Poznámky k verzi aplikace Symantec™ Endpoint Protection 14.3 RU1

Aktualizováno: Prosinec 2020

Table of Contents

Prohlášení o autorských právech 3
Novinky v aplikaci Symantec Endpoint Protection 14.3 RU1 4
Známé problémy a řešení pro aplikaci Symantec Endpoint Protection 9
Systémové požadavky na aplikaci Symantec Endpoint Protection (SEP) 15
Podporované a nepodporované možnosti upgradu na nejnovější verzi aplikace Symantec Endpoint Protection 14.x 24
Další zdroje informací 26

Prohlášení o autorských právech

Novinky v aplikaci Symantec Endpoint Protection 14.3 RU1

Tato část popisuje nové funkce v této verzi.

Funkce ochrany

- Zahrnuje novou aplikaci Symantec Agent pro systém Mac a aplikaci Symantec Agent pro systém Linux, kterou můžete nainstalovat a spravovat z místní aplikace Symantec Endpoint Protection Manager nebo z integrované cloudové konzole Cyber Defense Manager.
  Instalace klienta Symantec Endpoint Protection pro systém Mac
  Instalace aplikace Symantec Agent for Linux 14.3 RU1
- Zabraňuje novým a neznámým hrozbám v systému macOS tím, že sleduje chování téměř 1400 souborů v reálném čase. Nová aplikace Agent pro systém Mac obsahuje tyto možnosti behaviorální ochrany. Behaviorální ochrana, nebo funkce SONAR, využívá umělou inteligenci a pokročilé strojové učení pro ochranu nultého dne k účinnému zastavení nových hrozeb.
  Správa funkce SONAR
- Blokuje nedůvěryhodné nepřenosné spustitelné soubory (PE), například soubory PDF a skripty, které ještě nejsou identifikovány jako hrozba. V zásadě Výjimky klikněte na možnost **Výjimky systému Windows** > **Přístup k souboru**.
- Předvídá webové hrozby na základě skóre hodnocení webové stránky. Zásady prevence narušení zahrnují filtrování hodnocení adres URL, což blokuje webové stránky s skórem hodnocení pod určitou mezní hodnotou. Skóre hodnocení se pohybuje od -10 (špatné) do +10 (dobré). Možnost **Povolit hodnocení adres URL** je ve výchozím nastavení povolena.
- Můžete vynutit, aby aplikace Symantec Endpoint Protection získala aplikaci na základě hodnoty hash aplikace. V zásadě Výjimky klikněte na možnost **Výjimky systému Windows** > **Aplikace** > **Přidat aplikaci prostřednictvím neopakovatelného identifikátoru**.
- Chrání koncové body a uživatele před webovými útoky na škodlivých webech pomocí funkce Přesměrování síťového provozu. Přesměrování síťového provozu přesměruje veškerý síťový provoz (libovolný port) nebo pouze webový provoz (porty 80 a 443) do služby Symantec Web Security Service, která povoluje nebo blokuje síťový provoz a přístup k aplikacím SaaS na základě podnikových zásad. Zásada přesměrování síťového provozu má novou metodu přesměrování nazývanou metoda využívající tunelu. Metoda využívající tunelu automaticky přesměruje veškerý internetový provoz do služby Symantec WSS, kde je provoz povolen nebo blokován na základě zásad služby Symantec Web Security Service. Metoda využívající tunelu je považována za beta funkci. Měli byste provést důkladné testování aplikací na základě zásad služby WSS. Společnost Broadcom má beta webové stránky, které nabízí testovací průvodce a místo, kde můžete zanechat zpětnou vazbu o vašich zkušenostech. Přihlaste se na následující webové stránky pomocí přihlašovacích údajů Broadcom: Validate.broadcom.com.
  Konfigurace přesměrování síťového provozu
- Zásada integrací byla přejmenována na zásadu přesměrování síťového provozu.
- Poskytuje podporu pro události obohacené o MITRE na serveru Symantec EDR. Využijte rozhraní MITRE ATT&CK k zajištění kontextu k tomu, co se odehrává ve vašem prostředí.
- Zajišťuje podporu pro následující události Symatec EDR, které odhalují větší viditelnost do koncových bodů:
  – Události AMSI poskytují přehled o metodách aktéra hrozby, který se dokáže vyhnout tradičním metodám dotazování z příkazového řádku.
  – Události ETW poskytují přehled o událostech, ke kterých dochází ve spravovaných koncových bodech systému Windows.
- Zahrnuje možnost spuštění programu Windows Defender a aplikace Symantec Endpoint Protection ve stejném počítači. Funjce Auto-protect se spustí po programu Windows Defender a dokáže zjistit všechny hrozby, které program Windows Defender nezachytí. Možnost **Používat souběžně s aplikací Windows Defender** zajišťuje, že funkce Auto-

Protect bude spuštěna v případě, kdy je aplikace Microsoft Defender zakázána. Pokud chcete tuto možnost zakázat, klikněte na zásadu Ochrana před viry a spywarem > **Různé** > karta **Různé**.

- V případě hybridně spravovaných klientů je nyní podporováno zmírnění řetězce útoků.

