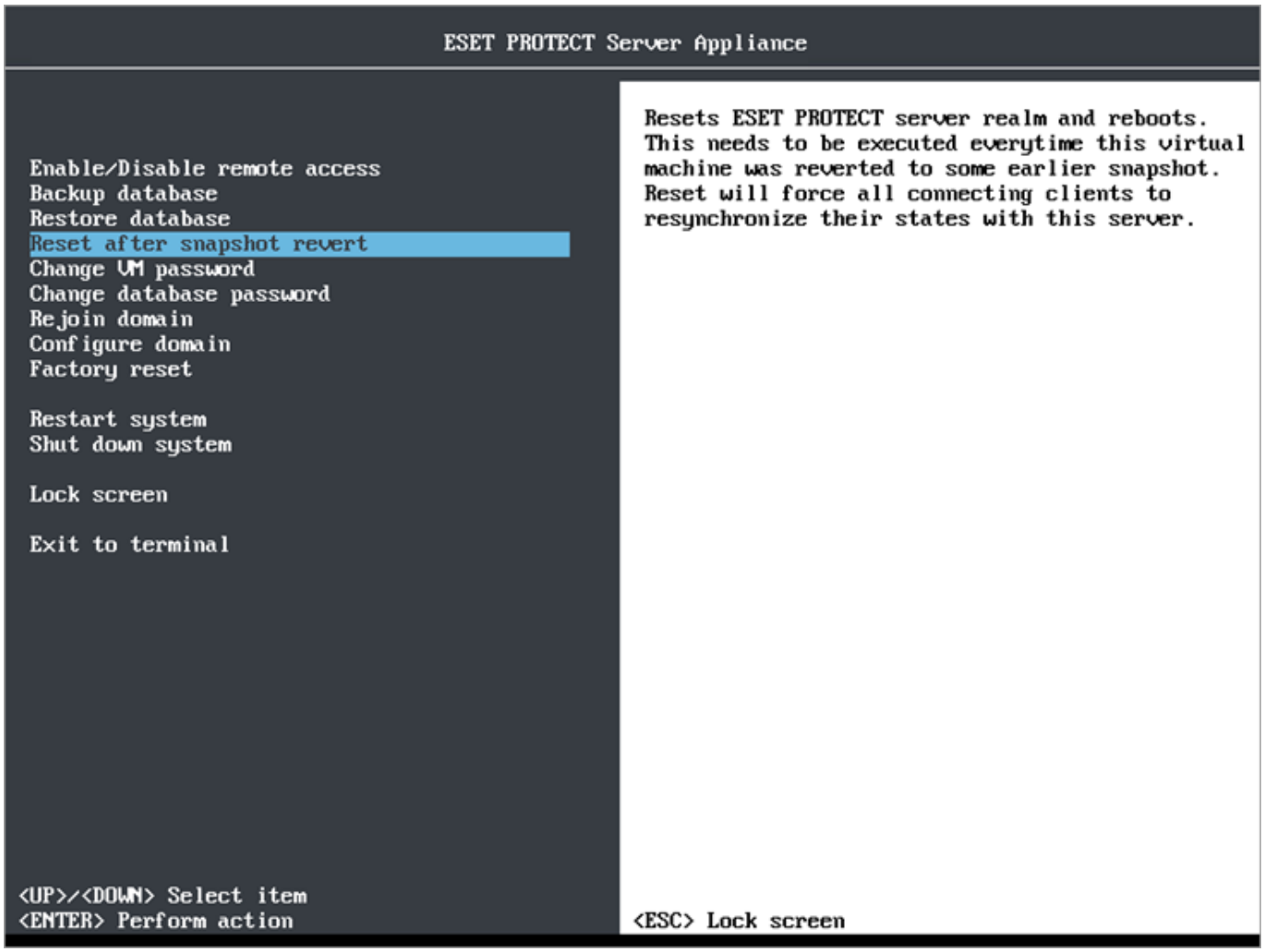
Tento proces môže trvať od niekoľkých sekúnd až po niekoľko hodín v závislosti od veľkosti vašej databázy.

Vždy skontrolujte, či sa na obrazovke nenachádzajú chybové hlásenia. Ak nájdete chybové hlásenia, obnovenie databázy nebolo úspešné. Skúste **obnovu databázy** vykonať znova.

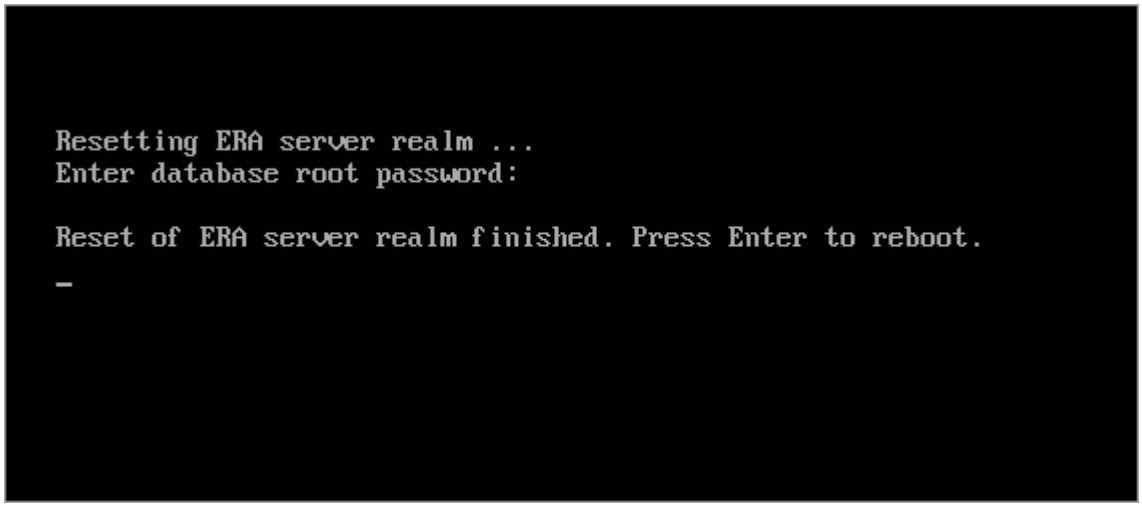
Reset after snapshot revert (Vykonanie obnovy po vrátení zmien k snímke)

Vždy, keď vrátite stav svojho virtuálneho počítača k staršej snímke (snapshot), budete musieť použiť funkciu **Reset after snapshot revert**, aby sa všetky klienty, ktoré sa pripájajú na server, zosynchronizovali s daným serverom.

1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Reset after snapshot revert** a stlačte kláves **Enter**.



2. Pred vykonaním obnovy pre **ESET PROTECT Server realm** vás systém vyzve, aby ste zadali svoje root heslo databázy.



Migrácia databázy z iného servera

Táto funkcia vám umožňuje preniesť ESET PROTECT databázu z existujúceho ESET PROTECT VA bežiaceho vo vašej infraštruktúre. Je podporovaná len na ESET PROTECT Serveri, na ostatných súčastiach (MDM) podporovaná nie je. Je to užitočné v prípadoch, keď chcete aktualizovať svoje ESMC VA alebo staršie ESET PROTECT VA na najnovšie ESET PROTECT VA, alebo chcete migrovať svoje ESET PROTECT VA.

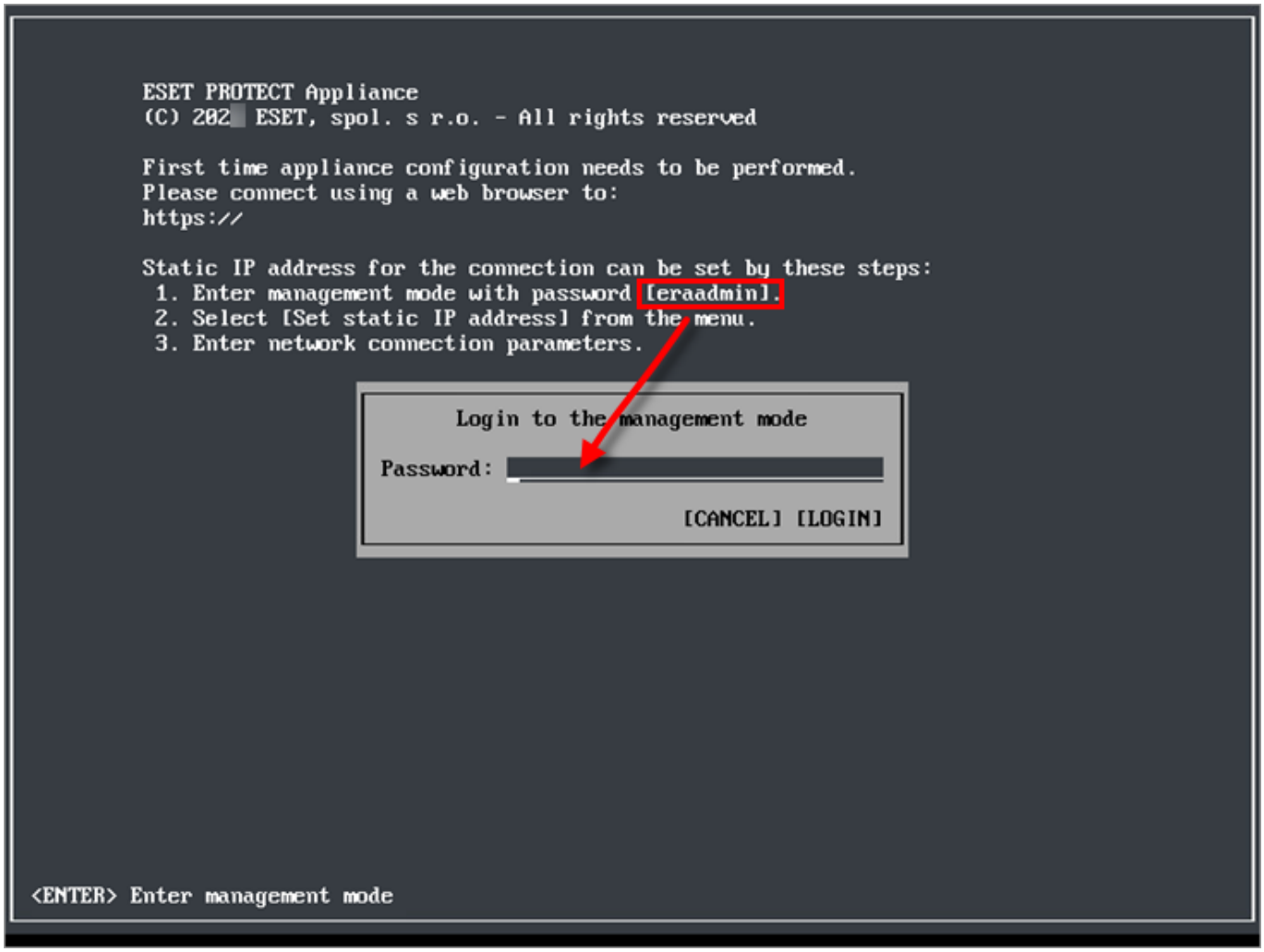
V prípade migrácie bude potrebné ponechať vaše staré ESET PROTECT VA dostupné, aby mohla byť politika zmeny názvu hostiteľa/IP adresy uplatnená na všetky klientske počítače. V opačnom prípade sa klienty nebudú pripájať na vaše nové ESET PROTECT VA, ale budú sa pokúšať pripojiť sa na staré PRODUCT VA. Uistite sa, že SSH je na vašom starom ESET PROTECT VA povolené.
Migrácia databázy môže byť vykonaná iba v prípade migrácie na novšiu alebo rovnakú verziu ESET PROTECT Servera. Počas migrácie je štruktúra databázy aktualizovaná, avšak tento proces zlyhá v prípade, že ide o migráciu obsahu databázy na starší server. Migrácia databázy je jedným z dvoch spôsobov, ako aktualizovať virtuálne zariadenie.

Pre vykonanie migrácie databázy postupujte podľa nasledujúcich krokov:

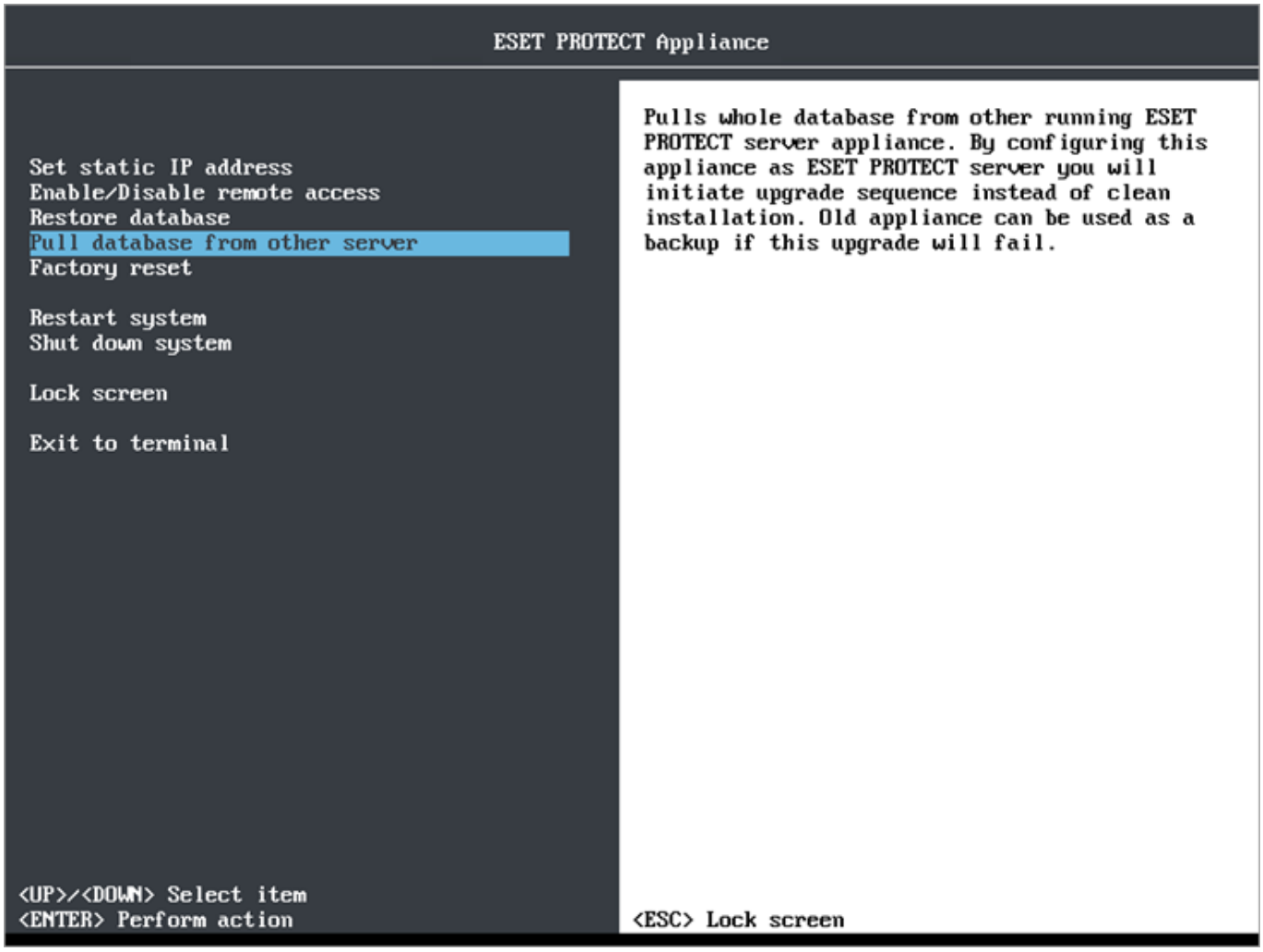
1. Nasaďte nové ESET PROTECT VA, ale zatiaľ ho nekonfigurujte.

2. Otvorte konzolu virtuálneho počítača a na hlavnej obrazovke stlačte **Enter**, čím vstúpite do **režimu správy** vášho nového ESET PROTECT VA.

3. Napíšte `eraadmin` a dvakrát stlačte kláves **Enter** pre **prihlásenie**.



4. Zvoľte možnosť **Pull database from other server** pomocou šípok a stlačte kláves **Enter**.



5. **Zadajte root heslo databázy** na vzdialenom ESET PROTECT VA, z ktorého chcete načítať ESET PROTECT databázu (vaše staré ESET PROTECT VA). Ak používate iba jedno heslo na vašom starom ESET PROTECT VA, zadajte ho tu.

6. **Zadajte údaje pripojenia na vzdialené ESET PROTECT VA (SSH)** – zadajte používateľské meno (`root`) a názov hostiteľa alebo IP adresu svojho starého ESET PROTECT VA v nasledujúcom formáte: `root@IPaddress` alebo `root@hostname`.

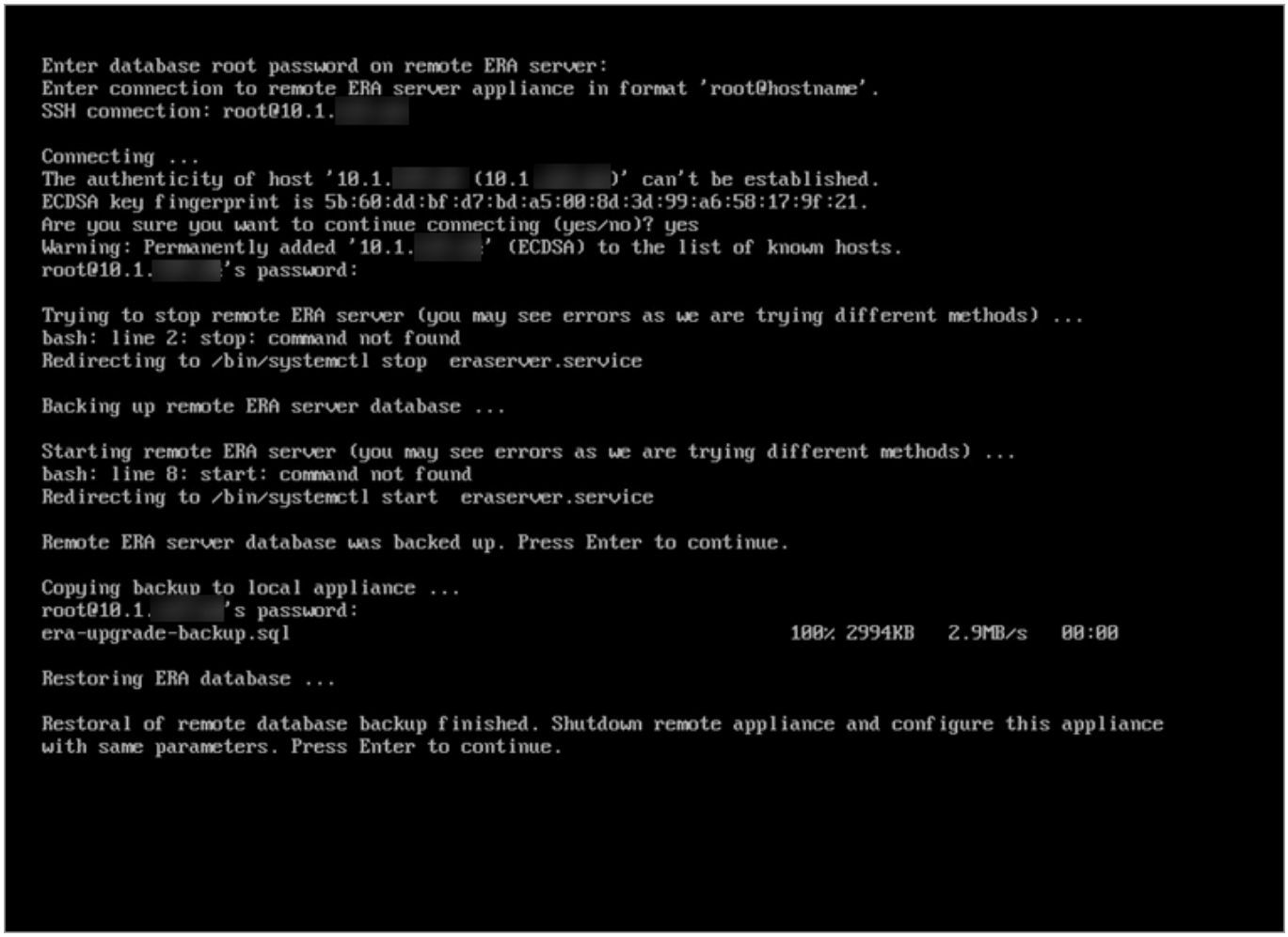
7. Ak sa vás systém opýta na **pravosť hostiteľa**, napíšte `yes`. V opačnom prípade tento krok ignorujte.

8. Zadajte **heslo virtuálneho počítača** svojho starého ESET PROTECT VA a stlačte **Enter**. Po dokončení zálohovania sa zobrazí nasledujúca správa: **Remote ERA Server database was backed up** (Databáza vzdialeného servera bola zálohovaná).

Čas potrebný na dokončenie operácií súvisiacich so zálohovaním a obnovou závisí od veľkosti databázy.

9. Znova zadajte **heslo virtuálneho počítača** svojho starého ESET PROTECT VA. V závislosti od času potrebného na skopírovanie databázy sa vám počas kopírovania môže niekoľkokrát zobraziť výzva na zadanie hesla.

10. Počkajte, kým neprebehne obnova databázy.



11. Ak vykonávate aktualizáciu: Po úspešnej migrácii databázy ESET PROTECT vypnite staré ESET PROTECT VA a vyraďte ho z prevádzky.

- Odporúčame vám ponechať si vaše staré ESET PROTECT VA, až kým nebudete mať istotu, že nová inštancia funguje správne.
- Dôrazne odporúčame, aby ste neodinštalovali starý ESET PROTECT VA Server pomocou skriptu určeného na odinštalovanie. Odinštalovaním zároveň dôjde k odstráneniu všetkých licencií z novej databázy ESET PROTECT VA Servera. Aby ste predišli tomuto problému, pred odinštalovaním odstráňte starú databázu ESET PROTECT VA Servera (`DROP DATABASE`).

12. Nakonfigurujte svoje nové zariadenie:

- **Aktualizácia** – nakonfigurujte svoje nové VA presne tak ako svoje predchádzajúce ESET PROTECT VA.
- **Migrácia** – zmeňte konfiguráciu tak, aby vyhovovala novej doméne (konfigurácia alebo opätovné pripojenie k doméne) alebo vlastnostiam siete, napr. ak ste premiestnili svoje ESET PROTECT VA do inej siete.

Uistite sa, že všetky dáta sú zachované, všetky klienty sa pripájajú na váš nový server a že sa vaše ESET PROTECT VA správa rovnako ako predchádzajúce.

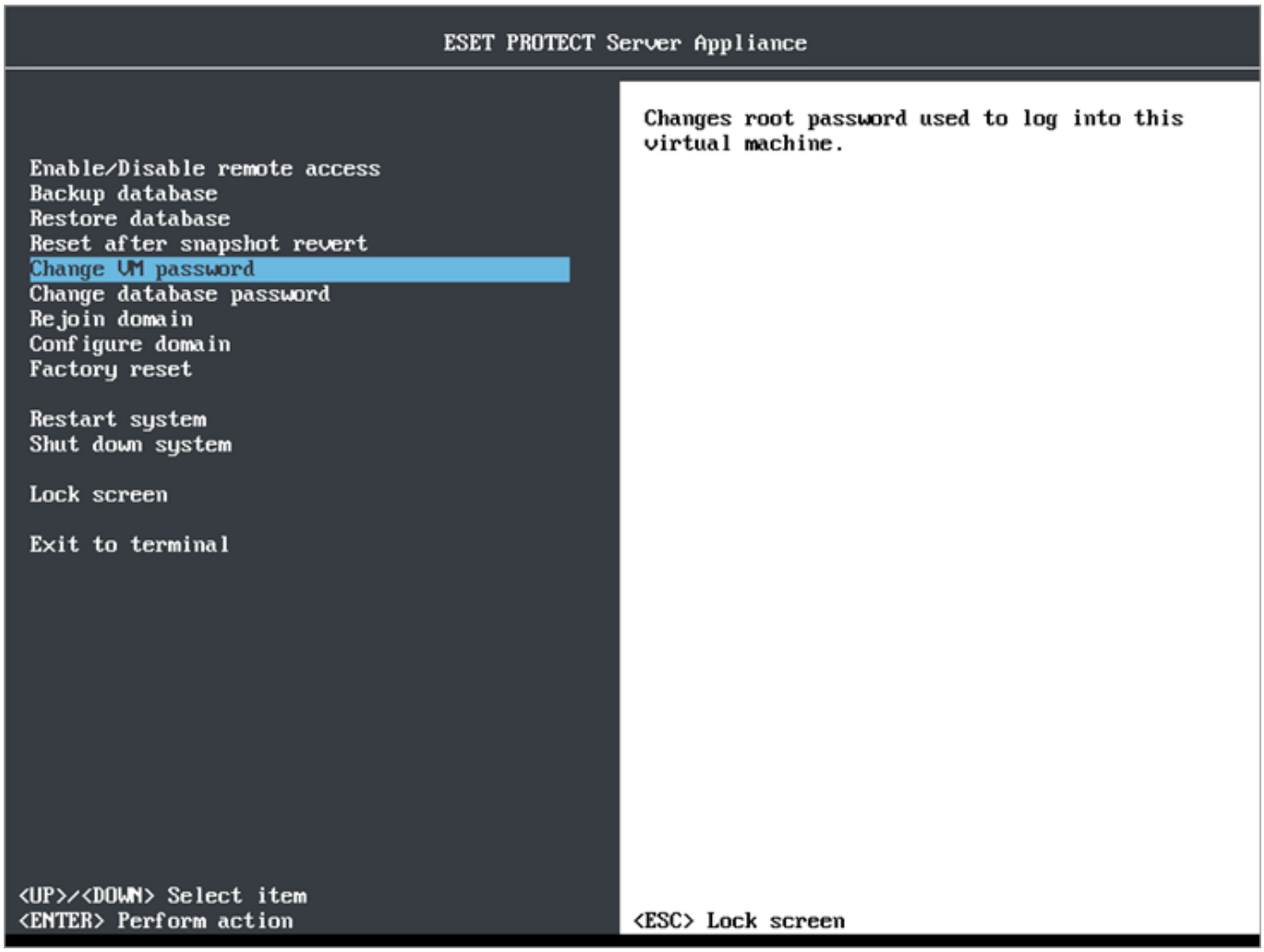
Change VM password (Zmena hesla pre virtuálny počítač)

Heslo vášho virtuálneho počítača sa používa na prihlasovanie do vášho nasadeného virtuálneho zariadenia ESET PROTECT. Ak chcete zmeniť vaše heslo pre virtuálny počítač alebo chcete, aby bol váš virtuálny počítač viac zabezpečený, odporúčame používať silné heslá a pravidelne ich meniť.

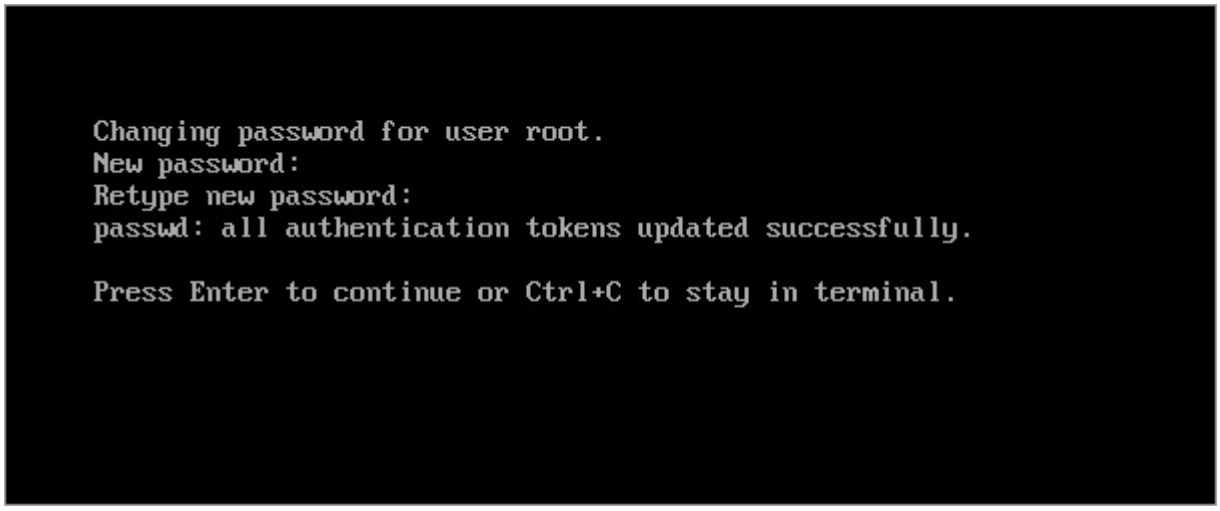
Týmto postupom sa zmení iba heslo pre virtuálny počítač. Heslo pre ESET PROTECT Web Console a root heslo databázy nebudú zmenené. Viac informácií nájdete v časti Heslá pre virtuálne zariadenie ESET PROTECT.

Ak ste zabudli svoje heslo, pozrite si kapitolu Obnova zabudnutého hesla pre ESET PROTECT VA.

1. Aktivujte **režim správy** zadaním hesla a stlačením klávesu **Enter** dvakrát. Zvoľte možnosť **Change VM password** pomocou šípok a stlačte kláves **Enter**.



2. Zadajte vaše **Nové heslo** do prázdneho poľa, stlačte **Enter** a potom heslo **zadajte znova** pre potvrdenie.

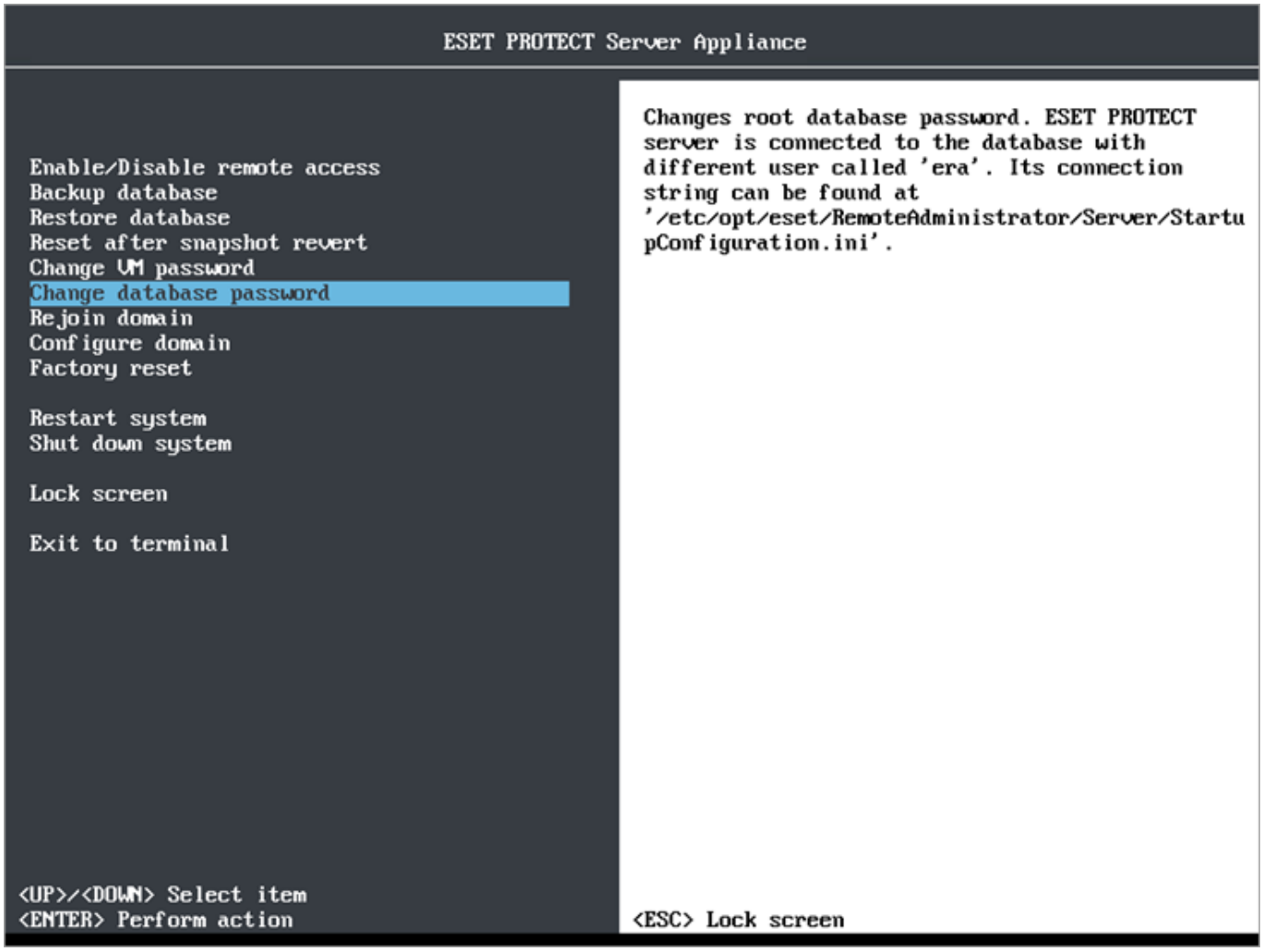


Po dokončení sa zobrazí správa „all authentication tokens updated successfully“ a vaše **Nové heslo** bude odteraz vyžadované pre prihlásenie.

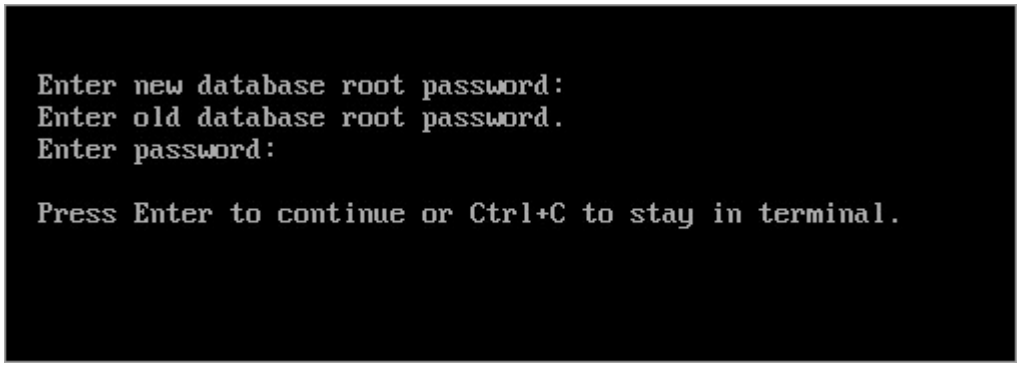
Change database password (Zmena hesla pre databázu)

`Root` heslo databázy umožňuje úplný prístup na databázový server MySQL. `Root` používateľ MySQL má úplnú kontrolu iba nad serverom MySQL.

1. Aktivujte **režim správy** zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Change database password** a stlačte kláves **Enter**.



2. Ak budete vyzvaný na **zadanie starého root hesla databázy**, zadajte heslo, ktoré ste nastavili počas konfigurácie ESET PROTECT VA. Toto heslo sa môže líšiť od vášho **hesla pre virtuálny počítač**, ak ste ho zmenili osobitne.



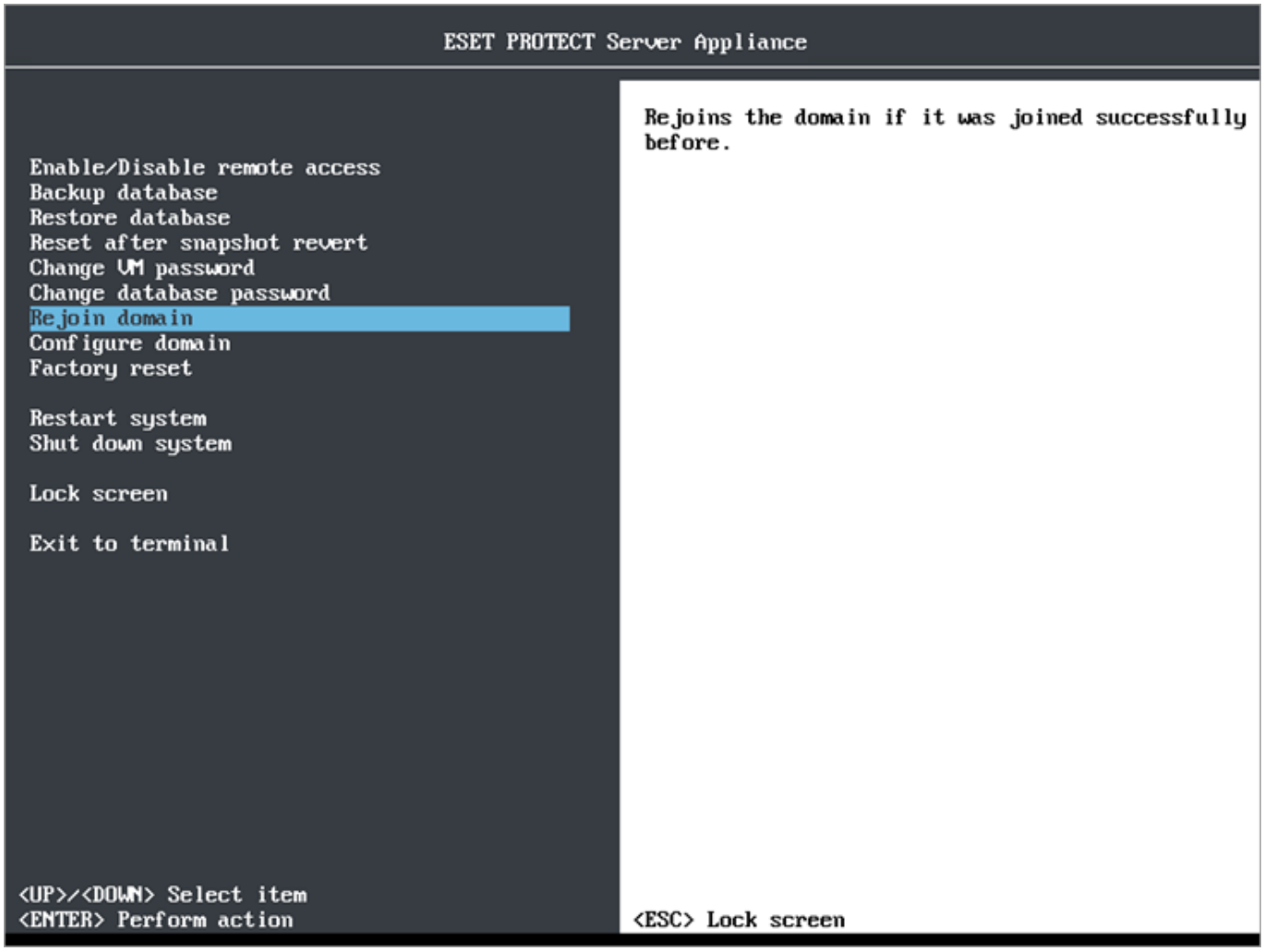
Root heslo databázy bolo zmenené.

Opätovné pripojenie k doméne

Túto funkciu použite, ak máte problémy s Active Directory alebo dôveryhodnosťou domény.

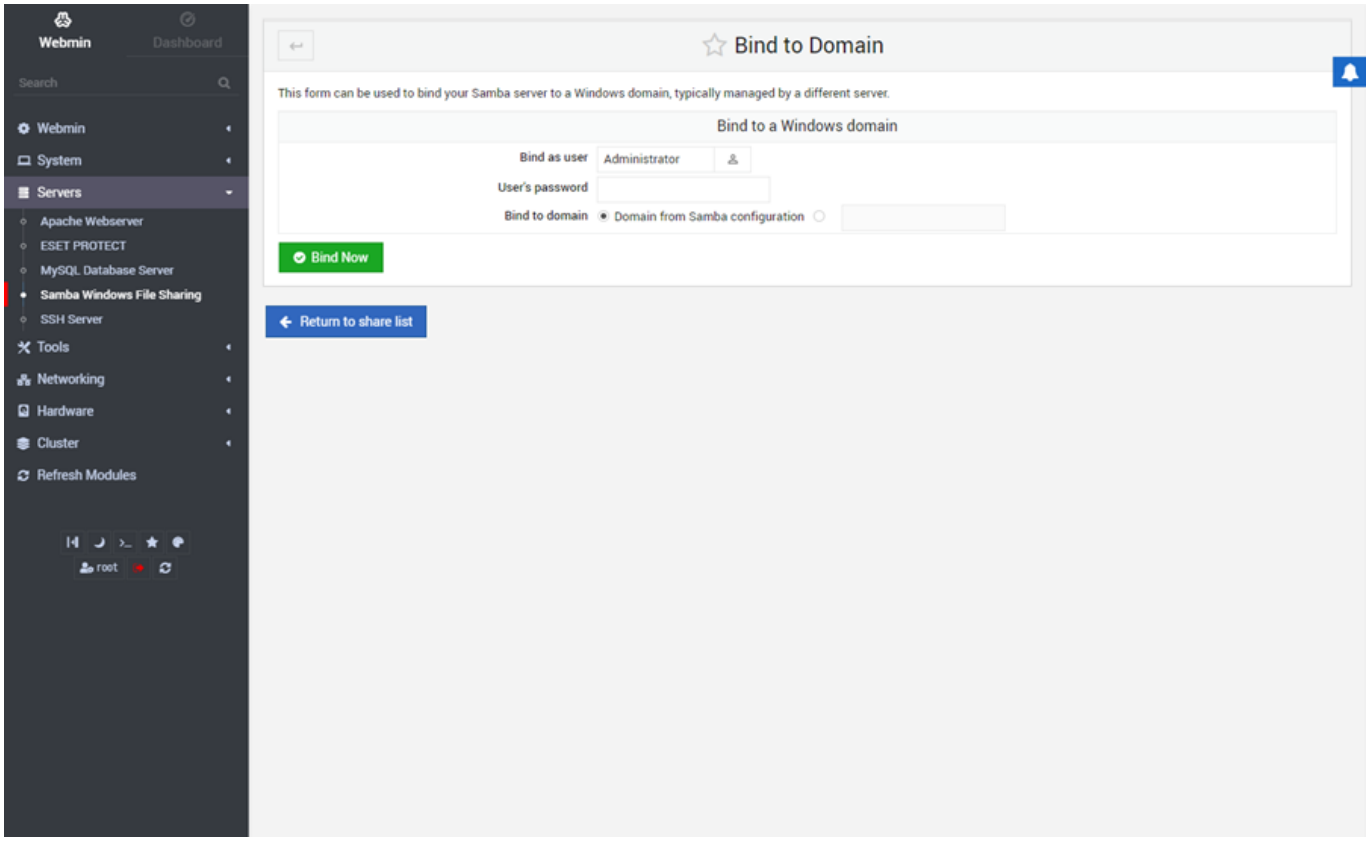
Je dôležité, aby bola doména nastavená správne, pretože v opačnom prípade funkcia Rejoin domain nemusí fungovať.

1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Rejoin domain** a stlačte kláves **Enter**.



2. Zadajte doménové používateľské meno, ktoré bude použité na pripojenie k doméne.

Ak nemáte skúsenosti so systémom Linux a terminálom, môžete použiť rozhranie Webmin a funkciu **Bind to Domain** nástroja Samba Windows File Sharing.



Configure domain (Nastavenie domény)

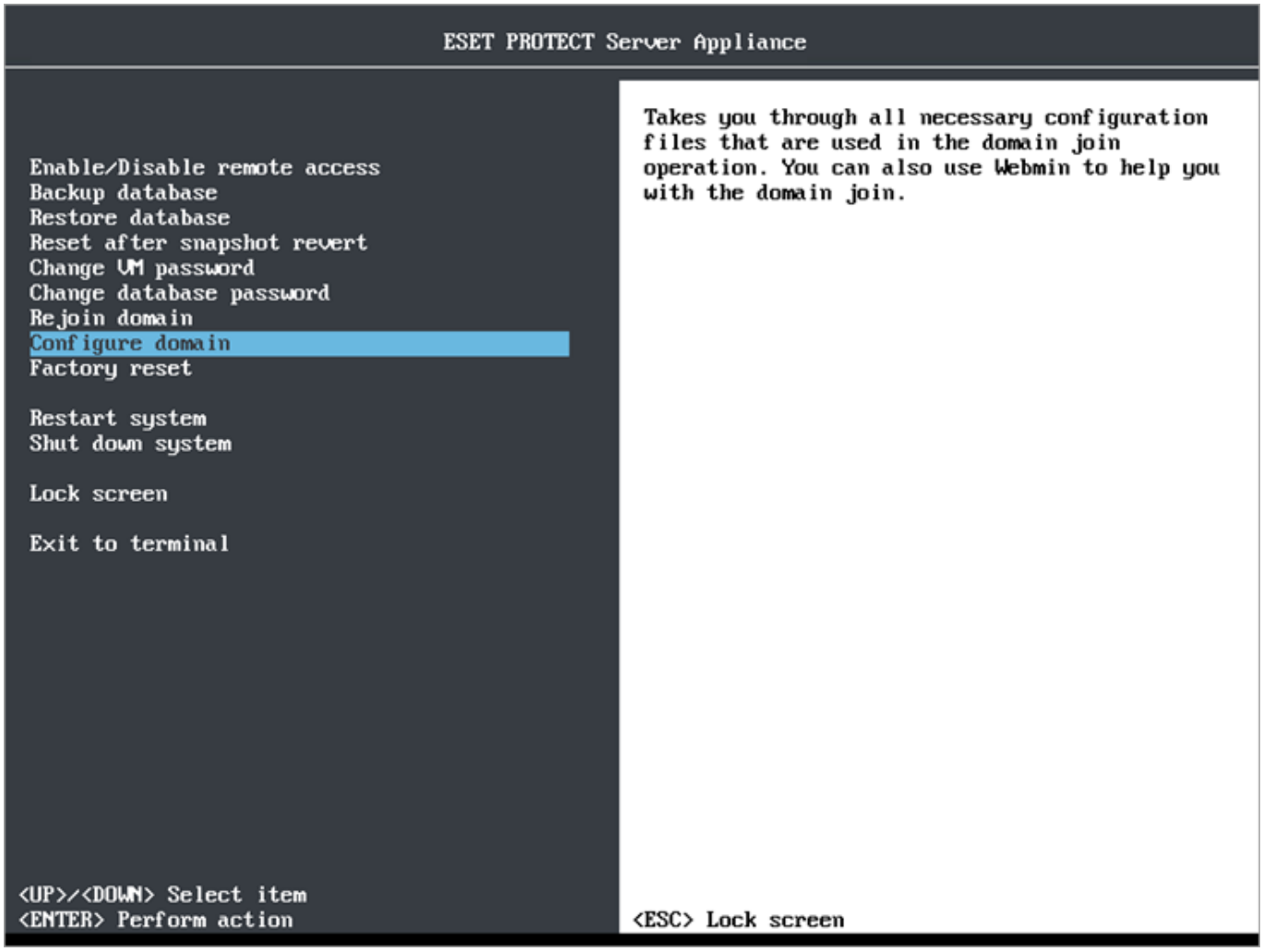
Ak zlyhá operácia pripojenia k doméne, je to zvyčajne spôsobené nesprávnym nastavením súborov ESET PROTECT VA. Funkcia **Configure Domain** vám umožňuje upravovať konfiguračné súbory tak, aby do nich bolo možné zahrnúť vlastné nastavenia vášho prostredia. Sú dostupné tieto typy konfiguračných súborov:

Názov súboru	Popis
/etc/hosts	Súbor Hosts by mal byť správne namapovaný k názvu vášho doménového radiča a jeho IP adrese.
/etc/krb5.conf	Konfiguračný súbor Kerberos by mal byť správne vygenerovaný. Uistite sa, že `kinit <user-from-domain>` funguje.
/etc/ntp.conf	Konfiguračný súbor NTP by mal obsahovať záznam o pravidelných aktualizáciách synchronizácie času s doménovým radičom.
/etc/samba/smb.conf	Konfiguračný súbor Samba by mal byť správne vygenerovaný.

Tieto súbory sú prednastavené a vyžadujú minimálne úpravy, napr. pri špecifikovaní názvu domény, názvu doménového radiča, názvu servera DNS atď.

1. Aktivujte **režim správy** zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Configure domain** a stlačte kláves **Enter**.

> Toto je pokročilý postup, ktorý odporúčame len pre skúsených správcov.



2. Stlačte **Enter** pre úpravu prvého konfiguračného súboru.

3. Stlačte klávesy **Ctrl + X** pre zatvorenie textového editora. Stlačte kláves **Y** pre uloženie alebo kláves **N** pre zahodenie zmien. Ak ste nevykonali žiadne zmeny, textový editor sa zatvorí. Ak chcete urobiť ďalšie zmeny, nepoužite **Ctrl + X**, ale stlačte **Ctrl + C** pre zrušenie a vráťte sa do textového editora. Príklady úpravy konfiguračných súborov nájdete v tomto článku databázy znalostí.

Pozrite si súbor */root/help-with-domain.txt* na svojom ESET PROTECT VA. Najrýchlejšou cestou je vyhľadať súbor *help-with-domain.txt* pomocou nástroja Webmin File manager. Na zobrazenie tohto súboru môžete tiež použiť príkaz `nano help-with-domain.txt`.
Ak nemáte skúsenosti so systémom Linux a terminálom, môžete použiť nástroj Webmin a nakonfigurovať doménové pripojenie (Kerberos, NTP alebo sieťové nastavenia prostredníctvom Samba Windows File Sharing).

4. Po dokončení konfigurácie domény vyberte možnosť **Rejoin domain** a zadajte meno správcu a heslo pre pripojenie k doméne.

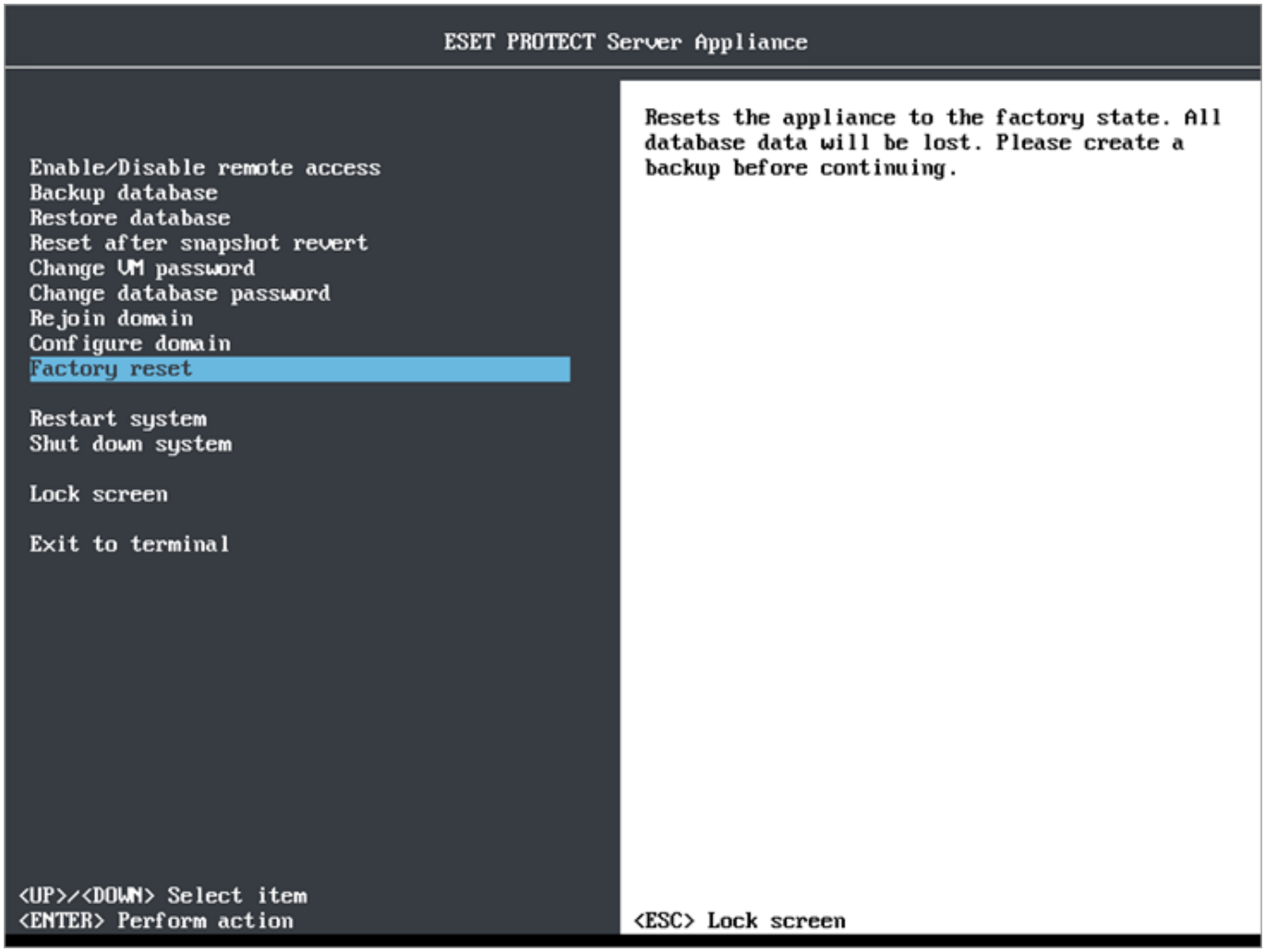
Factory reset (Obnovenie pôvodných nastavení)

Pre vrátenie virtuálneho zariadenia ESET PROTECT do pôvodného stavu môžete použiť funkciu **Factory reset**. Všetky nastavenia budú vynulované a celá ESET PROTECT databáza bude odstránená.

Dôrazne odporúčame, aby ste si pred **obnovením pôvodných nastavení** zálohovali vašu ESET PROTECT databázu. Po vynulovaní ostane vaša databáza prázdna.

Funkcia obnovenia pôvodných nastavení (**Factory reset**) obnoví len tie nastavenia, ktoré boli zmenené počas konfigurácie ESET PROTECT VA. Ostatné zmeny a nastavenia budú ponechané. V ojedinelých prípadoch sa môže stať, že funkcia obnovenia pôvodných nastavení nevráti vaše virtuálne zariadenie do pôvodného stavu úplne. Ak máte problémy s ESET PROTECT VA, odporúčame nasadiť nový počítač. Pre aktualizáciu/migráciu alebo vykonanie obnovy po nehode postupujte podľa nasledujúcich krokov:

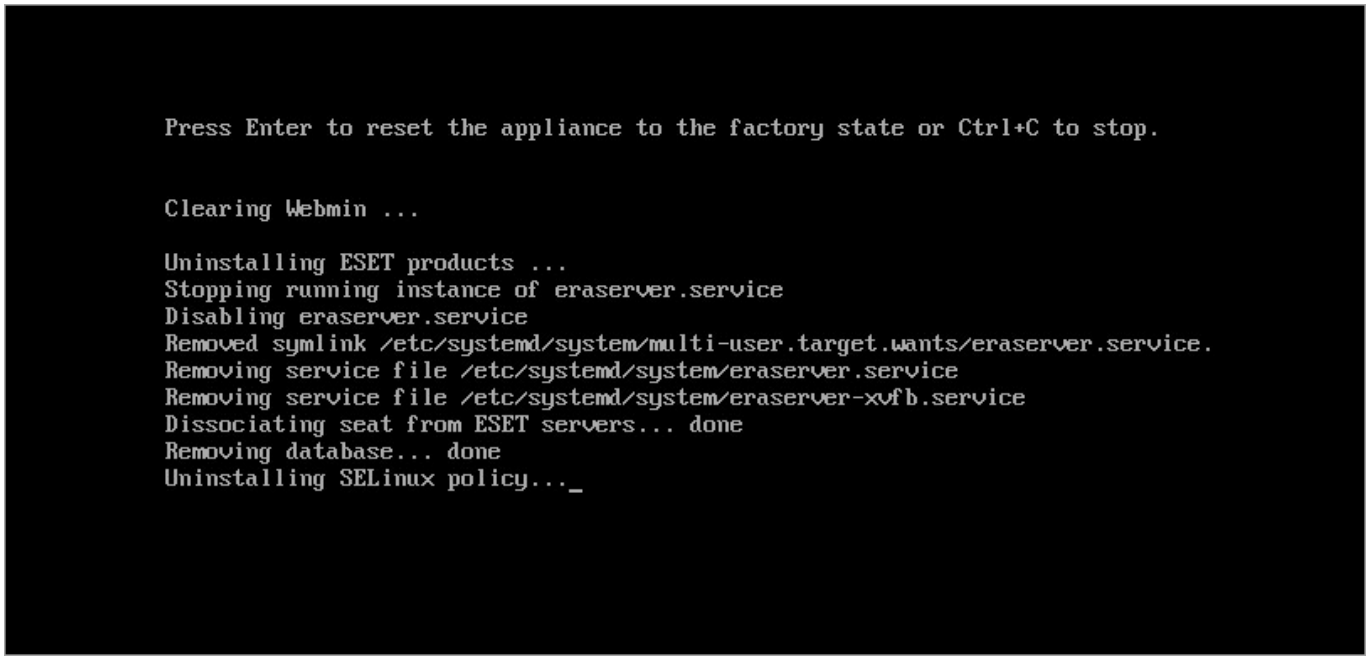
1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Factory reset** a stlačte kláves **Enter**.



2. Stlačením klávesu **Enter** obnovíte pôvodné nastavenia svojho virtuálneho zariadenia ESET PROTECT.

V tomto bode sa ešte stále môžete vrátiť späť do menu stlačením klávesovej skratky **Ctrl + C**.

Nepoužívajte skratku **Ctrl + C**, ak je už obnova spustená, pretože to môže poškodiť virtuálne zariadenie.



Ak uvidíte na obrazovke akékoľvek chybové hlásenia počas obnovy pôvodných nastavení, skúste spustiť obnovu znova. V prípade, že opätovné spustenie obnovy pôvodných nastavení nepomohlo, odporúčame vykonať nové nasadenie. Môžete postupovať podľa rovnakých krokov ako v prípade aktualizácie/migrácie alebo vykonať obnovu po nehode.

Funkcia **Factory reset** vykoná nasledujúce akcie:

- vynuluje nastavenia siete, všetky heslá a názov hostiteľa,
- vyčistí nástroj Webmin, konfiguračné súbory zariadenia, balíky a systémové protokoly,
- odstráni z ESET PROTECT databázy všetky dáta,
- vynuluje používateľské heslo pre ESET PROTECT databázu.

Po reštarte bude vaše ESET PROTECT VA obnovené do pôvodného stavu ako je to v prípade, keď je čerstvo nasadené, a vy budete môcť začať s nastaveniami od základov.

Vlastné úpravy alebo nastavenia, ktoré sa netýkajú ESET PROTECT, ostanú nezmenené.

Rozhranie na správu Webmin

Webmin je webové rozhranie tretej strany, ktoré zjednodušuje správu Linuxového systému. Webmin bol vyvinutý pre používateľov, ktorí majú určité skúsenosti so systémom Linux, ale nie sú oboznámení s komplexnosťou správy systému. Umožňuje vám vykonávať tieto úlohy vo webovom rozhraní, ktoré je jednoduché na použitie, a automaticky za vás aktualizuje potrebné konfiguračné súbory. Vďaka tomu je spravovanie systému oveľa jednoduchšie.

- Rozhranie Webmin je dostupné pomocou webového prehliadača a môžete sa doň prihlásiť z akéhokoľvek systému (klientsky počítač alebo mobilné zariadenie), ktorý je pripojený do vašej siete. Používať ho prostredníctvom siete je jednoduchšie ako lokálne používať iné grafické konfiguračné programy.
- Všetky novšie verzie nástroja Webmin môžu byť voľne šíriteľné a modifikované na komerčné aj nekomerčné

účely. Viac informácií nájdete na webových stránkach Webmin.

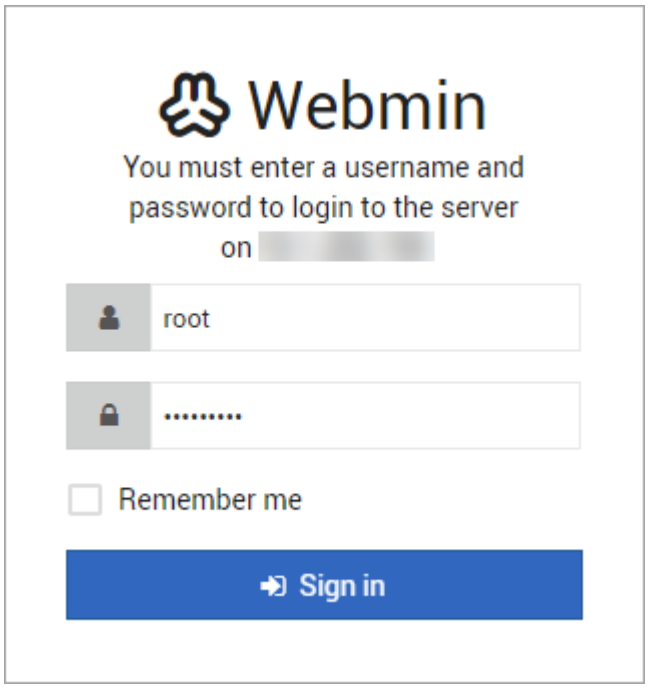
Webmin je súčasťou vášho virtuálneho zariadenia ESET PROTECT. Ak ho chcete začať používať, musíte ho najprv povoliť. Používa HTTPS a je spustené na porte 10000. IP adresa pre Webmin sa zobrazí na obrazovke konzoly na správu virtuálneho zariadenia ESET PROTECT.

Pre prístup do rozhrania Webmin vykonajte nasledovné:

Otvore webový prehliadač, zadajte IP adresu alebo hostiteľský názov vášho nasadeného ESET PROTECT VA do poľa s adresou a použite port 10000. URL adresa by mala mať nasledujúci formát: *https://<host name or IP address>:10000*, napr. *https://10.1.119.162:10000* alebo *https://esmcva:10000.*.

Zadajte prihlasovacie meno a heslo:

- Prihlasovacie meno je **root**.
- Prednastavené heslo je **eraadmin**, ale ak ste ho už zmenili, použite heslo, ktoré ste špecifikovali počas konfigurácie ESET PROTECT VA.



Po úspešnom prihlásení sa zobrazí Riadiaci panel nástroja Webmin.

Riadiaci panel

Po prihlásení do rozhrania Webmin **Riadiaci panel** zobrazí systémové informácie o vašom ESET PROTECT VA. Ide o informácie, ako napr. názov hostiteľa, OS, doba prevádzky od spustenia systému, využitie pamäte atď. Uvidíte tiež oznámenie v dolnej časti obrazovky, kde sa zobrazujú položky, ktoré si vyžadujú vašu pozornosť. Napríklad, môže sa zobraziť oznámenie, že je dostupná nová verzia nástroja Webmin, pričom zároveň bude možné vykonať aktualizáciu pomocou tlačidla **Upgrade Webmin Now**. Odporúčame, aby ste v takomto prípade aktualizáciu vykonali. Keď sa aktualizácia dokončí, zobrazí sa správa **Webmin install complete**.

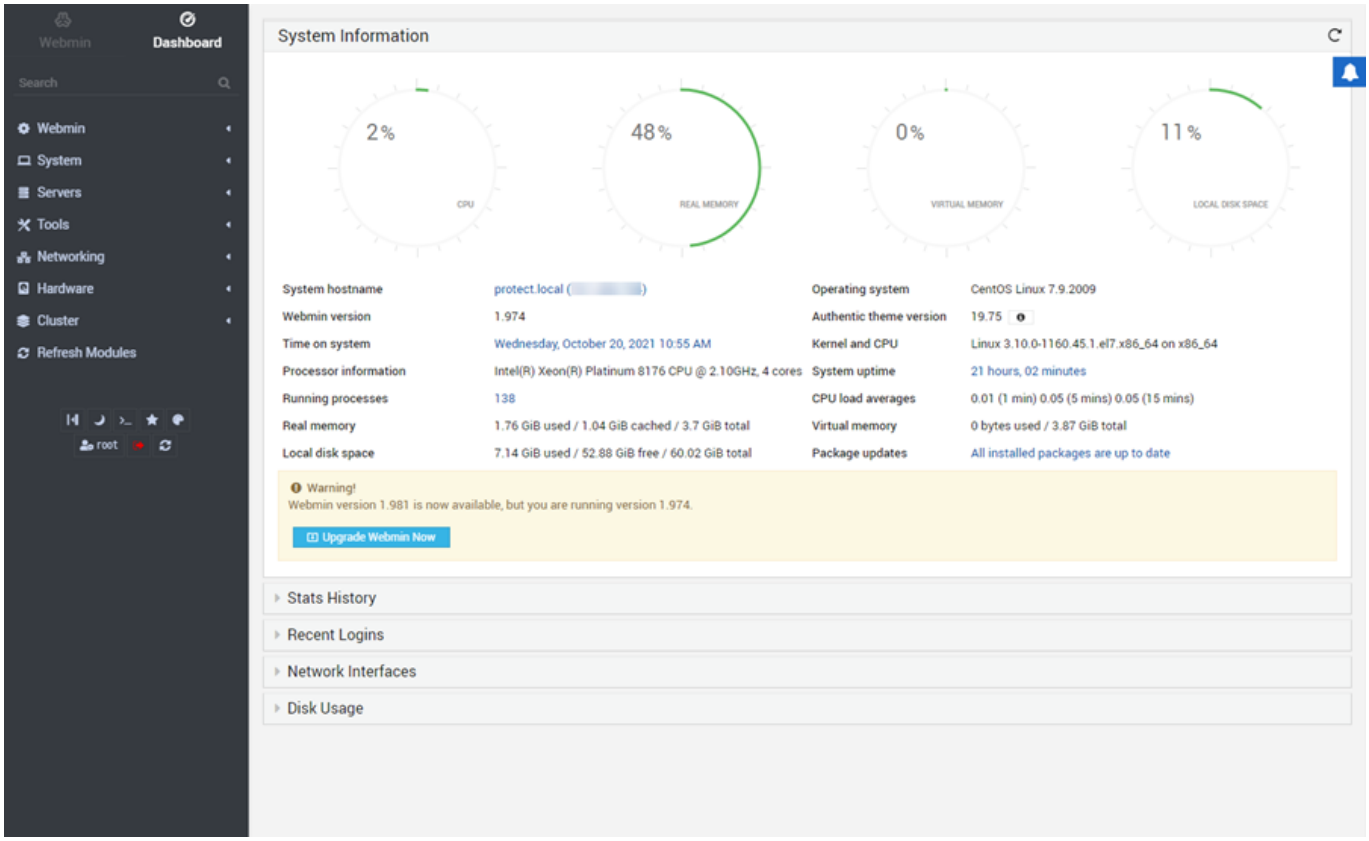
V hlavnom menu sa nachádzajú kategórie modulov: **Webmin**, **System**, **Servers**, **Tools**, **Networking**, **Hardware** a **Cluster**. Viac informácií o moduloch nájdete na webovej stránke Webmin Modules.

Nástroj Webmin automaticky zistí, čo je presne nastavené v rámci VA a na základe toho zobrazí relevantné moduly.

Najdôležitejšie moduly pre správu ESET PROTECT VA sú:

- System
- Servers
- Nástroje
- Networking

Webmin pracuje s kompletnými **oprávneniami root** systému Linux, čo znamená, že môže vo vašom systéme upravovať akýkoľvek súbor a spúšťať akýkoľvek príkaz. V prípade, že urobíte chybu, je možné vymazať všetky súbory vo vašom systéme alebo spôsobiť to, že sa nebude dať spustiť. Z tohto dôvodu je dôležité, aby ste boli pri práci s nástrojom Webmin opatrný. Aj napriek tomu, že vás Webmin zvyčajne upozorní v prípade, že sa chystáte vykonať potenciálne nebezpečnú akciu, nerobte zmeny v konfigurácii pre položky, ktoré vám nie sú známe.



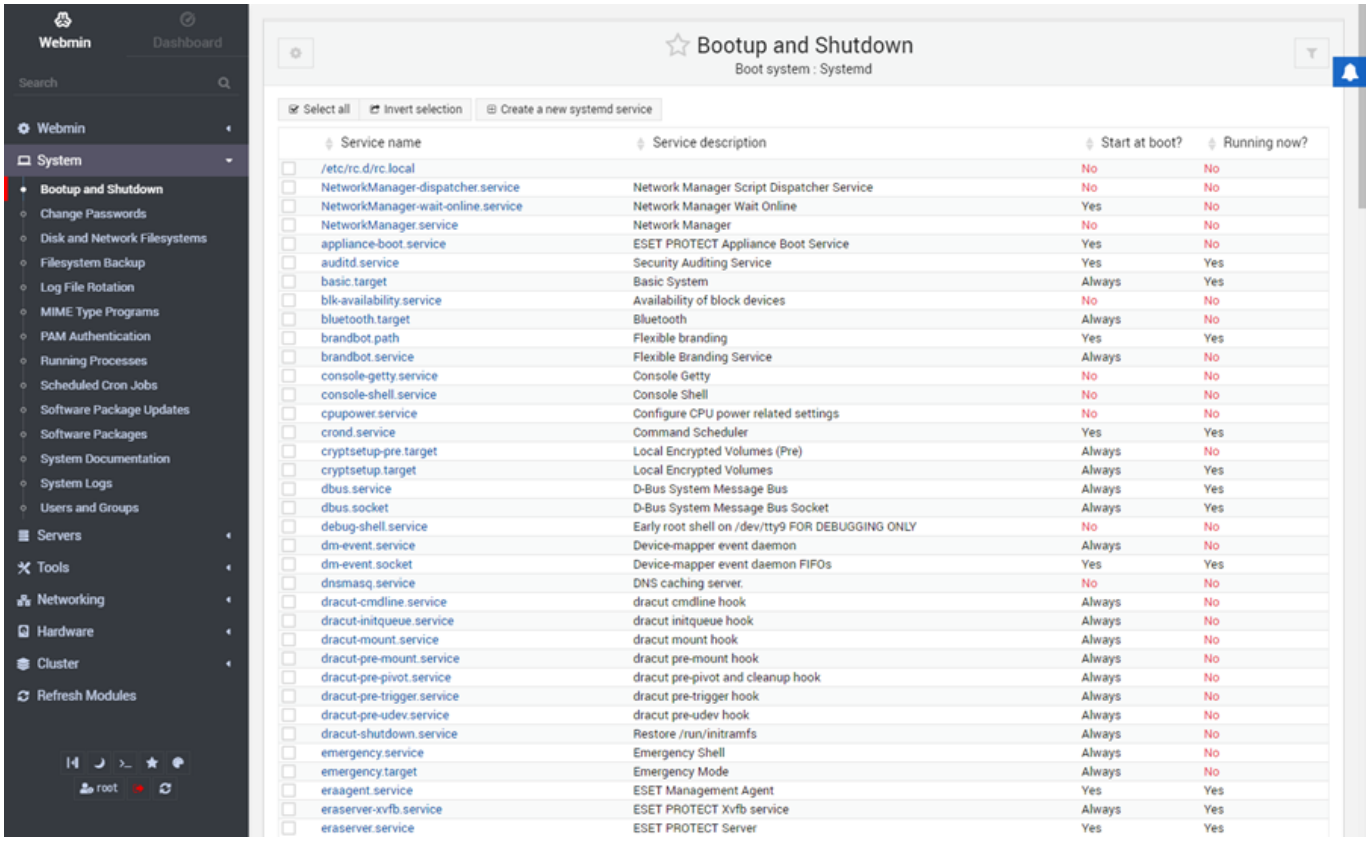
Oznámenie – ak vás chce nástroj Webmin na niečo upozorniť, oznámenie bude zobrazené v dolej časti riadiaceho panelu.

Odhlásenie – keď dokončíte prácu v nástroji Webmin, použite ikonu odhlásenia v menu naľavo.

Systém

V tejto časti môžete nakonfigurovať niektoré **systémové** moduly:

Bootup and Shutdown – umožní vám spravovať služby, upravovať ich, spustiť/zastaviť/reštartovať každú službu alebo viacero služieb naraz. Môžete tiež vytvárať a upravovať skripty, ktoré sa spúšťajú pri spustení alebo vypnutí systému atď. Ďalej môžete **Reštartovať** alebo **Vypnúť** virtuálny počítač pre ESET PROTECT pomocou tlačidiel umiestnených v dolnej časti.



Change Passwords – umožní vám zmeniť používateľské heslá virtuálneho počítača používané pri prihlásení do operačného systému.

> Nepoužívajte túto funkciu, ak chcete zmeniť heslo pre ESET PROTECT VA alebo ESET PROTECT databázu. V takýchto prípadoch použite funkcie Change VM password alebo Change database password v konzole na správu virtuálneho zariadenia ESET PROTECT.

Running Processes – môžete spravovať všetky spustené procesy vo svojom systéme pomocou nástroja Webmin. Tento modul môže byť použitý na zobrazenie, zrušenie, zmenu priorít a spustenie procesov na vašom systéme.

Software Package Updates – zobrazí dostupné aktualizácie a umožní vám aktualizovať všetky alebo iba zvolené softvérové balíky.

System Logs – slúži na zobrazenie protokolov vo vašom systéme.

Servery

V tejto časti môžete nakonfigurovať niektoré moduly **serverov**:

Apache Webserver – jeden z najkomplexnejších a najvýkonnejších modulov Webmin, umožňuje vám nakonfigurovať skoro každú funkciu Apache. Môžete ho použiť ako HTTP server na poskytovanie inštalačných súborov alebo aktualizácií. Je potrebné, aby ste nastavili Firewall pridaním pravidiel pre povolenie príslušných portov.

> Hoci to nie je to isté ako v prípade Apache Webserver pre ESET PROTECT Web Console, môžete použiť tento Apache Webserver na akýkoľvek iný účel.

ESET PROTECT – tento modul vám umožňuje **spustiť diagnostický nástroj**, **resetovať heslo správcu ESET PROTECT Servera**, **opraviť certifikát ESET PROTECT Servera** a **certifikačnú autoritu**, **opraviť certifikát ESET Management Agenta** a **certifikačnú autoritu**, **opraviť pripojenie ESET Management Agenta** alebo **upraviť Apache Tomcat server.xml** na zmenu HTTPS certifikátov a algoritmov šifrovania Web Console.

MySQL Database Server – umožňuje vám spravovať oprávnenia používateľov, meniť heslo a zobrazovať obsah databázy.

> Nepoužívajte MySQL Database Server na zálohovanie alebo obnovu ESET PROTECT databázy, miesto toho použite konzolu na správu virtuálneho zariadenia ESET PROTECT. Pre viac informácií si pozrite časť Zálohovanie databázy.

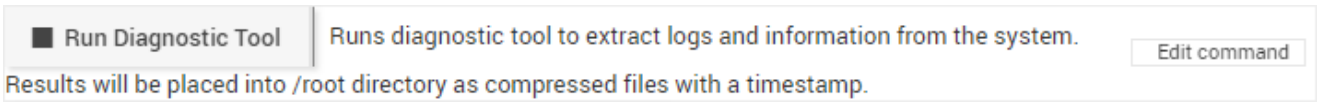
Samba Windows File Sharing – umožňuje vám vybrať adresáre, ktoré majú byť zdieľané pre Windows klienty pomocou SMB protokolu (Server Message Block). V prípade potreby môžete nastaviť modul Samba tak, aby boli súbory na vašom ESET PROTECT VA dostupné pre Windows klienty. Môžete tiež nakonfigurovať a pripojiť sa na doménu systému Windows. Ak je zdieľanie povolené, porty Samba musia byť povolené vo firewalle.

SSH Server – tento modul sa používa na konfiguráciu SSH a OpenSSH serverov a predpokladá, že máte základné používateľské znalosti o klientskych programoch. Na vašom systéme môžete nakonfigurovať SSH Server a klienty.

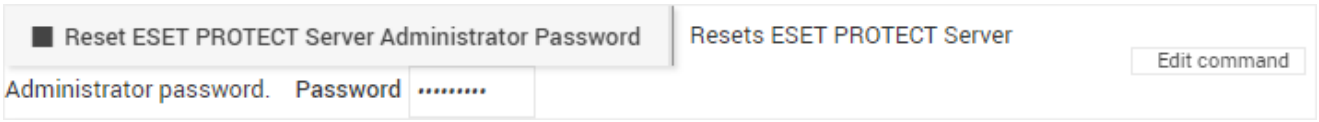
ESET PROTECT

Modul **ESET PROTECT** vám umožňuje spúšťať určité prednastavené príkazy, hlavne čo sa týka opravy certifikátov ESET PROTECT, spustenia diagnostického nástroja alebo resetovania hesla pre ESET PROTECT Server.

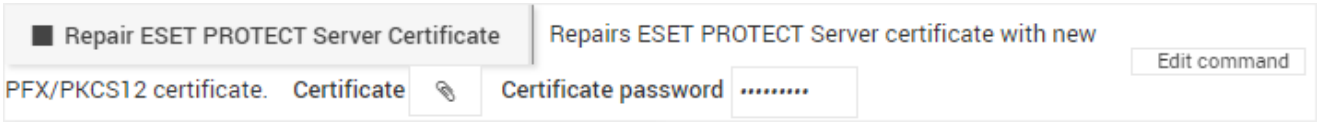
Run Diagnostic Tool – kliknutím na tlačidlo extrahujete protokoly a informácie zo systému. Protokoly budú exportované pre ESET PROTECT Server a ESET Management Agent. Na vyhľadanie a stiahnutie exportovaných diagnostických protokolov vo formáte *.zip* môžete použiť modul File Manager.



Reset ESET PROTECT Server Administrator Password – ak ste zabudli heslo ESET PROTECT Servera alebo si ho želáte resetovať, zadajte svoje nové heslo pre účet správcu ESET PROTECT Servera a stlačte tlačidlo na spustenie príkazu.



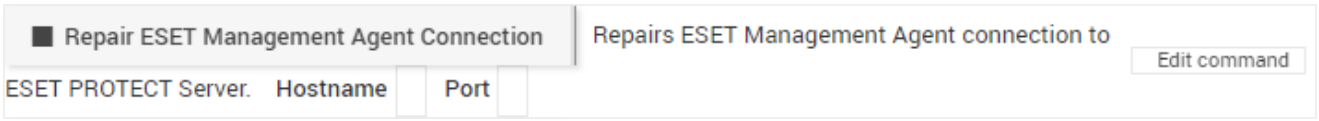
Repair ESET PROTECT Server Certificate – opraví certifikát ESET PROTECT Servera novým certifikátom PFX/PKCS12. Kliknite na ikonu **spinky**, vyberte súbor certifikátu PFX alebo PKCS12 pre ESET PROTECT Server a kliknite na **Open**. Zadajte heslo pre certifikát ESET PROTECT Servera a stlačte tlačidlo pre spustenie príkazu.



Repair ESET PROTECT Server Certification Authority – opraví certifikačnú autoritu ESET PROTECT Servera certifikátom DER. Kliknite na ikonu **spinky**, vyberte súbor certifikačnej autority *.der* a kliknite na **Open**.

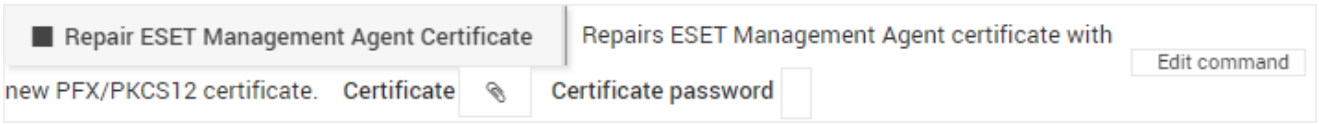


Repair ESET Management Agent Connection – opraví pripojenie ESET Management Agenta na ESET PROTECT Server. Zadajte **Hostiteľský názov** a číslo **portu** pre ESET PROTECT Server a stlačte tlačidlo pre spustenie príkazu.

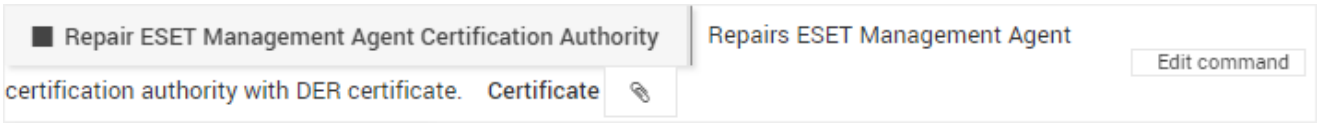


Repair ESET ManagementAgent Certificate – opraví certifikát ESET Management Agenta novým certifikátom PFX/PKCS12. Kliknite na ikonu **spinky**, vyberte súbor certifikátu *PFX* alebo *PKCS12* pre ESET Management Agenta a kliknite na **Open**. Zadajte heslo pre certifikát ESET Management Agenta a stlačte tlačidlo pre spustenie príkazu.

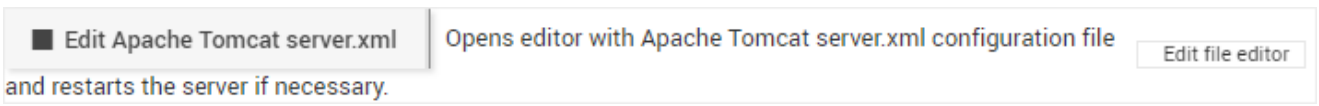
Prístupová fráza certifikátu nesmie obsahovať nasledujúce znaky: " \ Tieto znaky spôsobujú kritickú chybu počas inicializácie agenta.



Repair ESET Management Agent Certification Authority – opraví certifikačnú autoritu ESET Management Agenta certifikátom DER. Kliknite na ikonu **spinky**, vyberte súbor certifikačnej autority *.der* a kliknite na **Open**.



Edit Apache Tomcat server.xml – môžete upraviť konfiguračný súbor Apache Tomcat server.xml na zmenu HTTPS certifikátov a algoritmov šifrovania Web Console. Keď stlačíte tlačidlo, otvorí sa textový editor a budete môcť upraviť súbor `/etc/tomcat/server.xml`. Kliknite na tlačidlo **Save** pre uloženie zmien. Ak je potrebný reštart, bude vykonaný automaticky. Ak nechcete uložiť vykonané zmeny, kliknite na **Return to commands**.



Nástroje

Táto časť rozhrania Webmin obsahuje niekoľko rôznych modulov. Sú tu dva veľmi užitočné moduly:

File Manager – umožní vám zobraziť a manipulovať so súbormi na serveri pomocou HTML rozhrania. Keď prvýkrát načítate File manager (tiež známy pod názvom **Filemin**), ukáže sa obsah root priečinka na vašom virtuálnom zariadení ESET PROTECT v závislosti od toho, pod akým používateľským účtom ste prihlásený.

- Navigácia v rámci štruktúry adresárov je jednoduchá. Kliknite na názov adresára alebo jeho ikonu (priečinok). V hornej ľavej časti okna Filemin uvidíte aktuálny adresár. Kliknite na ľubovoľnú časť cesty pre zobrazenie obsahu daného adresára.

- Filemin môže byť tiež použitý na vyhľadávanie súborov. Kliknite na **Tools** v lište nástrojov (horná pravá časť okna Filemin) a zvoľte možnosť **Search**. Do poľa **Search query** zadajte vzorec vyhľadávania.

- Ak chcete stiahnuť súbor z vášho ESET PROTECT VA do počítača, na ktorom je spustený váš webový prehliadač, kliknite na názov súboru alebo jeho ikonu.

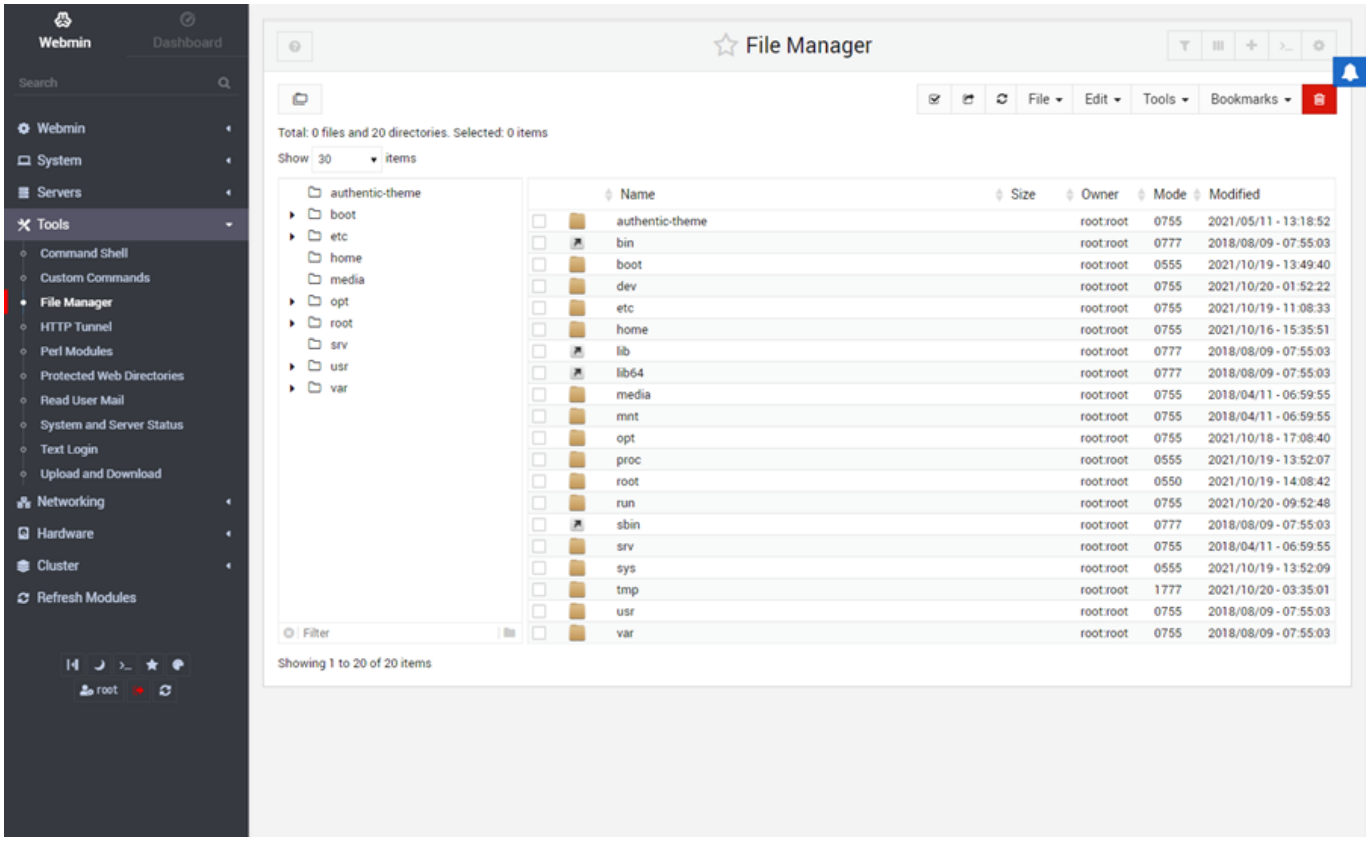
- Ak chcete nahrať súbor z počítača, na ktorom je spustený váš webový prehliadač, kliknite na **File** a potom na **Upload to current directory**. Týmto sa otvorí dialógové okno. Kliknite na ikonu spinky pre vyhľadanie súboru, ktorý chcete nahrať. Môžete vybrať viacero súborov a nahrať ich kliknutím na tlačidlo **Upload Files**. Nahrané súbory budú uložené vo vašom aktuálnom adresári. Po dokončení nahrávania sa zoznam adresárov aktualizuje a vy uvidíte súbory, ktoré ste nahrali.

- K súboru sa môžete dostať aj pomocou vzdialenej URL adresy. Stačí kliknúť na **File** a vybrať možnosť **Get from URL**.

- Obsah akéhokoľvek súboru vo vašom systéme môže byť zobrazený a upravovaný kliknutím na **ikonu Edit** v stĺpci **Actions**.

- Pre vytvorenie nového prázdneho textového súboru kliknite na **File**, potom na **Create new file** a zadajte názov nového súboru.

- Ak chcete premenovať súbor alebo adresár, kliknite na **ikonu Rename** v kontextovom menu, ktoré otvoríte kliknutím pravého tlačidla myši.



Upload and download – ďalší užitočný modul nástroja Webmin v kategórii **Tools**. Umožňuje vám vykonávať so súbormi tri rôzne akcie:

- **Download from web** – zadajte URL adresu súboru, ktorý chcete stiahnuť z internetu do vášho ESET PROTECT VA a upresnite umiestnenie, kde chcete daný súbor uložiť.
- **Upload to server** – kliknite na ikonu spinky pre vyhľadanie súboru, ktorý chcete nahrať. Naraz môžete nahrať maximálne 4 súbory. Upresnite umiestnenie, kde chcete súbory uložiť.
- **Download from server** – upresnite cestu vrátane názvu súboru v textovom poli **File to download** alebo kliknite na ikonu vedľa a prehľadávaním súborového systému ESET PROTECT VA vyberte súbor, ktorý chcete stiahnuť na počítač, na ktorom je spustený váš webový prehliadač. Kliknite na tlačidlo **Download** pre začatie sťahovania súboru.

Networking

Väčšinu času nie je potrebné meniť sieťové nastavenia, ale v prípade, že ich potrebujete zmeniť, môžete to urobiť v časti **Networking**. V tejto časti môžete nakonfigurovať niektoré užitočné moduly:

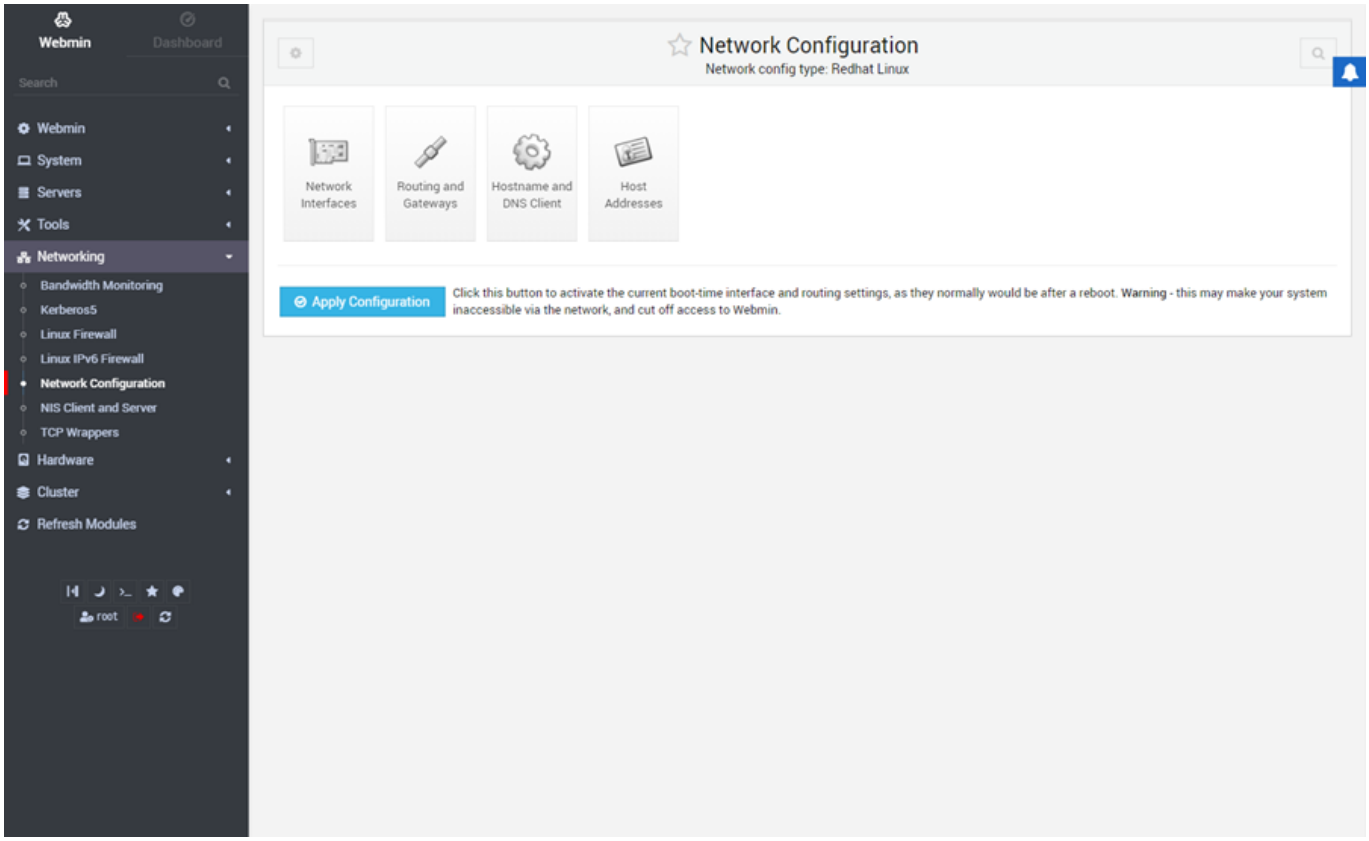
Kerberos5 configuration – je potrebné mať správne nastavené Kerberos tickets (tzv. vstupenky), aby mohla prebiehať AD synchronizácia. Keď sú Kerberos vstupenky nakonfigurované, môžete použiť funkciu Rejoin domain.

Linux Firewall – firewall založený na IPtables. Ak potrebujete povoliť porty, môžete tak učiniť tu pridaním pravidiel alebo úpravou už existujúcich pravidiel.

Network configuration – môžete nastaviť sieťový adaptér, zmeniť IP adresu, názov hostiteľa, DNS a ďalšie sieťové nastavenia.

Po dokončení konfigurácie stlačte tlačidlo **Apply Configuration**, aby sa uplatnili zmeny.

Tento postup je určený len pre skúsených správcov. V prípade, že sieť nie je nastavená správne, sa môže stať, že váš systém nebude prístupný prostredníctvom siete a taktiež sa preruší prístup do nástroja Webmin. Budete však mať aj naďalej prístup do konzoly na správu virtuálneho zariadenia ESET PROTECT pomocou terminálu virtuálneho počítača.



ESET PROTECT certifikáty

Na nasadenie ESET PROTECT MDM typov zariadení ESET PROTECT sú potrebné certifikáty ESET PROTECT.

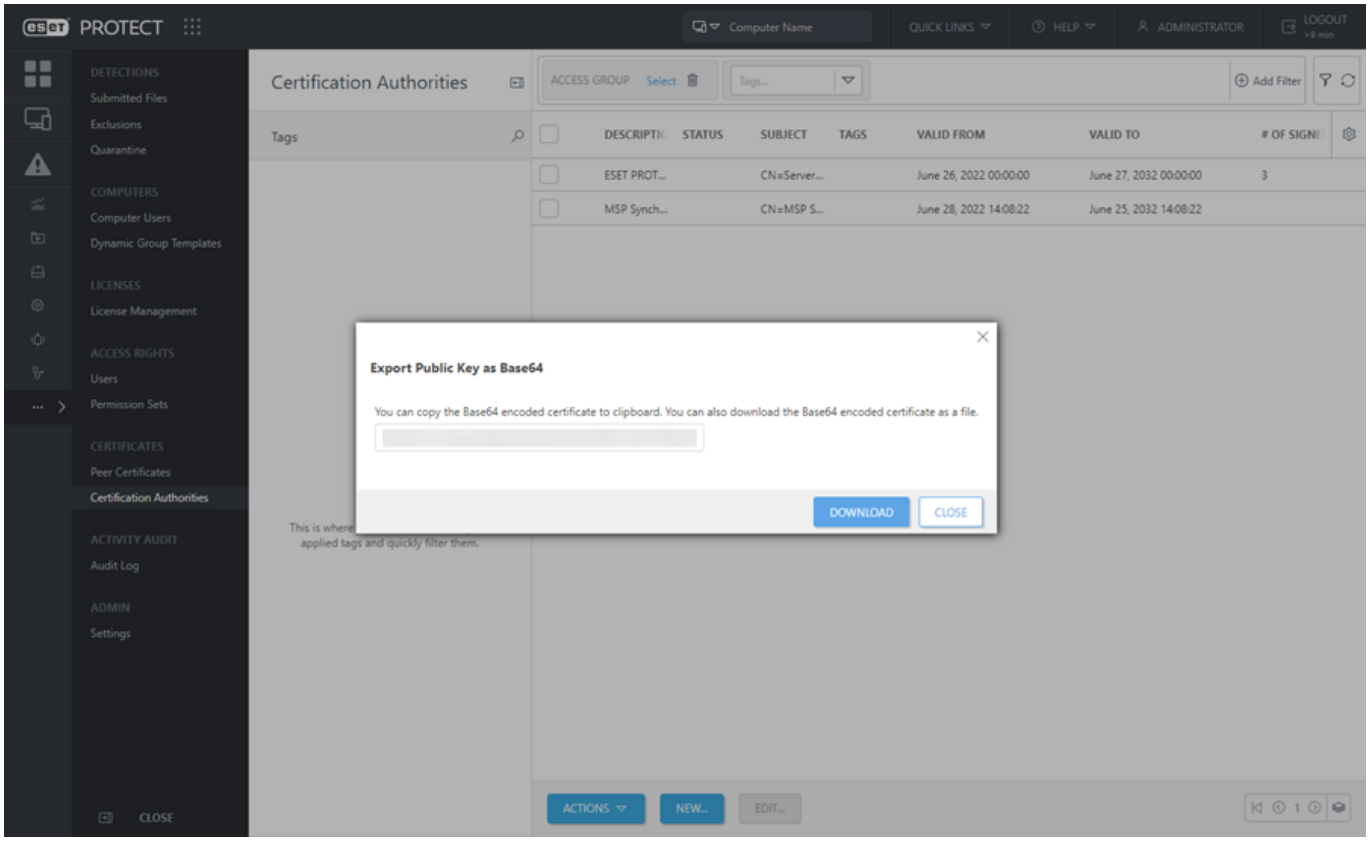
Certifikáty pre súčasti ESET PROTECT sú dostupné v nástroji Web Console.

Pri kopírovaní obsahu certifikátu vo formáte Base64 postupujte takto:

1. Kliknite na **Viac** > **Partnerské certifikáty**.

2. Vyberte certifikát a zvoľte možnosť Exportovať ako Base64. Certifikát môžete stiahnuť aj ako súbor.

Tento postup zopakujte pre všetky certifikáty súčastí, ako aj pre certifikačnú autoritu.



Na export certifikátu musí mať používateľ pridelené povolenie na **použitie** certifikátov (v rámci kategórie povolení **Certifikáty**). Podrobnejšie informácie nájdete v tejto kapitole obsahujúcej kompletný zoznam povolení.

ESET PROTECT VA aktualizácia/migrácia

Pre aktualizáciu alebo migráciu vášho VA môžete postupovať nasledovne:

- **Aktualizácia** – inštalácia novšej verzie súčastí ESET PROTECT.
- **Migrácia** – premiestnenie ESET PROTECT VA do inej inštancie rovnakej verzie.
- **Migrácia a aktualizácia** – premiestnenie ESET PROTECT VA do inej inštancie vyššej verzie.

Pri novom nasadení ESET PROTECT VA 8.1 a novších verzií je štandardne povolené Pokročilé zabezpečenie. Ak používate ESMC alebo ESET PROTECT VA verzie 8.0 s vypnutým Pokročilým zabezpečením, pri prechode na ESET PROTECT VA 8.1 alebo novšie verzie zostane Pokročilé zabezpečenie vypnuté.

Pred aktualizáciou/migráciou

Pred migráciou alebo aktualizáciou ESMC Servera si zálohujte svoju databázu a exportujte certifikačnú autoritu a partnerské certifikáty zo svojho starého ESET PROTECT/ESET PROTECT VA.

Migrácia databázy verzus Aktualizácia súčastí

Sú dostupné dva hlavné spôsoby aktualizácie virtuálneho zariadenia:

• Použitím migrácie databázy – aktualizácia celého zariadenia vrátane operačného systému, nielen ESET PROTECT Servera. Tento proces je zložitejší a vyžaduje si v priebehu migrácie dve súbežne bežiace zariadenia. Odporúčame použiť migráciu databázy pri prechode medzi hlavnými verziami alebo v rámci riešenia problémov.

• Aktualizácia pomocou úlohy Aktualizácia súčastí vo Web Console – tento proces je jednoduchší a nevyžaduje si prístup k zariadeniu, ale iba do Web Console. Tento postup odporúčame použiť v prípade rýchlych opráv a menších aktualizácií.

Proces migrácie a aktualizácie (odporúčaný spôsob aktualizácie)

Pre migráciu a aktualizáciu vášho ESET PROTECT VA sa riaďte nasledujúcimi pokynmi.

1. Stiahnite si najnovší súbor *protect_appliance.ova* (alebo `protect_appliance.vhd.zip` v prípade, že používate Microsoft Hyper-V).

2. Nasaďte nové ESET PROTECT VA. Prečítajte si inštrukcie v časti Proces nasadenia ESET PROTECT zariadenia. Nové ESET PROTECT VA zatiaľ prostredníctvom webového rozhrania **nekonfigurujte**.

3. Vykonajte migráciu databázy zo svojho starého VA. Podrobné inštrukcie nájdete v kapitole Migrácia databázy z iného servera.

Svoj starý VA Server zatiaľ neodinštalujte ani nevyraďte z prevádzky.

4. Nakonfigurujte nové virtuálne zariadenie ESET PROTECT pomocou webového rozhrania.

5. Skontrolujte, či sa vaše nové ESET PROTECT VA správa rovnako ako predchádzajúce.

- Ak má nové ESET PROTECT VA **inú IP adresu**:

  a) Vytvorte politiku na svojom starom VA, ktorá bude definovať novú IP adresu ESET PROTECT Servera, a priraďte ju k všetkým počítačom.

  b) Počkajte, kým sa politika aplikuje na všetky ESET Management Agenty.

  c) Uistite sa, že sa všetky počítače pripájajú k novému ESET PROTECT VA.

  d) Vypnite a vyraďte z prevádzky staré virtuálne zariadenie.

Dôrazne odporúčame, aby ste neodinštalovali starý ESET PROTECT VA Server pomocou skriptu určeného na odinštalovanie. Odinštalovaním zároveň dôjde k odstráneniu všetkých licencií z novej databázy ESET PROTECT VA Servera. Aby ste predišli tomuto problému, pred odinštalovaním odstráňte starú databázu ESET PROTECT VA Servera (`DROP DATABASE`).

- Ak má nové ESET PROTECT VA **rovnakú IP adresu**:

Uistite sa, že váš nový ESET PROTECT Server má rovnaké sieťové nastavenia (IP adresa, FQDN, názov počítača, DNS SRV záznam) ako váš starý VA Server. Môžete tiež použiť názov hostiteľa zmenou DNS záznamu tak, aby odkazoval na nový server.

  a) Vypnite staré virtuálne zariadenie.

b)Zapnite nové ESET PROTECT VA.

c)Uistite sa, že sa všetky počítače pripájajú k novému ESET PROTECT VA.

d)Vyraďte z prevádzky staré virtuálne zariadenie.

Dôrazne odporúčame, aby ste neodinštalovali starý ESET PROTECT VA Server pomocou skriptu určeného na odinštalovanie. Odinštalovaním zároveň dôjde k odstráneniu všetkých licencií z novej databázy ESET PROTECT VA Servera. Aby ste predišli tomuto problému, pred odinštalovaním odstráňte starú databázu ESET PROTECT VA Servera (`DROP DATABASE`).

6.Aktualizujte vzorkovú skupinu ESET Management Agentov cez ESET PROTECT pomocou úlohy Aktualizácia súčastí.

7.Ak bola aktualizácia vzorkovej skupiny úspešná a agenty sa pripájajú, pokračujte s ďalšími agentmi.

Proces aktualizácie (alternatívny spôsob aktualizácie)

Aktualizáciou ESMC alebo staršieho ESET PROTECT na najnovší ESET PROTECT na rovnakom VA nevykonáte aktualizáciu softvéru virtuálneho zariadenia (operačný systém a balíky potrebné na správne fungovanie ESET PROTECT Servera). Z tohto dôvodu odporúčame po dokončení čistej aktualizácie vykonať migráciu servera.

Aktualizácia virtuálneho zariadenia pomocou úlohy na aktualizáciu súčastí:

1.Najskôr reštartujte službu ESET PROTECT Server.

2.Aktualizujte vzorkovú skupinu ESET Management Agentov.

3.Ak bola aktualizácia vzorkovej skupiny úspešná a agenty sa pripájajú, pokračujte s ďalšími agentmi.

Obnova virtuálneho zariadenia ESET PROTECT po nehode

V prípade nešťastnej udalosti, kde dôjde k poškodeniu vášho ESET PROTECT VA, jeho zmazaniu z úložiska alebo sa nedá znova spustiť, sa môžete riadiť postupom obnovy po nehode.

Pre úspešnú obnovu je nevyhnutné, aby ste mali zálohu databázy svojho ESET PROTECT VA.

1. **Stiahnite si** najnovšiu verziu súboru *protect_appliance.ova* alebo `protect_appliance.vhd.zip` v prípade, že používate Microsoft Hyper-V. Výhodou tohto postupu obnovy je, že vaše ESET PROTECT VA bude aktuálne.

2. **Nasaďte nové ESET PROTECT VA**, ale zatiaľ ho nekonfigurujte. Prečítajte si inštrukcie v časti Proces nasadenia ESET PROTECT zariadenia.

3. **Povoľte Webmin**, aby bolo možné nahrať záložný súbor MySQL. Viac informácií nájdete v časti Povolenie/zakázanie vzdialeného prístupu.

4. **Obnovte databázu** z posledného záložného súboru. Postupujte podľa krokov popísaných v kapitole Obnova

databázy.

5. **Nakonfigurujte** vaše čerstvo nasadené ESET PROTECT VA s obnovenou databázou tak, ako vaše predchádzajúce VA. Viac informácií nájdete v časti Konfigurácia ESET PROTECT VA.

Riešenie problémov

Na riešenie problémov s virtuálnym zariadením ESET PROTECT môžete použiť súbory protokolov uvedené nižšie. Môžete byť tiež požiadaný technickou podporou spoločnosti ESET o poskytnutie diagnostických protokolov. Na analýzu môžete odoslať nasledujúce súbory protokolov:

Názov protokolu	Umiestnenie	Popis
Konfigurácia ESET PROTECT VA	*/root/appliance-configuration-log.txt*	Ak zlyhalo nasadenie ESET PROTECT VA, nereštartujte zariadenie a skontrolujte súbor protokolu.
ESET PROTECT Server	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log* */var/log/eset/RogueDetectionSensor/RDSensorInstaller.log*	Súbor protokolu inštalácie ESET PROTECT Servera. Ostatné súčasti ESET PROTECT majú podobné umiestnenie s príslušným názvom súboru.
Protokol sledovania ESET PROTECT Servera Protokol sledovania ESET Management Agenta	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/Agent/*	Skontrolujte vaše protokoly sledovania: *trace.log* *status.html* *last-error.html* Ostatné súčasti ESET PROTECT majú podobné umiestnenie s príslušným názvom súboru.
Apache HTTP Proxy	*/opt/apache/logs/* */var/log/httpd*	Súbor protokolu pre staršie verzie virtuálneho zariadenia ESET PROTECT. Súbor protokolu pre novšie verzie virtuálneho zariadeniaESET PROTECT.
Výpisy pri zlyhaní pre ESET PROTECT Server	*/var/opt/eset/RemoteAdministrator/Server/Dumps/*	
Spúšťanie diagnostického nástroja ESET PROTECT Serverom alebo ESET Management Agentom	*/root/RemoteAdministratorAgentDiagnostic.zip*	Ak máte problémy s ESET PROTECT VA, môžete použiť možnosť **Run diagnostic tool** (spustiť diagnostický nástroj). Podrobné informácie nájdete v kapitole ESET PROTECT Webmin modul.

Ak Agent alebo Server zlyháva a nedokážete prostredníctvom Web Console zmeniť úroveň zapisovania do protokolu, môžete aktivovať úplné zapisovanie sledovania vytvorením prázdneho súboru:

Pre Agenta:

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

Pre Server:

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

> Odporúčame používať nástroj Webmin File manager, pomocou ktorého môžete ľahko vyhľadať súbory a v prípade potreby stiahnuť protokoly.

Ak dostanete upozornenie, že **servery služby EPNS nie sú prístupné**, pozrite si, ako problém vyriešiť.

Najčastejšie otázky o virtuálnom zariadení ESET PROTECT

Táto kapitola obsahuje niektoré z najčastejšie sa vyskytujúcich otázok a problémov, s ktorými sa môžete stretnúť. Kliknite na názov kapitoly pre zobrazenie riešenia vášho problému:

- Ako zistiť, ktoré súčasti produktu ESET PROTECT sú nainštalované?
- Ako povoliť ping na virtuálnom zariadení ESET PROTECT?
- Potrebujem do svojho virtuálneho zariadenia ESET PROTECT pridať ďalšie súčasti?
- Ako povoliť Apache HTTP Proxy na virtuálnom zariadení ESET PROTECT po počiatočnej konfigurácii?
- Ako nastaviť LDAP pre povolenie synchronizácie statických skupín na virtuálnom zariadení ESET PROTECT?
- Konfigurácia pripojenia LDAPS k doméne
- Ako obnoviť zabudnuté heslo pre virtuálne zariadenie ESET PROTECT?
- Ako zmeniť reťazec pripojenia pre ESET PROTECT databázu?
- Ako nastaviť Hyper-V Server pre RD Sensor?
- Ako zmeniť číslo portu pre virtuálne zariadenie ESET PROTECT?
- Ako zvýšiť veľkosť pamäte pre MySQL Server?
- Mám problém s nástrojom ESET PROTECT bežiacom na Hyper-V Serveri 2012 R2.
- Ako zlepšiť výkon nástroja Oracle VirtualBox?
- Ako povoliť príkaz YUM, ak používam HTTP proxy?
- Ako aktualizovať operačný systém na počítači, na ktorom je nainštalovaný ESET PROTECT VA Server?
- Ako natrvalo vypnúť SELinux?

- Ako reštartovať konzolu na správu virtuálneho zariadenia?
- Ako použiť Proxy pre pripájanie Agentov?
- Ako povoliť SSH?

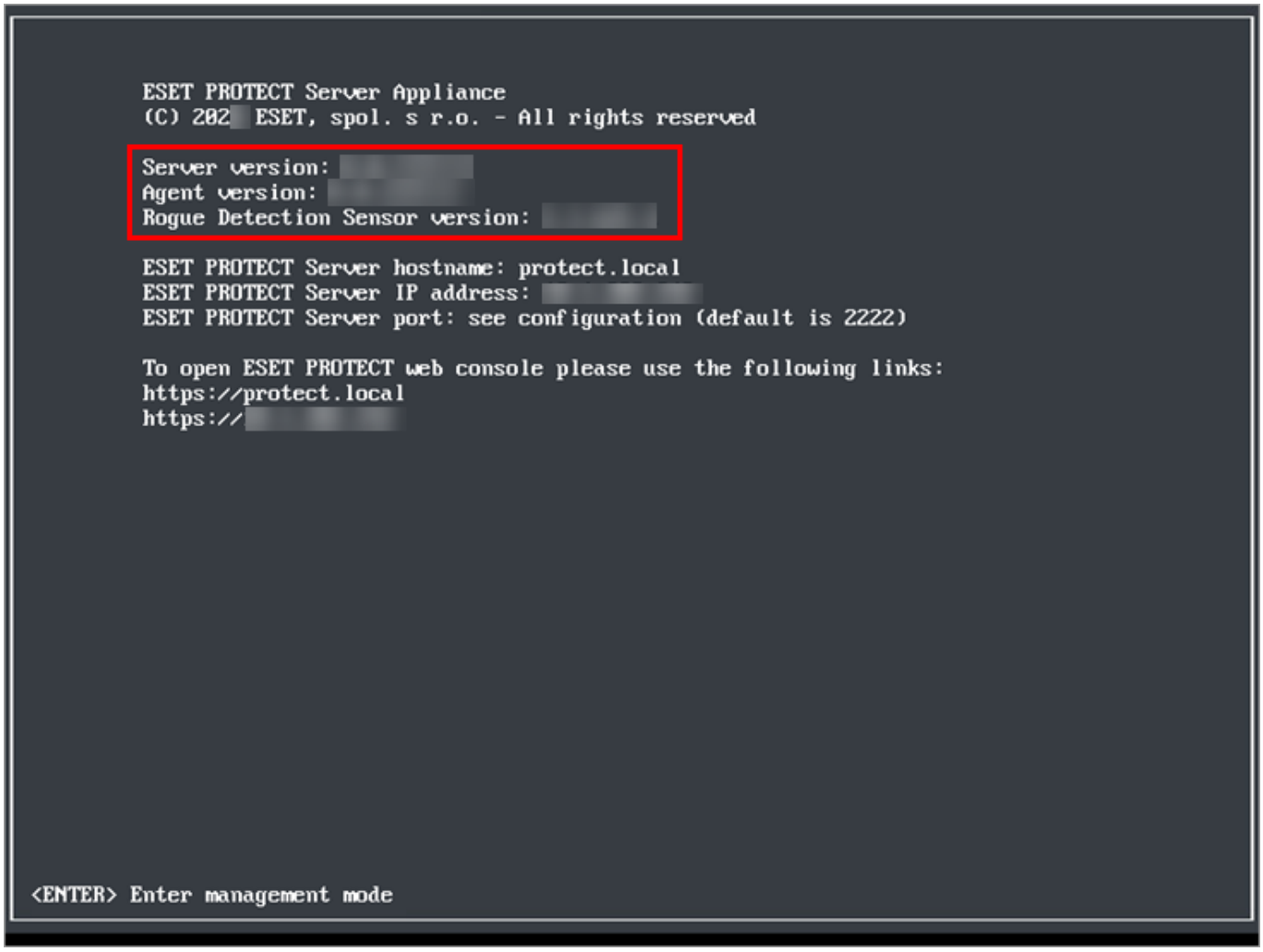
Ak sa váš problém nenachádza v tomto zozname, skúste hľadať podľa kľúčových slov alebo fráz, ktoré vystihujú váš problém, v pomocníkovi programu ESET PROTECT.

Ak nenájdete riešenie vášho problému alebo odpoveď na vašu otázku v pomocníkovi, môžete vyskúšať našu pravidelne aktualizovanú Databázu znalostí.

Ak vám pomocník programu ani databáza znalostí nepomohli, môžete sa obrátiť na technickú podporu spoločnosti ESET. Kontaktný formulár nájdete v ESET PROTECT Web Console v časti **Pomocník** > **Kontaktovať technickú podporu**.

Ako zistiť, ktoré súčasti produktu ESET PROTECT sú nainštalované?

Zoznam nainštalovaných súčastí ESET PROTECT a ich verzií je zobrazený v okne konzoly vášho virtuálneho zariadenia ESET PROTECT. Ak chcete obnoviť toto dialógové okno po aktualizácii súčasti (komponentu), môžete reštartovať virtuálne zariadenie. Ďalší spôsob je spustiť režim správy, vybrať možnosť **Exit to terminal**, opustiť terminál a vrátiť sa späť na obrazovku uzamknutia.



`

Ako povoliť ping na virtuálnom zariadení ESET PROTECT?

Ak chcete povoliť ping na počítači s virtuálnym zariadením ESET PROTECT, otvorte terminál a spustite nasledujúce príkazy ako root používateľ.

Skôr ako začnete, skontrolujte verziu svojho operačného systému CentOS pomocou príkazu `hostnamectl`. Následne podľa verzie svojho operačného systému spustite nasledujúce príkazy ako root používateľ:

CentOS 7

1. Zavolajte príkaz iptables:

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

2. Uložte iptables:

```
service iptables save
```

Teraz môžete vykonávať ping test pre virtuálne zariadenie ESET PROTECT z ostatných počítačov nachádzajúcich sa v rovnakej podsieti.

Potrebujem do svojho virtuálneho zariadenia ESET PROTECT pridať ďalšie súčasti?

Nie, virtuálne zariadenie ESET PROTECT je funkčné ihneď po nasadení. Je potrebné len nasadiť zariadenie a nakonfigurovať ho. Je to skutočne najjednoduchší spôsob nasadenia nástroja ESET PROTECT, ak používate podporovaný nástroj hypervisor.

Ako povoliť Apache HTTP Proxy na virtuálnom zariadení ESET PROTECT po počiatočnej konfigurácii?

Primárne využitie Apache HTTP Proxy spočíva v ukladaní súborov aktualizácií detekčného jadra a informácií z ESET LiveGrid® do vyrovnávacej pamäte. Pre povolenie Apache HTTP Proxy otvorte terminál a podľa verzie vášho operačného systému spustite nasledujúce príkazy ako root používateľ:

- Umiestnenie `apachectl` a `htcacheclean` sa môže líšiť v závislosti od vášho systému – pred spustením skriptu umiestnenie skontrolujte.
- Parameter `/var/cache/httpd/proxy` určuje umiestnenie priečinka pre ukladanie do vyrovnávacej pamäte. Toto umiestnenie sa nastavuje v konfiguračnom súbore `/etc/httpd/conf.d/proxy.conf` pod `CacheRoot`.

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`

Parametre pre údržbu vyrovnávacej pamäte Apache HTTP Proxy je možné upravovať: `-d` definuje interval čistenia v minútach, `-p` definuje cestu ako koreňový adresár diskovej vyrovnávacej pamäte, `-t` vymaže všetky prázdne adresáre, `-i` inteligentne vymaže vyrovnávaciu pamäť len v tom prípade, ak došlo k zmene v diskovej vyrovnávacej pamäti, `-l` definuje limit pre celkovú veľkosť diskovej vyrovnávacej pamäte.

6. Vo firewalle povoľte port 3128:

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. Budete musieť vytvoriť politiky, aby bola všetkým produktom spoločnosti ESET a súčastiam ESET PROTECT umožnená komunikácia prostredníctvom Apache HTTP Proxy, a budete tiež musieť povoliť ukladanie inštalačných a aktualizačných súborov do vyrovnávacej pamäte. Uistite sa, že konfiguračný súbor Apache HTTP Proxy obsahuje segment ProxyMatch definujúci hostiteľa servera. Viac informácií nájdete v našom článku Databázy znalostí v časti **II. Nastavenie politík pre klientske počítače**.

Riešenie problémov

Ak dostanete upozornenie, že **servery služby EPNS nie sú prístupné**, podľa nasledovných krokov vypnite časové limity pripojenia:

1. Vytvorte konfiguračný súbor *reqtimeout.conf*:
`sudo touch /etc/httpd/conf.d/reqtimeout.conf`

2. Otvorte konfiguračný súbor v textovom editore:
`nano /etc/httpd/conf.d/reqtimeout.conf`

3. Do súboru zadajte nasledujúce nastavenie:
`RequestReadTimeout header=0 body=0`

4. Uložte zmeny a zatvorte súbor:
Stlačte CTRL+X > zadajte **Y** > stlačte **Enter**

5. Otvorte súbor *httpd.conf*:
`nano /etc/httpd/conf/httpd.conf`

6. Na koniec súboru pridajte nasledujúci riadok:
`IncludeOptional conf.d/reqtimeout.conf`

7. Uložte zmeny a zatvorte súbor:
Stlačte CTRL+X > zadajte **Y** > stlačte **Enter**

8. Reštartujte službu Apache HTTP Proxy:
`systemctl restart httpd`

Ako nastaviť LDAP pre povolenie synchronizácie statických skupín na virtuálnom zariadení ESET PROTECT?

Ak zlyháva pripojenie k doméne, je to zvyčajne spôsobené nesprávnym nastavením virtuálneho zariadenia ESET PROTECT. Viac informácií nájdete v nasledujúcom článku našej databázy znalostí.

Konfigurácia pripojenia LDAPS k doméne

ESET PROTECT Server na systéme Windows predvolene používa šifrovaný protokol LDAPS (LDAP cez SSL) pre všetky pripojenia Active Directory.

Ak chcete nastaviť virtuálne zariadenie ESET PROTECT tak, aby sa pripájalo k Active Directory cez LDAPS, postupujte podľa krokov nižšie.

Požiadavky

- Nastavte LDAPS na doménovom radiči – uistite sa, že ste exportovali verejný kľúč certifikačnej autority DC.
- Uistite sa, že Kerberos je správne nastavený na vašom ESET PROTECT VA.

Zapnite LDAPS na ESET PROTECT VA.

1. Otvorte terminálové okno virtuálneho počítača, na ktorom prevádzkujete ESET PROTECT VA.
2. Stlačte **Enter**, zadajte heslo, ktoré ste nastavili počas konfigurácie ESET PROTECT VA, a dvakrát stlačte **Enter**.
3. Zvoľte možnosť **Exit to terminal** a stlačte **Enter**.
4. Zastavte službu ESET PROTECT Server.

```
systemctl stop eraserver
```

5. Zadajte nasledujúci príkaz:

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

6. Pridajte nasledujúci riadok do sekcie **[Service]**:

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

7. Stlačte **CTRL + X** a zadajte **Y** pre uloženie zmien v súbore. Stlačte **Enter** pre ukončenie editora.
8. Spustite nasledujúci príkaz pre opätovné načítanie konfigurácie:

```
systemctl deamon-reload
```

9. Reštartujte službu ESET PROTECT Server.

```
systemctl start eraserver
```

10. Skopírujte súbor certifikátu, ktorý ste vygenerovali na doménovom radiči, do nasledujúceho umiestnenia na svojom ESET PROTECT VA Serveri:

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

11. Spustite nasledujúci príkaz:

```
update-ca-trust
```

Ako obnoviť zabudnuté heslo pre virtuálne zariadenie ESET PROTECT?

Spustite ESET PROTECT VA v režime Single-User. Pokyny nájdete v dokumentácii pre CentOS 7. Keď budete v príkazovom riadku v režime Single-User, zmeňte vaše root heslo pomocou príkazu `passwd`.

Ak sa vám zobrazí hlásenie „`passwd: Authentication token manipulation error`“, postupujte podľa nasledujúcich krokov.

Ako zmeniť reťazec pripojenia pre databázu ESET PROTECT?

Reťazec pripojenia pre databázu ESET PROTECT môžete zmeniť vo svojom ESET PROTECT VA upravením konfiguračného súboru `StartupConfiguration.ini`.

Zmeniť reťazec pripojenia pre databázu ESET PROTECT môžete podľa nasledujúcich inštrukcií:

1. Aktivujte **režim správy** zadaním hesla a stlačením klávesu **Enter** dvakrát. Pomocou šípok zvoľte možnosť **Exit to terminal** a stlačte kláves **Enter**.

2. Zadajte nasledujúci príkaz:

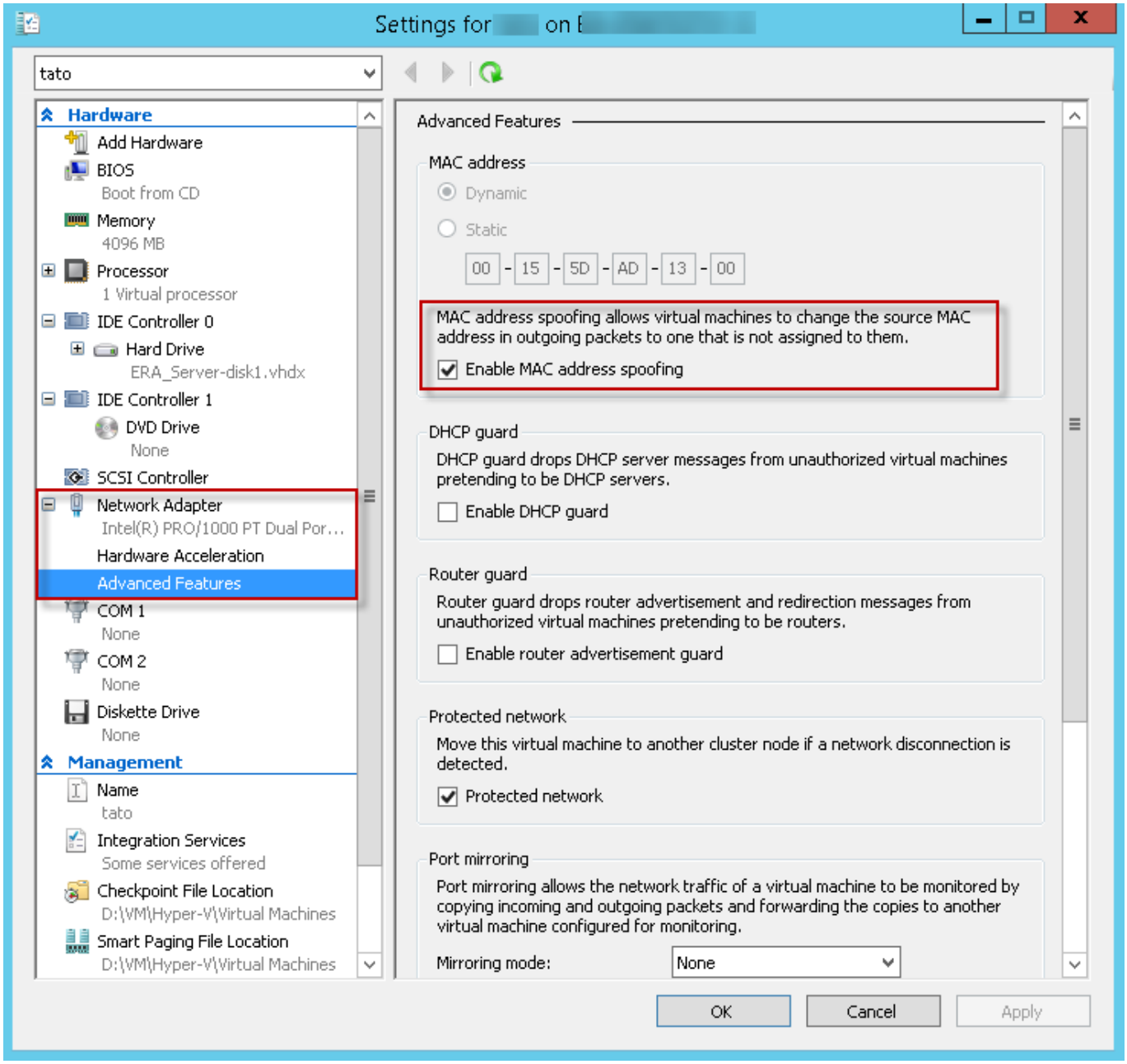
```
nano /etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

3. Vykonajte potrebné zmeny v reťazci pripojenia pre databázu ESET PROTECT.

4. Stlačením `Ctrl+X` a `y` zmeny uložíte.

Ako nastaviť Hyper-V Server pre RD Sensor?

Uistite sa, že v nastaveniach nástroja Hyper-V Manager je povolená možnosť MAC address spoofing (pozrite obrázok).



Ako zmeniť číslo portu pre virtuálne zariadenie ESET PROTECT?

Pre zmenu čísla portu je potrebné vykonať nasledujúce zmeny pre príslušnú súčasť ESET PROTECT:

ESET PROTECT Web Console port (predvolene 8443)

1.Otvorte rozhranie Webmin.

2.Prejdite do časti **Servers** > **ESET PROTECT** a kliknite na **Edit Apache Tomcat server.xml**

3.Pre pridanie vlastného portu upravte riadok `<Connector port="8443"` a kliknite na **Save and close**.

4.Otvorte súbor *EraWebServerConfig.properties*:

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

5.Pre pridanie vlastného portu upravte riadok `server_port=` a zmeny uložte.

6.Reštartujte službu Tomcat: `systemctl restart tomcat`

Porty ESET PROTECT Servera (štandardne 2222, 2223) – prihláste sa do rozhrania ESET PROTECT Web Console, prejdite do časti **Viac** > **Nastavenia** > **Pripojenie** a vykonajte potrebné zmeny.

Ak ste zmenili ktorýkoľvek z portov uvedených vyššie, bude potrebné upraviť nastavenia aj pre firewall. Otvorte rozhranie Webmin, prejdite do časti **Networking** > **Linux Firewall** a zmeňte čísla portov v už existujúcich pravidlách. Môžete tiež prípadne pridať nové pravidlá.

Ako zvýšiť veľkosť pamäte pre MySQL Server?

Pre zvýšenie veľkosti pamäte pre MySQL Server postupujte podľa nasledujúcich krokov:

1. Aktivujte **režim správy** zadaním hesla a stlačením klávesu Enter dvakrát. Zvoľte možnosť **Exit to terminal** pomocou šípok a stlačte kláves **Enter**.

2. Zadajte nasledujúci príkaz:
`nano /etc/my.cnf`

3. Nájdite riadok `innodb_buffer_pool_size = 1024M` a zmeňte uvedené číslo tak, aby zodpovedalo 50 % pamäte RAM virtuálneho počítača. `1024M` znamená 1024 megabajtov.

4. Ukončite textový editor stlačením `Ctrl + X` a stlačte `Y` pre uloženie.

5. Reštartujte zariadenie pomocou možnosti **Restart system** v **režime správy**.

Mám problém s nástrojom ESET PROTECT bežiacom na Hyper-V Serveri 2012 R2.

Po prihlásení do rozhrania ESET PROTECT Web Console sa zobrazuje chybové hlásenie „Unable to handle Kernel NULL pointer dereference at (null)“.

Pre riešenie tohto problému vypnite funkciu **Dynamic memory** (dynamická pamäť) v nastaveniach virtuálneho počítača.

Ako zlepšiť výkon nástroja Oracle VirtualBox?

V **Nastaveniach** virtuálneho zariadenia ESET PROTECT môžete zmeniť počet procesorov (jadier). Prejdite na kartu **System** > **Processor**. Znížte počet procesorov pre virtuálne zariadenie. Napríklad, ak máte 4 fyzické procesory, zmeňte nastavenia tak, aby virtuálne zariadenie využívalo iba 2 procesory.

Ako povoliť príkaz YUM, ak používam HTTP proxy server?

Ak vo vašej sieti používate na pripojenie k internetu proxy server, môže sa stať, že príkaz `yum` nie je nakonfigurovaný správne a teda nemusí fungovať.

Pre konfiguráciu príkazu `yum` pri používaní proxy postupujte podľa nasledujúcich krokov:

1. Aktivujte režim správy zadaním hesla a stlačením klávesu **Enter** dvakrát. Zvoľte možnosť **Exit** to terminal pomocou šípok a stlačte kláves **Enter**.

2. Zadajte nasledujúci príkaz:
```
nano /etc/yum.conf
```

3. Do konfiguračného súboru pridajte riadok s informáciou o vašom proxy. Napríklad:
```
proxy=http://proxysvr.yourdom.com:3128
```

4. Ak proxy vyžaduje prihlasovacie meno a heslo, pridajte do konfigurácie nasledujúce riadky. Napríklad:
```
proxy=http://proxysvr.yourdom.com:3128
proxy_username=YourProxyUsername
proxy_password=YourProxyPassword
```

5. Stlačením `Ctrl + X` a `y` zmeny uložíte.

> Majte na pamäti, že informácie uložené v konfiguračnom súbore `/etc/yum.conf` sú v čitateľnej podobe, aby mohol príkaz `yum` správne fungovať. To znamená, že prihlasovacie meno a heslo si môže prečítať akýkoľvek používateľ. Z tohto dôvodu neodporúčame používať rovnaké heslo na žiadnom inom mieste.

Viac informácií nájdete v dokumentácii dodávateľa.

Ako aktualizovať operačný systém na počítači, na ktorom je nainštalovaný ESET PROTECT VA Server?

V prípade, že sa vám v ESET PROTECT Web Console zobrazí pre zariadenie, na ktorom je nainštalovaný ESET PROTECT VA Server, upozornenie **Operačný systém nie je aktualizovaný**, je nutné tento operačný systém aktualizovať. Pre vykonanie tejto akcie prostredníctvom ESET PROTECT Web Console spustite úlohu Aktualizácia operačného systému. Po dokončení aktualizácie uvedené upozornenie zmizne.

> Pri aktualizácii operačného systému cez rozhranie Webmin, z terminálu alebo pomocou nástrojov tretích strán, zobrazené upozornenie nezmizne ani po úspešnom dokončení aktualizácie. V tomto prípade vám odporúčame spustiť úlohu **Aktualizácia operačného systému** cez ESET PROTECT Web Console.

Ako natrvalo vypnúť SELinux?

SELinux je vo virtuálnom zariadení predvolene aktívny. Pre jeho trvalé vypnutie postupujte podľa nižšie uvedených krokov:

1. V konzole na správu virtuálneho zariadenia vyberte **Exit to Terminal**.

2. Spustite príkaz:
```
nano /etc/selinux/config
```

3. Zmeňte riadok:
```
SELINUX=permisive
```
na
```
SELINUX=disabled
```

4. Uložte zmeny a ukončite editor.

5. Pre uplatnenie zmien reštartujte počítač nasledujúcim príkazom:
```
reboot
```

Ako reštartovať konzolu na správu virtuálneho zariadenia?

Grafické rozhranie virtuálneho zariadenia je možné reštartovať bez potreby reštartovať celý virtuálny počítač. Týmto spôsobom vynútite obnovenie všetkých dát zobrazených v konzole. (Toto je užitočné napríklad v prípade, že ste upravili nastavenie, no táto zmena sa v konzole ešte neprejavila.)

1. V konzole na správu virtuálneho zariadenia vyberte **Exit to Terminal**.

2. Spustite príkaz:
```
./appliance-gui restart
```

Ako použiť Proxy na pripájanie agentov?

Prostredníctvom Proxy je možné v rámci ESET Management preposielať komunikáciu z ESET PROTECT Agentov na ESET PROTECT Server, pričom využiť môžete Apache HTTP Proxy. Pri inštalácii Apache HTTP Proxy sa riaďte inštrukciami v tejto kapitole o inštalácii na Linux.

Ako povoliť SSH?

Pre povolenie SSH na ESET PROTECT VA (alebo ESMC VA) si pozrite časť Povolenie/zakázanie vzdialeného prístupu.

Riešenie problémov týkajúcich sa SSH

Otvorte terminál a spustite nasledujúce príkazy:

• `sudo systemctl status sshd` – uistite sa, že SSH je spustené. Ak SSH nie je spustené, môžete ho spustiť pomocou nasledujúceho príkazu: `sudo systemctl start sshd`

• `sudo iptables -S` – ak je otvorený port 22, uvidíte nasledujúci riadok: `-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`. Pre pridanie portu 22 do iptables spustite príkaz nižšie:
`sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT`

Licenčná dohoda s koncovým používateľom

S účinnosťou od 19. októbra 2021.

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.**

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532 („ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou („Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody a prijímate Zásady ochrany osobných údajov. Ak s niektorými podmienkami a požiadavkami tejto Dohody a/alebo Zásad ochrany osobných údajov nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru („Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto zmluvy a dodržiavate všetky jej zmluvné podmienky, poskytovateľ vám udeľuje nasledujúce práva („licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií.** Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent („MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač. Jednu licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má Koncový používateľ právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Home/Business Edition.** Verzia Softvéru Home Edition je určená výlučne na domáce a rodinné používanie v súkromných alebo nekomerčných prostrediach. Na použitie v komerčnom prostredí, ako aj na použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie.** Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér.** Softvér klasifikovaný ako OEM je obmedzený len na počítač, s ktorým bol získaný. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér.** Softvér označený ako „Nepredajný“, „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie.** Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zrušenia licencie musíte softvér a všetky záložné kópie okamžite odstrániť, zničiť alebo na svoje náklady vrátiť spoločnosti

ESET alebo na miesto, kde ste softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4. **Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a príslušné zhromažďovanie údajov je nevyhnutné na fungovanie Softvéru a na aktualizáciu a inováciu Softvéru. Poskytovateľ môže vydávať aktualizácie alebo inovácie Softvéru („Update“), nie je však povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Pre poskytovanie aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

Na poskytovanie akýchkoľvek aktualizácií sa môžu vzťahovať Zásady Ukončenia životného cyklu („Zásady Ukončenia životného cyklu“), ktoré sú k dispozícii na adrese https://go.eset.com/eol_business. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebudú sa poskytovať žiadne aktualizácie.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom

pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Dohody budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, tým nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Dohody.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Na vaše právo používať Softvér a ktorúkoľvek z jeho funkcií sa môžu vzťahovať Zásady Ukončenia životného cyklu. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, vaše právo používať Softvér zanikne. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ

PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY, ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ INŠTALÁCIOU, POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebude sa poskytovať žiadna technická podpora. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti Softvéru.** Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo).

Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**.

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje.

(právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez toho, aby bolo dotknuté právo spoločnosti ESET oznámiť vám akékoľvek zmeny tejto Dohody, Zásad ochrany osobných údajov, Zásad Ukončenia životného cyklu a Dokumentácie v súlade s článkom 22 Dohody. Spoločnosť ESET vám môže posielať e-maily, oznámenia v aplikácii prostredníctvom Softvéru alebo uverejniť komunikáciu na svojej webovej lokalite. Súhlasíte s tým, že budete od spoločnosti ESET dostávať právnu komunikáciu v elektronickej forme vrátane akejkoľvek komunikácie o zmene podmienok, osobitných podmienok alebo zásad ochrany osobných údajov, akýchkoľvek návrhov/prijatí zmluvy alebo pozvánok, upozornení alebo inej právnej komunikácie. Takáto elektronická komunikácia sa bude považovať

za prijatú v písomnej forme, pokiaľ príslušné právne predpisy osobitne nevyžadujú inú formu komunikácie.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky. Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. Táto Dohoda bola vyhotovená v angličtine. V prípade, že je z praktických dôvodov alebo na akýkoľvek iný účel vypracovaný akýkoľvek preklad Dohody, alebo v prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí verzia v angličtine.

Spoločnosť ESET si vyhradzuje právo kedykoľvek vykonať zmeny v Softvéri, ako aj kedykoľvek upraviť podmienky tejto Dohody, jej prílohy, dodatky, Zásady ochrany osobných údajov, Zásady Ukončenia životného cyklu a dokumentáciu, prípadne ich ľubovoľnú časť tak, že aktualizuje príslušný dokument: (i) aby zohľadňoval zmeny v Softvéri alebo v tom, ako spoločnosť ESET vykonáva podnikateľskú činnosť, (ii) z právnych, regulačných alebo bezpečnostných dôvodov alebo (iii) na zabránenie zneužitiu alebo ublíženiu. O každej úprave Dohody vás informujeme prostredníctvom e-mailu, oznámenia v aplikácii alebo iným spôsobom elektronickej komunikácie. Ak s navrhovanými zmenami Dohody nebudete súhlasiť, môžete ju v súlade s článkom 10 ukončiť do 30 dní od prijatia oznámenia o zmene. Ak Dohodu v tejto časovej lehote neukončíte, navrhované zmeny sa budú považovať za prijaté a nadobudnú voči vám účinnosť k dátumu prijatia oznámenia o zmene.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

DODATOK K DOHODE

Preposielanie Informácií Poskytovateľovi. Na preposielanie Informácií Poskytovateľovi sa vzťahujú ďalšie ustanovenia, ako je uvedené nižšie:

Softvér obsahuje funkcie, ktoré zhromažďujú údaje o procese inštalácie, Počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, informácie o prevádzke a fungovaní Softvéru a informácie o spravovaných zariadeniach (ďalej len „Informácie“) a potom ich odosielajú Poskytovateľovi. Informácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov), ktoré sa týkajú spravovaných zariadení. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Informácie v súlade so Zásadami ochrany osobných údajov a príslušnými právnymi predpismi.

Softvér vyžaduje, aby bola v spravovanom počítači nainštalovaná súčasť, ktorá umožňuje prenos informácií medzi spravovaným počítačom a softvérom na vzdialenú správu. Informácie, ktoré sa prenášajú, obsahujú údaje správy, napríklad informácie o hardvéri a softvéri spravovaného počítača, a pokyny na správu od softvéru na vzdialenú správu. Iný obsah údajov prenášaných zo spravovaného počítača závisí od nastavení softvéru nainštalovaného v spravovanom počítači. Obsah pokynov od softvéru na správu závisí od nastavení softvéru na vzdialenú správu.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Zásady ochrany osobných údajov

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, chce byť ako kontrolór údajov (ďalej len „ESET“ alebo „my“ alebo formulácie vyjadrené v prvej osobe množného čísla) pri spracovaní osobných údajov a ochrane osobných údajov svojich zákazníkov transparentná. S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať našich zákazníkov (ďalej len „koncový používateľ“ alebo „vy“ alebo formulácie vyjadrené v druhej osobe množného čísla) o nasledujúcich témach:

- Spracovávanie osobných údajov,
- Dôvernosť údajov,
- práva dotknutej osoby.

Spracovávanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho produktu sa poskytujú za podmienok Licenčnej zmluvy koncového používateľa (ďalej len "EULA"), niektoré z nich však môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o zhromažďovaní údajov, ktoré súvisí s poskytovaním našich služieb. Poskytujeme rôzne služby, ktoré sú opísané v zmluve EULA, ako aj v produktovej dokumentácii. Patria k nim napríklad služby aktualizácie/inovácie, ESET LiveGrid®, ochrana pred zneužitím údajov, podpora atď. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

- Počas spravovania bezpečnostných produktov ESET sa vyžadujú a lokálne ukladajú informácie, ako napríklad identifikátor a názov jednotky, názov produktu, licenčné informácie, informácie o aktivácii a uplynutí platnosti, informácie o hardvéri a softvéri spravovaného počítača s nainštalovanými bezpečnostnými produktmi ESET. Denníky týkajúce sa aktivít spravovaných bezpečnostných produktov a zariadení ESET sa zhromažďujú a sprístupňujú na zjednodušenie funkcií a služieb spravovania a dozoru bez toho, aby sa automaticky odosielali do spoločnosti ESET.
- Informácie týkajúce sa procesu inštalácie vrátane informácií o platforme, na ktorej je produkt nainštalovaný, a informácií o prevádzke a funkčnosti našich produktov, napríklad informácie o odtlačkoch hardvéru, identifikátoroch inštalácie, výpisoch pri zlyhaní, identifikátoroch licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu, ktoré môžu tiež zahŕňať spravované zariadenia.
- Licenčné informácie, ako napríklad identifikácia licencie, a osobné údaje, ako napríklad meno, priezvisko, adresa a e-mailová adresa, sa vyžadujú na fakturačné účely, overenie pravosti licencie a poskytovanie našich služieb.
- Kontaktné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa vyžadujú na poskytnutie technickej alebo inej podpory spoločnosťou ESET. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a opis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia podpory vás môžeme požiadať o poskytnutie ďalších informácií, napríklad vygenerovaných protokolov.
- Údaje týkajúce sa používania našich služieb sú na konci relácie úplne anonymné. Po skončení relácie sa neuložia žiadne informácie umožňujúce identifikáciu osôb.

Dôvernosť údajov

ESET je spoločnosť s celosvetovou pôsobnosťou prostredníctvom pridružených subjektov alebo partnerov, ktorí sú súčasťou našej distribučnej, servisnej či podpornej siete. Informácie spracúvané spoločnosťou ESET sa môžu na účely výkonu zmluvy EULA, napríklad na poskytovanie služieb či podpory alebo fakturácie, prenášať medzi jednotlivými pridruženými subjektmi alebo partnermi. V závislosti od vašej polohy a služby, ktorú si vyberiete, sa od nás môže žiadať prenos vašich údajov do krajiny, v ktorej neplatí príslušné rozhodnutie Európskej komisie. Aj v takom prípade podlieha každý prenos informácií úprave vychádzajúcej z právnych predpisov o ochrane údajov a uskutočňuje sa iba v prípade potreby. Bez výnimky musia byť zavedené štandardné zmluvné doložky, záväzné vnútropodnikové pravidlá alebo iné vhodné záruky.

Čo najviac sa snažíme zabrániť tomu, aby sa pri poskytovaní služieb podľa zmluvy EULA údaje uchovávali dlhšie, než je naozaj potrebné. Obdobie uchovávania môže prekračovať platnosť vašej licencie, aby ste mali čas na jej jednoduché a pohodlné obnovenie. Minimalizované a pseudonymizované štatistické a iné údaje zo systému ESET LiveGrid® sa môžu ďalej spracúvať na štatistické účely.

Spoločnosť ESET realizuje vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti, ktorá zodpovedá potenciálnym rizikám. Čo najlepšie sa snažíme zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania údajov. V prípade úniku údajov, ktorý má za následok ohrozenie vašich práv a slobôd, sme však pripravení informovať dozorný orgán, ako aj dotknuté osoby. Ako dotknutá osoba máte právo podať sťažnosť dozornému orgánu.

Práva dotknutej osoby

Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. V súlade s podmienkami určenými príslušnými zákonmi na ochranu údajov máte ako dotknutá osoba tieto práva:

- právo požiadať spoločnosť ESET o prístup k svojim osobným údajom;
- právo na opravu svojich osobných údajov, ak sú nepresné (máte tiež právo doplniť neúplné osobné údaje);
- právo požiadať o vymazanie svojich osobných údajov;
- právo požiadať o zákaz spracovania svojich osobných údajov;
- právo namietať voči spracovaniu
- právo podať sťažnosť, ako aj
- právo na prenosnosť údajov.

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk