Bitdefender

GravityZone

# PRŮVODCE INSTALACÍ

# Bitdefender GravityZone
# Průvodce instalací

Datum vydání 2021.04.20



## Právní oznámení



## Právní oznámení

**Všechna práva vyhrazena.** Žádná část tohoto dokumentu nemůže být reprodukována ani šířena dál v jakékoli formě a jakýmikoli prostředky, elektronicky ani mechanicky, včetně kopírování, záznamu nebo jakéhokoli systému pro uchovávání a sběr informací, bez písemného souhlasu oprávněného zástupce společnosti Bitdefender. Začlenění krátkých citací do recenzí je možné pouze s uvedením citovaného zdroje. Obsah nesmí být žádným způsobem modifikován.

# Obsah

# Předmluva

Tento návod je určený pro IT administrátory zodpovědnými za nasazení GravityZone ochranu uvnitř jejich firemní infrastruktury. IT manažeři hledající informace o GravityZone mohou najít v tomto návodu požadavky pro nasazení GravityZone a seznam dostupných modulů ochrany.

Tento dokument se zaměřuje na vysvětlení jak nainstalovat a nakonfigurovat řešení GravityZone a její bezpečnostní agenty na všech typech zařízení ve vaší společnosti.

# 1. Konvence použité v tomto návodu

## Typografické konvence

Tento průvodce používá několik typů textu pro lepší čitelnost. Jejich vzhled a význam je uveden v následující tabulce.

| Vzhed | Popis |
|---|---|
| `ukázka` | Názvy příkazů a syntaxí v řádku, cesty a názvy souborů, výstupy konfiguračních souborů a vstupní text jsou psány `neproporcionálním` písmem. |
| http://www.bitdefender.com | Webové stránky jsou umístěny na http nebo ftp serverech. |
| gravityzone-docs@bitdefender.com | Kontaktní E-mailové adresy vloženy v textu. |
| „Předmluva“ (str. viii) | Toto je interní odkaz, směřující na nějaké místo v dokumentu. |
| **možnost** | Všechna nastavení jsou zvýrazněna **tučným** písmem. |
| **klíčové slovo** | Možnosti rozhraní, klíčová slova nebo zkratky jsou zvýrazněny **tučným** písmem. |

## Poznámky k textu

Poznámky jsou v textu graficky značené, nabízejí vám dodatečné informace k stávajícímu odstavci.

**Poznámka**
Poznámka je jen krátké shrnutí. Ačkoli ji můžete vynechat,poznámky mohou poskytnout cenné informace, jako např. zvláštní funkce nebo odkaz na související téma.

**Důležité**
Toto vyžaduje vaši pozornost a není doporučeno toto přeskočit. Obvykle poskytuje ne rozhodující, avšak významné informace.

**Varování**
Toto je důležitá informace, se kterou byste měli zacházet se zvýšenou opatrností. Nic nezkazíte tím, budete-li se držet pokynů. Toto varování byste si měli přečíst a porozumět mu, jelikož popisuje něco velice riskantního.

# 1. O GRAVITYZONE

GravityZone je řešení zabezpečení pro firmy, které je od základu vytvořeno k virtualizovanému nebo cloudovému provozu, poskytující bezpečnostní služby fyzickým koncovým zařízením, mobilním zařízením a virtuálním zařízením v soukromém i veřejném cloudu, a poštovním serverům Exchange.

GravityZone je jeden produkt se sjednocenou správní konzolí, dostupný v cloudu hostovaném společností Bitdefender, nebo jako virtuální zařízení k instalaci ve firemně a poskytuje jediný bod pro nasazení, vynucení a správu bezpečnostních politik pro jakýkoli počet a typ koncových bodů, umístěných kdekoliv.

GravityZone doručuje několik vrstev zabezpečení pro koncová zařízení a pro Microsoft Exchange mail servery: Antimalware se sledováním chování, ochrana před zero day, kontrola aplikací a sandboxing, firewall, řízení zařízení, řízení obsahu, anti-phishing a antispam.

# 2. OCHRANNÉ VRSTVY GRAVITYZONE

GravityZone poskytuje následující ochranné vrstvy:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- HyperDetect
- Pokročilý Anti-Exploit
- Firewall
- Kontrola obsahu
- Patch Management
- Kontrola zařízení
- Šifrování celého disku
- Security for Exchange
- Kontrola aplikací
- Sandbox Analyzer
- Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

## 2.1. Antimalware

Vrstva antimalwarové ochrany je založena na skenování signatur a heuristické analýze (B-HAVE, ATC) proti: virům, červům, trojským koním, spywaru, adwaru, keyloggerům, rootkitům a dalším druhům škodlivého softwaru.

Protimalwarová skenovací technologie Bitdefender se opírá o následující vrstvy:

- Nejprve je použita tradiční metoda skenování, kde skenovaný obsah je porovnáván s databází signatur. Databáze signatur obsahuje bajtové vzory, specifické pro známé hrozby, a Bitdefender ji pravidelně aktualizuje. Tato metoda skenování je účinná proti ověřeným hrozbám, které byly prozkoumány a zdokumentovány. Nehledě na to, jak rychle je databáze signatur aktualizována, v mezičase mezi zjištěním nové hrozby a vydání nápravy vždy vznikne trhlina se zranitelností.
- Proti zbrusu novým, nezdokumentovaným hrozbám, **B-HAVE**, heuristický stroj Bitdefender, poskytuje druhou vrstvu ochrany. Heuristické algoritmy rozpoznají

malware na základě chrakteristiky chování. B-HAVE spouští podezřelé soubory ve virtuálním prostředí, aby otestoval jejich dopad na systém a ujistil se, že nepředstavují hrozbu. Pokud je zjištěna hrozba, programu je zabráněno ve spuštění.

## Skenovací nástroje

Bitdefender GravityZone je schopna automaticky nastavit skenovací nástroje při vytváření balíčků agenta zabezpečení podle konfigurace koncového bodu.

Administrátor si může vybrat mezi několika skenovacími technologiemi a tím upravovat skenovací nástroje:

1. **Místní sken**, když je skenování prováděno na místním koncovém bodě. Režim lokálního skenování je vhodný pro výkonné stroje, které mají všechny signatury a nástroje uloženy lokálně.
2. **Hybridní skenování s odlehčenými nástroji (Veřejný cloud)**, se středním vytížením zdrojů koncového bodu, které využívá skenování v cloudu a částečně místní bezpečnostní nástroje. Tento režim skenování s sebou nese výhodu lepší spotřeby zdrojů, zatímco zahrnuje mimoprostorové skenování.
3. **Centrální skenování ve veřejném nebo soukromém cloudu**, s malou stopou a vyžadující Security Server pro skenování. V tomto případě žádný set signatur není uložen lokálně a skenování je přeloženo na Security Server.

   **Poznámka**
   Minimální sada nástrojů, potřebná k rozbalení komprimovaných souborů, je uložena lokálně.

4. **Centrální skenování (skenování veřejného nebo osobního cloudu pomocí Security Server) * v podobě Lokálního skenování (plnohodnotný agent)**
5. **Centrální skenování (skenování veřejného nebo osobního cloudu pomocí Security Server) s alternativní variantou* v podobě Hybridního skenování (Veřejný cloud s odlehčeným agentem)**

* V případě skenování pomocí dvou strojů najednou, pokud je jeden z nich nedostupný, bude použit záložní. Spotřeba zdrojů a využití sítě záleží na použitém typu skenování.

## 2.2. Pokročilá ochrana před hrozbami (ATC)

Pro hrozby, které uniknou i heuristickému nástroji, je zde třetí vrstva ochrany, přítomná ve formě Pokročilé ochrany před hrozbami (ATC).

Pokročilá ochrana před hrozbami nepřetržitě monitoruje spuštěné procesy a hodnotí podezřelé chování, jako například pokusy o: maskování typu procesu, spuštění kódu v umístění jiného procesu (zmocnění se procesové paměti za účelem zvýšení privilegií), replikaci, přetahování souborů, schovávání před aplikacemi pro výpočet procesů, atd. Každé podezřelé chování zvyšuje hodnocení procesu. Po dosažení prahové hodnoty,se spustí poplach.

## 2.3. HyperDetect

Bitdefender HyperDetect je další vrstva zabezpečení, která je speciálně navržena tak, aby detekovala pokročilé útoky a podezřelé aktivity ještě předtím, než proběhnou. HyperDetect obsahuje modely strojového učení a detekci útoků proti stealth útoku a proti hrozbám, jako jsou například: útoky nultého dne, pokročilé přetrvávající hrozby (APT), obfuskační malware, bezsouborové útoky (zneužití PowerShell, Windows Management Instrumentation atd. .), Krádeže pověření, cílené útoky, obyčejný malware, útoky založené na skriptech, exploity, nástroje hackování, podezřelý síťový provoz, potenciálně nežádoucí aplikace (PUA), ransomware.

## 2.4. Pokročilý Anti-Exploit

Tato nová proaktivní technologie, poháněná strojovým učením, zastaví útoky nultého dne prováděný pomocí exploitů. Advanced Anti- Exploit zachycuje nejnovější exploity v reálném čase a zmírňuje zranitelnosti v oblasti poškození paměti, které se mohou vyhnout stávajícím řešením. Chrání nejčastěji používané aplikace, jako jsou prohlížeče, Microsoft Office nebo Adobe Reader, stejně jako ostatní, na které si vzpomenete. Sleduje systémové procesy a chrání před narušením bezpečnosti a únosem stávajících procesů.

## 2.5. Firewall

Firewall kontroluje přístup aplikací k síti a k internetu. Přístup je automaticky povolen souhrnné databázi známých, legitimních aplikací. Firewall dokáže chránit systém proti skenování portů, zamezit ICS a varovat, když se k Wi-Fi síti připojí nové uzly.

## 2.6. Kontrola obsahu

Modul Kontrola obsahu pomáhá vymáhat podniková pravidla pro povolený přenos, přístup k webu, ochranu dat a kontrolu aplikací. Administrátoři mohou určit nastavení skenování přenosu a výjimky, naplánovat přístup k webu současně s blokováním vybraných webových kategorií nebo URL, konfigurovat pravidla ochrany dat, a definovat povolení pro užívání určitých aplikací.

## 2.7. Network Attack Defense

Modul Network Attack Defense se spoléhá na technologii Bitdefender zaměřenou na detekci síťových útoků určených k získávání přístupu ke koncovým bodům pomocí specifických technik, jako jsou: přímé útoky, zneužití sítě, odcizení hesla, Infekce vektory, roboty a trojskými koňmi.

## 2.8. Patch Management

Plně integrovaný v GravityZone, modul Patch Management udržuje operační systémy a softwarové aplikace aktuální, a poskytuje souhrnný přehled o stavu oprav na vašich koncových bodech s Windows.

Modul GravityZone Správa aktualizací zahrnuje několik funkcí, jako je skenování aktualizací na vyžádání / plánované, automatické / manuální opravy, nebo hlášení chybějících oprav.

Více informací o výrobcích a produktech podporovaných GravityZone Správou aktualizací se můžete dočíst v tomto KB článku.

**Poznámka**
Modul Patch Management e doplněk, který je dostupný společně se samostatným licenčním klíčem pro všechny dostupné licenční balíčky GravityZone.

## 2.9. Kontrola zařízení

Modul Device Control umožňuje prevenci úniku citlivých dat a malwarových infekcí skrze externí zařízení připojená ke koncovým bodům pomocí aplikování pravidel pro blokování a výjimky prostřednictvím politik pro širokou škálu typů zařízení (jako jsou flash disky USB, zařízení Bluetooth, přehrávače CD/DVD, paměťová zařízení, atd.).

## 2.10. Šifrování celého disku

Tato ochranná vrstva umožňuje poskytovat úplné šifrování na koncových bodech pomocí správy nástroje BitLocker ve Windows a FileVault a na macOS. Můžete šifrovat a dešifrovat bootovatelné a nebootovatelné svazky pouze několika kliky, zatímco GravityZone se stará o celý proces, s minimálním zásahem od uživatelů. GravityZone má uložené klíče pro obnovu, potřebné k odemčení svazku v případě, že uživatelé zapomenou své heslo.

**Poznámka**
Modul Full Disk Encryption je doplněk, který je dostupný pro všechny verze GravityZone ve formě separátního licenčního klíče.

## 2.11. Security for Exchange

Bitdefender Security for Exchange poskytuje filtrování proti malwaru, spamu, phishingu a filtrování příloh a obsahu, které je hladce zakomponované do Microsoft Exchange Serveru, a zajišťuje tak bezpečné posílání zpráv a prostředí spolupráce, čímž zvyšuje produktivitu. Díky oceňovaným antimalwarovým a antispamovým technologiím chrání uživatele Exchange proti tomu nejnovějšímu, nejpropracovanějšímu malwaru a proti pokusům o krádež důvěrných a cenných uživatelských údajů.

**Důležité**
Security for Exchange je určen k ochraně celé Exchange, ke které patří chráněný Exchange Server. To znamená, že chrání všechny aktivní poštovní schránky, včetně uživatele/prostoru/zařízení/sdílených poštovních schránek.
Kromě ochrany Microsoft Exchange zahrnuje licence také moduly ochrany koncových bodů instalované na serveru.

## 2.12. Kontrola aplikací

Modul Kontrola aplikací chrání před malwarem, útoky zero-day a posiluje zabezpečení, aniž by měla vliv na výkonnost. Kontrola aplikací zavádí pružná pravidla pro whitelisting aplikací, která identifikují a brání v instalaci a spouštění všech nežádoucích, nedůvěryhodných nebo škodlivých aplikací.

## 2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer poskytuje silnou ochrannou vrstvu proti pokročilým hrozbám díky tomu, že provádí automatickou hloubkovou analýzu podezřelých

souborů, které ještě nejsou v signaturách antimalwarové ochrany Bitdefender. Karanténa využívá rozsáhlou sadu technologií Bitdefender k provádění užitečného zatížení v uzavřeném virtuálním prostředí hostovaném společností Bitdefender nebo při lokálním nasazení, analyzuje jejich chování a hlásí jakékoli jemné systémové změny, které svědčí o zákeřném záměru.

Sandbox Analyzer používá řadu senzorů k detonaci obsahu ze spravovaných endpointů, toků síťového provozu, centralizované karantény a serverů ICAP.

Kromě toho Sandbox Analyzer umožňuje ruční odesílání prostřednictvím API.

**Poznámka**
Funkčnost těchto modulů může být zajištěna pomocí Sandbox Analyzer Cloud a Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises je dostupný pouze se separátním licenčním klíčem

## 2.14. Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))

EDR je komponenta korelující události, schopná identifikovat pokročilé hrozby a nebo probíhající útoky. Jakožto součást komplexní a plně integrované platformy pro ochranu koncových bodů, EDR přináší společnou inteligenci pro všechna zařízení napříč vaší firemní sítí. Toto řešení přichází pomoci vašemu týmu bezepečnostních specialistů při řešení incidentů a pomáhá jim tak v úsilí při investigacích a také s odpovědmi na pokročilé hrozby.

Skrze Bitdefender Endpoint Security Tools klienta, si můžete na vámi spravovaných koncových bodech aktivovat ochranný modul zvaný EDR Senzor, abyste mohli schraňovat data z jejich hardware a z jejich operačních systémů. Následně díky klient-server struktuře systému, jsou metadata schraňována a zprocesovávaná na obou stranách.

Tato komponenta (vrstva ochrany) přináší datailní informaci o detekovaných hrozbách, interaktivní mapu incidentů, následných akcí oprav a integraci s komponentami (vrstvami ochrany)Sandbox Analyzer a HyperDetect.

## 2.15. Hypervisor Memory Introspection (HVI)

Je známé, že vysoce organizovaní, profit vyhledávající útočníci hledají neznámé zranitelnosti (zero-day zranitelnosti) nebo používají jednorázové útoky, účelně

vystavěné exploity (zero-day exploity) a jiné nástroje. Útočníci používají také pokročilé způsoby pro pozdržení a dávkování zatížení útoků tak, aby maskovali podezřelou činnost. Nové, ziskem motivované útoky jsou navrženy tak, aby byly nenápadné a dokázaly prorazit tradiční bezpečnostní nástroje.

Pro virtualizovaná prostředí je problém nyní vyřešen, HVI chrání datacentra s vysokou koncentrací virtuálních strojů proti pokročilým a sofistikovaným hrozbám, se kterými si stroje založené na signaturách neumí poradit. Prosazuje silnou izolaci a zajišťuje tak detekci útoků v reálném čase, blokuje je hned ve chvíli jejich výskytu a okamžitě odstraňuje hrozby.

Ať je chráněný stroj Windows nebo Linux, sever nebo počítač, HVI poskytuje vhled na úrovni, které je nemožné dosáhnout na hostujícím operačním systému. Stejně jako hypervizor kontroluje přístup k hardwaru za každý hostující virtuální stroj, HVI má důvěrnou znalost jak ohledně uživetelského režimu, tak kernel režimu v paměti hosta. Výsledkem je, že HVI má kompletní vhled do paměti hosta, a tím pádem do veškerého kontextu. Zároveň je HVI izolovaný od chráněných hostů, stejně jako je izolovaný samotný hypervizor. Tím, že operuje na úrovni hypervizoru a využívá hypervizorové funkce, HVI překonává technologické výzvy tradiční bezpečnosti pro odhalení škodlivé činnosti v datových centrech.

HVI rozpoznává spíše útočné techniky, než jejich vzorce. Tímto způsobem je technologie schopna rozpoznávat, hlásit a zabraňovat běžným metodám zneužívání. Jádro je chráněno proti technikám rootkit hookingu, které jsou využívány během útočného řetězce (attack kill chain) útoku pro jeho nenápadnost. Uživatelské operace jsou také chráněné před infikováním kódu, funkce detouring a provedení kódu ze stack nebo haldy

**Poznámka**
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

## 2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) je řešení pro zabezpečení sítě, které analyzuje datové toky protokolu IPFIX na přítomnost škodlivého chování a škodlivého softwaru.

Bitdefender NTSA má sloužit vedle stávajících bezpečnostních opatření jako doplňková ochrana, která je schopna pokrýt slepá místa, která tradiční nástroje nemonitorují.

Tradiční nástroje pro zabezpečení sítě se obecně pokoušejí zabránit infekcím malwarem kontrolou příchozího provozu (přes sandbox, firewally, antivirové programy atd.). Bitdefender NTSA se zaměřuje výhradně na monitorování odchozího provozu sítě a zjišťuje podezřelé chování.

## 2.17. Security for Storage

GravityZone Security for Storage dodává ochranu v reálném čase pro vedoucí systémy pro sdílení souborů (file-sharing systems) a systémy síťových úložišť (network-storage systems). Aktualizace algoritmu pro detekci hrozeb probíhá automaticky - aniž by od vás bylo třeba vynaložit jakékoli úsilí a bez jakéhokoliv narušení činnosti koncových uživatelů.

Dva či více GravityZone Security Serverů Multi-Platform spolu tvoří roli ICAP serveru dodávajícího antimalware služby pro síťová uložiště (NAS) a také pro řešení pro sdílení souborů (file-sharing solutions) kompatibilních s Internet Content Adaptation Protokolem (ICAP, jak je definováno v RFC 3507).

Jakmile uživatel požádá o otevření, přečtení, zapsání, nebo zavření souboru z laptopu, pracovnístanice, mobilu, nebo jiného zařízení, tak pošle ICAP klient (tzn. NAS nebo systém pro sdílení souborů) požadavek na proskenování na Security Server a následně přijme verdikt (rozhodnutí o závadnosti) ohledně souboru. V závislosti na výsledku, Security Server povolí přístup, zamezí v přístupu a nebo smaže soubor.

**Poznámka**
Tento modul je dostupný jako doplněk se samostatným licenčním klíčem.

## 2.18. Security for Mobile

Na celopodnikové úrovni spojuje zabezpečení s managementem a kontrolou souladu pro zařízení iPhone, iPad a Android díky spolehlivé distribuci softwaru a aktualizací prostřednictvím trhu Apple a Android. Řešení bylo navrženo tak, aby umožnilo kontrolované přijetí iniciativ bring-your-own-device (BYOD) díky tomu, že setrvale prosazuje práva používání na všech přenosných zařízeních. Bezpečnostní funkce zahrnují zámek obrazovky, autentizační kontrolu, polohu zařízení, vymazání na dálku, detekci zařízení s rootem nebo jailbreakem a bezpečnostní profily. Pro zařízení Android je bezpečnostní úroveň zvýšena o skenování v reálném čase a šifrování vyměnitelných médií. Ve výsledku máte mobilní zařízení pod kontrolou a citlivé obchodní údaje uložené na zařízení jsou chráněny.

## 2.19. Dostupnost ochranných vrstev GravityZone

Dostupnost ochranných vrstev GravityZone se liší podle operačního systému koncového bodu. Další informace naleznete v článku GravityZone Protection Layers Availability.

# 3. ARCHITEKTURA GRAVITYZONE

Jedinečná architektura GravityZone mu umožňuje snadné přizpůsobení se a zabezpečení pro libovolný počet systémů. GravityZone lze nastavit tak, aby využívala více virtuálních zařízení a několika určitých rolí (databáze, komunikační server, aktualizační server a webová konzole) pro zajištění spolehlivosti a přizpůsobitelnosti.

Každá role může být nainstalována na jiném zařízení. Zabudované vyrovnávače rovnováhy rolí ručí za to, že zavedení GravityZone ochrání i ty nejrozsáhlejší podnikové sítě, aniž by způsobovala zpomalení nebo překážky. Místo vestavěného vyrovnávače rovnováhy lze použít i již existující software nebo hardware pro vyrovnání rovnováhy zatížení, pokud je přítomný síti.

Jelikož je GravityZone dodávána formou virtuálního kontejneru (virtuálního stroje), tak může být naimportována a spuštěna na prakticky kterékoliv virtualizační platformě, včetně VMware, Citrix, Microsoft Hyper-V a Nutanix Prism, Microsoft Azure.

Integrace s VMware vCenter, Citrix XenServer, Microsoft Active Directory, Nutanix Prism Element a Microsoft Azure snižuje úsilí nutné pro nasazení ochrany na fyzických a virtuálních koncových strojích.

Řešení GravityZone obsahuje následující komponenty:

- Virtuální zařízení GravityZone
- Security Server
- Doplňkový balíček HVI
- Bezpečnostní agenty

## 3.1. GravityZone VA

GravityZone on-premise řešení je dodáváno jako Linuxová (Ubuntu) samokonfigurovatelná vytvrzená (hardened) virtuální appliance (VA), která je vnořená do obrazu virtuálního stroje a je jednoduše instalovatelná a konfigurovatelná pomocí CLI (Command Line Interface). Virtuální zařízení je dostupné v několika formátech, kompatibilních s hlavními virtualizačními platformami (OVA, XVA, VHD, OVF, RAW).

### 3.1.1. Databáze GravityZone

Centrální logika architektury GravityZone. Bitdefender používá nerelační databázi MongoDB, kterou lze snadno přizpůsobit a replikovat.

### 3.1.2. Aktualizační server GravityZone

Aktualizační server hraje důležitou roli v aktualizaci řešení GravityZone a agentů koncových bodů tak, že replikuje a vydává potřebné balíčky nebo instalační soubory.

### 3.1.3. Komunikační server GravityZone

Komunikační server je spojení mezi bezpečnostními agenty a databází, který přenáší pravidla a příkazy na chráněné koncové body ,a také události hlášené bezpečnostními agenty.

### 3.1.4. GravityZone Incident Server

Incident Server je spojením mezi agenty zabezpečení a databází, shromažďováním dat koncových bodů a generováním incidentů na základě hrozeb detekovaných preventivními technologiemi a algoritmy strojového učení.

### 3.1.5. Webovou konzoli (GravityZone Control Center)

Bezpečnostní řešení Bitdefender jsou spravovány z jediného správního bodu, webové konzole Control Center. Tímto je umožněna snadnější správa a přístup k celkovému bezpečnostnímu postoji, globálním bezpečnostním hrozbám a kontrole nad všemi bezpečnostními moduly, které chrání virtuální nebo fyzické počítače, servery a přenosná zařízení. Poháněna architekturou Gravity, Control Center je schopna naplnit potřeby i těch největších organizací.

Control Center se integruje s existujícími systémy správy a monitorovacími systémy, tak aby to bylo co nejjednodužší automaticky aplikuje ochranu na nespravované pracovní stanice , servery nebo mobilní zařízení, které se objevují v Microsoft Active Directory, VMware vCenter, Nutanix Prism Element nebo Citrix XenServer systémech nebo které jsou jednoduše detekovány v síti.

## 3.2. Security Server

Security Server je specializovaný virtuální stroj, který reduplikuje a centralizuje většinu antimalwarových funkcí antimalwarových agentů a funguje jako skenovací server.

Existují tři verze Security Server, pro každý typ virtualizačního prostředí:

- **Security Server pro VMware NSX.** Tato verze se automaticky instaluje na každého hostitele ve svazku, kde byl zaveden Bitdefender.
- **Security Server pro VMware vShield Endpoint.** Tuto verzi je nutné nainstalovat na každého hostitele, aby byl chráněn.
- **Security Server Multi-Platform.** Tato verze je pro další různá virtualizovaná prostředí a musí být nainstalována na jednom nebo více hostech, aby se přizpůsobila počtu chráněných virtuálních strojů. Při používání HVI, Security Server musí být nainstalován na každém hostu, který obsahuje virtuální stroje, které mají být chráněny.

## 3.3. Doplňkový balíček HVI

Balíček HVI zajišťuje spojení mezi hypervizorem a Security Server na daném hostu. Tímto způsobem je Security Server schopný monitorovat paměť využívanou na hostiteli, na kterém je nainstalován, na základě bezpečnostních pravidel GravityZone.

**Poznámka**
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

## 3.4. Bezpečnostní agenty

Pro ochranu vaší sítě pomocí Bitdefender, musíte nainstalovat vhodné bezpečnostní agenty GravityZone na koncové síťové body.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac
- GravityZone Mobile Client
- Bitdefender Tools (vShield)

### 3.4.1. Bitdefender Endpoint Security Tools

GravityZone zajišťuje fyzickým a virtuálním strojům ochranu pomocí Bitdefender Endpoint Security Tools, inteligentního bezpečnostního agenta, který rozpozná prostředí, a adaptuje se podle typu koncového bodu. Bitdefender Endpoint Security Tools může být nasazen na jakékoli zařízení, virtuální nebo fyzické, poskytuje flexibilní skenovací systém a je ideální volbou pro smíšená prostředí (fyzická, virtuální a cloudová).

Kromě souborové ochrany systému Bitdefender Endpoint Security Tools obsahuje také mail server ochranu pro Microsoft Exchange Servers.

Bitdefender Endpoint Security Tools používá jednu šablonu zásad pro fyzické a virtuální počítače a jeden zdroj instalační sady pro jakékoli prostředí (fyzické nebo virtuální) se systémem Windows.

## Úroveně ochrany

S klientem Bitdefender Endpoint Security Tools jsou dostupné následující ochranné vrstvy:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- HyperDetect
- Firewall
- Kontrola obsahu
- Network Attack Defense
- Patch Management
- Kontrola zařízení
- Šifrování celého disku
- Security for Exchange
- Sandbox Analyzer
- Systém detekce hrozeb a následných opatření pro ochranu koncových bodů (Endpoint Detection and Response (EDR))
- Kontrola aplikací

## Role koncových bodů

- Pokročilý uživatel
- Relay
- Patch Caching Server
- Exchange Ochrana

### Pokročilý uživatel

Administrátoři centrální správy mohou udělit práva pokročilého uživatele uživatelům koncových bodů skrze nastavení politik. Modul Pokročilý uživatel aktivuje administrátorská práva na uživatelské úrovni, čímž umožní uživateli koncového bodu přístup a možnost úpravy bezpečnostních nastavení prostřednictvím lokální konzole. Control Center dostává hlášení, když je koncový uživatel v módu

Pokročilého uživatele a správce Control Center může přepsat místní bezpečnostní nastavení.

**Důležité**
Tento modul je dostupný pouze pro počítače a servery s podporovaným systémem Windows.

## Relay

Agenti koncových bodů s rolí Bitdefender Endpoint Security Tools Relay slouží jako komunikační proxy a aktualizační servery pro ostatní koncové body v síti. Agenti koncových bodů s rolí relay jsou nezbytní zvláště v organizacích s izolovanými sítěmi, kde veškerý přenos probíhá skrze jediný přístupový bod.

Ve společnostech s velkými distribuovanými sítěmi, relay agenti napomáhají snížení využití šířky pásma tím, že brání chráněným koncovým bodům a bezpečnostním serverům v komunikaci napřímo s zařízením GravityZone.

Jakmile je agent Bitdefender Endpoint Security Tools Relay nainstalovaný v síti, ostatní koncové body mohou být nastaveny pomocí pravidel pro komunikaci s Control Center prostřednictvím relay agenta.

Agenti Bitdefender Endpoint Security Tools Relay slouží k následujícím účelům:

- Odhalení všech nechráněných koncových bodů v síti.
- Nasazení agenta na koncový bod v rámci místní sítě.
- Aktualizace chráněných koncových bodů v síti.
- Zajištění komunikace mezi Control Center a připojenými koncovými body.
- Role proxy serveru pro chráněné koncové body.
- Optimalizace síťového přenosu během aktualizací, nasazení, skenování a dalších zátěžových úkolů.

## Patch Caching Server

Koncové body s funkcí relay mohou také sloužit jako server pro aktualizaci programového vybavení. Je-li tato funkce povolena, Relay ukládá softwarové aktualizace stažené ze stránek prodejců, a distribuuje je do cílových koncových bodů ve vaší síti. Jakmile je na připojeném koncovém bodě se objeví software s chybějícími aktualizacemi, stáhne si je ze serveru a ne ze stránek prodejce, čímž optimalizuje vzniklý přenos a zatížení šířky pásma.

**Důležité**
Tato přídatná funkce je dostupná s registrovaným doplňkem Správa oprav.

### Exchange Ochrana

Bitdefender Endpoint Security Tools s Exchange rolí může být nainstalován na Microsoft Exchange servery pro ochranu uživatelů Exchange před hrozbami skrytými v emailech.

Bitdefender Endpoint Security Tools s rolí Exchange chrání jak samotný server, tak řešení Microsoft Exchange.

## 3.4.2. Endpoint Security for Mac

Endpoint Security for Mac je bezpečnostní agent vytvořený k ochraně pracovním stanic a laptopů s Macintosh OS postavených na platformě Intel. Dostupná technologie skenování je dostupná **Místní skenování** s lokálně uloženým obsahem zabezpečení.

### Úroveně ochrany

Následující ochranné vrstvy jsou dostupné na Endpoint Security for Mac:

- Antimalware
- Pokročilá ochrana před hrozbami (ATC)
- Kontrola obsahu
- Kontrola zařízení
- Šifrování celého disku

## 3.4.3. GravityZone Mobile Client

GravityZone Mobile Client snadno rozšiřuje bezpečnostní pravidla na jakýkoli počet zařízení s Android nebo iOS, a tak je chrání proti neoprávněnému využívání, riskwaru nebo ztrátě důvěrných dat. Bezpečnostní funkce zahrnují zámek obrazovky, autentizační kontrolu, polohu zařízení, vymazání na dálku, detekci zařízení s rootem nebo jailbreakem a bezpečnostní profily. Pro zařízení Android je bezpečnostní úroveň zvýšena o skenování v reálném čase a šifrování vyměnitelných médií.

GravityZone Mobile Client je distribuován exkluzivně prostřednictvím Apple App Store a Google Play.

## 3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools je lehký agent pro virtualizovaná prostředí VMware integrovaných s vShield Endpoint. Bezpečnostní agent se nainstaluje na virtuální stroje chráněné

Security Serverem a vy díky tomu můžete využívat výhod přídatných funkcí, které poskytuje:

- Umožňuje vám spouštět úlohy Skenování paměti a Skenování procesů na zařízení.
- Informuje ostatní uživatele o nalezených infekcích a akcích, které na nich byly provedeny.
- Přidá více možností pro výjimky z antimalwarového skenování.

## 3.5. Sandbox Analyzer Architektura

Bitdefender Sandbox Analyzer poskytuje silnou ochrannou vrstvu proti pokročilým hrozbám díky tomu, že provádí automatickou hloubkovou analýzu podezřelých souborů, které ještě nejsou v signaturách antimalwarové ochrany Bitdefender.

Sandbox Analyzer je k dispozici ve dvou variantách:

- Sandbox Analyzer Cloud, hostovaný Bitdefender.
- Sandbox Analyzer On-Premises, je k dispozici jako virtuální appliance, které lze nasadit lokálně.

### Sandbox Analyzer Cloud

Sandbox Analyzer Cloud obsahuje následující komponenty:

- **Portál Sandbox Analyzer** - hostovaný komunikační server, užívaný pro zpracování požadavků mezi koncovými body a sandbox clusterem Bitdefender.
- **Sandbox Analyzer Cluster** - hostovaná sandboxová infrastruktura, ve které probíhá behaviorální analýza. Na této úrovni jsou podané soubory detonovány na virtuálních strojích s operačním systémem Windows 7.

**GravityZone Control Center** funguje jako konzole pro správu a reporting, kde nastavujete politiky zabezpečení a zobrazujete analytické zprávy a oznámení.

**Bitdefender Endpoint Security Tools**,bezpečnostní agent nainstalovaný na koncových bodech funguje jako datový sensor pro Sandbox Analyzer.

### Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises je dodáván jako virtuální Linux Ubuntu zařízení zabudované do image virtuálního stroje. Snadno se instaluje a konfiguruje pomocí rozhraní příkazového řádku (CLI). Sandbox Analyzer On-Premises je k dispozici ve formátu OVA a lze jej nasadit na VMWare ESXi.

Sandbox Analyzer On-Premises obsahuje následující komponenty:

- **Sandbox Manager**. Tato komponenta je sandbox orchestrator. Sandbox Manager se připojuje k hypervizoru ESXi přes API a používá tyto hardwarové prostředky k vytváření a provozu prostředí pro analýzu malwaru.
- **Detonační virtuální stroje** . Tato součást se skládá z virtuálních strojů využívaných programem Sandbox Analyzer ke spouštění souborů a analýze jejich chování. Detonační virtuální stroje mohou spouštět 64bitové operační systémy Windows 7 a Windows 10.

**GravityZone Control Center** funguje jako konzole pro správu a reporting, kde nastavujete politiky zabezpečení a zobrazujete analytické zprávy a oznámení.

Sandbox Analyzer On-Premises pracuje s následujícími senzory:

- **Sensor koncového bodu** . Bitdefender Endpoint Security Tools pro Windows funguje jako dodávající senzor nainstalovaný na koncových bodech. Agent Bitdefender používá pokročilé strojové učení a algoritmy neuronové sítě k určení podezřelého obsahu a jeho odeslání do Sandbox Analyzer, včetně objektů z centralizované karantény.
- **Síťový senzor (Network sensor)**. Network Security Virtual Appliance (NSVA) je virtuální zařízení, které lze nasadit ve stejném virtualizovaném prostředí ESXi jako instanci Sandbox Analyzer. Síťový sensor získává obsah ze síťových toků a odešle jej do Sandbox Analyzer.
- **ICAP sensor**. Nasazeno na síťových úložných zařízeních (NAS) pomocí protokolu ICAP, Bitdefender Security Server podporuje odesílání obsahu do Sandbox Analyzer.

Kromě těchto senzorů Sandbox Analyzer On-Premises podporuje ruční odesílání a prostřednictvím API. Podrobnosti viz **Použití Sandbox Analyzer** kapitola v GravityZone administrátorském průvodci.

# 4. POŽADAVKY

Všechna GravityZone řešení jsou nainstalována a spravována pomocí Control Center.

## 4.1. Virtuální zařízení GravityZone

### 4.1.1. Podporované formáty a Virtualizační platformy

GravityZone je dodávána formou virtuální appliance (VA) (tzn. předinstalovaný stroj pro virtuální prostředí). Je k dispozici a podporuje následující formáty, které podporují většinu běžně dostupných virtualizačních platforem:

- OVA (Kompatibilní s VMware vSphere, View, VMware Player)
- XVA (Kompatibilní s Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatibilní s Microsoft Hyper-V)
- VMDK (Kompatibilní s Nutanix Prism)
- OVF (kompatibilní s Red Hat Enterprise Virtualization)*
- OVF (kompatibilní s Oracle VM)*
- RAW (kompatibilní s Kernel-based Virtual Machine nebo KVM)*

*OVF a RAW balíčky jsou archivy ve formátu tar.bz2.

Pro kompatibilitu platformy Oracle VM VirtualBox, obraťte se na tento článek KB.

Podporu pro jiné formáty a virtuatualizační platformy můžeme dodat na vyžádání.

### 4.1.2. Hardware

Nároky na potřebný Hardware pro chod vaší GravityZone virtual appliance závisí od velikosti vaší sítě a na druhu architektury nasazení, kterou si vyberete. Pro sítě s vekikostí do 3000 koncových bodů, můžete si vybrat instalaci všech rolí GravityZone na jediné appliance, přičemž pro větší sítě, musíte zvažovat rozdistribuovat role na více appliancí. Zdroje potřebné pro chod apliance záleží na rolích, které na ní budete instalovat a jestli použijete Replica Set a nebo ne.

**Poznámka**
Replica Set je funkce MongoDB která se stará o replicaci databáze a zajišťuje zároveň redundanci a vysokou dostupnost ukládaných dat. Pro více podrobností, si přečtěte MongoDB dokumentaci a „Správa GravityZone Appliance“ (str. 106).

Bitdefender HVI také vyžaduje značný počet zdrojů. Pokud chcete využít tuto službu, prosím zkontrolujte si potřebná specifická data v tabulkách. Ohledně úplných požadavků služby, se podívejte do „HVI“ (str. 48).

**Důležité**
Měření jsou výsledkem Bitdefender interních testů na základní GravityZone konfiguraci a během běžného užívání. Výsledky se můžou lišit podle použité síťové konfigurace, nainstalovaného software, počtu generovaných událostí, etc. Pro vlastní metriky a potřeby škálovatelnosti, prosím kontaktujteBitdefender.

## vCPU

Následující tabulka vás informuje o počtu vCPU každá role virtuální appliance vyžaduje.

Každá vCPU musí být minimálně 2GHz.

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| **GravityZone základní funkce** | | | | | | | | |
| Aktualizační Server (Update Server)* | 10 | 14 | 16 | 18 | 4 | 4 | 6 | 8 |
| Webová Konzole (Web Console)** | | | | | 6 | 10 | 12 | 12 |
| Komunikační server | | | | | 6 | 10 | 12 | 18 |
| Databáze (Database)*** | | | | | 6 | 6 | 9 | 12 |
| Server Incidentů | | | | | 4 | 4 | 6 | 6 |
| **Celkem** | **10** | **14** | **16** | **18** | **26** | **34** | **45** | **56** |
| **GravityZone s Bitdefender HVI** | | | | | | | | |
| Aktualizační Server (Update Server)* | 10 | 4 | 4 | 4 | 4 | 4 | 6 | 8 |

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| Webová Konzole (Web Console)** | | 6 | 8 | 8 | 10 | 10 | 12 | 12 |
| Komunikační server | | 6 | 8 | 8 | 10 | 10 | 16 | 20 |
| Databáze (Database)*** | | 6 | 6 | 6 | 6 | 6 | 9 | 12 |
| Server Incidentů | | 2 | 2 | 2 | 4 | 4 | 6 | 6 |
| **Celkem** | **10** | **24** | **28** | **28** | **34** | **34** | **49** | **58** |

* Doporučeno, když se nasazují role Relay.
** Za každou aktivní integraci, přidejte jednu vCPU na virtuální applianci s rolí Webové Konzole rolí (Web Console role).
*** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

## RAM (GB)

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| **GravityZone základní funkce** | | | | | | | | |
| Aktualizační server | 18 | 18 | 20 | 22 | 2 | 2 | 3 | 3 |
| Webová Konzole (Web Console)* | | | | | 8 | 8 | 12 | 16 |
| Komunikační server | | | | | 6 | 12 | 12 | 16 |
| Databáze (Database)** | | | | | 8 | 10 | 12 | 12 |
| Server Incidentů | | | | | 2 | 2 | 4 | 4 |
| **Celkem** | **18** | **18** | **20** | **22** | **26** | **34** | **43** | **51** |
| **GravityZone s Bitdefender HVI** | | | | | | | | |
| Aktualizační server | 18 | 2 | 2 | 2 | 2 | 2 | 3 | 3 |
| Webová Konzole (Web Console)* | | 8 | 10 | 10 | 10 | 10 | 12 | 16 |

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| Komunikační server | | 8 | 10 | 10 | 12 | 12 | 16 | 20 |
| Databáze (Database)** | | 8 | 8 | 8 | 8 | 12 | 12 | 12 |
| Server Incidentů | | 2 | 2 | 2 | 2 | 2 | 4 | 4 |
| **Celkem** | **18** | **28** | **32** | **32** | **36** | **40** | **47** | **55** |

** Za každou aktivní integraci, přidejte jeden GB RAM na virtuální applianci s rolí Webové Konzole rolí (Web Console role).
*** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

## Volné místo na disku (GB)

| Komponenta | Počet koncových bodů (do) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 250 | 250* | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| **GravityZone základní funkce** | | | | | | | | | |
| Aktualizační server | 150 | **190** | 190 | 230 | 230 | 80 | 80 | 80 | 80 |
| Webová Konzole | | | | | | 80 | 80 | 80 | 80 |
| Komunikační server | | | | | | 80 | 80 | 80 | 80 |
| Databáze (Database)** | | | | | | 110 | 150 | 230 | 530 |
| **Celkem** | **150** | **190** | **190** | **230** | **230** | **350** | **390** | **470** | **770** |
| **GravityZone s Bitdefender HVI** | | | | | | | | | |
| Aktualizační server | 150 | 190 | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Webová Konzole | | | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Komunikační server | | | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Databáze (Database)** | | | 110 | 110 | 130 | 130 | 190 | 330 | 730 |
| **Celkem** | **150** | **190** | **350** | **350** | **370** | **370** | **430** | **570** | **970** |

**Důležité**
Důrazně doporučujeme použít SSD disky (Solid-state drives).

* Další místo na SSD disku je potřeba v případě že používáte automatickou instalaci, protože také instaluje roli Security Server. Po dokončení instalace můžete odinstalovat Security Server pro uvolnění místa na disku.
*** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

**Poznámka**
Je-li nainstalována role serveru Incident, je pro databázi potřeba dalších 30 GB místa. Množství místa již bylo přidáno do role databáze ve výše uvedené tabulce.

## 4.1.3. Internetové připojení

GravityZone appliance potřebuje Internetový přístup.

## 4.2. Control Center

K přístupu do Control Center webové konozole správy, je potřeba následující:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Doporučené rozlišení monitoru: 1280 x 800 nebo vyšší
- Počítač, který připojíte, musí mít síťové připojení ke Control Center.

**Varování**
Control Center nebude pracovat / zobrazovat se správně v Internet Exploreru 9+ se zapnutou funkcí kompatibility zobrazení (Compatibility View feature enabled), což se rovná defakto použití nepodporované verze prohlížeče.

## 4.3. Ochrana Koncových zařízení

Abyste ochránili vaši síť v rámci vaší Bitdefender, musíte nainstalovat GravityZone bezpečnostní agenty na koncových bodech v síti.  pro optimalizovanou ochranu, můžete také nainstalovat Security Servers (bezpečnostní servery). Za tímto účelem potřebujete Control Center uživatele s administračníma právama pro služby které potřebujete nainstalovat a také pro koncové body v síti pod vaší správou.

Požadavky pro bezpečnostní agenty jsou rozdílná, podle toho jestli mají další server role, jakožto třeba role Relay, Ochranu Exchange (Exchange Protection) nebo Patch Caching Server. Pro další informace k rolím agentů čtěte „Bezpečnostní agenty“ (str. 13).

## 4.3.1. Hardware

### Bezpečnostní agenti bez rolí

#### Utilizace CPU

| Cílové systémy | Druh CPU | Podporované Operační Systémy (OS) |
|---|---|---|
| Pracovní stanice | Intel® Pentium kompatibilní procesory, 2 GHz nebo rychlejší | Microsoft Windows desktopové OS |
| | Intel® Core 2 Duo, 2 GHz nebo rychlejší | macOS |
| Chytrá zařízení | Intel® Pentium kompatibilní procesory, 800 MHZ nebo rychlejší | Microsoft Windows embedded OS |
| Servery | Minimum: Intel® Pentium compatibilní processory, 2.4 GHz | Microsoft Windows Server OS a Linux OS |
| | Doporučené: Intel® Xeon multi-core CPU, 1.86 GHz nebo rychlejší | |

**Varování**
Procesory ARM v současné době nejsou podporovány.

#### Volná Paměť RAM

**Instalace (MB)**

| OS | JEDNOTLIVÝ ENGINE | | | | | |
|---|---|---|---|---|---|---|
| | Lokální Skenování | | Hybridní Skenování | | Centralizované Skenování | |
| | Pouze AV | Úplné Možnosti | Pouze AV | Úplné Možnosti | Pouze AV | Úplné Možnosti |
| Windows | 1024 | 1200 | 512 | 660 | 256 | 400 |
| Linux | 1024 | 1024 | 512 | 512 | 256 | 256 |
| macOS | 1024 | 1024 | n/a | n/a | n/a | n/a |

**Pro každodenní používání (MB)***

| OS | Antivirus (Jednotlivý Engine) | | | Ochranné Moduly | | | | |
|---|---|---|---|---|---|---|---|---|
| | Lokální | Hybrid | Centralizované | Sken Chování | Firewall | Kontrola Obsahu | Power User | Update Server |
| Windows | 75 | 55 | 30 | +13 | +17 | +41 | +29 | +80 |
| Linux | 200 | 180 | 90 | - | - | - | - | - |
| macOS | 650 | - | - | +100 | - | +50 | - | - |

* Měření pokrývá každodenní použití klientů zařízení, aniž by byly zohledněny další úkoly, jako jsou skenování na vyžádání nebo aktualizace produktu.

## Uvolnit místo na disku

**Instalace (MB)**

| OS | JEDNOTLIVÝ ENGINE | | | | | | DVOJITÝ ENGI | | |
|---|---|---|---|---|---|---|---|---|---|
| | Lokální Skenování | | Hybridní Skenování | | Centralizované Skenování | | Centralizované + Lokální Skenování | | Centr H Sk |
| | Pouze AV | Úplné Možnosti | Pouze AV | Úplné Možnosti | Pouze AV | Úplné Možnosti | Pouze AV | Úplné Možnosti | Pouz AV |
| Windows | 1024 | 1200 | 500 | 700 | 350 | 570 | 1024 | 1200 | 500 |
| Linux | 1600 | 1600 | 1100 | 1100 | 600 | 600 | 1600 | 1600 | 110 |
| macOS | 1024 | 1024 | n/a | n/a | n/a | n/a | n/a | n/a | n/a |

**Pro každodenní používání (MB)***

| OS | Antivirus (Jednotlivý Engine) | | | Ochranné Moduly | | | | |
|---|---|---|---|---|---|---|---|---|
| | Lokální | Hybrid | Centralizované | Sken Chování | Firewall | Kontrola Obsahu | Power User | Update Server |
| Windows | 410 | 190 | 140 | +12 | +5 | +60 | +80 | +10 |
| Linux | 500 | 200 | 110 | - | - | - | - | - |
| macOS | 1700 | - | - | +20 | - | +0 | - | - |

* Měření pokrývá každodenní použití klientů zařízení, aniž by byly zohledněny další úkoly, jako jsou skenování na vyžádání nebo aktualizace produktu.

## Bezpečnostní Agent s rolí Relay

Relay role potřebuje další hardware zdroje navíc v porovnání s základní konfiguraci bezpečnostního agenta. Tyto nároky na zdroje jsou potřebné pro podporu Aktualizačního Serveru (Update Serveru) a instalaci balíčků hostovaných na koncovém bodu:

| Počet připojených koncových bodů | CPU potřebné pro podporu Aktualizačního Serveru (Update Serveru) | RAM | Volné nísto na disku pro Aktualizační Server (Update Server) |
|---|---|---|---|
| 1-300 | Minimálně Intel® Core™ i3 nebo srovnatelný procesor, 2 vCPU per core | 1.0 GB | 10 GB |
| 300-1000 | minálně Intel® Core™ i5 nebo srovnatelný processor, 4 vCPU per core | 1.0 GB | 10 GB |

**Varování**

- Procesory ARM v současné době nejsou podporovány.
- Agenti Relay potřebují SSD disky, aby mohli podporovat vysoké číslo read/write operací.

**Důležité**

- Pokud chcete ukládat instalační balíčky a aktualizace na jiném oddílu než tam kde je nainstalovaný agent, ujistěte se že oba oddíly mají dostatek volného místa na disku (10 GB), v opačném případě agent přeruší instalaci. Toto je potřeba pouze při instalaci.
- V koncových bodech Windows musí být povoleny místní symbolické odkazy.

## Bezpečnostní Agent s Rolí Ochrany Exchange (Exchange Protection Role)

Karanténa pro Exchange servery vyžaduje na oddílu, na kterém je nainstalovaný bezpečnostní agent, místo na pevném disku navíc.

Velikost karantény závisí na počtu uložených položek a jejich velikosti.

Ve výchozím stavu se agent, nainstaluje na systémový oddíl.

## Bezpečnostní Agent s Patch Caching Server rolí

Agent s rolí Patch Caching Serveru musí splňovat následující kumulativní požadavky:

- Veškeré nároky na hardware jednoduchého agenta (bez rolí)
- Veškeré nároky na hardware pro roli Relay
- Navíc 100 GB volného místa na disku pro ukládání stažených záplat

**Důležité**
Pokud chcete ukládat instalační balíčky a aktualizace na jiném oddílu než tam kde je nainstalovaný agent, ujistěte se že oba oddíly mají dostatek volného místa na disku (100 GB), v opačném případě agent přeruší instalaci. Toto je potřeba pouze při instalaci.

## Požadavky pro VMware vShield prostředí

Toto jsou požadavky pro Bitdefender Tools a provozní zátěž pro systémy integrované do prostředí VMware s vShield koncovým bodem.

| Platforma | RAM | Prostor na disku |
|---|---|---|
| Windows | 6-16* MB (~ 10 MB pro GUI) | 24 MB |
| Linux | 9-10 MB | 10-11 MB |

*5 MB pokud je zapnutá volba tichého módu (Silent Mode option) a 10 MB v případě když je vypnutý. Pokud je tichý mód zapnutý, tak není Bitdefender Tools grafické rozhraní (GUI) spuštěno automaticky při startu systému, proto aby byly uvolněny přidružené zdroje.

## 4.3.2. Podporované Operační Systémy

### Windows Desktop

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Windows 10 říjen 2018 Update (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1 (1)(2)
- Windows 8 (3)
- Windows 7

**Varování**
(1) VMware vShield platform (Bezagentová verze) podporuje Windows 8.1 (32/64 bit) a je dostupná od VMware vSphere 5.5 – ESXi build 1892794 nebo vyšší.
(2) V VMware NSX, je podporována od vSphere 5.5 Patch 2.
(3) VMware NSX, je podporována od vSphere 5.5.

**Varování**
Bitdefender nepodporuje vytváření programů Windows Insider

### Windows Tablet a Embedded

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7

## Windows Server

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2[(1)(2)]
- Windows Server 2012[(3)(4)]
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2[(4)]

**Varování**
(1) VMware vShield platform (Agentless version) podpora pro Windows Server 2012 R2 (64 bit) je dostupná od verze VMware vSphere 5.5 – ESXi build 1892794 a nebo novější.
(2) V VMware NSX, je podporována od vSphere 5.5 Patch 2.
(3) VMware NSX, je podporována od vSphere 5.5.
(4) VMware NSX nepodporuje 32-bit verze Windows 2012 a Windows Server 2008 R2.

## Linux

**Důležité**
Koncové body se systém Linux používají licenční místa ze skupiny licencí pro operační systémy serveru.

- Ubuntu 14. 04 LTS nebo vyšší
- Red Hat Enterprise Linux / CentOS 6.0 nebo vyšší[(2)]
- SUSE Linux Enterprise Server 11 SP4 nebo vyšší
- OpenSUSE Leap 42.x
- Fedora 25 a vyšší[(1)]

- Debian 8.0 a vyšší
- Oracle Linux 6.3 a vyšší
- Amazon Linux AMI 2016.09 nebo vyšší
- Amazon Linux 2

**Varování**
(1) Na Fedoře 28 a vyšší, Bitdefender Endpoint Security Tools vyžaduje ruční instalaci balíčku `libnsl`, spuštěním následujícího příkazu:

```
sudo dnf install libnsl -y
```

(2) Pro minimální instalace CentOS Bitdefender Endpoint Security Tools vyžaduje ruční instalaci balí čku `libnsl`, spuštěním následujícího příkazu:

```
sudo yum install libnsl
```

## Předpožadavky Active Directory

Při integraci koncových bodů Linuxu s doménou služby Active Directory prostřednictvím systému System Security Services Daemon (SSSD) zajistěte, aby **ldbsearch, krb5-user,** a **Jsou nainstalovány nástroje krb5-config** a kerberos je správně nakonfigurován.

```
/etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
        ccache_type = 4
        forwardable = true
        proxiable = true
```

```
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab

[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

**Poznámka**
Všechny položky rozlišují velká a malá písmena.

## Podpora Skenování Při Přístupu

Skenování při přístupu je dostupné pro všechny podporované guest operační systémy. Na systémech Linux, podpora skenování při přístupu je poskytnutá při následujících situacích:

| Verze Kernel | Distribuce Linux | Požadavky Při Přístupu |
|---|---|---|
| 2.6.38 a vyšší* | Red Hat Enterprise Linux / CentOS 6.0 a vyšší<br>Ubuntu 14.04 a vyšší<br>SUSE Linux Enterprise Server 11 SP4 nebo vyšší | **Fanotify** (možnost kernel) musí být povolen |

| Verze Kernel | Distribuce Linux | Požadavky Při Přístupu |
|---|---|---|
| | OpenSUSE Leap 42.x<br>Fedora 25 a vyšší<br>Debian 9.0 a vyšší<br>Oracle Linux 6.3 a vyšší<br>Amazon Linux AMI 2016.09 nebo vyšší | |
| 2.6.38 a vyšší | Debian 8 | **Fanotify** musí být povolen a nastaven na režim vynucení a poté musíte přestavit balíček kernel.<br>Pro detaily, se obraťte se na tento KB článek. |
| 2.6.32 - 2.6.37 | CentOS 6.x<br>Red Hat Enterprise Linux 6.x | Bitdefender poskytuje podporu přes **DazukoFS** s před vystavěnými moduly kernel. |
| Všechny další kernel | Všechny ostatní podporované systémy | Modul **DazukoFS** musí být ručně kompilován. Více informací naleznete na „Manuálně zkompilujte DazukoFS module“ (str. 152). |

* S určitými omezeními popsanými níže.

## Omezení Skenování Při Přístupu

| Verze Kernel | Distribuce Linux | Podrobnosti |
|---|---|---|
| 2.6.38 a vyšší | Všechny podporované systémy | Sledování skenování při přístupu na připojené síťové sdílení podle těchto podmínek:<br>• **Fanotify** je povolen na obou jak na vzdáleném tak i na lokálním systému.<br>• Sdílení je založené na CIFS a NGS souborových systémech. |

| Verze Kernel | Distribuce Linux | Podrobnosti |
|---|---|---|
| | | **Poznámka**<br>Skenování při přístupu neskenuje síťově sdílené položky připojené pomocí SSH nebo FTP. |
| Všechny kernel | Všechny podporované systémy | Skenování při přístupu není podporováno na systémech s **DazukoFS** pro připojené síťová sdílení na cesty, které jsou již chráněny module Při přístupu. |

### Podpora Endpoint Detection and Response (EDR)

Úplný a aktuální seznam verzí jádra a distribucí Linuxu, které podporují senzor EDR, najdete na této webové stránce .

## macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Kontrola obsahu není v macOS Big Sur (11.0) podporována.

## 4.3.3. Podporované Souborové Systémy

Bitdefender instaluje na a chrání následující souborové systémy:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

**Poznámka**
Podpora skenování při přístupu není poskytnuta pro NFS a CIFS/SMB.

### 4.3.4. Podporované Prohlížeče

Zabezpečení koncového prohlížeče je ověřeno u těchto následujících prohlížečů:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

### 4.3.5. Podporované Virtualizační Platformy

Security for Virtualized Environments poskytuje podporu "mimo krabici" pro následující virtualizační platformy:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  **Poznámka**
  Funkce Workload Management ve vSphere 7.0 není podporována.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (včetně Xen Hypervisor)
- Virtuální aplikace a desktopy Citrix 7 1808, 7 1811, 7 1903, 7 190
- Citrix XenApp a XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 nebo Windows Server 2008 R2, 2012, 2012 R2 (zahrnuje Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (zahrnující KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1

- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

**Poznámka**
Podpora ostatních virtualizačních platforem, může být poskytnuta na vyžádání.

## Integrace s požadavky VMware NSX-V

- ESXi 5.5 nebo novější na každém serveru
- vCenter Server 5.5 nebo novější
- NSX Manager 6.2.4 nebo novější.
- VMware Tools 9.1.0 nebo novější, s agentem Guest Introspection.
  - Informace o Windows virtuálních strojích naleznete v následujícím článku článek o VMware Docs.
  - Informace o Linux virtuálních strojích naleznete v následujícím článku článek o VMware Docs.

**Poznámka**
VMware doporučuje použití těchto verzí VMware Tools:
- 10.0.8 nebo novějšír, pro vyřešení pomalých Virtuálních strojů po upgradu VMware Tools ve NSX / vCloud Networking and Security (článek znalostní databáze VMware 2144236).
- 10.0.9 a nebo novější pro Windows 10 podporu.

**Důležité**
Doporučuje se abyste udržovali VMware produkty aktualizované pomocí aktualizací.

## Požadavky na integraci s VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 nebo 3.0
- SXi kompatibilní s verzí NSX-T Manageru
- vCenter Server a vSphere kompatibilní s verzí NSX-T Manageru

- VMware Tools s tenkým agentem Guest Introspection, kompatibilní s verzí NSX-T Manageru

Další podrobnosti o kompatibilitě najdete na těchto webových stránkách VMware:

- Průvodce VMware Compatibility Guide - GravityZone vs. NSX-T Manager
- Matice interoperability produktů VMware - NSX-T Data Center vs. VMware vCenter a VMware Tools

## Požadavky na Integraci s Nutanix Prism Element

- Přístupové údaje Nutanix Prism Element uživatele s administračními právy (Cluster Admin nebo User Admin)
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

## Podporované Cloud Platformy

Společně s on premise virtualizačními prostředími, GravityZone se může integrovat také s následujícími cloud platformami:

- **Amazon EC2**

  Jakožto zákazník Amazon EC2, můžete integrovat inventáře EC2 instancí seskupených podle regionů a zón dostupnosti se síťovým inventářem GravityZone.

- **Microsoft Azure**

  Jakožto Microsoft Azure zákazník, si můžete zintegrovat virtuální stroje v Microsoft Azure seskupené podle regionů a zóny dostupnposti spolu s síťovým inventářem GravityZone.

## Kompatibilita s technologiemi pro virtualizaci desktopů a aplikací

GravityZone je kompatibilní s následujícími virtualizačními technologiemi, počínaje Bitdefender Endpoint Security Tools verzí 6.6.16.226:

- **VMware:**

  VMware V-App (stejná verze jako vCenter Server)

VMware ThinApp 5.2.6

VMware AppVolumes 2.180

**Důležité**
Doporučuje se neinstalovat do zásobníku aplikací nebo zapisovatelných svazků.

- **Microsoft:**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix:**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

  **Důležité**
  Přiřaďte zásady na základě uživatelských pravidel, aby Řízení zařízení nezabránilo vytváření vrstev OS a platforem.
  Možná bude nutné nakonfigurovat pravidla brány firewall GravityZone, aby bylo možné povolit síťový provoz pro každou z těchto aplikací. Další informace naleznete v dokumentaci k produktu Citrix App Layering .

## Podporované Nástroje Správy Virtualizace

Control Center se právě integruje s následujícími nástroji správy virtualizace:

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

Pro vytvoření integrace, musíte poskytnout uživatelské jméno a heslo administrátora.

## 4.3.6. Security Server

Security Server je předkonfigurový virtální stroj běžící na Ubuntu Serveru s následujícími verzemi:

- 16.04 (VMware NSX a Multi-Platform)
- 12.04 LTS (VMware vShield)

## Paměť a CPU

Alokované zdroje Paměti a CPU pro Security Server závisí na počtu a typu běžících VM na hostovi. Následující tabulka ukazuje doporučované zdroje k alokování:

| Počet chráněných VM | RAM | CPU |
|---|---|---|
| 1-50 VM | 2 GB | 2 CPU |
| 51-100 VM | 2 GB | 4 CPU |
| 101-200 VM | 4 GB | 6 CPU |

Security Server v případě NSX se dodává s předdefinovanou hardwarovou konnfigurací (CPU and RAM),kterou si můžete upravit ve VMware vSphere Web klientovi když vypnete tento stroj, upravíte jeho nastavení a zase ho zapnete. Podrobné informace viz „Instalace Security Server pro VMware NSX“ (str. 124).

## Místo na HDD

| Prostředí | HDD Space Provisioning |
|---|---|
| VMware NSX-V / NSX-T | 40 GB |
| VMware with vShield Endpoint | 40 GB |
| Jiné | 16 GB |

## Security Server Distribuce na hostitelích

| Prostředí | Security Server vs. Hosts |
|---|---|
| VMware NSX-V / NSX-T | Při nasazení Bitdefender služby se Security Server automaticky instaluje na každém ESXi hostu v clusteru, tak aby byl mohl být chráněn. |
| VMware with vShield Endpoint | Security Server musí být nainstalován na každém ESXi hostu, tak aby byl chráněn. |
| Jiné | I když to není povinné, Bitdefender doporučuje nainstalovat Security Server na každého fyzického host pro zlepšení výkonu. |

### Síťové zpoždění

Komunikační latence mezi Security Server a chráněnými koncovými body musí být menší než 50 ms.

### Nahrání ochrany pro uložiště

Dopad na ochranu úložiště na Security Server při skenování 20 GB je následující:

| Stav ochrany úložišť (Storage Protection status) | zdroje Security Serveru | zatížení Security Serveru | Čas přenosu (mm:ss) |
|---|---|---|---|
| Vypnutá základna (baseline) | N/A | N/A | 10:10 |
| Zapnuto | 4 vCPU<br>4 GB RAM | Normální | 10:30 |
| Zapnuto | 2 vCPU<br>2 GB RAM | těžký (náročný na zdroje) | 11:23 |

**Poznámka**
Tyto výsledky jsou získávány společně s variací příkladů různých druhů souborů (.exe, .txt, .doc, .eml, .pdf, .zip etc.), v rozsahu od 10 KB do 200 MB. Čas přenosu je adekvátní k přenášenému objemu dat 20 GB obsažených v 46,500 souborech.

## 4.3.7. Využití Provozu

- **Provoz aktualizací produktu mezi koncovým klientem a aktualizačním serverem**

  Každá pravidelná aktualizace produktu Bitdefender Endpoint Security Tools se generuje následující provoz stahování na každém koncovém klientu:

  - Na OS Windows: ~20 MB
  - Na OS Linux: ~26 MB
  - Na macOS: ~25 MB

- **Stažené aktualizace obsahu zabezpečení mezi koncovým klientem a aktualizačním serverem (MB / denně)**

| Typ Aktualizačního Serveru | Typ Skenovacího Enginu | | |
|---|---|---|---|
| | Lokální | Hybrid | Centralizované |
| Relay | 65 | 58 | 55 |
| Bitdefender veřejný Aktualizační (Update) Server | 3 | 3.5 | 3 |

- **Provoz Centrálního Skenu mezi koncovým klientem a Security Server**

| Skenované Objekty | Typ Provozu | | Stažené (MB) | Nahrané (MB) |
|---|---|---|---|---|
| Soubory* | První sken | | 27 | 841 |
| | Cached sken | | 13 | 382 |
| Weby** | První sken | Webový přenos | 621 | N/A |
| | | Security Server | 54 | 1050 |
| | Cached sken | Webový přenos | 654 | N/A |
| | | Security Server | 0.2 | 0.5 |

* Poskytnutá data byla změřena v 3.49 GB souborů (6,658 souborů), ze kterých 1.16 GB jsou Přenosné Spustitelné (PE) soubory.

** Poskytnutá data byla změněna pro 500 webů z nejvyšších pozic.

- **Hybridní sken provozu mezi koncovým klientem a Bitdefender Cloudovými Službami**

| Skenované Objekty | Typ Provozu | Stažené (MB) | Nahrané (MB) |
|---|---|---|---|
| Soubory* | První sken | 1.7 | 0.6 |
| | Cached sken | 0.6 | 0.3 |
| Webový přenos** | Webový přenos | 650 | N/A |
| | Bitdefender Cloudové Služby | 2.6 | 2.7 |

* Poskytnutá data byla změřena v 3.49 GB souborů (6,658 souborů), ze kterých 1.16 GB jsou Přenosné Spustitelné (PE) soubory.

** Poskytnutá data byla změněna pro 500 webů z nejvyšších pozic.

- **Provoz mezi klienty Bitdefender Endpoint Security Tools Relay a aktualizačním serverem pro stahování obsahu zabezpečení**

  Klienti s rolí Bitdefender Endpoint Security Tools Relay stáhnou ~16 MB / den* z aktualizačního serveru.

  * Dostupné s klienty Bitdefender Endpoint Security Tools od verze 6.2.3.569.

- **Provoz mezi koncovým klientem a webovou konzolí Control Center**

  Průměrný provoz 618 KB / den je generovaný mezi koncovými klienty a webovou konzolí Control Center.

## 4.4. Exchange Ochrana

Security for Exchange je doručován skrze Bitdefender Endpoint Security Tools, který může ochránit jak souborový systém tak i mail server Microsoft Exchange.

### 4.4.1. Podporované Prostředí Microsoft Exchange

Security for Exchange podporuje následující verze Microsoft Exchange a role:

- Exchange Server 2019 s Edge Transport nebo rolí Mailbox
- Exchange Server 2016 s Edge Transport nebo rolí Mailbox
- Exchange Server 2013 s Edge Transport nebo rolí Mailbox
- Exchange Server 2010/2007 s rolí Edge Transport, Hub Transport nebo Mailbox
- Exchange Server 2007/2007 s rolí Edge Transport, Hub Transport nebo Mailbox

Security for Exchange je kompatibilní s Microsoft Exchange Database Availability Groups (DAGs).

### 4.4.2. Systémové požadavky

Security for Exchange je kompatibilní s jakýmkoli fyzickým nebo virtuálním 64-bitovým serverem (Intel nebo AMD) na kterém běží podporovaná verze a role Microsoft Exchange Serveru. Pro detaily ohledně systémových požadavků Bitdefender Endpoint Security Tools, obraťte se na „Bezpečnostní agenti bez rolí“ (str. 25).

Doporučená dostupnost zdrojů serveru:

- Volná Paměť RAM: 1 GB
- Volné Místo na HDD: 1 GB

### 4.4.3. Další Softwarové Požadavky

- Pro Microsoft Exchange Server 2013 se Servisním Balíčkem 1: KB2938053 from Microsoft.
- Pro Microsoft Exchange Server 2007: .NET Framework 3.5 Servisní Balíček 1 a vyšší

## 4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises má následující specifické požadavky:

- ESXi Hypervisor (virtualizační platforma, která bude prostředí provozovat).
- Sandbox Analyzer Virtual Appliance (zařízení pro správu, které bude řídit detonační virtuální stroje).
- Network Security Virtual Appliance (VM, který zapouzdřuje síťový senzor schopný extrahovat užitečné zatížení ze síťového provozu).
- Propojení se stávajícím GravityZone Control Center používaným pro správu na vysoké úrovni prostředí karantény.
- Připojení k internetu ke stažení virtuálního zařízení Sandbox Analyzer s minimální šířkou pásma 5 MBps.

**Důležité**
Ujistěte se, že při stahování a instalaci Sandbox Analyzer nejsou k dispozici žádné jiné aplikace nebo procesy, které by mohly blokovat připojení k internetu.

### 4.5.1. ESXi Hypervisor

Virtuální zařízení Sandbox Analyzer je k dispozici ve formátu OVA a lze jej nasadit na jediného fyzického hostitele, na kterém běží hypervisor VMware ESXi (verze 6.5 nebo 6.7).

#### Hardwarové požadavky na fyzického hostitele

- CPU: celkový počet jader CPU (s ohledem na hyperthreading) lze extrapolovat pomocí výpočtu uvedeného v sekci „Fyzické požadavky na hostitele a škálování hardwaru“ (str. 46).

- RAM: Celkové množství paměti RAM potřebné pro fyzického hostitele lze extrapolovat pomocí výpočtu uvedeného v sekci „Fyzické požadavky na hostitele a škálování hardwaru“ (str. 46).
- Místo na disku: alespoň 1 TB úložiště SSD (přiměřené pro prostředí detonace 8 VM, škálovatelné minimálně 50 GB pro každý další detonační virtuální počítač).
- Síť: jedna vyhrazená karta fyzického síťového rozhraní (NIC).

  Tento NIC lze rozdělit do dvou virtuálních NICu s následujícím mapováním:

  – Jedna NIC pro rozhraní pro správu.

  – Jedna NIC pro detonační síť.

  **Poznámka**
  Pokud to konfigurace hardwaru umožňuje, doporučuje se používat vyhrazené fyzické NIC se stejnými mapováními jako výše uvedené vNIC.

### Softwarové Požadavky

Podporované verze serveru ESXi: 6.5 nebo vyšší, VMFS verze 5.

Další konfigurace na hostiteli ESXi:

- SSH povoleno při spuštění.
- NTP služba nakonfigurována a aktivní.
- Možnost **start/stop s hostitelem** povolena.

**Poznámka**
Sandbox Analyzer je kompatibilní se zkušební verzí VMware ESXi. Pro realné nasazení se však doporučuje provozovat na licencované verzi ESXi.

## 4.5.2. Sandbox Analyzer Virtuální Appliance

Sandbox Analyzer Virtual Appliance poskytuje prakticky neomezenou škálovatelnost, pokud jsou k dispozici dostatečné hardwarové prostředky.

Z celkového množství dostupných zdrojů ESXi Sandbox Analyzer sdílí CPU a RAM mezi správcem Sandbox a detonačními virtuálními stroji.

### Minimální systémové požadavky správce karantény

- 6 vCPU

- 20 GB RAM
- 600 GB místa na disku

Sandbox Manager má tři interní virtuální NICs přidělené takto:

- Jeden NIC pro komunikaci s řídící konzolí (GravityZone Control Center).
- Jeden NIC pro připojení k internetu.
- Jeden NIC pro komunikaci s detonačními VM.

**Poznámka**
Pro umožnění komunikace musí být jak správa ESXi vNIC, tak správa vNIC pro správu Sandbox Manager, ve stejné síti.

## Detonační virtuální stroje

**Systémové požadavky**

- 4 vCPU (overprovisioned v poměru 4:1, viz „Fyzické požadavky na hostitele a škálování hardwaru“ (str. 46))
- 3 GB RAM
- 50 GB místa na disku

Sandbox Analyzer On-Premises poskytuje podporu pro obrazy vlastních virtuálních strojů. To umožňuje detonaci vzorků v prostředí (runtime environment), které napodobuje realistické produkční prostředí.

Vytvoření obrazu virtuálního stroje vyžaduje následující podmínky:

- Obraz virtuálního počítače je ve formátu VMDK, verze 5.0.
- Podporované operační systémy pro budování detonačních virtuálních strojů:
  - Windows 7 64-bit (Jakákoli úroveň aktualizace)
  - Windows 10 64-bit (Jakákoli úroveň aktualizace)

**Důležité**

- Operační systém musí být nainstalován do druhého oddílu v tabulce oddílů a připojen k jednotce C: (výchozí konfigurace instalace systému Windows).
- Místní účet „Administrator“ musí být povolen a musí mít prázdný řetězec hesla (vypnuto heslo).

- Před exportem obrazu VM musíte správně licencovat operační systém a veškerý nainstalovaný software v obrazu virtuálního počítače.

### Software virtuálního stroje

Sandbox Analyzer podporuje detonaci široké škály formátů a typů souborů. Více informací naleznete na „Objekty Sandbox Analyzeru “ (str. 216).

Pro přesvědčivé zprávy se ujistěte, že jste do vlastního obrazu nainstalovali software, který dokáže otevřít konkrétní typ souboru, který chcete detonovat. Více informací naleznete na „Doporučené použití pro detonační VMs“ (str. 217).

## 4.5.3. Síťová Bezpečnostní Virtuální Appliance (Network Security Virtual Appliance)

Network Security Virtuální Appliance provozuje síťový senzor, který extrahuje užitečná zatížení ze síťových toků a odešle je do Sandbox Analyzer. Minimální požadavky na hardware jsou:

- 4 vCPU
- 4 GB RAM
- 1 TB místa na disku
- 2 vNIC

## 4.5.4. Fyzické požadavky na hostitele a škálování hardwaru

Algoritmus škálování prostředí Sandbox Analyzer zvažuje následující vzorec, kde "K" se rovná počtu detonačních slotů (nebo detonačních VM):

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

Podobně jako algoritmus škálování pro hostitele je následující:

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPU
- ESXi Host RAM = 20 GB RAM + K x 5 GB

Hlavní rozdíl mezi prostředky Sandbox Analyzer VA a ESXi je dán prostředky přidělenými každému detonačnímu VM.

Typické detonační prostředí (8 VM) by proto mělo následující požadavky:

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1vCPU = 14 vCPUs
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2GB = 36GB RAM
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

  **Poznámka**
  Každá detonační VM potřebuje 1 vCPU přidělenou pro VA Sandbox Analyzer VA a 1 vCPU pro detonační VM. Detonační VM bude vybavena 4 vCPU, ale bude nadměrně zajištěna v poměru 4:1, což povede k tomu, že pro hostitele ESXi bude potřeba pouze 1 vCPU.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

  **Poznámka**
  RAM se používá v poměru 1:1 mezi Sandbox Analyzer VA, detonačními VM a hostitelem ESXi. Každá detonační VM tedy bude vyžadovat 5 GB RAM od hostitele ESXi, z nichž 2 GB bude přiděleno Sandbox Analyzer VA a 3 GB budou přiděleny samotné detonační VM.

Výsledný fyzický hostitel vyžaduje, ve výše uvedeném scénáři, alespoň 22 jader CPU (včetně hyperthreadingu) a alespoň 60 GB RAM, přičemž dalších 10 až 20% RAM je vyhrazeno pro samotný hypervisor.

Detonace vzorku obvykle trvá devět minut, než se spustí a vygeneruje zpráva o detonaci, a používá všechny zajištěné prostředky. Doporučujeme navrhnout prostředí pro sandboxing počínaje kapacitou detonace (soubory/hodinu) a poté tuto metriku transformovat do potřebných zdrojů na úrovni hostitele a VM.

### 4.5.5. Sandbox Analyzer Požadavky na komunikaci

Sandbox Analyzer Komponenty On-Premises využívají určité komunikační porty vázané na určitá síťová rozhraní, aby mohly mezi sebou komunikovat a/nebo s veřejnými servery Bitdefender.

Prostředí karantény vyžaduje tři síťová rozhraní:

- **eth0 - Správa síťového rozhraní** . Připojuje se k GravityZone a k hostiteli ESXi.

  Doporučuje se připojit eth0 ke stejné síti jako rozhraní pro správu ESXi. Doporučuje se také mapovat na vyhrazený fyzický adaptér.

  Následující tabulka popisuje požadavky na síťovou komunikaci pro eth0:

| Směr | Komunikační porty (na TCP) | Zdroj/cíl |
|---|---|---|
| Odchozí | 8443 | Komunikační server GravityZone |
| | 443 | Virtuální zařízení GravityZone |
| | 80 | Virtuální zařízení GravityZone |
| | 22 | ESXi hostitel |
| | 443 | ESXi API hostitele |
| Příchozí | 8443 | Vše |

- **eth1 - Detonační síť** . Nevyžaduje žádnou konfiguraci. Instalační proces vytvoří potřebné virtuální prostředky.
- **eth2 - síť pro přístup k internetu** . Doporučujeme mít neomezené a nefiltrované připojení k internetu.

  Doporučuje se, aby byla síť pro správu a síť pro přístup k internetu přiřazena k různým podsítím.

GravityZone Virtual Appliance vyžaduje přístup k Sandbox Analyzer Virtual Appliance na portu 443 (na TCP) pro prohlížení a stahování reportů Sandbox Analyzer.

GravityZone Virtual Appliance vyžaduje připojení k Sandbox Analyzer Virtual Appliance na portu 443 (na TCP) pro vyžádání stavu detonovaných vzorků.

## 4.6. HVI

HVI funguje s pomocí dvou komponent: Security Server a HVI Doplňkový Balíček Tyto produktu musí být nainstalovány na hostovi ve vašem virtualizovaném prostředí, kde máte virtuální stroje, které chcete chránit.

**Poznámka**
Službu HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Před nasazením HVI na hosty, ujistěte se, že jsou splněny následující požadavky:

### Podporované Virtualizační Platformy

- Citrix XenServer 7.1 Enterprise Edition nebo vyšší, s nejnovějšími opravami

**Důležité**
Pro jakýkoli XenServer počínaje verzí 7.1, který dosáhl EOL, poskytuje Bitdefender podporu HVI na další dva měsíce. Nejpozději do konce této časové periody, doporučujeme přejít na XenServer s novější Citrixem podporovanou verzi. Další informace najdete v Citrix Legacy Products Matrix a Tabulka Produktů Citrix .

- Citrix Hypervisor 8.0 Enterprise Edition nebo vyšší, s nejnovějšími opravami

**Varování**
Pro Citrix Hypervisor 8.0 musíte nainstalovat opravu XS80E004.

## Podpočované Guest Virtuální Stroje

Virtuální stroje, které chcete chránit pomocí HVI musí splnit následující podmínky:

1. Stroje jsou v režimu HVM virtualizace, to znamená, že jsou plně virtualizované.
2. Na strojích běží podporovaný operační systém:
   - **Operační systémy Windows Desktop (32bitové a 64bitové)**
     - Windows 10 May 2020 Update (20H1)
     - Windows 10 November 2019 Update (19H2)
     - Windows 10 May 2019 Update (19H1)
     - Windows 10 říjen 2018 Update (Redstone 5)
     - Windows 10 April 2018 Update (Redstone 4)
     - Windows 10 Fall Creators Update (Redstone 3)
     - Windows 10 Creators Update (Restone 2)
     - Windows 10 Anniversary Update (Redstone 1)
     - Windows 10 November Update (Threshold 2)
     - Windows 10
     - Windows 8.1
     - Windows 8
     - Windows 7
   - **Operační systémy Windows Server (64bitové)**

Windows Server 2019

Windows Server 2016

Windows Server 2012 / Windows Server 2012 R2

Windows Server 2008 R2

- **Operační systémy Linux (64bitové)**

| Distribuce | Verze | Kernel verze |
|---|---|---|
| Debian | 10 | 4.19 |
| Debian | 9 | 4.9 |
| Debian | 8 | 3.16 |
| Ubuntu | 20.04 LTS | 5.4 |
| Ubuntu | 18.04 LTS | 4.15 |
| Ubuntu | 16.04 LTS | 4.4 |
| Ubuntu | 14.04 LTS | 3.13.139 a novější |
| CentOS | 8.2 | 4.18 |
| CentOS | 8 | 4.18 |
| CentOS | 7 | 3.10 |
| Red Hat Enterprise Linux | 8.2 | 4.18 |
| Red Hat Enterprise Linux | 8 | 4.18 |
| Red Hat Enterprise Linux | 7 | 3.10 |
| Red Hat Enterprise Linux | 6.8 / 6.9 / 6.10 | 2.36.32 |
| SUSE Linux Enterprise Server | 15 SP1 | 4.12 |
| SUSE Linux Enterprise Server | 12 SP4 | 4.12 |
| SUSE Linux Enterprise Server | 12 SP3 | 4.4 |
| SUSE Linux Enterprise Server | 12 SP2 | 4.4 |
| SUSE Linux Enterprise Server | 12 SP1 | 3.12 |
| Oracle Linux | Novější než 7. 5 | 4.1 (UEK/RHCK) |
| Oracle Linux | 7.5 a novější | 4.14 (UEK/RHCK) |

# Hardwarové požadavky pro GravityZone VA

- **Potřebné vCPU**

  Následující tabulka vás informuje o počtu vCPU každá role virtuální appliance vyžaduje.

  Každá vCPU musí být minimálně 2GHz.

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| Aktualizační Server (Update Server)* | 10 | 4 | 4 | 4 | 4 | 4 | 6 | 8 |
| Webová Konzole (Web Console)** | | 6 | 8 | 8 | 10 | 10 | 12 | 12 |
| Komunikační server | | 6 | 8 | 8 | 10 | 10 | 16 | 20 |
| Databáze (Database)*** | | 6 | 6 | 6 | 6 | 6 | 9 | 12 |
| **Celkem** | | **10** | **24** | **28** | **28** | **34** | **34** | **49** | **58** |

  * Doporučeno, když se nasazují role Relay.
  ** Za každou aktivní integraci, přidejte jednu vCPU na virtuální applianci s rolí Webové Konzole rolí (Web Console role).
  *** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

- **Potřebná RAM (GB)**

| Komponenta | Počet koncových bodů (do) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 250 | 500 | 1000 | 3000 | 5000 | 10000 | 25000 | 50000 |
| Aktualizační server | 18 | 2 | 2 | 2 | 2 | 2 | 3 | 3 |
| Webová Konzole (Web Console)* | | 8 | 10 | 10 | 10 | 10 | 12 | 16 |
| Komunikační server | | 8 | 10 | 10 | 12 | 12 | 16 | 20 |
| Databáze (Database)** | | 8 | 8 | 8 | 8 | 12 | 12 | 12 |
| **Celkem** | | **18** | **28** | **32** | **32** | **36** | **40** | **47** | **55** |

** Za každou aktivní integraci, přidejte jeden GB RAM na virtuální applianci s rolí Webové Konzole rolí (Web Console role).
*** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

- **Potřebné místo na pevném disku (GB)**

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Aktualizační server | 150 | 190 | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Webová Konzole | | | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Komunikační server | | | 80 | 80 | 80 | 80 | 80 | 80 | 80 |
| Databáze (Database)** | | | 110 | 110 | 130 | 130 | 190 | 330 | 730 |
| **Celkem** | **150** | **190** | **350** | **350** | **370** | **370** | **430** | **570** | **970** |

* Další místo na SSD disku je potřeba v případě že používáte automatickou instalaci, protože také instaluje roli Security Server. Po dokončení instalace můžete odinstalovat Security Server pro uvolnění místa na disku.
*** V případě, že používáte distribuované instalace různých rolí spolu s Replica Setem: za každou další instanci Databáze, přidejte vyspecifikované číslo k celkovému počtu.

**Poznámka**
Je-li nainstalována role serveru Incident, je pro databázi potřeba dalších 30 GB místa. Množství místa již bylo přidáno do role databáze ve výše uvedené tabulce.

## Hardwarové požadavky pro Hosty

- **CPU mikroarchitektura:**
  - Jakýkoli Intel® Sandy Bridge procesor a vyšší, který podporujte Intel® Virtualization Technology.
  - VT-x nebo VT-d přípony musí být povoleny v BIOSu.
- **Volné místo na disku:** Kromě požadovaného místa pro Security Server, HVI vyžaduje dalších 9 MB pro Doplňkový Baláček na každého hosta.

## Požadavky Security Server

Alokované zdroje Paměti a CPU pro Security Server závisí na počtu a typu běžících VM na hostovi. Následující tabulka ukazuje doporučované zdroje k alokování:

| Počet chráněných VM | RAM | CPU |
|---|---|---|
| 1-50 VM | 6 GB | 4 CPU |
| 51-100 VM | 8 GB | 6 CPU |
| 101-200 VM | 16 GB | 8 CPU |

**Volné místo na disku:** Musíte poskytnout 8 GB místa na disku pro každého hosta pro Security Server.

Pro optimální výkon v prostředí XenAPP, upravte zdroje pro Security Server na základě vaší konfigurace, následovně:

| Počet VDA XenAPP | VDA | | Security Server | |
|---|---|---|---|---|
| | CPU | RAM (GB) | CPU | RAM (GB) |
| 1 VDA | 4 / 8 | 12 / 24 | 2 | 4 |
| 2 VDA | 4 / 8 | 12 / 24 | 2 | 8 |
| 4 VDA | 8 | 24 | 2 | 16 |
| 8 VDA | 4 | 12 | 4 | 16 |

### Požadavky Guest Virtuálních Strojů

V běžném nastavení prostředí, pro optimální výkon a poměr konsolidace VM, doporučujeme mít následující minimální hardwarové konfigurace pro guest virtuální stroje:

- **vCPU:** 2 x vCPU
- **RAM:** 3 GB

## 4.7. Šifrování celého disku

GravityZone Full Disk Encryption umožňuje provozovat BitLocker na koncových bodech Windows a FileVault a nástroj příkazového řádku diskutil na koncových bodech MacOS přes Control Center.

Pro zajištění ochrany dat, tento modul poskytuje full disk encryption pro boot a non-boot svazky, na pevné disky, a ukládá klíče k obnově v případě, že uživatel zapomene jejich hesla.

Modul Šifrování používá existující hadwarové zdroje ve vašem prostředí GravityZone.

Z pohledu softwaru jsou požadavky téměř stejné jako u aplikací BitLocker a FileVault a většina omezení se týká těchto dvou nástrojů.

## Na Windows

GravityZone Encryption podporuje BitLocker, počínaje verzí 1. 2, na počítačích s čipem Trusted Platform Module (TPM) a bez něj.

GravityZone podporujte BitLocker na zařízeních s následujícími operačními systémy:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro
- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (s TPM)
- Windows 7 Enterprise (s TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (s TPM)

*BitLocker není součástí operačního systému a musí být nainstalován zvlášť. Pro více informací o nasazení BitLocker na Windows Server, obraťte se ba tyto články KB, které poskytl Microsoft:

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

**Důležité**
GravityZone nepodporuje šifrování na Windows 7 a Windows 2008 R2 s TPM.

Pro detaily ohledně požadavků BitLocker, obraťte se na tento článek KB, který poskytl Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

### Na Mac

GravityZone podporuje FileVault na Mac zařízeních s běžícími následujícími operačními systémy:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

## 4.8. Ochrana Úložiště

Podporovaná řešení pro ukládání a sdílení souborů:

- Systémy síťového úložiště (NAS) kompatibilní s ICAP a systémy SAN (Storage Area Network) od společností Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle®, a další
- Nutanix® Soubory 3.x až do 3.6.2
- Citrix® ShareFile

## 4.9. Ochrana mobilních zařízení (Mobile Protection)

### 4.9.1. Podporované Platformy

Security for Mobile podporuje následující druhy mobilních zařízení a operačních systémů:

- Apple iPhony a iPad tablety (iOS 8.1+)
- Chytré telefony a tablety Google Android (4.2+)

### 4.9.2. Požadavky na konektivitu

Mobilní zařízení musí mít zapnutá aktivní mobilní data a nebo Wi-Fi připojení a navázané spojení s Komunikačním Serverem (Communication Server).

### 4.9.3. Push Notifikace

Security for Mobile používá push notifikace pro upozornění na mobilních klientech v případě, že jsou pro ně dostupné aktualizace politik a nebo nějaké úlohy. Push notifikace posílá komunikační server (Communication Server) prostřednictvím služby dodávané výrobcem operačního systému:

- Služba Firebase Cloud Messaging (FCM) pro zařízení Android. Aby FCM fungovalo, je potřeba splnit následující podmínky:
  - Musí být nainstalován Google Play Store.
  - Zařízení se systémem Android 4.2 nebo novějším.
  - Aby bylo možné posílat push notifikace, příslušná čísla portů musí být otevřena.
- Služba Apple Push Notifications (APNs) pro iOS zařízení. Pro více informací si přečtěte Článek v znalostbí databázi Apple (Apple KB article).

Zda mobilní push notifikace fungují správně se můžete ujistit v sekci **Ověření Push Mobile Notifikací (Mobile Push Notifications)** v **Konfigurace (Configuration) > Různé (Miscellaneous)**.

Pro další informace k GravityZone Pracovním postupům správy mobilních zařízení (Mobile Device Management workflow), si prosím přečtěte Tento článek v znalostní databázi.

### 4.9.4. Správa iOS Certifikátů

Abyste mohli nastavit infrastruktůru pro správu iOS mobilních zařízení, tak musíte poskytnout několik bezpečnotních certifikátů.

Další informace viz „Certifikáty“ (str. 98).

## 4.10. GravityZone Komunikační Porty

GravityZone je distribuované řešení, což znamená, že jeho komponenty komunikují navzájem pomocí lokální sítě nebo Internetu. Každá komponenta využívá sérii portů

pro komunikaci s ostatními. Musíte se ujistit, že tyto porty jsou otevřené pro GravityZone.

Pro detailní informace ohledně GravityZone portů, se obraťte na tento článek KB.

# 5. INSTALOVÁNÍ OCHRANY

GravityZone je řešení typu klient-server. Chcete-li chránit svou síť pomocí Bitdefender, musíte nasadit role serveru GravityZone, zaregistrovat svou licenci, nakonfigurovat instalační balíčky a nasadit je prostřednictvím bezpečnostních agentů na koncových bodech. Některé ochranné vrstvy vyžadují instalaci a konfiguraci dalších součástí.

## 5.1. GravityZone instalace a nastavení

Aby proběhla instalace hladce, proveďte následující kroky:

1. Připravte se na instalaci
2. Nasadit a nastavit GravityZone
3. Připojte se do Control Center a nastavte si prvotní uživatelský účet
4. Nakonfigurujte Control Center nastavení

### 5.1.1. Připravte se na Instalaci

Pro instalaci potřebujete GravityZone předpřipravený instalační obraz virtuálního stroje (virtual appliance image). Po nasazení a nastavení appliance GravityZone, můžete vzdáleně instalovat klienty nebo stahovat nezbytné instalační balíčky pro všechny komponenty bezpečnostních služeb z webového rozhraní Control Center.

GravityZone appliance image (předpřipravený instalační obraz virtuálního stroje) je dostupný v mnoha rozdílných formátech, kompatibilní s hlavními virtualizačními platformami. Licenční klíč můžete získat zasláním požadavku na web společnosti Bitdefender v sekci Business Products Inquiry .

Pro instalaci a prvotní nastavení musíte mít následující k dispozici:

- DNS jména nebo pevné IP adresy (buď statickou konfigurací nebo přes DHCP rezervaci) pro všechny vaše GravityZone appliance
- Uživatelské jméno a heslo administrátora domény
- Detailní informace pro vCenter Server, vShield Manager, XenServer (hostname nebo IP adresa, Kommunikační port, jméno administrátora a heslo)
- Licenční klíče (zkontrolujte zkušební registraci nebo e-mail s nákupem)
- Nastavení pro odchozí mail server

- Pokud potřeba, nastavení pro proxy server
- Bezpečnostní certifikáty

## 5.1.2. Nasadit GravityZone

Nasazení GravityZone sestává z jednoho nebo několika zařízení provozujících role serveru. Počet zařízení závisí na různých kritériích, například na: velikosti a designu vaší síťové infrastruktury nebo na funkcích GravityZone, které budete používat. Role serveru jsou tří typů: základní, pomocná a volitelná.

**Důležité**
Pomocné a volitelné role jsou k dispozici pouze u některých řešení GravityZone.

| GravityZone Role | Typ pravidla | Instalovat |
|---|---|---|
| Databázový Server<br>Update Server<br>Webová Konzole<br>Komunikační server | Základní (požadováno) | Alespoň jedna instance každé role.<br>A Zařízení GravityZone může provozovat jednu, několik nebo všechny tyto role. |
| | Pomocný | Jedna appliance pro každou roli |
| Security Server | Volitelné | Doporučeno pouze pro malé sítě nebo na sítě s nízkými zdroji. Jinak nasaďte samostatný Security Server z Control Center po dokončení nasazení GravityZone. |
| Server Incidentů | Vyžadováný | Lze jej nasadit na zařízení all-in-one i distribuovaná. Při instalaci více instancí použijte vestavěný balancerový software. |

Podle toho, jak distribuujete role GravityZone, nasadíte jedno nebo více zařízení GravityZone. Databázový server je první nainstalovaný.

V případě vícero GravityZone appliances, nainstalujte nejprve roli Databázového Serveru na první appliance a pak konfigurujte všechny ostatní appliance tak že je připojíte do stávající databázové instance.

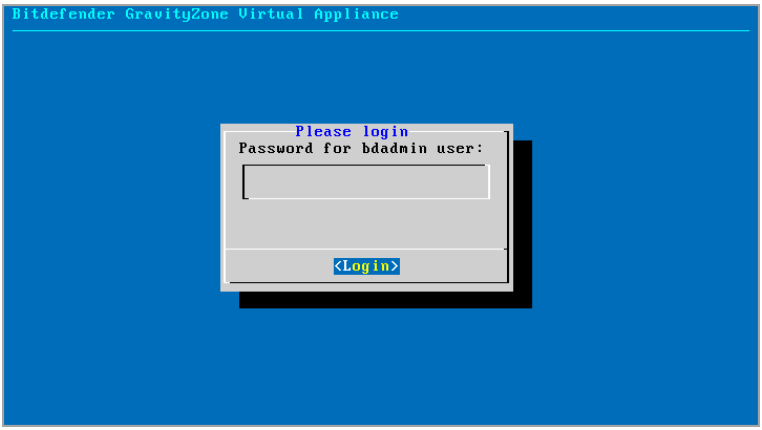
Můžete nasadit více instancí rolí databázového serveru, webové konzoly a komunikačního serveru. V tomto případě použijete sadu replik pro databázový server a vyvažovače zátěže pro webovou konzoli a komunikační server na zařízeních GravityZone.

Nasazení a nastavení GravityZone:

1. Stáhněte si obrázek virtuálního zařízení GravityZone z webu Bitdefender (odkaz uvedený v registračním nebo nákupním e-mailu).
2. Naimportujte GravityZone předpřipravený instalační obraz virtuálního stroje (virtual appliance image) do vašeho virtualizovaného prostředí.
3. Nastartujte appliance.
4. Z nástroje pro správu vašeho virtualizovaného prostředí se připojte do konzole rozhraní (console interface) od GravityZone appliance.
5. Nakonfigurujte heslo pro `bdadmin` , integrovaného správce systému.


Appliance console interface: vložte nové heslo

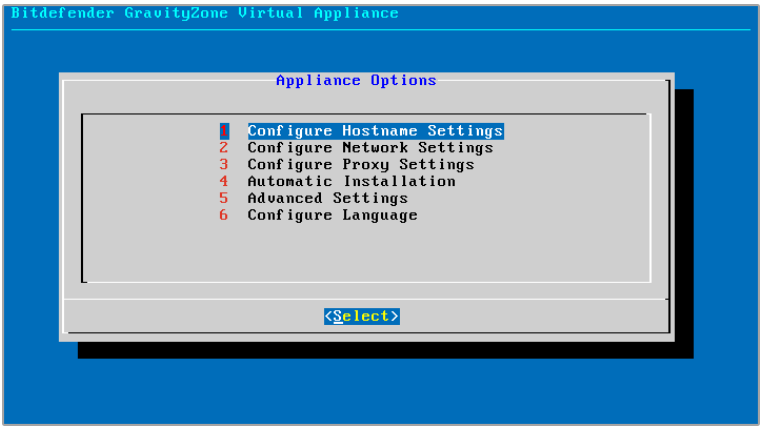
6. Přihlaste se pomocí hesla, které jste právě nastavili.




Appliance console interface: přihlášení

Následně budete přistupovat ke konfiguračnímu rozhraní appliance.

Použijte směrová tlačítka a `Tab` tlačítko k navigaci skrze nabídku menu a možností (options). Stiskněte `Enter` pro vybrání specifické možnosti funkce.




Appliance console interface: hlavní menu

7. Pokud potřebujete změnit jazyk rozhraní, vyberte možnost **Konfigurovat jazyk** . Podrobnosti o konfiguraci najdete v „Nastavit Jazyk“ (str. 68).

8. Nakonfigurujte název hostitele zařízení.
9. Nastavte nastavení sítě.
10. Konfigurujte nastavení serveru proxy. (v případě potřeby)
11. Nainstalujte role serveru GravityZone. Máte dvě možnosti:
    - Automatická Instalace. Tuto možnost vyberte, pokud potřebujete do sítě nasadit pouze jedno zařízení GravityZone.
    - Pokročilá nastavení . Tuto možnost vyberte, pokud potřebujete nasadit GravityZone ručně nebo v distribuované architektuře.

Poté co jste nasadili a nastavili GravityZone appliance, můžete kdykoliv editovat nastavení pomocí konfiguračního rozhraní (configuration interface). Pro více informací ohledně nastavení GravityZone appliance, čtěte „Správa GravityZone Appliance“ (str. 106).

## Nakonfigurujte nastavení Hostname

Komunikace s GravityZone rolemi se provádí skrze použití IP addresy nebo DNS jména appliance na které jsou nainstalovány. Standartně GravityZone komponenty komunikují použitím IP adres. Pokud chcete zapnout komunikaci skrze DNS jména, tak musíte nastavit tyto GravityZone appliance s DNS jménem a zajistit aby tato jména byly korektně překládána na nakonfigurované IP adresy všech vašich appliancí.

Podmínky:

- Nakonfigurujte DNS záznam ve vašem DNS serveru.
- Jméno DNS musí být správně přeloženo na nakonfigurovanou IP adresu apliance. Proto musíte zajistit aby byla appliance nakonfigurována se správnou IP adresou.

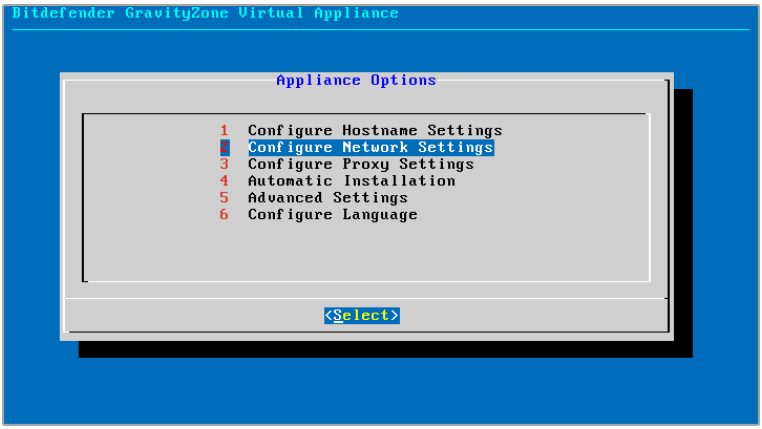
Pro konfiguraci nastavení jména hosta (hostname):

1. Vyberte z hlavního menu **Konfigurace nastavení jména hosta**.
2. Vložte jméno hosta od appliance a název Active Directory domény (pokud potřeba).
3. Vyberte **OK** pro uložení změn.

## Nakonfigurujte Nastavení Sítě

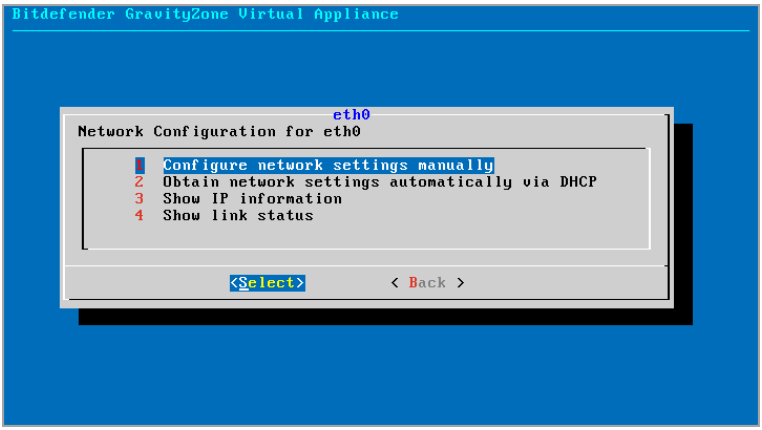
Můžete nakonfigurovat appliance tak aby získala síťová nastavení automaticky od DHCP serveru a nebo můžete nakonfigurovat síťová nastavení ručně. V případě že si vyberete použít DHCP, tak musíte nakonfigurovat DHCP Server tak aby pro appliance rezervoval konkrétní IP adresu.

1. Z hlavního menu vyberte **Konfigurace síťových nastavení (Configure Network Settings)**.




Appliance console interface: konfigurace síťových nastavení

2. Vyberte síťové rozhraní.
3. Vyberte konfigurační metodu:
   - **Nastavit nastavení sítě ručně.** Musíte nastavit IP adresu, masku sítě, adresu brány a adresu DNS serveru.
   - **Získá síťová nastavení automaticky pomocí DHCP.** Použijte tuto volbu pouze když jste nakonfigurovali DHCP Server aby pro vaší appliance rezervoval konkrétní IP adresu.



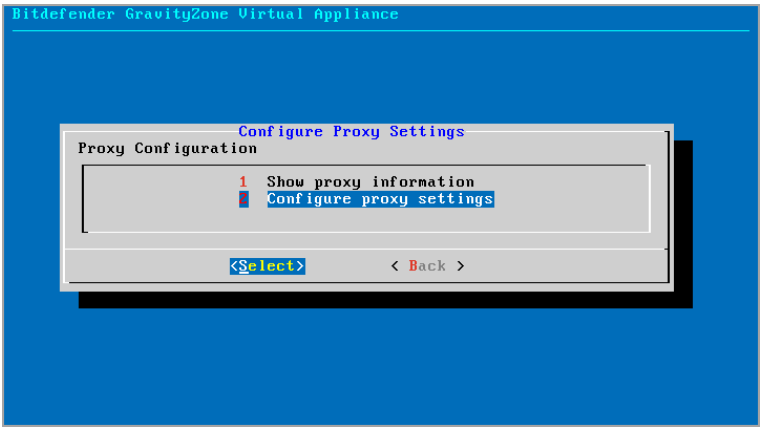

Appliance console interface: síťová konfigurace

4. Můžete si ověřit detaily stávající IP konfigurace nebo stav spojení výběrem odpovídajících opcí.

## Konfigurovat nastavení Proxy

Pokud chcete, aby se zařízení připojilo k Internetu prostřednictvím serveru proxy, musíte nakonfigurovat nastavení serveru proxy.

1. Vyberte z hlavního menu **Konfigurace nastavení proxy**.
2. Vyberte **Zobrazit informace o serveru proxy** a zkontrolujte, zda je server proxy povolen.
3. Výběrem **OK** se vrátíte na předchozí obrazovku.
4. Vyberte znovu **Konfigurovat nastavení serveru proxy** .




Appliance console interface: nakonfigurujte nastavení proxy

5. Zadejte adresu proxy serveru. Použijte následující syntaxi:
   - Pokud proxy server nevyžaduje autentizaci:

     `http(s)://<IP/hostname>:<port>`
   - Pokud proxy server vyžaduje autentizaci:

     `http(s)://<username>:<password>@<IP/hostname>:<port>`
6. Vyberte **OK** pro uložení změn.

## Automatická Instalace

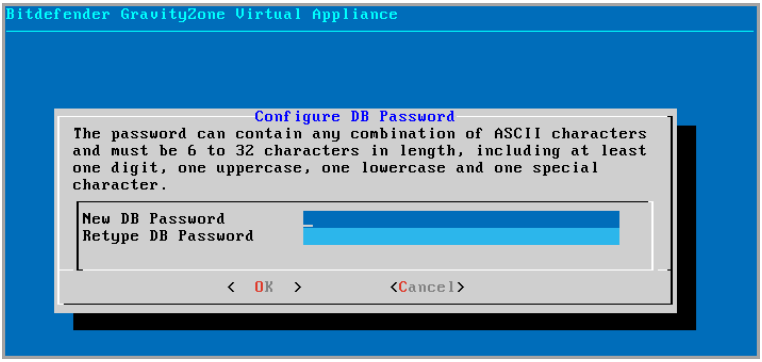
Během automatické instalace se všechny základní role instalují na stejné zařízení. Informace o distribuovaném nasazení GravityZone viz „Pokročilá nastavení“ (str. 66).

**Důležité**
Automatické nasazení také nainstaluje Security Server, zabudovaný do zařízení GravityZone. Informace o Security Server naleznete v části „Architektura GravityZone “ (str. 11).
Možnost automatické instalace rolí je k dispozici pouze při počátečním nastavení GravityZone.

Pro instalaci rolí automaticky:

1. Z hlavního menu, vyberte **Automatická Instalace**.
2. Chcete-li pokračovat, přečtěte si a přijměte licenční smlouvu s koncovým uživatelem (EULA).
3. Potvrďte role, které mají být nainstalovány.
4. Nastavte heslo pro databázový server.

   Heslo může obsahovat jakoukoliv kombinaci ASCII znaků a musí mít délku mezi 6-ti a 32 znaky, zahrnující jednu číslici, jednou velké písmeno, jedno malé písmeno a jeden speciální znak.




Rozhraní konzole Appliance: nastavit heslo databáze

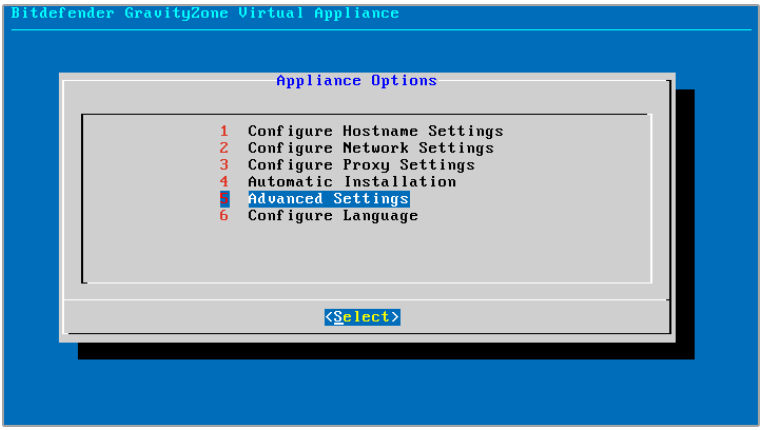
5. Počkejte na dokončení procesu instalace.

## Pokročilá nastavení

Tuto možnost použijte k instalaci pouze části nebo všech rolí GravityZone jednotlivě nebo k rozšíření vaší GravityZone infrastruktury. Role můžete nainstalovat do jednoho nebo více zařízení. Tento způsob instalace je vyžadován při vytváření aktualizací nebo v distribuovaných architekturách GravityZone, aby se škálovalo GravityZone ve velkých sítích a aby byla zajištěna vysoká dostupnost služeb GravityZone.

Chcete-li nainstalovat role jednotlivě:

1. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.




Appliance console interface: instalace rolí

2. Vyberte **Instalace/deinstalace rolí (Install/Uninstall Roles)** pro instalaci appliance v GravityZone prostředí s jedním databázovým serverem.

   **Poznámka**
   Další možnosti jsou pro rozšíření nasazení GravityZone na distribuovanou architekturu. Další informace naleznete v „Připojit k Existující Databázi“ (str. 117) nebo v „Připojit ke stávající databázi (Zabezpečený VPN cluster)“ (str. 118).

3. Vyberte **Přidání nebo odebrání rolí (Add or remove roles)**. Zobrazí se potvrzovací okno.
4. Potvrďte zmáčknutím klávesy `Enter` pro pokračování.
5. Chcete-li nainstalovat roli databázového serveru, stiskněte klávesu `Space` a potom klávesu `Enter` . Potvrďte váš výběr opakovaným stisknutím klávesy `Enter`.
6. Nastavit heslo databáze.

   Heslo může obsahovat jakoukoliv kombinaci ASCII znaků a musí mít délku mezi 6-ti a 32 znaky, zahrnující jednu číslici, jednou velké písmeno, jedno malé písmeno a jeden speciální znak.
7. Zmáčkněte `Enter` a čekejte na dokončení instalace.

8. Nainstalujte další role. Vyberte **Přidat nebo odebrat role** z nabídky **Instalovat/Odinstalovat** a poté nainstalovat role.
   a. V nabídce **Instalovat/Odinstalovat role** vyberte **Přidat nebo odebrat role** .
   b. Přečtěte si licenční smlouvu s koncovým uživatelem. Stiskněte `Enter` pro přijetí a pokračování.

      **Poznámka**
      To je vyžadováno pouze jednou po instalaci databázového serveru.

   c. Vyberte role, které chcete nainstalovat. Stiskněte `Space` (mezerník) pro výběr role a pak `Enter` pro pokračování.
   d. Potvrďte stisknutím klávesy `Enter` a poté počkejte na dokončení instalace.

**Poznámka**
Každá z rolí se nainstaluje standartně během několika minut. Během instalace se požadované soubory stahují z internetu. A proto může v případě pomalého internetového spojení zabrat instalace více času. Pokud instalace zamrzne, tak applianci nasaďte znova od začátku.

## Nastavit Jazyk

Nejprve, je nastaveno konfigurační rozhraní appliance (appliance configuration interface) na Angličtinu.

Pro změnu jazyka konfiguračního rozhraní:

1. Vyberte **Konfigurace Jazyka (Configure Language)** v hlavním menu.
2. Vyberte jazyk z dostupných možností: Zobrazí se potvrzovací okno.

   **Poznámka**
   Případně budete muset listovat dolů abyste našli váš jazyk.

3. Vyberte **OK** pro uložení změn.

## 5.1.3. Control Center Prvotní nastavení

Po nasazení a nastavení GravityZone appliance, se musíte přihlásit do Control Center webového rozhraní (web interface) a nastavit váš firemní administrátorský účet.

1. Do pole pro adresu ve svém webovém prohlížeči zadejte IP adresu nebo DNS hostitelské jméno zařízení Control Center (s prefixem `https://`). Zobrazí se Vám konfigurační pomocník (configuration wizard).
2. Poskytněte licenční klíč, požadovaný k ověření zakoupeného GravityZone řešení.Můžete také poskytnou GravityZone add-on klíč, pokud nějaký máte.

   Prověřte email s registračními údaji ohledně vašich testovacích nebo zakoupených licenčních klíčů.

   a. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.

   b. Vyberte typ licenční registrace (online nebo offline).

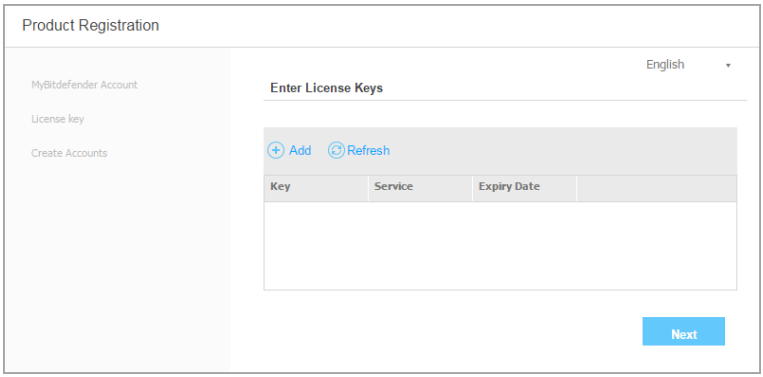
   c. Zadejte licenční klíč do pole **Licenční klíč**. Pro offline registraci, budete také zažádání, aby jste poskytli také registrační kód.

   d. Počkejte dokud nebude licenční klíč validován. klikněte na **Add** pro dokončení.

   Licenční klíč a datum jeho expirace se zobrazí v licenční tabulce.

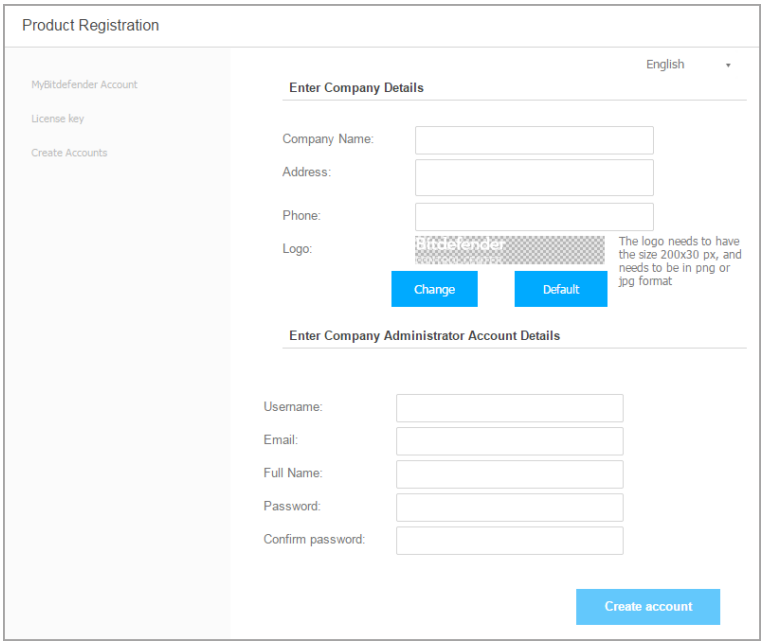
**Poznámka**

- Během počáteční instalace, musíte poskytnou platný základní licenční klíč pro spuštění využívání GravityZone. Můžete později přidat licenční klíče pro add-ony nebo upravit již existující.
- Můžete používat klíče pro rozšíření funkcionalit (add-on licenses) dokud máte platný základní klíč produktu (basic license). V opačném případě sice uvidíte tyto rozšířené funkcionality, ale nebudete je moci používat.




Prvotní nastavení - Zadání licenčního klíče

3. Pokračujte kliknutím na tlačítko **Další**.
4. Vyplňte informace k vaší firmě, jakožto názef firmy, adresa a telefon.
5. Podle následujících pokynů můžete změnit logo zobrazující se v Control Center, a také hlášení a emailová upozornění pro vaši firmu:
   - Klikněte na **Změnit** pro vyhledání obrázku s logem ve vašem počítači. Formát obrázku musí být .png nebo .jpg a jeho velikost musí být 200x30 pixelů.
   - Klikněte na **Výchozí** pro smazání obrázku a obnovení obrázku nastaveného společností Bitdefender.
6. Zadejte potřebné informace k vašemu firemnímu administrátorkému účtu: uživatelské jméno, emailová adresa a heslo. Heslo musí obsahovat alespoň jedno velké písmeno, malé písmeno a alespoň jednu číslici nebo zvláštní znak.




Prvotní nastavení - Konfigurace Vašeho účtu

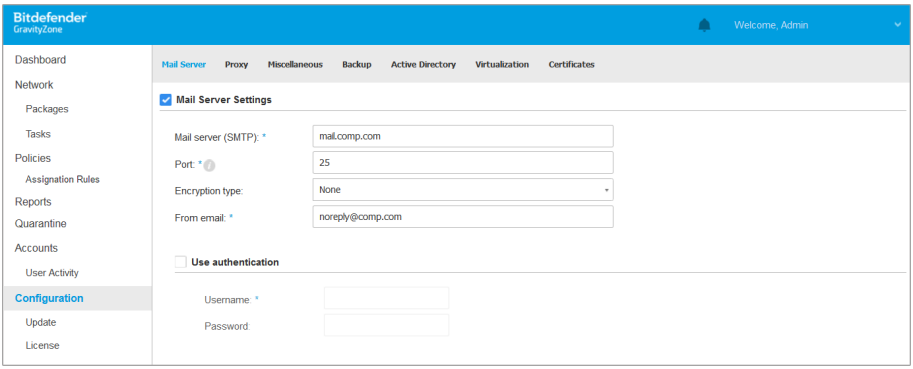
7. Klikněte na **Vytvořte účet (Create account)**.

Firemní administrátorský účet bude vytvořen a vy budete automaticky přihlášeni s tímto novým účtem do Bitdefender Control Center.

## 5.1.4. Nakonfigurujte Control Center nastavení

Po prvotním nastavení potřebujete nakonfigurovat Control Center nastavení. Jakožto firemní administrátor máte právo dělat následující:

- Konfigurovat mail, proxy and jiná všeobecná nastavení.
- Spouštět a plánovat zálohy databáze Control Center.
- Nastavit integraci s Active Directory a nástroji pro správu virtualizace (vCenter Server, XenServer).
- Nainstalovat bezpečnostní certifikáty.




Nastavení Mail Serveru

## Mail Server

Control Center potřebuje externí mailový server pro zasílání emailové kommunikace.

**Poznámka**
Doporučuje se vytvořit dedikovaný mailový účet používaný pro Control Center.

Pro umožnění Control Center posílání emailů:

1. Přejděte na **Konfigurace (Configuration)** stránku.
2. Vyberte **Mail Server** štítek.
3. Vyberte **Nastavení poštovního serveru (Mail Server Settings)** a nakonfigurujte potřebná nastavení:
   - **Mail Server (SMTP).** Zadejte IP adresu nebo název hosta (hostname) poštovního serveru který bude rozesílat emaily.
   - **Port.** zadejte číslo portu pro spojení s poštovním serverem.
   - **Typ šifrování.** Pokud poštovní server potřebuje šifrované spojení ,tak vyberte náležitý typ z menu (SSL, TLS nebo STARTTLS).
   - **Z Emailu.** Vložte emailovou adresu, kterou chcete aby se zobrazovala příjemcům v poli Od (emailová adresa odesílatele).
   - **Použijte ověření.** Vyberte tento zaškrtávací rámeček pokud poštovní server vyžaduje autentizaci. Musíte zadat platné uživatelské jméno / emailovou adresu a heslo.

4. Klikněte na tlačítko **Save**.

Control Center automaticky validuje nastavení pošty jakmile je uložíte. Pokud nemohou být zadané údaje validované, chybová hláška vás bude informovat o nesprávném nastavení. Opravte nastavení správnými údaji a zkuste to znova.

## Proxy

Pokud se vaše firma spojuje do Internetu přes proxy server, tak musíte nakonfigurovat nastavení proxy:

1. Přejděte na **Konfigurace (Configuration)** stránku.
2. Vyberte **Proxy** štítek.
3. Vyberte **Použijte nastavení proxy (Use Proxy Settings)** a nakonfigurujte potřebná nastavení:
   - **Address** - zadejte IP adresu vašeho proxy serveru.
   - **Port** - zadejte číslo portu používaného ke spojení s proxy serverem.
   - **Uživatelské jméno** - zadejte uživatelské jméno rozpoznávané proxy serverem.
   - **Heslo** - zadejte platné heslo pro předtím specifikovaného uživatele.
4. Klikněte na tlačítko **Save**.

## Různé

Z **Konfigurace (Configuration)** stranky > **Různé (Miscellaneous)** štítku můžete nakonfigurovat následující všeobecné předvolby:

- **Kdy budete potřebovat standartně nedostupný Security Server image (předpřipravený instalační obraz virtuálního stroje security serveru).** GravityZone appliance neobsahuje standartně Security Server virtual machine images (předpřipravený instalační obraz virtuálního stroje od security serveru). Pokud administrator zkusí stáhnout Security Server image nebo zkusí spustit instalační úlohu pro Security Server, tak tento pokus skončí nezdarem. Můžete nastavit automatickou akci pro tuhle situaci tím že si vyberete některou z těchto možností:
  - **Stáhnout image automaticky**
  - **Upozorněte administrátora a nestahujte**

**Poznámka**

Abyste zabránili střetu s prací administrátora, tak si můžete manuálně stáhnout potřebné Security Server balíčky z **Update** stránky, na **Aktualizace produktu (Product Update)** štítku. Další informace viz „Stahování produktových aktualizací“ (str. 185).

- **Když je potřebný nedostupný balíček.** Můžete nastavit automatickou akci pro tuhle situaci tím že si vyberete některou z těchto možností:
  - **Automatické stáhnutí balíčku**
  - **Upozorněte administrátora a nestahujte**
- **Současná nasazení.** Administrátor může vzdáleně nasadit jednotlivé bezpečnostní komponenty spuštěním instalačních úloh. Použijte tuto volbu pro specifikaci maximálního počtu nasazení, které mohou být prováděny zároveň.

  Například, pokud bude nastaven maximální počet simultálních úloh pro vzdálenou instalaci klientů na 10 a úloha vzdálené instalace byla přiřazena 100 počítačům tak Control Center pošle prvotně skrze síť v první fázi instalace 10 instalačních balíčků . V případě, že klientská instalace performuje zároveň simultálně na svém maximálním počtu 10 počítačů, tak všechny ostatní pod úlohy jsou přechodně ve frontě ve stavu čekání. Jakmile je pod úloha hotova, tak další instalační balíček je poslán a tak dále...
- **Vynutit dvoufaktorové ověření pro všechny účty.** Dvou faktorová autentizace (2FA) přidává další bezpečnostní vrstvu k ochraně GravityZone účtů, tím že vyžaduje autentizační kód navíc k přihlašovacím údajům do Control Center. Tato funkce vyžaduje stažení a instalaci aplikace pro ověřování Google Authenticator, Microsoft Authenticator nebo jakékoli dvoufaktorové aplikace TOTP (Time-Based One-Time Password Algorithm) - kompatibilní se standardním RFC6238 - na mobilním zařízení uživatele, poté aplikaci propojit s účtem GravityZone a používat ji s každým přihlášením Control Center. Aplikace pro ověřování generuje každých 30 sekund šestimístný kód. Pro dokončení přihlášení do Control Center bude uživatel po zadání hesla muset poskytnout také šestimístný ověřovací kód.

  S touto aktualizací je dvoufaktorová autentizace povolena jako výchozí stav při vytváření společnosti. Po přihlášení se uživatelům zobrazí konfigurační okno s výzvou k povolení této funkce. Uživatelé budou mít možnost přeskočit zapnutí 2FA pouze třikrát. Po čtvrtém pokusu o přihlášení nebude možné přeskočit konfiguraci 2FA ověření a uživatel se nebude moci přihlásit.

Pokud chcete deaktivovat vynucení 2FA ověření pro všechny účty GravityZone ve vaší společnosti, zrušte tuto volbu v nastavení. Než změny vstoupí v platnost, budete informováni potvrzovací zprávou. Od tohoto okamžiku budou mít uživatelé stále 2FA zapnutou, ale budou mít možnost deaktivovat tuto volbu v nastavení jejich účtů.

**Poznámka**

- Nastavení 2FA stavu si můžete prohlédnout pro uživatelský účet na stránce **Účty (Accounts)**.
- V případě, že uživatel se zapnutou 2FA autentizací se nemůže přihlásit do GravityZone (v případě nového zařízení či ztráty tajného klíče), tak můžete resetovat jeho dvou faktorovou autentizaci (2FA) na stránce účtu uživatele v sekci **Dvou-faktorová autentizace (Two-factor authentication)**. Pro více detailních informací, si přečtěte kapitolu z příručky Administátora : **Uživatelské účty (User Accounts) > Správa dvou-faktorové autentizace (Managing Two-factor Authentication)** .

- **Nastavení NTP serveru (NTP Server Settings)**. The NTP server je použit k synchronizaci mezi všemi GravityZone appliancemi. Standartní adresa NTP serveru je předzadaná. Tuto adresu můžete kdykoliv změnit v **Adresa NTP serveru (NTP Server Address)** poli.

  **Poznámka**
  Aby mohly GravityZone appliance komunikovat s NTP Serverem, port 123 (UDP) musí být otevřený.

- **Enable Syslog**. Zapnutím této funkcionality dovolíte GravityZone zasílat notifikace na logging server který používa Syslog protokol. Což Vám umožňuje lepší dohled nad GravityZone událostmi.

  Chcete-li zobrazit nebo nakonfigurovat seznam oznámení odeslaných na server Syslog, viz kapitolu **Oznámení** z Příručky správce GravityZone.

  Abyste umožnili logování na vzdálený syslog server:

  1. Zaškrtněte políčko **Enable Syslog** .
  2. Zadejte jméno serveru nebo IP adresu, preferovaný protokol a port na kterém Syslog poslouchá.
  3. Vyberte formát, ve kterém budou data odeslána na server Syslog:

– **JSON Formát**. JSON je lehký formát pro výměnu dat, který je zcela nezávislý na jakémkoli programovacím jazyce. JSON představuje data ve formátu čitelném pro člověka. Ve formátu JSON jsou podrobnosti každé události strukturovány do objektů, přičemž každý objekt se skládá z dvojice název/hodnota.

  Například:

```
{
    "name":"Login from new device",
    "created":"YYYY-MM-DDThh:mm:ss+hh:ss",
    "company_name":"companyname",
    "user_name":"username",
    "os":"osname",
    "browser_version":"browserversion",
    "browser_name":"browsername",
    "request_time":"DD MMM YYYY, hh:mm:ss +hh:ss",
    "device_ip":"computerip"
}
```

  Pro více informací jděte na www.json.org.

  Toto je výchozí formát v GravityZone.

– **Běžný formát úloh (CEF)**. CEF je otevřený standard vyvinutý společností ArcSight, který zjednodušuje správu protokolu.

  Například:

```
CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new
device|3|start=MMM DD YYYY hh:mm:ss+hh:mm
BitdefenderGZCompanyName=companyname suser=username
BitdefenderGZLoginOS=osname
BitdefenderGZAuthenticationBrowserName=browsername
BitdefenderGZAuthenticationBrowserVersion=browserversion
dvchost=computerip
```

  Další informace naleznete v implementačním standardu ArcSight Common Event Format (CEF) .

V kapitole **Oznámení** v Příručce správce můžete zobrazit dostupné typy oznámení pro každý formát.

4. Klikněte na ⊕ **Přidat(Add)** Tlačítko z **Akce(Action)** sloupce.

Kliknutím na tlačítko **Uložit** aplikujete změny.

## Záloha

Abyste se ujistili, že jsou všechna vaše Control Center data v bezpečí, tak nejspíš budete chtít zálohovat GravityZone databázi. Můžete spouštět manuálně zálohovacích úloh kolik se vám zamane a nebo budete chtít nastavit pravidelné automatické spouštění záloh ve specifikovaném intervalu.

Každý databázový zálohovací příkaz vytvoří `tgz` soubor (GZIP Komprimovaný Tar Archive soubor) do lokace specifikované v nastavení záloh.

V případě, že má vícero administrátorů práva na správu nad nastavením Control Center, tak můžete nakonfigurovat **Nastavení upozornění (Notification Settings)** za účelem upozornění pokaždé když byla záloha databáze dokončena. Pro více informací, si vyhledejte kapitolu **Upozornění (Notifications)** v příručce GravityZone Administrátora.

### Vytváření databázových záloh

Pro spuštění zálohy databáze:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center a klikněte na **Záloha (Backup)** tab.
2. Klikněte na **Zálohovat nyní (Backup Now)** tlačítko na vrchní straně tabulky. Zobrazí se konfigurační okno.
3. Vyberte si typ umístění kam bude záloha uložena:
   - **Lokálně(Local)**, pro uložení zálohy přímo na GravityZone applianci. V tomto případě, musíte specifikovat cestu ke konkrétnímu adresářiGravityZone appliance kam bude záloha uložena.

     GravityZone appliance má adresářovou strukturu Linuxu. Například si můžete vybrat, že se budou vytvářet zálohy v `tmp` adresáři. V tomto případě zadejte `/tmp` v **Cesta(Path)** poli.
   - **FTP**, pro ukládání záloh na FTP server. V tomto případě, zadejte FTP informace v následujících polích.

- **Síť(Network)**, pro ukládání záloh na sdílený síťový disk. V tomto případě zadejte síťovou cestu vaší volby (například, `\\computer\folder`), název domény a přístupové údaje doménového uživatele.

4. Klikněte na tlačítko **Testování nastavení (Test Settings)**. Upozornění formou textového hlášení vás bude notifikovat zda jsou vaše nastavení platná či ne.

   Abyste mohli provést zálohu , tak musí být všechna nastavení platná.

5. Klikněte na tlačítko **Vytvořit**. Stránka **Záloha (Backup)** se vám zobrazí. Nový záznam o provedené záloze bude přidán do seznamu. Zkontrolujte **Stav (Status)** nové zálohy. Jakmile bude záloha dokončena, naleznete `tgz` soubor archivu na předem vyspecifikovaném místě.

> **Poznámka**
> Seznam dostupný na **Záloha (Backup)** stránce obsahuje logy všech vytvořených záloh. Tyto logy nezprostředkovávají přístup k zálohám ale pouze zobrazují detailní informace o vytvořených zálohách.

Pro naplánování zálohy databáze:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center a klikněte na **Záloha (Backup)** tab.
2. Klikněte na tlačítko **Nastavení záloh (Backup Settings)** na vrchní straně tabulky. Zobrazí se konfigurační okno.
3. Vyberte **Plánovaná záloha (Scheduled Backup)**.
4. Nastavte zálohovací interval na (denně, týdně , měsíčně)a zadejte čas spouštění.

   Například můžete nastavit pravidelné plánované zálohy týdně na každý pátek ve 22:00.

5. Nakonfigurujte cílovou cestu pro plánovanou zálohu:
6. Vyberte si typ umístění kam bude záloha uložena:

   - **Lokálně(Local)**, pro uložení zálohy přímo na GravityZone applianci. V tomto případě, musíte specifikovat cestu ke konkrétnímu adresářiGravityZone appliance kam bude záloha uložena.

     GravityZone appliance má adresářovou strukturu Linuxu. Například si můžete vybrat, že se budou vytvářet zálohy v `tmp` adresáři. V tomto případě zadejte `/tmp` v **Cesta(Path)** poli.

- **FTP**, pro ukládání záloh na FTP server. V tomto případě, zadejte FTP informace v následujících polích.
- **Síť(Network)**, pro ukládání záloh na sdílený síťový disk. V tomto případě zadejte síťovou cestu vaší volby (například, `\\computer\folder`), název domény a přístupové údaje doménového uživatele.

7. Klikněte na tlačítko **Testování nastavení (Test Settings)**. Upozornění formou textového hlášení vás bude notifikovat zda jsou vaše nastavení platná či ne.

   Abyste mohli provést zálohu , tak musí být všechna nastavení platná.

8. Klikněte na **Uložit (Save)** pro vytvoření plánované zálohy.

## Obnova z databázové zálohy

Když z jakéhokoliv důvodu vaše GravityZone instance nepracuje správně (nefungujou aktualizace, nefunkční rozhraní/interface, poškozené soubory, chyby, apod.), tak můžete obnovitGravityZone databázi ze zálohy použitím:

- Stejné appliance
- Čerstvého GravityZone image (nově předpřipraveného instalačního obrazu virtuálního stroje)
- Funkce replika setu

Vyberte si volbu která nejlépe odpovídá vaší situaci a proveďte proces obnovy jen poté co jste si pečlivě přečetli nutné podmínky a předpoklady.

### Obnova Databáze do stejné GravityZone VA

#### Podmínky

- Připojte se pomocí SSH na GravityZone applianci, použitím **root** přístupových práv.

  Můžete použít **putty** a **bdadmin** ská přístupová práva k připojení na applianci pomocí SSH, poté spusťte příkaz `sudo su` pro přepnutí na **root** účet.

- GravityZone infrastruktůra se nezměnila od poslední zálohy.
- Záloha je novější než 30. duben 2017 a GravityZone verze je vyšší než 6.2.1-30. V ostatních případech kontaktujte Technický tým podpory.
- V distribuovaných architektůrách GravityZone kde zatím nebyla nastavena funkce replikace databáze (Replica Set).

  Pro ověření správné konfigurace, následujte tyto kroky:

1. Otevřete `/etc/mongodb.conf` soubor.
2. Ujistěte se zda `replSet` není nakonfigurován, jak je popsáno na příkladu níže:

```
# replSet = setname
```

**Poznámka**
Pro obnovu databáze, když je Replica Set zapnutý nastavený, se podívejte na „Obnova databáze v Replica Set prostředí“ (str. 84).

- Neběží Žádné CLI procesy.
  Abyste se ujistili, že neběží žádné CLI procesy spusťte následující příkaz:

```
# killall -9 perl
```

- **mongoconsole** balíček je nainstalován na vaší applianci.
  Pro potvrzení, že podmina je splněna, spusťte následující příkaz:

```
# /opt/bitdefender/bin/mongoshellrestore --version
```

  Příkaz by neměl vrátit žádné chyby, jinak spusťte:

```
# apt-get update
# apt-get install --upgrade mongoconsole
```

### Obnova databáze

1. Přejít na umístění obsahující archiv databáze:

```
# cd /adresář-se-zálohou
```

, Kde `adresář se zálohou` je cesta k umístění se záložními soubory.
Například:

```
# cd /tmp/backup
```

2. Obnova databáze.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_heslo
--authenticationDatabase admin --gzip --drop --archive < \
gz-backup-$rrrrMMDDčasové razítko
```

**Důležité**

Nezapomeňte nahradit `GZ_db_password` skutečným heslem databázového serveru GravityZone a proměnnými časových razítek v názvu archivu za skutečné datum.
Například skutečné datum by mělo vypadat takto:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

3. Restartujte zařízení.

   Obnovení databáze je nyní dokončeno.

## Obnova Databáze z vyřazené (Decommissioned) GravityZone VA

### Podmínky

- Nová instalace GravityZone VA:
  - Se stejnou IP adresou jako puvodní stará appliance
  - V případě že je pouze nainstalována role databázového serveru.

  Můžete stáhnout GravityZone VA image od tut.
- Vytvořte SSH spojení na GravityZone virtualní applianci, použitím **root** přístupových práv.
- GravityZone infrastruktůra se nezměnila od té doby co byl backup vytvořen.
- Záloha je mladší než 30. duben 2017.
- V distribuovaných architektůrách GravityZone kde zatím nebyla nastavena funkce replikace databáze (Replica Set).

Pokud používáte Replica Set ve svém GravityZone prostředí, tak máte také roli Databázopvého Serveru nainstalovnou na dalších appliance instances.

Pro obnovu databáze, když je Replica Set zapnutý nastavený, se podívejte na „Obnova databáze v Replica Set prostředí“ (str. 84).

### Obnova databáze

1. Připojte se k zařízení GravityZone přes SSH a přepněte na **root** .
2. Zastavte VASync:

```
# stop vasync
```

3. Zastavte CLI:

```
# # killall -9 perl
```

4. Přejděte do umístění kde se záloha nachází:

```
# cd /adresář-se-zálohou
```

, Kde `adresář se zálohou` je cesta k umístění se záložními soubory.

Například:

```
# cd /tmp/backup
```

5. Obnova databáze.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_heslo
--authenticationDatabase=admin --gzip --drop \
--archive='/home/bdadmin/gz-backup-$rrrrMMDDčasové razítko
```

**Důležité**

Nezapomeňte nahradit `GZ_db_password` skutečným heslem databázového serveru GravityZone a proměnnými časových razítek v názvu archivu za skutečné datum.

Například skutečné datum by mělo vypadat takto:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

6. Obnovte původní staré appliance ID:

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ-db_password
--eval print(db.applianceInstalls.findOne({name:'db'}).\
applianceId)" --quiet > /opt/bitdefender/etc/applianceid
```

**Důležité**
Nezapomeňte nahradit `GZ_db_password` skutečným heslem databázového serveru GravityZone.

7. Odstraňte odkaz na staré role.

```
# /opt/bitdefender/bin/mongoshell -u bd -p 'GZ_db_heslo
'db.applianceInstalls.remove({ip:db.applianceInstalls.findOne(
{name:"db"}).ip,name:{"$ne": "db"}});' --quiet devdb
```

**Důležité**
Nezapomeňte nahradit `GZ_db_password` skutečným heslem databázového serveru GravityZone.

8. Spusťte VAsync:

```
# start vasync
```

9. Spusťte CLI:

```
# /opt/bitdefender/eltiw/installer
```

10. Instalovat další role.

```
# dpkg -l gz*
```

Všimněte si, že schéma databáze bylo úspěšně aktualizováno na nejnovější verzi.

```
> db.settings.findOne().database
{
"previousVersion" : "000-002-009",
"ranCleanUpVersions" : {
"b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
},
"updateInProgress" : false,
"updateTimestamp" : 1456825625581,
"version" : "000-002-011"
}
```

11. Restartovat applianci.

    Obnovení databáze je nyní dokončeno.

### Obnova databáze v Replica Set prostředí

Pokud jste nasadili databáze v Replica set prostředí, tak můžete najít oficiální postup pro obnovu na mongoDB online manual (English only)

**Poznámka**
Tyto procesy vyžadují pokročilé technické schopnosti a měly by být prováděny vyškoleným technickým personálem. Pokud se setkáte s potížemi tak neváhejte kontaktovat naší Technickou podporu aby vám pomohla s obnovou databáze.

## Active Directory

Díky integraci s Active Directory je možné naimportovat do Control Center existující inventář z Active Directory buď on-premises a nebo z Active Directory hostovaného na Microsoft Azure, čímž se značně zjednosuší nasazení bezpečnostního řešení, jeho správa, dohledování a reportování. Navíc, uživatelům Active Directory mohou být přiděleny různé role v Control Center.

Pro integraci a synchronizaci GravityZone s Active Directory doménou:

1. Přejděte na **Konfigurace (Configuration) > Active Directory > Domény (Domains)** a klikněte na ⊕ **Přidat (Add)**.

2. Konfigurujte požadovaná nastavení:
   - Intervaly synchronizace (hodiny)
   - Active Directory název domény (včetně domény nejvyššího řádu)
   - Uživatelské jméno a heslo administrátora domény
   - Umístění v inventáři sítě (Network Inventor), kde se zobrazují koncové body služby AD:
     - Udržujte AD strukturu a ignorujte prázdné OU
     - Ignorovat strukturu AD, importovat do vlastních skupin
     - Udržujte AD strukturu pouze s vybranými OU
   - Řadiče Domény se kterými se Control Center synchronizuje. Rozšířit sekci **Požádat Řadiče Domény** a vyberte řadiče z tabulky.
3. Klikněte na tlačítko **Save**.

**Důležité**
Při každé změně uživatelského hesla, nezapomeňte jej aktualizovat v Control Center.

## Přístupová oprávnění

S oprávněními k přístupu můžete udělit GravityZone Control Center přístup uživatelům služby Active Directory (AD) na základě přístupových pravidel. Informace o integraci a synchronizaci domén AD naleznete v Active Directory. Další informace o správě uživatelských účtů prostřednictvím přístupových pravidel naleznete v kapitole **Uživatelské účty** v Průvodci instalací GravityZone.

## Poskytovatelé Virtualizace

GravityZone lze momentálně integrovat s VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 a Microsoft Azure.

- „Integrace s vCenter Server“ (str. 86)
- „Integrace s XenServer“ (str. 89)
- „Integrace s Nutanix Prism Element“ (str. 90)
- „Integrace s Amazon EC2“ (str. 91)
- „Integrace s Microsoft Azure“ (str. 92)
- „Správa integrací Platforem“ (str. 93)

**Důležité**
Kdykoliv nastavíte novou integraci s dalšími systémy jako jsou vCenter Server, XenServer, Nutanix Prism Element nebo Microsoft Azure, pamatujte také na to, že je nutné vždy zkontrolovat a aktualizovat přístupová práva pro existující uživatele.

## Integrace s vCenter Server

Můžete integrovat GravityZone s jedním nebo vícero vCenter Server systémy. vCenter Server systémy v Režimu Připojené musí být přidány zvlášť do Control Center.

Pro nastavení integrace s vCenter Server:

1. Jděte na stránku **Konfigurace** v Control Center a přejděte na **Poskytovatelé virtualizace > platformy pro správu**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky a vyberte **vCenter Server** z menu. Zobrazí se konfigurační okno.
3. Zadejte detaily vCenter Server.
   - Název systému vCenter Server v Control Center
   - Hostname nebo IP adresa systému vCenter Server
   - Port vCenter Server (výchozí `443`)
4. Zadejte přihlašovací údaje pro ověření s vCenter Server. Můžete si vybrat použít přihlašovací údaje poskytnuté pro integraci s Active Directory nebo jinou sadu přihlašovacích údajů. Uživatele, kterého přihlašovací údaje jste poskytli musí mít root nebo administrátorská oprávnění ve vCenter Server.
5. Vyberte si nainstalovanou platformu VMware, kterou máte ve vašem prostředí a nakonfigurujte si adekvátní nastavení:
   - **Žádné**. Vyberte tuto možnost pro NSX-T nebo pokud není nainstalována žádná konkrétní platforma VMware a klikněte na **Uložit**. Pro integraci je vyžadováno přijetí bezpečnostního certifikátu s vlastním podpisem.

     Chcete-li konfigurovat integraci s NSX-T Manager a aplikovat ochranu koncových bodů na virtuální stoje prostřednictvím politik GravityZone Guest Introspection, podívejte se na následující článek článek KB.
   - **vShield**. Specifikujte detailní informace pro vShield Manager systém integrovaným s vCenter Serverem.
     - Jméno hosta (Hostname) nebo IP adresa vShield Manager systému
     - vShield Manager port (standartně `443`)

- **NSX-V**. Specifikujte detailní informace pro NSX Manager integrovaný s vCenter Serverem.

  **Poznámka**
  Chcete-li upgradovat z VMware vShield na NSX, přečtěte si tento článek KB.

  – Jméno hosta (Hostname) nebo IP adresa NSX Managera
  – NSX Manager port (standartně `443`)
  – Jméno uživatele a heslo použité k autentizaci na NSX Manager systému.

    Tyto přihlašovací údaje budo uloženy na chráněné entitě, ne ve správě přihlašovacích údajů (Credentials Manager).
  – Vyberte si označovací rámeček **Označit pokud je nalezen virus (Tag if a virus is found)** pro pužití standartních NSX bezpečnostních označení (NSX security tags) jakmile je škodlivý kód (malware) nalezen na virtuálním stroji.

    Stroj může být označen třemi rozdílnými tagy, odvíjejících se podle úrovně závažnosti hrozeb:

    - `ANTI_VIRUS.VirusFound.threat=low` platí pro zařízení, když na něm Bitdefender nalezne malware s nízkým rizikem, který dokáže odstranit.
    - `ANTI_VIRUS.VirusFound.threat=medium` platí pro zařízení, ze kterých Bitdefender nedokáže odstranit infikované soubory, a místo toho je dezinfikuje.
    - `ANTI_VIRUS.VirusFound.threat=high` platí pro zařízení, Bitdefender nedokáže ani odstranit, ani dezinfikovat jeho infikované soubory, ale zablokuje k nim přístup.

    Když se na stejném stroji detekují rozdílné úrovně hrozeb, všechny asociované tagy budou aplikovány. Například, takový stroj na kterém byly detekovány oba druhy hrozeb (malware) jak s nízkou tak s vysokopu úrovní, obdrží oba bezpečnostní tagy.

    **Poznámka**
    Můžete najít bezpečnostní tagy v VMware vSphere, pod štítkem **Sítě (Networking) & Bezpečnost (Security) > NSX Managers >** `NSX Manager` **> (správa) Manage > Bezpečnostní tagy (Security Tags)**.

Ovšem, ikdyž si můžete vytvářet tolik tagů kolik chcete, pouze zmíněné tři fungují s Bitdefender.

6. **Omezení přiřazení politiky ze záložky síť**. Použijte tuto možnost pro kontrolu oprávnění síťových administrátorů pro změnu politik virtuálních strojů pomocí zobrazení **Počítače a Virtuální Stroje** v záložce **Síť**. Pokud je tato možnost vybrána, administrátoři mohou měnit politiky virtuálních strojů pouze ze zobrazení **Virtuální Stroje** síťového inventáře.
7. Klikněte na tlačítko **Save**. Budete zažádán o přijmutí bezpečnostních certifikátů pro vCenter Server a NSX Manager. Tyto certifikáty zajišťují zabezpečenou komunikaci mezi GravityZone a VMware komponent, vyřeší rizika útok man-in-the-middle.

   Můžete ověřit, jestli byl nainstalovány správné certifikáty zkontrolováním informací v prohlížeči pro každou komponent VMware proti informacím certifikátu zobrazením v Control Center.
8. Vyberte zaškrtávací pole pro přijmutí využívání certifikátů.
9. Klikněte na tlačítko **Save**. Budete moci zobrazit vCenter Server v seznamu aktivních integrací.
10. Pokud používáte platformu NSX-V:
    a. Přejděte na štítek **Aktualizace (Update) > Komponenty (Components)** .
    b. Stáhněte si a publikujte **Security Server (VMware with NSX)** balíček. Pro další podrobnější informace ohledně jak aktualizovat GravityZone komponenty, si přečtěte „Aktualizuje se GravityZone“ (str. 181).
    c. Přejděte na štítek **Konfigurace (Configuration) > Poskytovatelé Virtulalizace (Virtualization Providers)**.
    d. Na řádku **Akce (Action)** klikněte na tlačítko **Register** korespondujícím s vCenter integrovaným s NSX pro regsitraci Bitdefender služby s VMware NSX Managerem.

**Varování**
Jakmile vyprší platnos bezpečnostního certifikátu a vCenter se pokusí synchronizaci, tak se zobrazí vyskakovací okno za účelem jeho aktualizace. Vstupte do kongfiguračního okna vCenter Serverové integrace (vCenter Server integration), klikněte na **Uložit (Save)**, akceptovat nový certifikát a pak klikněte znova na **Uložit (Save)**.

Po registraci, Bitdefender se přidá so VMware vSphere konzole:

- Bitdefender služba (service)
- Bitdefender správce služeb (service manager)
- Tři nové standartní servisní profily pro permisivní, norální a agresivní (permissive, normal and aggressive) mód.

> **Poznámka**
> Můžete su shlédnout tyto profily také na stránce **Politiky (Policies)** v Control Center. Klikněte na tlačítko **Sloupce (Columns)** na vrchní pravé straně tabulky k zobrazení dalších informací.

Na konci, si můžete zobrazit, které vCenter server se synchronizují. Počkejte pár minut dokud se nedokončí synchronizace.

## Integrace s XenServer

Můžete integrovat GravityZone s jedním nebo vícero XenServer Server systémy.

Pro nastavení integrace s XenServer:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center klikněte na štítek **Poskytovatelé virtualizačních platforem (Virtualization Providers)**.
2. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky a vyberte **XenServer**z menu. Zobrazí se konfigurační okno.
3. Zadejte detaily XenServer.
   - Název systému XenServer v Control Center
   - Hostname nebo IP adresa systému XenServer
   - XenServer port (výchozí `443`)
4. Zadejte přihlašovací údaje pro ověření s XenServer. Můžete si vybrat použít přihlašovací údaje poskytnuté pro integraci s Active Directory nebo jinou sadu přihlašovacích údajů.
5. **Omezení přiřazení politiky ze záložky síť**. Použijte tuto možnost pro kontrolu oprávnění síťových administrátorů pro změnu politik virtuálních strojů pomocí zobrazení **Počítače a Virtuální Stroje** v záložce **Síť**. Pokud je tato možnost vybrána, administrátoři mohou měnit politiky virtuálních strojů pouze ze zobrazení **Virtuální Stroje** síťového inventáře.

6. Klikněte na tlačítko **Save**. Budete moci zobrazit vCenter Server v seznamu aktivních integracích a které se synchronizují. Počkejte pár minut dokud se nedokončí synchronizace.

## Integrace s Nutanix Prism Element

Můžete integrovat GravityZone s jedním nebo vícero Nutanix Prism Element klastrů, nehledě jestli jsou registrovány do Nutanix Prism Central nebo ne.

Pro nastavení integrace s Nutanix Prism Elementem:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center klikněte na štítek **Poskytovatelé virtualizačních platforem (Virtualization Providers)**.
2. Klikněte na tlačítko ⊕ **Přidat (Add)** na vrchní straně tabulky a vyberte **Nutanix Prism Element** z menu. Zobrazí se konfigurační okno.
3. Specifikujte Nutanix Prism Element detaily:
   - Jméno Nutanix Prism Elementu v Control Center.
   - IP adresa Řadiče Virtuálního Stroje (Controller Virtual Machine) z Nutanix Prism Element klastru nebo IP adresa KLastru Virtuální IP.
   - Nutanix Prism Element port (standartní `9440`).
4. Specifikujte přístupové údaje pro autentizaci s Nutanix Prism Element.

   **Důležité**
   Uživatelé jejihž přístupová práva použijete musí mít administrátorská práva Klastrového Admina nebo uživatele s právami admina pro Nutanix Prism Element.

5. **Omezení přiřazení politiky ze záložky síť**. Použijte tuto volbu pro správu práv síťových administrátorů pro změnu politik pro virtuální stroje v náhledu **Počítače a Virtuální stroje (Computers and Virtual Machines)** na stránce **Síť (Network)**. Když je tato volba vybrána administrátoři mohou změnit politiky virtuálních strojů pouze z síťového inventáře na virtuálním stroji.
6. Klikněte na tlačítko **Save**. Budete vyzváni akceptovat bezpečnostní certifikáty pro Nutanix Prism. Tyto certifikáty zabezpečují kommunikaci mezi GravityZone a Nutanix Prism Element, zabraňující riziku útoku skrz prostředníka.

   Jestli byly správné certifikáty nainstalovány si můžete zkontrolovat jednoduše kontrolou srovnáním stránky prohlížeče, pro každý Nutanix Prism Element klastr nebo CVM oproti informaci zobrazené k certifikátu v Control Center.

7. Vyberte zaškrtávací pole pro přijmutí využívání certifikátů.
8. Klikněte na tlačítko **Save**.

   Pokud jste již vložili CVM IP za účelem konfigurace integrace, tak budete vyzváni v novém okně jestli chcete použít Cluster Virtual IP namísto CVM IP:

   a. Klikněte na **Ano (Yes)** pokud chcete použít Cluster Virtual IP pro integraci. Cluster Virtual IP nahradí CVM IP v detailních nastaveních Nutanix Prism Element.

   b. Klikněte na **Ne (No)** pro zachování CVM IP k dalšímu použití.

      **Poznámka**
      Jakožto ideální správný postup (best practice), vám doporučujeme použít spíše Cluster Virtual IP než CVM IP. Touto cestou, integrace zůstane aktivní ikdyž některý z hostů se stane nedostupným.

   c. V okně **Přidat (Add) Nutanix Prism Element** klikněte na **Uložit (Save)**.

Poté budete schopni vidět Nutanix Prism Element v seznamu aktivních integrací. Počkejte pár minut než se synchronizace dokončí.

## Integrace s Amazon EC2

Můžete integriovat GravityZone s vaším Amazon EC2 inventářem a chránit vaše EC2 instance hostované v Amazon cloudu.

Podmínky:

- Přístupové a tajné klíče platného AWS účtu
- AWS účet musí mít následující práva:
  - `IAMReadOnlyAccess`
  - `AmazonEC2ReadOnly` pro všechny AWS regiony

Můžete vytvořit vícero Amazon EC2 integrací. Pro každou integraci, potřebujete zadat platný AWS uživatelský účet.

**Poznámka**
Není možné přidat vícero integrací použitím přístupových údajů od IAM rolí vytvořených pro stejný AWS účet.

Pro nastavení Amazon EC2 integrace:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center klikněte na štítek **Poskytovatelé virtualizačních platforem (Virtualization Providers)**.
2. Klikněte na tlačítko ⊕ **Přidat (add)** v horní části tabulky a vyberte **Amazon EC2 Integrace (Integration)** z menu. Zobrazí se konfigurační okno.
3. Zadejte detailní nastavení pro Amazon EC2 integraci:
   - Jméno (název) integrace Pokud přidáváte několikero Amazon EC2 integrací, tak je můžete rozlišit podle jejich názvu (jména).
   - Přístupové a tajné klíče (access and secret keys) AWS uživatelského účtu.
4. **Omezení přiřazení politiky ze záložky síť**. Použijte tuto možnost pro kontrolu oprávnění síťových administrátorů pro změnu politik virtuálních strojů pomocí zobrazení **Počítače a Virtuální Stroje** v záložce **Síť**. Pokud je tato možnost vybrána, administrátoři mohou měnit politiky virtuálních strojů pouze ze zobrazení **Virtuální Stroje** síťového inventáře.
5. Klikněte na tlačítko **Save**. Pokud jsou jsou použité přístupové daje platné, tak bude integrace vytvořena a přidána do gridu (sítě).

Počkejte chvíli než se GravityZone sesynchronizuje s Amazon EC2 inventářem.

## Integrace s Microsoft Azure

Můžete integrovat GravityZone s Microsoft Azure a chránit vaše virtuální stroje hostované v Microsoft cloudu.

Podmínky:

- Aplikace Azure s právy na čtení
- ID Active Directory
- ID Aplikace
- Application Secret

Pro další detailní informace k tomu jak získat potřebé přístupové údaje a jak nastavit Azure applikaci, si přečtěte Článek ve znalostní databázi (KB article).

Můžete vytvořit vícero integrací s Microsoft Azure. Pro každou integraci, musíte mít platné Active Directory ID.

Pro nastavení integrace s Microsoft Azure:

1. Přejděte na stránku **Konfigurace (Configuration)** v Control Center klikněte na štítek **Poskytovatelé virtualizačních platforem (Virtualization Providers)**.

2. Klikněte na tlačítko ⊕ **Přidat (Add)** na vrchní straně tabulky a vyberte z menu **Azure Integrace (Azure Integration)**. Zobrazí se konfigurační okno.
3. Zadejte detailní nastavení a informace k integraci s Azure:
   - **Název integrace (The integration name)**. Pokud přidáváte několikero Azure integrací, tak je můžete rozlišit podle jejich názvu (jména).
   - **Active Directory ID**. Každá instance Azure Active Directory má unikátní identifikační číslo (identifier) dostupné v detailních nastaveních účtu v Microsoft Azure.
   - **ID aplikace (Application ID)**. Každá Azure aplikace má unikátní identifikátor (identifier) dostupný v detailních nastaveních aplikace.
   - **Heslo Aplikace (Application Secret)**. Heslo aplikace (application secret) je hodnota zobrazená při ukládání klíče v nastaveních Azure aplikace.
4. Vyberte si volbu **Omezení přiřazení politiky z náhledu sítě (Restrict policy assignment from the network view)** pro možnost změny politiky pouze z náhledu **Virtální stroje (Virtual Machines)**. Když tuto volbu odznačíte, tak budete moci měnit politiku z náhledu **Počítače a Virtuální stroje (Computers and Virtual Machines)**.
5. Klikněte na tlačítko **Save**. Pokud jsou jsou použité přístupové daje platné, tak bude integrace vytvořena a přidána do gridu (sítě).

Počkejte chvíli, než se GravityZone sesynchronizuje s inventářem Microsoft Azure.

## Správa integrací Platforem

Pro editaci a aktualizaci integrací platforem:

1. Přejděte v Control Center na štítek **Konfigurace (Configuration) > Poskytovatelé Virtulalizace (Virtualization Providers)**.
2. Klikněte na tlačítko ✎ **Upravit** ve sloupci **Akce**.
3. Nakonfigurujte nastavení pravidla dle potřeby. Pro více informací, se obraťte na jednu z následujících sekcí, podle toho, co vám stalo:
   - „Integrace s vCenter Server“ (str. 86)
   - „Integrace s XenServer“ (str. 89)
   - „Integrace s Nutanix Prism Element“ (str. 90)
   - „Integrace s Amazon EC2“ (str. 91)
   - „Integrace s Microsoft Azure“ (str. 92)

4. Klikněte na tlačítko **Save**. Vyčkejte několik minut dokud se server ne znovu synchronizuje.

Nutanix Prism Element, Amazon EC2 a Microsoft Azure integrace se automaticky synchronizují každých 15 minut. Manuálně můžete synchronizovat integraci kdykoliv, jak je popsáno níže:

1. Přejděte v Control Center na štítek **Konfigurace (Configuration) > Poskytovatelé Virtulalizace (Virtualization Providers)**.
2. Klikněte na tlačítko **Resynchronizace Inventáře (Resync Inventory)** ve sloupci **Úlohy (Action)**.
3. Klikněte na **Ano (Yes)** pro potvrzení úlohy.

Tlačítko **Resynchronizace inventáře (Resync Inventory)** je velmi užitečné v případě, že se stav integrace změní a vyžaduje synchronizaci, jako třeba v těchto situacích:

- V případě integrace Nutanix Prism Element:
  - Uživatel už nemá administační práva k inventáři.
  - Uživatel se stane neplatným (Změněné nebo smazané heslo).
  - Bezpečnostní certifikát se stane neplatným.
  - V případě chyby spojení.
  - Host se přidá nebo odebere v Nutanix Prism Element clusteru.
- V případě integrace s Microsoft Azure:
  - A subscripce je přidána nebo odebrána v Microsoft Azure.
  - Virtuální stroje jsou přidány nebo odebrány v Microsoft Azure inventáři.

Můžete také synchrnizovat integrace kliknutím na tlačítko **Edit**, a pak kliknutím na **Ulož (Save)**.

K odstranění vShield, XenServer, Nutanix Prism Element, Amazon EC2 nebo Microsoft Azure integrace:

1. Přejděte v Control Center na štítek **Konfigurace (Configuration) > Poskytovatelé Virtulalizace (Virtualization Providers)**.
2. Klikněte na tlačítko **Smazat (Delete)** v sloupci **Akce (Action)**, korespondující s integrací která se má odebrat.
3. Klikněte na **Ano (Yes)** pro potvrzení úlohy.

K odebrání NSX integrace:

1. Přihlašte se do VMware vSphere konzole a smažte veškeré Bitdefender politiky a Security Servery.
2. Přejděte v Control Center na štítek **Konfigurace (Configuration) > Poskytovatelé Virtulalizace (Virtualization Providers)**.
3. Ve sloupci **Akce (Action)** korespondující s integrací která má být odstraněna, klokněte na **Odregistrovat (Unregister)** a pak **Smazat (Delete)**.
4. Klikněte na **Ano (Yes)** pro potvrzení úlohy.

Ujistěte se, že se zobrazují ty nejnovější informace kliknutím na tlačítko **Obnovit** v horní části tabulky.

## Poskytovatelé zabezpečení

GravityZone Security for Virtualized Environmentsintegruje se s datovým centrem VMware NSX-T prostřednictvím NSX-T Manager.

### Integrace s NSX-T Manager

NSX-T Manager je řídící rovina vašich serverů vCenter integrovaných s datovým střediskem NSX-T Aby integrace fungovala, musíte nastavit integraci serverů vCenter spojených se správcem NSX-T. Další informace naleznete v tématu Integrace se serverem vCenter.

Nastavení integrace s NSX-T Managerem:

1. V Control Center přejděte na **Konfigurace > Poskytovatelé virtualizace > Poskytovatelé zabezpečení**.
2. Klikněte na tlačítko **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.
3. Specifikujte podrobnosti integrace s NSX-T:
   - Název integrace s NSX-T.
   - Název hostitele nebo adresa IP přidruženého systému vCenter Server.
   - Port NSX-T (výchozí 433).
4. Zadejte přihlašovací údaje pro ověření s vCenter Server. Můžete si vybrat použít přihlašovací údaje poskytnuté pro integraci s Active Directory nebo jinou sadu přihlašovacích údajů. Uživatele, kterého přihlašovací údaje jste poskytli musí mít root nebo administrátorská oprávnění ve vCenter Server.

5. Klikněte na tlačítko **Save**.

   Control Center je nyní integrována s NSX-T. Chcete-li použít ochranu koncových bodů na své virtuální počítače prostřednictvím zásady GravityZone Guest Introspection, přejděte na Konfigurovat a aplikovat ochranu koncových bodů na VMware NSX - Hostující počítače VM prostřednictvím zásad pro kontrolu hostitele GravityZone Článek KB.

**Poznámka**
GravityZone lze použít pouze k ochraně přidruženého serveru vCenter.

## NTSA

V této sekci můžete konfigurovat integraci s Bitdefender [NTSA_ LONG], což je řešení podnikového zabezpečení, které přesně detekuje narušení a poskytuje přehled o pokročilých útocích analýzou síťového provozu. Další informace o tomto řešení naleznete v dokumentaci Bitdefender [NTSA_ SHORT] .

**Důležité**
Sekce NTSA je k dispozici pouze po zadání platného licenčního klíče NTSA na stránce **Konfigurace > Licence** .

Chcete-li nakonfigurovat integraci NTSA, musíte mít ve svém prostředí nainstalované řešení [NTSA_ SHORT] a přístupy pro k webové konzoli NTSA.

Během integrace budete požádáni o poskytnutí adresy webové konzole NTSA (IP nebo název hostitele) a token (párovací klíč) vygenerovaný v konzoli NTSA, jak je vysvětleno dále.

### Konfigurace integrace NTSA

1. Přihlašte se do GravityZone Control Center.
2. Přejděte na stránku **Konfigurace** a klikněte na kartu [NTSA_ SHORT].
3. Aktivujte možnost **Integrovat s Network Traffic Security Analytics (NTSA)**
4. Zadejte následující data:
   - Adresa webové konzole NTSA (IP / Hostname).
   - Port používaný GravityZone pro komunikaci s NTSA (standardně 443).
   - Párovací klíč (token) generovaný webovou konzolí NTSA:
     a. Otevřete webovou konzoli [NTSA_ SHORT] a přejděte na stránku **Licence**.

b. Vyberte možnost **Integrace s GravityZone**.

c. Klikněte na **Generovat párovací klíč**. Klíč se zobrazí automaticky.

d. Pomocí tlačítka **Kopírovat do schránky** získáte párovací klíč.

e. Potvrďte kliknutím na **OK**.

5. Ověřte, zda se zobrazený fingerprint hostitele shoduje s hash SSL certifikátu ze zařízení [NTSA_ SHORT], poté povolte možnost **Přijímám certifikát** .
6. Klikněte na tlačítko **Save**.

Po dokončení úspěšné konfigurace se integrace zobrazí jako **Synchronizováno**. Integrace NTSA může mít následující statusy:

- **N/A**: integrace dosud nebyla nakonfigurována.
- **Synchronizováno**: Integrace je nakonfigurována a povolena.
- **Neplatný token**: párovací klíč z webové konzole NTSA je neplatný.
- **Chyba připojení**: Nelze se připojit k zadané adrese NTSA webové konzole (neplatný název IP / hostitele).
- **Chyba certifikátu**: aktuální fingerprint certifikátu SSL ze zařízení [NTSA_ SHORT] neodpovídá původně přijatému fingerprintu.
- **Neznámá chyba**: došlo k neznámé chybě komunikace.

Pole **Poslední změna stavu** zobrazuje datum a čas poslední úspěšné změny nastavení integrace nebo po změně stavu integrace.

Jakmile je integrace s NTSA nakonfigurována, můžete integraci zakázat / povolit pomocí zaškrtávacího políčka, které je k dispozici v horní části **NTSA** stránky.

## Propojení účtů GravityZone a NTSA

Po konfiguraci integrace budou vaše účty GravityZone a [NTSA_ SHORT] propojeny a můžete snadno přejít na webovou konzoli [NTSA_ SHORT] takto:

1. V GravityZone Control Center klikněte na tlačítko **[NTSA_ SHORT]** umístěném v levém dolním rohu okna.
2. Budete přesměrováni na přihlašovací stránku webové konzole [NTSA_ SHORT]. Po zadání přihlašovacích údajů pro NTSA můžete začít navigovat webovou konzoli NTSA.

Přihlašovací údaje [NTSA_ SHORT] musíte zadat pouze poprvé. Poté obdržíte automaticky přístup ke konzoli NTSA kliknutím na tlačítko **[NTSA_ SHORT]**, aniž byste byli vyzváni k přihlášení.

## Odstranění integrace [NTSA_ SHORT]

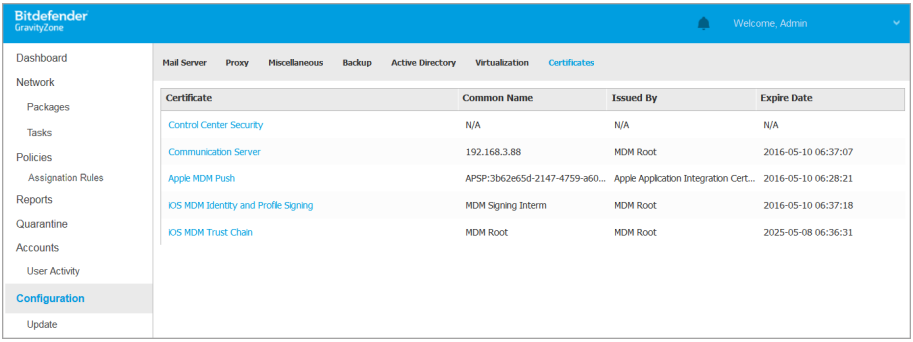
Odstranění licenčního klíčeNTSA ze stránky **Konfigurace > Licence** také odstraní integraci s NTSA.

**Poznámka**
Vaš NTSA účet a GravityZone budou odpojeny v následujících situacích:

- Licenční klíč NTSA byl odebrán.
- Vaše heslo NTSA bylo změněno.
- Vaše heslo ke GravityZone bylo změněno.
- Nastavení integrace s NTSA bylo změněno.

## Certifikáty

Aby vaše nasazené řešení GravityZone fungovalo správně a také z bezpečnostních důvodů, musíte vytvořit a zadat počet kolik bezpečnostních certifikátů máte nainstalovaných v Control Center.




Záložka Certifikáty

Control Center podporuje následující druhy certifikátů:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)

- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)

**Poznámka**
Následující certifikáty jsou zapotřebí excklusivně pro správu bezpečnostni na Apple iOS zařízeních:

- Certifikát Komunikačního Serveru (Communication Server Certificate)
- Certifikát Serveru Incidentů
- Apple MDM Push Certifikát
- iOS MDM identifikační a podpisový certifikát profilu(iOS MDM Identity and Profile Signing Certificate)
- iOS MDM certifikát důvěryhodného řetězce(iOS MDM Trust Chain Certificate)

Pokud neplánujete rozinstalovat iOS mobile device management,tak nepotřebujete vytvářet a zadávat tyto certifikáty.

## Control Center bezpečnostní Certifikát

Control Center bezpečnostní certifikát je potřeba pro identifikaciControl Center webové konsole jakožto důvěryhodné webové stránky v prohlížeči. Control Center používá standartní SSL certifikát podepsaný Bitdefender. Tento zabudovaný certifikát není rozpoznávaný webovými prohlížeči a spouští bezpečnostní varování. Abyste zamezili bezpečnostním varováním, přidejte SSL certifikát podepsaný vaší firmou a nebo externí certifikační autoritou (CA)

Pro vložení a nahrazení Control Center certifikátu:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klickněte na jméno certifikátu.
3. Vyberte si druh certifikátu (se separátním nebo vloženým private key).
4. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
5. Pro certifikáty se separátním privátním klíčem, klikněte na tlačítko **Přidat (Add)** hned vedle pole **Privátní klíč (Private key)** a následně nahrajte samotný privátní klíč.
6. Pokud je certifikát chráněn heslem, tak zadejte heslo v daném poli.

7. Klikněte na tlačítko **Save**.

## Koncový bod - Security Server Komunikační bezpečnostní certifikát

Tento certifikát obstrává bepečnou komunikaci mezi bezpečnostními agenty a Security Server (Multi-Platform) které jím byly přiřazené.

Během samotného nasazení Security Server generuje standartní sebou-podepsané certifikáty. Vy můžete nahradit tento zabudovaný certifikát jiným vámi zvoleným přímo v Control Center.

Pro přidání a nahrazení Certifikátu pro komunikaci Security Server s koncovými body:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klickněte na jméno certifikátu.
3. Vyberte si druh certifikátu (se separátním nebo vloženým private key).
4. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
5. Pro certifikáty se separátním privátním klíčem, klikněte na tlačítko **Přidat (Add)** hned vedle pole **Privátní klíč (Private key)** a následně nahrajte samotný privátní klíč.
6. Pokud je certifikát chráněn heslem, tak zadejte heslo v daném poli.
7. Klikněte na tlačítko **Save**. Pozor, mohou se zobrazovat upozornění v případě že certifikát je samopodepsany a nebo vypršel. Pokud váš certifikát vypršel , prodlužte si ho.
8. Klikněte na **Ano (Yes)** pro samotné nahrání certifikátu. Okamžitě po nahrání Control Center zašle bezpečnostní certifikát na všechny Security Servery.

V případě potřeby, se můžete vrátit k původnímu zabudovanému certifikátu pro každý Security Serveru následujícím způsobem:

1. Klikněte na jméno certifikátu na stránce **Certifikáty (Certificates)**.
2. Vyberte **Žádný certifikát (použijte jako standartní volbu)** jakožto typ certifikátu.
3. Klikněte na tlačítko **Save**.

## Certifikát Komunikačního Serveru (Communication Server Certificate)

Certifikát Komunikačního Serveru je použit pro zabezpečení komunikace mezi Kommunikačním Serverem a iOS mobilními zařízeními.

Požadavky:

- Tento SSL certifikát může být podepsán buď vaší firmou a nebo externí Certifikační Autoritou.

  **Varování**
  Certifikát může být zneplatněn pokud nebyl vydán důvěryhodnou "public/trusted" Certifikační Autoritou (Například, u použití "self-signed" certifikátů).

- Název certifikátu (certificate common name) musí obsahovat a shodovat se přesně s názvem domény nebo IP adresy používané mobilními klienty pro spojení s Kommunikačním Serverem. Toto je konfigurováno jakožto externí adresa MDM v konfiguračním rozhraní (configuration interface) v GravityZone appliance konsoli.
- Mobilní klienti musí důvěřovat tomuto certifikátu. Proto je musíte také zadat do iOS MDM důvěryhodného řetězce (Trust Chain).

Pro přidání a nahrazení certifikátu komunikačního serveru:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klickněte na jméno certifikátu.
3. Vyberte si druh certifikátu (se separátním nebo vloženým private key).
4. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
5. Pro certifikáty se separátním privátním klíčem, klikněte na tlačítko **Přidat (Add)** hned vedle pole **Privátní klíč (Private key)** a následně nahrajte samotný privátní klíč.
6. Pokud je certifikát chráněn heslem, tak zadejte heslo v daném poli.
7. Klikněte na tlačítko **Save**.

## Certifikát Serveru Incidentů

Přidání nebo nahrazení certifikátu Incident Server:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klickněte na jméno certifikátu.
3. Vyberte si druh certifikátu (se separátním nebo vloženým private key).
4. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
5. Pro certifikáty se separátním privátním klíčem, klikněte na tlačítko **Přidat (Add)** hned vedle pole **Privátní klíč (Private key)** a následně nahrajte samotný privátní klíč.
6. Pokud je certifikát chráněn heslem, tak zadejte heslo v daném poli.
7. Klikněte na tlačítko **Save**.

## Apple MDM Push Certifikát

Apple potřebuje MDM Push certifikát, pro zajištění bezpečné komunikace mezi Komunikačním Serverem a Apple Push notifikační službou (APNs), při zasílání notifikací. Push notifikace jsou používány pro vyzvání zařízení k spojení se s Komunikačním Serverem, jakmile jsou nové úlohy nebo změny politik k dispozici.

Apple vystavuje tento certifikát přímo na vaší firmu, ale potřebuje k tomu takzvany "Certificate Signing Request" (CSR) tak aby mohl být podepsán Bitdefenderem. Ovladací panel (Control Center) poskytuje pomocný nástroj (wizard) pro pomoc s vytvořením a zízkáním Apple MDM Push certifikátu.

**Důležité**

- Potřebujete Apple ID, k tomu abyste získali a spravovali tento certifikát. Pokud nemáte Apple ID, tak si ho můžete vytvořit na stránce Moje (My) Apple ID. Použijte všeobecnou emailovou adresu firmy a ne specifickou adresu zaměstnance pro registraci na Apple ID, protože ji budete později potřebovat pro obnovu certifikátu.
- Webová stránka Apple nepracuje správně s Internet Explorerem. Doporučujeme používat nejnovější verze buď Safari nebo Chrome prohlížečů.
- Apple MDM Push certifikát je platný pouze jeden rok. Před tím než certifikát vyprší si ho musíte obnovit a naimportovat obnovený certifikát do Control Center. Pokud dovolíte certifikátu vypršet, tak si budete muset vytvořit nový reaktivovat všechny vaše zařízení.

### Přidání Apple MDM Push Certifikátu

Pro získání Apple MDM Push certifikátu a jeho naimportování doControl Center:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klikněte na název certifikátu a následujte instrukce pomocníka s instalací (instalačního wizardu) jak je popsáno níže:

   **Krok 1 - Zažádat o Podepsání Certifikátu Bitdefender**

   Vyberte si vhodnou možnost:

   - **Potřebuji si vygenerovat "certificate signing request" (CSR) podepsaný Bitdefender** (Doporučeno)
     a. Vložte si svůj název firmy, vaše celé jméno a emailovou adresu do adekvátních polí.
     b. Klikněte na **Generovat (Generate)** pro stažení CSR souboru podepsaného firmou Bitdefender.
   - **Mám podepsanou žádost o certifikát a musím ji podepsat Bitdefenderem**
     a. Nahrajte váš CSR soubor a asociovaný privátní klíč tím že kliknete na tlačítko **Přidat (Add)** vedle těchto polí.

        Kommunikační Server potřebuje privátní klíč když se autentizuje s APNs servery.
     b. Vyspecifikujte heslo chránící privátní klíč, pokud nějaký máte.
     c. Klikněte na tlačítko **Podpesat (Sign)** pro stažení CSR souboru podepsaného firmou Bitdefender.

   **Krok 2 - Požadovat push certifikát od Applu**

   a. Klikněte na odkaz **Portál Apple Push Certifikátů** a přihlašte se použitím Apple ID a hesla.
   b. Klikněte na tlačítko **Vytvoření Certifikátu (Create a Certificate)** a akceptujte podmínky pro užívání.
   c. Klikněte na **Vybrat soubor (Choose file)**, zvolte si CSR soubor a pak klikněte na **Nahrát (Upload)**.

      **Poznámka**
      Můžete najít tlačítko **Vybrat soubor (Choose file)** i pod jinými názvy jako třeba **Vybrat (Choose)** nebo **Prohlížet (Browse)**, v závislosti na prohlížeči, který právě používáte.

   d. Z potvrzovací stránky, klikněte na tlačítko **Stahovat (Download)** pro příjem vašeho MDM Push certifikátu.

e. Přejděte zpátky k pomocníkovi instalace (instalation wizard) z Control Center.

**Krok 3 - Importovat Push certifikát Applu**

Klikněte na tlačítko **Add Certificate** pro nahrání souboru certifikátu z vašeho Počítače.

Můžete si zjistit detailní informace k certifikátu v poli níže.

3. Klikněte na tlačítko **Save**.

### Obnovení Apple MDM Push Certifikátu

Pro obnovení Apple MDM certifikátu a a jeho aktualizaci v Control Center:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klikněte na jméno certifikátu abyste otevřeli pomocníka importu (Import wizard).
3. Získání "Certificate Signing Request" (CSR) podepsaného firmou Bitdefender. Tento proces je stejný jako pro získání nového certifikátu.
4. Klikněte na odkaz **Portál Apple Push Certifikátů** a přihlašte se stejným použitím Apple ID a hesla, které jste použili pro vytvoření certifikátu.
5. Lokalizujte MDM Push certifikát pro Bitdefender a klikněte na příslušné tlačítko **Obnovit (Renew)**.
6. Klikněte na **Vybrat soubor (Choose file)**, zvolte si CSR soubor a pak klikněte na **Nahrát (Upload)**.
7. Klikněte ma **Stáhnout (Download)** pro uložení certifikátu do vašeho počítače.
8. Přejděte zpět do Control Center a naimportujte si zde nový Apple push certifikát.
9. Klikněte na tlačítko **Save**.

## iOS MDM identifikační a podpisový certifikát profilu(iOS MDM Identity and Profile Signing Certificate)

Certifikát pro iOS MDM Identitu (iOS MDM Identity certificate) a Podpisový Certifikát Profilu (Profile Signing certificate) se používají Komunikačním Serverem pro podepsání certifikátů totožnosti a konfiguraci profilů odeslaných na mobilní zařízení.

Požadavky:

- Musí to být zprostředkovaný (Intermediate) nebo přímý koncový (End-Entity) certifikát, podepsaný buď vaší firmou a nebo externí Certifikační Autoritou.
- Mobilní klienti musí důvěřovat tomuto certifikátu. Proto je musíte také zadat do iOS MDM důvěryhodného řetězce (Trust Chain).

Pro přidání či náhradu iOS MDM Identity certifikátu a Podpisového certifikátu Profilu:

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klikněte na jméno certifikátu.
3. Vyberte si druh certifikátu (se separátním nebo vloženým private key).
4. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
5. Pro certifikáty se separátním privátním klíčem, klikněte na tlačítko **Přidat (Add)** hned vedle pole **Privátní klíč (Private key)** a následně nahrajte samotný privátní klíč.
6. Pokud je certifikát chráněn heslem, tak zadejte heslo v daném poli.
7. Klikněte na tlačítko **Save**.

## iOS MDM certifikát důvěryhodného řetězce(iOS MDM Trust Chain Certificate)

iOS MDM Trust Chain certifikáty jsou potřeba na mobilních zařízeních k zajištění důvěry k Certifikátu Komunikačního Serveru (Communication Server certificate) a k Certifikátu iOS MDM Identity a Podpisu Profilu (iOS MDM Identity and Profile Signing certificate. Kommunikační Server posílá tento certifikát na mobilní zařízení během jejich aktivace.

Tento iOS MDM důvěryhodný řetězec (Trust Chain) musí obsahovat všechny mezičlánkové certifikáty (intermediate certificates) až po kořenový certifikát (root certificate) vaší firmy a nebo až po mezičlánkový certifikát (intermediate certificate) vystavený externí Certifikační Autoritou.

Pro přidání nebo náhradu certifikátů iOS MDM důvěryhodného řetězce (Trust Chain certificates):

1. Přejděte na stránku **Konfigurace (Configuration)** a klikněte na **Certifikáty (Certificates)** štítek.
2. Klikněte na jméno certifikátu.
3. Klikněte na **Přidat (Add)** tlačítko vedle certifikátu **Certifikát (Certificate)** pole a nahrajte samotný certifikát.
4. Klikněte na tlačítko **Save**.

### Úložiště

Na této kartě jsou zobrazeny informace o aktualizacích agentů zabezpečení včetně verzí produktů uložených na aktualizačním serveru a verzí dostupných v oficiálním úložišti Bitdefender, aktualizačních okruzích, datu a času aktualizace a poslední kontrole nových verzí.

**Poznámka**
Verze produktu nejsou k dispozici pro bezpečnostní servery.

## 5.1.5. Správa GravityZone Appliance

GravityZone appliance je dodávána se základním konfiguračním rozhraním, dostupným z nástroje pro správu používaným pro správu virtualizovaného prostředít tam kde jste vaší appliance nasadili.

Toto jsou dostupné hlavní možnosti po prvním nasazení zařízení GravityZone:

- Nakonfigurujte nastavení Hostname
- Nakonfigurujte Nastavení Sítě
- Konfigurovat nastavení Proxy
- MDM Komunikační Server
- Pokročilá nastavení
- Nastavit Jazyk

Použijte směrová tlačítka a `Tab` tlačítko k navigaci skrze nabídku menu a možností (options). Stiskněte `Enter` pro vybrání specifické možnosti funkce.

### Konfigurace jména hosta a nastavení

Komunikace s GravityZone rolemi se provádí skrze použití IP addresy nebo DNS jména appliance na které jsou nainstalovány. Standartně GravityZone komponenty komunikují použitím IP adres. Pokud chcete zapnout komunikaci skrze DNS jména, tak musíte nastavit tyto GravityZone appliance s DNS jménem a zajistit aby tato jména byly korektně překládána na nakonfigurované IP adresy všech vašich appliancí.

Podmínky:

- Nakonfigurujte DNS záznam ve vašem DNS serveru.

- Jméno DNS