Symantec Endpoint Protection Manager

- Vestavěná databáze byla aktualizována na databázi Microsoft SQL Express. Databáze SQL Server Express ukládá zásady a události zabezpečení efektivněji než výchozí vestavěná databáze a instaluje se automaticky pomocí aplikace Symantec Endpoint Protection Manager.
  Osvědčené postupy pro upgrade z vestavěné databáze na databázi Microsoft SQL Server Express
- Během instalace nebo upgradu aplikace Symantec Endpoint Protection Manager provede průvodce konfigurací serveru pro správu následující:
  - Automaticky nainstaluje obsah aktualizace LiveUpdate.
  - Poskytne možnost použití certifikátu TLS pro zabezpečenou komunikaci mezi serverem SQL Server a aplikací Symantec Endpoint Protection Manager.
- Aktualizace LiveUpdate používá nový modul v aplikaci Symantec Endpoint Protection Manager, který je optimalizován pro spuštění v cloudové konzoli.
  Poznámky k verzi a nové opravy nástroje LiveUpdate Administrator
- Možnost **Automaticky odinstalovat stávající bezpečnostní software třetích stran**, která nebyla ve verzi 14.3 MP1 k dispozici, je opět dostupná ve verzi 14.3 RU1 s aktualizovanou verzí. Tato možnost slouží k odinstalování bezpečnostního softwaru jiných výrobců. Pokud chcete získat přístup k této možnosti, klikněte na stránku **Správce** > **Balíčky** > **Nastavení instalace klienta**.
  Odebrání bezpečnostního softwaru třetích stran v aplikaci Endpoint Protection 14
  Odebrání bezpečnostního softwaru třetích stran v aplikaci Endpoint Protection 14.3 RU1
- Průvodce zavedením klienta, který se používá k zavedení klientských balíčků, musí mít ověřené přihlašovací údaje a musí se připojit k aplikaci Symantec Endpoint Protection Manager. Pokud se proces ověření nezdaří, proces zavedení klienta se zastaví, aby se zabránilo uzamčení uživatelských účtů služby Active Directory.
  Instalace klientů aplikace Symantec Endpoint Protection pomocí vzdáleného odeslání
- Protokoly a zprávy o stavu počítače nyní umožňují vybrat rozsah polí **Verze klienta** a **Verze IPS**. Filtr **Verze produktu** byl přejmenován na **Verze klienta**.
- Možnost **Zakázat ikonu v oznamovací oblasti** je k dispozici pro klienty, kteří jsou spuštěni na terminálovém serveru a kteří způsobují vysoké využití procesoru a paměti. Nyní můžete zakázat ikonu v oznamovací oblasti, známou také jako ikona na hlavním panelu, abyste zabráli spuštění více instancí procesů uživatelských relací (například SmcGui.exe a ccSvcHost.exe). Tuto možnost povolíte v možnosti **Klienti** > karta **Zásady** > **Nastavení zabezpečení** > karta **Obecné**.
- Byl aktualizován režim seznamu povolených a zakázaných položek tak, aby odrážel funkci povolení a blokování. Na stránce **Klienti** > karta **Zásady** > dialogovém okně **Uzamčení systému** se seznamy souborů aplikací změnily z **režimu seznamu povolených položek** a **režim seznamu zakázaných položek** listiny na **Režim povolení** a **Režim odmítnutí**.
- Na stránce **Správce** > karta **Servery** > **Konfigurovat externí protokolování** > karta **Obecné** se možnost **Hlavní server protokolování** změnila na **Primární server protokolování**.
- Typ protokolu **Systém** > protokol **Správy** a protokol **Auditu** uvádí název počítače.
- Protokoly brány firewall klienta jsou shromažďovány tak, abyste v cloudové konzoli dostávali méně oznámení.
- Jazyk Oracle Java SE byl nahrazen jazykem OpenJDK.
- Součásti JQuery třetích stran byly aktualizovány na novější verzi.

Aktualizace klienta a platformy

- Klient se systémem Windows podporuje systém Windows 10 20H2 (Windows 10 verze 2009).
- Klient pro systém Mac podporuje verzi macOS 10.15.7.
- Starší instalační balíčky klienta pro systém Mac byly přesunuty do složky Další balíčky.

Funkce odstraněny

- Možnosti **Závažnost rizika** a **Rozložení rizik podle závažnosti** byly z oznámení a zpráv odebrány.
- Karta **CASMA** a příkaz **Analyzovat** byly odebrány, protože tato funkce ve verzi 14.3 zastarala.
- Klient pro systém Mac již nepodporuje verzi macOS 10.13.

Dokumentace

Nápověda k aplikaci Symantec Endpoint Protection Manager je nyní online a nachází se na adrese: Příručka pro instalaci a správu aplikace Symantec Endpoint Protection Installation.

Schéma databáze

Schéma databáze prošlo následujícími změnami.

Tabulka	Změna sloupce
VÝSTRAHY	Byl přidán sloupec ENRICHED_DATA.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA PŘÍKAZ COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG ZPRÁVY SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Z každé tabulky byly odebrány následující sloupce: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabulka	Změna sloupce
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• Typ sloupce CONTENT se změnil z ‚image' na ‚varbinary'. • Byl přidán indexovaný sloupec FILESTREAM_ID. • Byl přidán index FILESTREAM_ID. • Následující sloupce byly odebrány: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Následující sloupce byly přidány: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• Byl přidán sloupec NTR_MESSAGE. • Následující sloupce byly odebrány: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Následující sloupce byly přidány: • VERZE • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Následující sloupce byly odebrány: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Byl přidán sloupec ENRICHED_DATA.

Novinky ve všech vydáních aplikace Symantec Endpoint Protection

Známé problémy a řešení pro aplikaci Symantec Endpoint Protection

Položky uvedené v této části se týkají této verze aplikace Symantec Endpoint Protection.

Table 1: Problémy s upgradem

Problém	Popis a řešení
Aplikace Symantec Endpoint Protection Manager ve vnitřní síti stahuje starý obsah systému CIDS (Client Intrusion Detection System) do nových klientů, protože aktualizace LiveUpdate během upgradu [14.3 RU1] neběží.	Pokud aplikace Symantec Endpoint Protection Manager verze 14.3 RU1 nemůže získat přístup k internetu nebo serveru LUA (LiveUpdate Administrator), zachová v mezipaměti starý, nekompatibilní obsah. Tento starý obsah se obvykle doručuje do nových klientů. Pokud chcete aktualizovat obsah v mezipaměti serveru pro správu, ručně stáhněte certifikované definice virů a soubory .jdb systému CIDS. [SEP-69125] Pokud chcete zajistit, aby noví klienti nedostávaly starý obsah, nainstalujte ručně soubor .jdb systému CIDS do aplikace SEPM předtím, než provedete instalaci nových klientů nebo upgrade starých klientů. Stažení souborů JDB pro aktualizaci definic pro aplikaci Endpoint Protection Manager
Když je karta síťového rozhraní zakázána [14.3 RU1], nelze se přihlásit k aplikaci Symantec Endpoint Protection Manager (SEPM)	Pokud se po instalaci aplikace Symantec Endpoint Protection Manager nemůžete přihlásit ke konzoli a zobrazí se následující chybová zpráva: `Neočekávaná chyba serveru` K tomuto problému může dojít, pokud je při instalaci aplikace SEPM zakázána karta síťového rozhraní počítače, což zabraňuje vygenerování certifikátu serveru. [SEP-67040] Pokud chcete zjistit, zda byla aplikace SEPM nainstalován se zakázanou kartou síťového rozhraní, podívejte se na certifikát serveru. Viz: Instalace aplikace SEPM se nezdaří, pokud nejsou k dispozici žádná síťová připojení.
Při odinstalaci aplikace SEPM a použití možnosti k odebrání výchozí databáze a opuštění instance serveru SQL Server Express se zobrazí následující chyba: „`Při pokusu o připojení k databázovému serveru došlo k chybě`“	Pokud odinstalujete aplikaci Symantec Endpoint Protection Manager a vyberete možnost **Odstranit pouze databázi a ponechat instanci serveru SQL Server Express instance nainstalovanou s aplikací SEPM**, může se zobrazit následující chyba: „`Při pokusu o připojení k databázovému serveru došlo k chybě`“. K tomuto problému dochází po přidání přihlašovacích údajů pro výchozí uživatelské DBA a může souviset s uživatelskými oprávněními. [SEP-68670] Pokud chcete tento problém vyřešit, proveďte odinstalaci spuštěním souboru setup.exe aplikace SEPM a během odinstalace klikněte na tlačítko **Odstranit pouze databázi a ponechat instanci serveru SQL Server Express instance nainstalovanou s aplikací SEPM**.

Problém	Popis a řešení
Upgrade serveru SQL Server z verze 2017 na verzi 2019 se nezdaří s povoleným režimem FIPS [14.3]	Může se zobrazit chyba: „Došlo k následující chybě. Při instalaci rozšiřující funkce došlo k chybě s chybovou zprávou: Vytvoření AppContainer se nezdařilo s chybovou zprávou NONE, state. Tato implementace není součástí ověřených kryptografických algoritmů FIPS na platformě Windows.“ K tomu dochází, pokud máte aplikaci Symantec Endpoint Protection Manager 14.3 s podporou FIPS a upgradujete z Microsoft SQL Server 2017 na 2019. [SEP-61473] Chcete-li tento problém vyřešit, zakažte FIPS na úrovni operačního systému: 1. Ve složce `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools` klikněte na možnost **Místní zásady zabezpečení** > **Místní zásady** > **Možnosti zabezpečení** a deaktivujte možnost **Systémová kryptografie: Používat algoritmy kompatibilní s FIPS k šifrování, hashování a podepisování** 2. Upgrade SQL Serveru z verze 2017 na verzi 2019. 3. Po úspěšném upgradu SQL Serveru znovu povolte FIPS. Upgrade SQL z verze 2017 na 2019 se nezdaří s povoleným režimem FIPS
Vlastní názvy mohou během upgradu na verzi 14.2 nebo novější zabránit dokončení aktualizace zásad brány firewall	V případě upgradu na aplikaci Symantec Endpoint Protection verze 14.2 nebo novější nemohou zásady brány firewall při změně některých výchozích názvů řádně reagovat na změny IPv6. Výchozím názvem je myšlen název výchozích zásad a výchozích pravidel. Pokud během upgradu nedojde k aktualizaci pravidel, možnosti IPv6 se nezobrazí. Na pravidla nově vytvořená po upgradu se tento problém nevztahuje. Pokud to bude možné, vraťte veškeré upravené názvy zpět do výchozí podoby. V opačném případě se ujistěte, že žádná vlastní pravidla, která přidáte do výchozí zásady, nebudou žádným způsobem blokovat komunikaci IPv6. To samé platí pro nově přidané zásady a pravidla.

Table 2: Problémy s aplikací Symantec Endpoint Protection Manager

Problém	Popis a řešení
Některé události EDR se v klientovi [14.3 RU1] nezobrazují.	Klient aplikace Symantec Endpoint Protection musí používat systém Windows 10 build 14393 nebo novější ke shromažďování trasování událostí Symantec EDR pro události pro Windows (ETW). [SEP-67175]
Funkce Přesměrování síťového provozu má určitá omezení [14.3 RU1].	• Služba Symantec Web Security Service je doručována v protokolu IPv4 a nikoli v protokolu IPv6. [SEP-68700] • Metoda přesměrování tunelu: – Běží pouze v systému Windows 10 x64 verze 1703 a novější (kanál pro půlroční údržbu). Tato metoda nepodporuje žádné jiné operační systémy Windows nebo klienta se systémem Mac. [SEP-67927] – Nepodporuje 64bitová zařízení s podporou HVCI systému Windows 10. [SEP-67648] – Přesměruje odchozí provoz z klienta aplikace Symantec Endpoint Protection do služby WSS dříve, než bude vyhodnocen pomocí brány firewall klienta nebo pravidel pro hodnocení adres URL. Místo toho bude tento provoz vyhodnocen na základě pravidel brány firewall služby WSS a pravidel adresy URL. Pokud například pravidlo brány firewall klienta aplikace SEP zablokuje web google.com a pravidlo služby WSS google.com povolí, klient uživatelům přístup na web google.com umožní. Příchozí místní provoz do klienta bude stále zpracovávána bránou firewall aplikace Symantec Endpoint Protection. [SEP-67488] – Portál Captive služby WSS není k dispozici pro metodu využívající tunelu a klient ignoruje přihlašovací údaje výzvy. V budoucí verzi ověřování SAML v agentovi služby WSS nahradí portál Captive a bude k dispozici v klientovi aplikace Symantec Endpoint Protection. – Pokud se klientský počítač připojí ke službě WSS pomocí metody využívající tunelu a hostuje virtuální počítače, musí každý uživatel typu Host nainstalovat certifikát SSL, který je k dispozici na portálu WSS. – Provoz pro místní sítě, jako je domácí adresář nebo ověřování služby Active Directory, není přesměrován. Metoda využívající tunelu je v současné době považována za beta funkci.
Duplicitní položky registrace agenta po upgradu z verze 14.2.x na verzi 14.3 MP1 a novější [14.3 RU1]	Upgrade klientů aplikace Symantec Endpoint Protection z verze 14.2.x na verzi 14.3 MP1 a novější vytvoří duplicitní položky registrace agenta těchto klientů na stránce **Zařízení** v aplikaci Symantec Endpoint Protection Manager. Není zde žádný funkční dopad, takže můžete pokračovat v práci s novými položkami pro klienty verze 14.3 RU1. Aplikace Symantec Endpoint Protection Manager odebere starší položky agenta.
Pokud používáte možnost hybridní správy, servery proxy nebo obvodovou bránu firewall, povolte adresy URL v aplikaci Symantec Endpoint Security [14.3].	V důsledku akvizice produktu Symantec Enterprise Security společností Broadcom se ve verzi 14.2.2.1 změnily adresy URL ke komunikaci mezi klientem a cloudem. [CDM-42467] Klienty je nutné upgradovat na verzi sestavení 14.2.5569.2100 nebo novější v následující situaci • Používáte produkt Symantec Endpoint Security ke správě svých klientů a zásad, když jsou vaše místní domény Symantec Endpoint Protection Manager zaregistrované v cloudové konzoli. • Používáte servery proxy. Povolíte adresy URL v agentech, kteří jsou buď plně spravovaní v cloudu, nebo hybridně spravovaní, povolíte server proxy nebo obvodovou bránu firewall. Viz: Adresy URL, které povolují připojení aplikací SEP a SES k serverům společnosti Symantec Viz část Upgrade agentů Symantec s cloudovou správou na verzi 14.2 RU2 MP1 a novější.

Problém	Popis a řešení
Vzdálená konzole aplikace Symantec Endpoint Protection Manager již nepodporuje 32bitovou platformu Windows [14.3]	Ve verzi 14.3 a novějších se nelze přihlásit k vzdálené konzoli aplikace Symantec Endpoint Protection Manager, pokud používáte 32bitovou verzi systému Windows. Prostředí Oracle Java SE Runtime Environment již nepodporuje 32bitové verze systému Microsoft Windows. [SEP-61106] Pokud se zobrazí následující zpráva, přihlaste se k aplikaci Symantec Endpoint Protection Manager z místního počítače: „Tato verze programu C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe není kompatibilní s verzí systému Windows, kterou používáte. Zkontrolujte informace o systému počítače a obraťte se na vydavatele softwaru.“
Při instalaci aplikace Symantec Endpoint Protection Manager [14.3] se zobrazí chyba „Instalace modulu Microsoft Visual C++ Runtime se nezdařila“	Při instalaci aplikace Symantec Endpoint Protection Manager v systému Windows 2012 R2 se může zobrazit následující chyba: „Nepodařilo se nainstalovat modul Microsoft Visual C++ Runtime“ [SEP-60396] Chcete-li tento problém vyřešit, aktivujte systém Windows a nainstalujte aktualizace systému Windows. Aktualizace Windows nainstaluje balíček Visual C++ 2017 Redistributable, což je předpokladem k instalaci aplikace Symantec Endpoint Protection Manager 14.3 v systému Windows 2012 R2.
Nelze povolit TLS 1.1 a TLS 1.2 jako výchozí zabezpečovací protokoly ve WinHTTP v systému Windows [14.3]	Po upgradu nebo instalaci aplikace Symantec Endpoint Protection Manager verze 14.3, která je zaregistrovaná do cloudové konzole, již server pro správu nenahrává úspěšně protokoly do cloudu. V souboru uploader.log se může zobrazit následující chyba: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Tento problém je způsoben chybějící aktualizací společnosti Microsoft, která poskytuje podporu pro TLS 1.1 a 1.2. Chcete-li tento problém vyřešit, nainstalujte aktualizaci společnosti Microsoft: KB3140245. Další informace viz: Nelze povolit TLS 1.1 a TLS 1.2 jako výchozí zabezpečovací protokoly ve WinHTTP v systému Windows
Poté, co klient obdrží aktualizované zásady ochrany proti hrozbám v aplikaci Endpoint pro službu AD [14.2 RU1 MP1 a novější] se v aplikaci Symantec Endpoint Protection Manager stále zobrazuje zpráva „Zavedení probíhá“.	Toto chování je běžné. Zásady aplikace Ochrana proti hrozbám v aplikaci Endpoint pro AD 3.3 jsou podporovány na straně klienta od verze 14.2 RU1 MP1. Použijete zásady ochrany proti hrozbám v aplikaci Symantec Endpoint pro službu Active Directory 3.3 na skupinu. Tato skupina obsahuje některé klienty, kteří používají aplikaci Symantec Endpoint Protection 14.2 RU1 nebo starší. Tito klienti přijímají a používají zásady podle očekávání, ale stav v aplikaci Symantec Endpoint Protection Manager stále zobrazuje zprávu Zavedení probíhá.

Table 3: Problémy s klienty systému Windows, Mac a Linux

Problém	Popis a řešení
Nesprávné zprávy v aplikaci Symantec Agenta týkající se protokolu instalačního programu systému Linux. [Verze 14.3 RU1]	V některých případech instalační program agenta protokoluje nesprávné zprávy související s neodpovídající verzí ovladače nebo požadovaným restartem. Tyto zprávy nemají vliv na funkčnost agenta.
Na zařízení se systémem SuSe Linux zypper odstraní balíčky klienta aplikace SEP se systémem Linux při odstraňování balíčku ‚at‘. [Verze 14.3 RU1]	Na zařízení se systémem SuSe Linux příkaz 'zypper remove at' odebere balíčky klienta aplikace SEP se systémem Linux, protože balíček ‚at‘ je přidán jako požadovaný závislý balíček a příkazy zypper se automaticky pokusí odebrat balíčky klienta aplikace SEP ‚sdcss-kmod‘ a ‚sdcss-sepagent‘ jako balíčky s nepoužívanými závislostmi. **Řešení:** Pokud chcete balíček ‚at‘ odebrat, spusťte následující příkaz: rpm -e --nodeps at

Problém	Popis a řešení
Problém s upgradem v systému macOS 10.15 a novějším [verze 14.3 MP1]	V systému macOS 10.15 a novějším se funkci **Instalovat aplikaci Symantec Endpoint Protection do vzdálených počítačů** v Průvodci zavedením klienta nepodaří upgradovat klienta aplikace Symantec Endpoint Protection ze starších verzí na verzi 14.3 MP1. **Řešení:** Použijte možnost **Automatický upgrade aplikace Symantec Endpoint Protection Manager** a proveďte upgrade klienta aplikace Symantec Endpoint Protection v systému macOS 10.15 a novějším.
Instalace klienta aplikace Symantec Endpoint Protection 14.3 pro systém Windows může selhat, pokud nejprve nenainstalujete podporu SHA-2 [14.3]	Pokud používáte starší verze operačního systému (Windows 7 RTM nebo SP1, Windows Server 2008 R2 nebo R2 SP1 nebo R2 SP2), je nutné mít na svých zařízeních nainstalovanou podporu podepisování kódu SHA-2, abyste mohli instalovat aktualizace systému Windows vydané od července 2019. Bez podpory SHA-2 se instalace klienta systému Windows občas nezdaří. Instalace může selhat bez ohledu na to, zda klienty instalujete poprvé nebo provádíte automatický upgrade z předchozí verze. [SEP-61175/61403] Chcete-li získat podporu podepisování kódu SHA-2 společnosti Microsoft, přečtěte si následující informace: Požadavky na podporu podepisování kódu SHA-2 od roku 2019 pro Windows a WSUS Instalace klienta Symantec Endpoint Protection 14.3 pro systém Windows může selhat, pokud není nainstalována podpora SHA-2
Klient Symantec Endpoint Protection pro systém Windows při instalaci v systému Windows 10 1803 s povolenou technologií UWF [14.3] se nespouští	Pokud je klient Symantec Endpoint Protection spuštěn v 32bitovém operačním systému Windows 10 RS4 1803, když je povolena technologie UWF (Unified Write Filter) a používá se k ochraně jednotky, na které je nainstalován klient systému Windows, nepracuje klient správně. Tento operační systém Windows obsahuje závadu UWF, která brání spuštění klienta systému Windows. Chcete-li tento problém vyřešit: • Proveďte upgrade na jinou verzi operačního systému, která neobsahuje vadu. • Zakažte UWF. Další informace: Aplikace Endpoint Protection nefunguje správně, když je nainstalovaná v systému Windows 10 1803 s povolenou technologií UWF
Klienti pro systém Mac, kteří povolují přesměrování přenosů služby WSS, nerespektují uživatelské nastavení proxy pro službu LiveUpdate [14.2 RU1 MP1 a novější]	Své spravované klienty systému Mac jste nakonfigurovali pro aplikaci Symantec Endpoint Protection 14.2 RU1 MP1 nebo novější tak, aby používali uživatelské nastavení proxy pro službu LiveUpdate pomocí možnosti Nastavení externí komunikace. Po povolení přesměrování přenosů služby WSS (WTR) pro své klienty systému Mac pomocí zásad aplikace Symantec Endpoint Protection Manager nicméně zjistíte, že přenos služby LiveUpdate nadále nerespektuje vaše uživatelské nastavení proxy. Místo toho se služba LiveUpdate pokouší o přímé připojení. Chcete-li tento problém vyřešit, použijte pouze uživatelské nastavení serveru proxy pro službu LiveUpdate při zakázaném přesměrování přenosů služby WSS.
Prohlížeč Microsoft Edge neočekávaně umožňuje stahovat soubory PDF při povoleném posílení zabezpečení [verze 14.2 RU1 MP1 a novější]	Při použití prohlížeče Microsoft Edge můžete v klientovi Symantec Endpoint Protection s povoleným posílením zabezpečení neočekávaně stahovat soubory PDF. Při používání ostatních prohlížečů funguje prevence stahování souborů PDF očekávaným způsobem. Oprava tohoto problému bude k dispozici v další verzi.

V souvislosti nedávným oznámením společnosti Broadcom, že se společnost Symantec Enterprise Protection oficiálně připojila k společnosti Broadcom, společnost Symantec provedla migraci dokumentace na portál Broadcom Symantec Security Tech Docs Portal.

Pokud hledáte dokumentaci produktu Endpoint Protection, klikněte na kartu **Symantec Security Software** a potom na tlačítko **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Problémy s dokumentací

Problém	Popis a řešení
Články s postupy vypršely.	Články s postupy, které tvořily duplicitní témata v nápovědě aplikace Symantec Endpoint Protection Manager, byly znovu publikovány na webu Endpoint Protection a nyní mají jinou adresu URL. Chcete-li článek vyhledat, použijte **vyhledávací pole**.
Soubory PDF	Společnost Symantec zveřejnila všechny soubory PDF v článcích DOC. Platnost těchto stránek vypršela. Chcete-li najít nejnovější verzi souboru PDF, přejděte na stránku Související dokumenty. V budoucnu bude společnost Broadcom přidávat starší soubory PDF a přeložené soubory PDF.

Vyřešené problémy naleznete v tématu:

Nové opravy a součásti pro aplikaci Symantec Endpoint Protection 14.3 RU1

Nové opravy a součásti pro aplikaci Symantec Endpoint Protection 14.3 MP1

Nové opravy a součásti pro aplikaci Symantec Endpoint Protection 14.3

Systémové požadavky na aplikaci Symantec Endpoint Protection (SEP)

Obecně jsou požadavky na systém následující aplikace stejné jako požadavky na operační systémy, ve kterých jsou tyto aplikace podporovány.

> **NOTE**
> Starší verze aplikace Symantec Endpoint Protection Manager nemusí být schopna správně spravovat klienta s novější verzí. Mohou nastat problémy s aktualizacemi obsahu a správou klienta. Například aplikace Symantec Endpoint Protection Manager 14.0.1 nebo starší nemůže správně poskytovat klientovi verze 14.2 jeho zástupné názvy specifické pro danou verzi. Aplikace Symantec Endpoint Protection Manager pro verze starší než 14 MP2 nemůže správně poskytovat klientům s verzí novější než 14.0.1 jejich zástupné názvy specifické pro danou verzi.

Následující tabulky obsahují požadavky na software a hardware pro aplikaci Symantec Endpoint Protection.

Table 5: Systémové požadavky softwaruSymantec Endpoint Protection Manager (SEPM)

Součást	Požadavky
Operační systém	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Operační systémy pro stolní počítače nejsou podporovány. **Note:** Edice Windows Server Core není podporována ve verzi 14.2x a starších.
Webový prohlížeč	Pro přístup k webové konzole aplikace Symantec Endpoint Protection Manager a zobrazení nápovědy aplikace Symantec Endpoint Protection Manager jsou podporovány následující prohlížeče: • Prohlížeč Microsoft Edge na základě prohlížeče Chromium (verze 14.3 a novější) • Microsoft Edge Poznámka: 32bitová verze systému Windows 10 nepodporuje v prohlížeči Edge přístup k webové konzole. • Microsoft Internet Explorer 11 (verze 14.2.x a starší) • Mozilla Firefox 5.x do verze 83 • Google Chrome 87

Součást	Požadavky
Databáze	Aplikace Symantec Endpoint Protection Manager zahrnuje výchozí databázi: • Microsoft SQL Server Express 2014 (pro Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Vestavěná databáze Sybase (pouze verze 14.3 MP.x a starší) Místo toho můžete použít databázi z jedné z následujících verzí serveru Microsoft SQL Server: • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM – SP4 • SQL Server 2014 RTM – SP3 • SQL Server 2016, RTM, SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (verze 14.3 a novější) **Note:** Podporovány jsou databáze SQL Server hostované ve službě Amazon RDS (od verze 14.0.1 MP2). **Note:** Pokud aplikace Symantec Endpoint Protection využívá databázi SQL Server a vaše prostředí využívá pouze protokol TLS 1.2, ověřte, zda SQL Server podporuje protokol TLS 1.2. Možná budete muset použít opravu systému SQL Server. Toto doporučení se vztahuje na SQL Server 2008, 2012, a 2014. Bez opravy systému SQL Server pro účely podpory protokolu TLS 1.2 může dojít k problémům při provádění upgradu z aplikace Symantec Endpoint Protection verze 12.1 na verzi 14. **Note:** Podpora TLS 1.2 pro Microsoft SQL Server
Další požadavky na prostředí	V sítích, kde se používá pouze protokol IPv6, musí být také nainstalován a deaktivován zásobník IPv4. Pokud je zásobník IPv4 odinstalován, nebude aplikace Symantec Endpoint Protection Manager fungovat.

Table 6: Hardwarové požadavky aplikace Symantec Endpoint Protection Manager

Součást	Požadavky
Procesor	Minimálně procesor Intel Pentium Dual-Core nebo obdobný, doporučen alespoň osmijádrový procesor **Note:** Procesory Intel Itanium IA-64 podporovány nejsou.
Fyzická paměť RAM	Minimálně 2 GB volné paměti RAM, doporučeno 8 GB nebo více **Note:** V závislosti na požadavcích ostatních již nainstalovaných aplikací na paměť RAM může server aplikace Symantec Endpoint Protection Manager vyžadovat další volnou paměť RAM. Pokud je na serveru aplikace Symantec Endpoint Protection Manager například nainstalován systém Microsoft SQL Server, mělo by být na serveru k dispozici minimálně 8 GB paměti.
Displej	1024 x 768 nebo více
Pevný disk v případě instalace na systémovou jednotku	S místní databází SQL Server: • Minimálně 40 GB volného místa (doporučeno 200 GB) pro server pro správu a databázi Se vzdálenou databází serveru SQL Server: • Minimálně 40 GB volného místa (doporučeno 100 GB) pro server pro správu • Další volné místo na disku vzdáleného serveru pro databázi

Součást	Požadavky
Pevný disk v případě instalace na alternativní jednotku:	S místní databází SQL Server: • Minimálně 15 GB volného místa na systémové jednotce (doporučeno 100 GB) • Minimálně 25 GB volného místa na instalační jednotce (doporučeno 100 GB) Se vzdálenou databází serveru SQL Server: • Minimálně 15 GB volného místa na systémové jednotce (doporučeno 100 GB) • Minimálně 25 GB volného místa na instalační jednotce (doporučeno 100 GB) • Další volné místo na disku vzdáleného serveru pro databázi
Ostatní	Povolená karta síťového rozhraní

Pokud používáte databázi SQL Server, může být potřeba více volného místa na disku. Množství dalšího požadovaného místa a jeho umístění závisí na jednotce používané serverem SQL Server, požadavcích na údržbu databáze a dalších nastaveních databáze.

Table 7: Softwarové požadavky na systém klienta Symantec Endpoint Protection pro systém Windows

Součást	Požadavky
Operační systém (stolní počítač)	• Windows 7 (32bitová verze, 64bitová verze, RTM a SP1) • Windows Embedded 7 Standard, POSReady a Enterprise (32bitová a 64bitová verze) • Windows 8 (32bitová verze, 64bitová verze) • Windows Embedded 8 Standard (32bitová a 64bitová verze) • Windows 8.1 (32bitová verze, 64bitová verze), včetně funkce Windows To Go • Windows 8.1, aktualizace z dubna 2014 (32bitová verze, 64bitová verze) • Windows 8.1, aktualizace ze srpna 2014 (32bitová verze, 64bitová verze) • Windows Embedded 8.1 Pro, Industry Pro a Industry Enterprise (32bitová a 64bitová verze) • Windows 10 (1507) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (1511) (32bitová verze, 64bitová verze) • Windows 10 Anniversary Update (1607) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (1703) (32bitová verze, 64bitová verze) • Windows 10 Fall Creators Update (1709) (32bitová verze, 64bitová verze) • Windows 10 April 2018 Update (1803) (32bitová verze, 64bitová verze) • Windows 10, aktualizace z října 2018 (1809) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2019 LTSC • Windows 10, aktualizace z května 2019 (1903) (32bitová verze, 64bitová verze) • Windows 10, aktualizace z listopadu 2019 (verze 1909) (32bitová verze, 64bitová verze) (verze 14.2 RU1 a novější) • Windows 10 20H1 (Windows 10 verze 2004) (verze 14.3 a novější) • Windows 10 20H2 (Windows 10 verze 2009) (od verze 14.3 RU1)
Operační systém (server)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2, aktualizace z dubna 2014 • Windows Server 2012 R2, aktualizace ze srpna 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, verze 1803 (Server Core) (14.2 a novější) • Windows Server, verze 1809 (Server Core) • Windows Server, verze 1903 (Server Core) (14.2 RU1 a novější) • Windows Server, verze 1909 (Server Core) (verze 14.2 RU1 a novější) • Windows Server, verze 2004 • Windows Server, verze 20H2 (verze 14.3 RU1)
Prevence narušení prohlížeče	Podpora prevence narušení prohlížeče závisí na verzi systému zjištění narušení klienta (CIDS). Viz téma Supported browsers for Browser Intrusion Prevention in Endpoint Protection (Podporované prohlížeče pro prevenci narušení prohlížeče v aplikaci Endpoint Protection).

Table 8: Hardwarové požadavky na systém klienta Symantec Endpoint Protection pro systém Windows

Součást	Požadavky
Procesor (fyzické počítače)	• 32bitový procesor: 2 GHz Intel Pentium 4 nebo ekvivalent (Intel Pentium 4 nebo ekvivalent) • 64bitový procesor: 2 GHz Pentium 4 s podporou x86-64 nebo ekvivalent **Note:** Nejsou podporovány procesory Itanium.
Procesor (virtuální počítače)	Minimálně jeden virtuální soket a jedno jádro na soket s frekvencí 1 GHz (doporučuje se jeden virtuální soket a dvě jádra na soket s frekvencí 2 GHz) **Note:** Je nutné povolit vyhrazení prostředků hypervisoru.
Fyzická paměť RAM	1 GB paměti (doporučeno 2 GB) nebo více, pokud to vyžaduje operační systém
Displej	800 x 600 nebo více
Pevný disk	Požadavky na místo na disku závisí na typu instalovaného klienta, instalační jednotce a umístění dat programu. Složka dat programu se obvykle nachází na systémové jednotce ve výchozím umístění C:\ProgramData. Bez ohledu na zvolenou instalační jednotku je vždy potřeba volné místo na systémové jednotce. **Note:** Požadavky na prostor vycházejí ze souborových systémů NTFS. Další místo je potřeba pro aktualizace obsahu a protokoly.

Table 9: Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na systémovou jednotku

Typ klienta	Požadavky
Standardní klient	V případě umístění složky dat programu na systémové jednotce: • 395 MB* V případě umístění složky dat programu na alternativní jednotce: • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 350 MB
Klient Embedded nebo VDI	V případě umístění složky dat programu na systémové jednotce: • 245 MB* V případě umístění složky dat programu na alternativní jednotce: • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 200 MB
Klient vnitřní sítě	V případě umístění složky dat programu na systémové jednotce: • 545 MB* V případě umístění složky dat programu na alternativní jednotce: • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 500 MB

* Během instalace je vyžadováno dalších 135 MB místa.

Table 10: Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na alternativní jednotku

Typ klienta	Požadavky
Standardní klient	V případě umístění složky dat programu na systémové jednotce: • Systémová jednotka: 380 MB • Alternativní instalační jednotka: 15 MB* V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 350 MB • Alternativní instalační jednotka: 150 MB
Klient Embedded nebo VDI	V případě umístění složky dat programu na systémové jednotce: • Systémová jednotka: 230 MB • Alternativní instalační jednotka: 15 MB* V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 200 MB • Alternativní instalační jednotka: 150 MB
Klient vnitřní sítě	V případě umístění složky dat programu na systémové jednotce: • Systémová jednotka: 530 MB • Alternativní instalační jednotka: 15 MB* V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 500 MB • Alternativní instalační jednotka: 150 MB

* Během instalace je vyžadováno dalších 135 MB místa.

** Pokud se složka dat programu nachází na alternativní instalační jednotce, připočítejte v celkovém součtu 15 MB k jednotce se složkou dat programu. Instalační program však bude během instalace stále potřebovat 150 MB volného místa na alternativní instalační jednotce.

Table 11: Požadavky na systém klienta Symantec Endpoint Protection pro systém Windows Embedded

Součást	Požadavky
Procesor	Intel Pentium 1 GHz
Fyzická paměť RAM	256 MB **Note:** Tato cifra je určena pro instalaci vloženého klienta Symantec Endpoint Protection. Pokud současně implementujete dodatečné funkce z integrovaného řešení, jako je služba EDR, může být zapotřebí více fyzické paměti RAM.
Pevný disk	Klient Symantec Endpoint Protection Embedded a VDI vyžaduje následující množství volného místa na pevném disku: • V případě instalace na systémovou jednotku: 245 MB • V případě instalace na alternativní jednotku: 230 MB na systémové jednotce a 15 MB na alternativní jednotce Během instalace je potřeba dalších 135 MB místa. Tyto údaje předpokládají umístění složky dat programu na systémové jednotce. Podrobnější informace a požadavky jiných typů klientů naleznete v požadavcích na systém klienta Symantec Endpoint Protection pro systém Windows.

Součást	Požadavky
Operační systém Embedded	• Windows Embedded Standard 7 (32bitová a 64bitová verze) • Windows Embedded POSReady 7 (32bitová a 64bitová verze) • Windows Embedded Enterprise 7 (32bitová a 64bitová verze) • Windows Embedded 8 Standard (32bitová a 64bitová verze) • Windows Embedded 8.1 Industry Pro (32bitová a 64bitová verze) • Windows Embedded 8.1 Industry Enterprise (32bitová a 64bitová verze) • Windows Embedded 8.1 Pro (32bitová a 64bitová verze)
Minimální požadované součásti systému	• Správce filtrů (FltMgr.sys) • Podpora sledování výkonu (pdh.dll) • Instalační služba systému Windows
Šablony	• Application Compatibility (výchozí) • Digital Signage • Industrial Automation • IE, Media Player, RDP • Set Top Box • Thin Client Šablona Minimum Configuration není podporována. Sjednocený filtr zápisu (UWF) ani rozšířený filtr zápisu (EWF) nejsou podporovány. Doporučuje se, aby souborový filtr zápisu (FBWF) byl nainstalován spolu s filtrem registru.

Table 12: Požadavky na systém klienta Symantec Endpoint Protection pro systém Mac

Součást	Požadavky
Procesor	64bitový procesor Intel Core 2 Duo nebo novější
Fyzická paměť RAM	2 GB paměti RAM
Pevný disk	1 GB pevného disku k dispozici pro instalaci
Displej	800 x 600
Operační systém	• macOS 10.14 macOS 10.14.5 a novější podporují požadavky na notářskou úpravu kext. Viz Endpoint Protection 14.2 RU1 a notarizace kext pro systém macOS 10.14.5. • macOS 10.15 až 10.15.7 Seznam podporovaných operačních systémů u předchozích vydání najdete v tématu Kompatibilita počítače Mac s klientem Endpoint Protection

Table 13: Požadavky na systém klienta Symantec Endpoint Protection pro systém Linux

Součást	Požadavky
Hardware	• Procesor Intel Pentium 4 (2 GHz) nebo novější • 500 MB paměti RAM • 2 GB volného místa na disku, pokud adresáře /var, /opt a /tmp sdílejí stejný souborový systém/svazek • 500 MB volného místa na disku v každém adresáři /var, /opt a /tmp, pokud jsou na různých svazcích
Operační systémy	Podporované operační systémy od verze 14.3 RU1: • Amazon Linux 2 • CentOS 6.x, 7.x, 8.x • Oracle Enterprise Linux 6.x, 7.x, 8.x • Red Hat Enterprise Linux 6.x, 7.x, 8.x • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Podporované operační systémy pro verzi 14.3 a starší: • Amazon Linux • CentOS 6U3–6U9, 7–7U7, 8; 32bitová a 64bitová verze • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32bitová a 64bitová verze • Fedora 16, 17; 32bitová a 64bitová verze • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2–6U9, 7–7U8, 8–8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 – 11 SP4, 32bitová a 64bitová verze; 12, 12 SP1, 12 SP3, 64bitová verze • SUSE Linux Enterprise Desktop (SLED) 11 SP1 – 11 SP4, 32bitová a 64bitová verze; 12 SP3, 64bitová verze • Ubuntu 12.04, 14.04, 16.04, 18.04 (od verze 14.3); 32bitová a 64bitová verze Seznam podporovaných jader operačního systému pro předchozí verze naleznete v tématu List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x (Seznam linuxových distribucí a jader s předkompilovanými ovladači/moduly funkce Auto-Protect pro aplikaci Symantec Endpoint Protection pro Linux 14.x.
Grafická počítačová prostředí	K zobrazení klienta Symantec Endpoint Protection pro systém Linux můžete použít následující grafická prostředí: • KDE • Gnome • Unity Aplikace Symantec Agent pro systém Linux verze 14.3 RU1 nemá grafické uživatelské rozhraní.

Součást	Požadavky

Další požadavky na prostředí (verze 14.3 MP1 a starší)	• Glibc
	Nejsou podporovány operační systémy, které používají knihovnu glibc verze 2.6 nebo starší.
	• net-tools nebo iproute2
	Aplikace Symantec Endpoint Protection používá jeden z těchto nástrojů podle toho, který je již nainstalován v počítači.
	• OpenSSL 1.0.2k-fips a novější
	• Vývojářské nástroje
	Funkce automatické kompilace a ruční kompilace modulu jádra funkce Auto-Protect vyžadují instalaci určitých nástrojů pro vývojáře. Mezi tyto vývojářské nástroje patří gcc, zdrojový kód jádra a hlavičkové soubory. Podrobné informace o tom, co a jak je třeba instalovat pro konkrétní verze systému Linux, naleznete v dokumentu:
	Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux (Ruční kompilace modulů jádra funkce Auto-Protect aplikace Endpoint Protection pro systémy Linux)
	• Závislé balíčky i686 na 64bitových počítačích
	Řada spustitelných souborů v klientovi pro systém Linux jsou 32bitové programy. U 64bitových počítačů je třeba před instalací klienta pro systém Linux nainstalovat závislé balíčky i686.
	Pokud jste závislé balíčky i686 ještě nenainstalovali, můžete tak učinit z příkazového řádku. Tato instalace vyžaduje oprávnění superuživatele, jak ukazují následující příkazy `sudo`:
	– Distribuce založené na systému Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Distribuce založené na systému Debian: `sudo apt-get install ia32-libs`
	– Distribuce založené na systému Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`

Prodejní verze, poznámky, nové opravy a systémové požadavky pro aplikaci Endpoint Security a všechny verze aplikace Endpoint Protection

Podporované a nepodporované možnosti upgradu na nejnovější verzi aplikace Symantec Endpoint Protection 14.x

V případě verzí aplikace Symantec Endpoint Protection starších, než je nejnovější verze, je zpravidla podporována každá verze před touto verzí uvedená v seznamu. Tuto možnost byste si však měli u své konkrétní verze ověřit v poznámkách k verzi.

Prodejní verze, poznámky, nové opravy a systémové požadavky pro aplikaci Endpoint Security a všechny verze aplikace Endpoint Protection

Podporované cesty upgradu

- Aplikace Symantec Endpoint Protection Manager verze 12.1.6 MP10 a novější s vestavěnou databází bez problémů upgraduje na databázi Microsoft SQL Server Express, verze 14.3 RU1. Upgrady z verze 12.1.6 MP9 a starších na verzi 14.3 RU1 jsou blokovány.
- Aplikace Symantec Endpoint Protection Manager 14.x se aktualizuje bez problémů od verze 12.1.x, s výjimkou případů, kde byla podpora zrušena, například: Windows Server 2003, operační systémy pro stolní počítače a 32bitové operační systémy, stejně jako některé verze serveru SQL Server.
- Klient aplikace Symantec Endpoint Protection 14.x bez problémů aktualizuje všechny předchozí verze klientů 12.1 a 11 nainstalované v podporovaných operačních systémech. Výjimkou je klient pro systém Mac starší než verze 12.1.4, který je nutné aktualizovat na verzi 12.1.4 nebo novější, popřípadě odinstalovat.

Důležité informace o migraci aplikace Symantec Endpoint Protection 14

Aplikace Symantec Endpoint Protection Manager a klient pro systém Windows

Následující verze aplikace Symantec Endpoint Protection Manager a klienta Symantec Endpoint Protection pro systém Windows lze upgradovat přímo na aktuální verzi:

- 11.x a Small Business Edition 12.0 (pouze klienti aplikace Symantec Endpoint Protection, v podporovaných operačních systémech)
- 12.1.x, až do verze 12.1.6 MP10
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

Klient pro systém Mac

Následující verze klienta Symantec Endpoint Protection pro systém Mac lze upgradovat přímo na aktuální verzi:

- 12.1.4 – 12.1.6 MP9
  Klient systému Mac nebyl aktualizován na verzi 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

NOTE

Klient Symantec Endpoint Protection pro systém Mac nebyl aktualizován na verzi 14.0.1 MP2.

Klient pro systém Linux

NOTE
Symantec Agent pro Linux 14.3 RU1 zjistí a odinstaluje staršího klienta aplikace Symantec Endpoint Protection pro systém Linux a pak provede novou instalaci. Staré konfigurace nebudou zachovány.

Následující verze klienta Symantec Endpoint Protection pro systém Linux lze upgradovat přímo na aktuální verzi:

- 12.1.x, až do verze 12.1.6 MP9
  Klient systému Linux nebyl aktualizován na verzi 12.1.6 MP10.t
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

Aplikace Symantec AntiVirus pro systém Linux 1.0.14 je jediná verze, kterou můžete převést přímo na aplikaci Symantec Endpoint Protection. Nejprve je třeba odinstalovat všechny ostatní verze aplikace Symantec AntiVirus pro systém Linux. Nelze převést spravovaného klienta na nespravovaného.

Nepodporované cesty upgradu

Migraci do produktu Symantec Endpoint Protection nelze provádět ze všech produktů společnosti Symantec. Před instalací klienta aplikace Symantec Endpoint Protection je nutné odinstalovat následující produkty.

- Symantec AntiVirus a Symantec Client Security, které nejsou podporovány.
- Všechny produkty Symantec Norton
- Aplikace Symantec Endpoint Protection pro systém Windows XP Embedded 5.1
- Všechny aplikace Symantec Endpoint Protection pro klienta systému Mac staršího než 12.1.4. Nebo ho můžete aktualizovat na verzi 12.1.4 a novější.

Poznámky:

- Migrace klienta aplikace Symantec Endpoint Protection na verzi starší než 12.1.x není podporována.
- Aplikaci Symantec Endpoint Protection Manager 11.0.x nebo aplikaci Symantec Endpoint Protection Manager Small Business Edition 12.0.x nelze aktualizovat přímo na libovolnou verzi aplikace Symantec Endpoint Protection Manager 14. Nejprve je nutné tyto verze odinstalovat nebo provést upgrade na verzi 12.1.x a teprve poté na nejnovější verzi 14.x.
- Aplikaci Symantec Endpoint Protection Manager 12.1.6 MP7 nelze upgradovat na verzi 14, protože verze schématu databáze ve verzi 12.1.6 MP7 je novější než ve verzi 14. Z verze 12.1.6 MP7 je nutné upgradovat na verzi 14 MP1 nebo novější.
- Verze 14.0.x již nepodporuje systém Windows XP, Server 2003 a jakýkoli operační systém Windows Embedded, který je založen na systému Windows XP. Aplikace Symantec Endpoint Protection Manager 14.2 RU1 může spravovat tyto počítače jako starší klienty verze 12.1.x, ačkoli klienti verze 12.1.x jsou na konci životnosti. Pro tyto klienty můžete použít produkt společnosti Symantec, který tyto starší operační systémy stále podporuje, například Data Center Security (DCS).
- Upgrade z verze 14 MP1 (14.0.2332.0100) na verzi 14 MP1 Refresh Build (14.0.2349.0100) není podporován.
- Downgrade není povolen. Pokud například chcete migorvat z aplikace Symantec Endpoint Protection 14.2.1.1 na verzi 12.1.6 MP10, je nutné nejprve aplikaci Symantec Endpoint Protection 14.2.1 odinstalovat.
- Pokud máte číslo sestavení, ale nejste si jistí, o jakou verzi vydání se jedná, viz:
  Informace o typech a verzích vydání aplikace Endpoint Protection

Další zdroje informací

Následující tabulka uvádí webové stránky, na kterých se nachází osvědčené postupy, informace o řešení potíží a další zdroje, které vám pomohou s použitím produktu.

Table 14: Informace o webu aplikace Endpoint Protection

Typ informací	Odkaz na webové stránky
Zkušební verze	Obraťte se na zástupce účtu.
Aktuální příručky a dokumentace	• Produktové příručky pro nejnovější verzi (anglicky) • Produktové příručky pro nejnovější verzi (jiné jazyky) • Příručky ke všem verzím aplikace Symantec Endpoint Protection 14.x (anglicky)
Technická podpora	Technická podpora aplikace Endpoint Protection Obsahuje články databáze znalostí, podrobné informace k vydání produktu, aktualizace a opravy a kontakty na podporu.
Informace a novinky o hrozbách	Symantec Security Center
Školení	Education Services Přístup k výukovým kurzům, knihovně eLibrary a dalším zdrojům
Fóra Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom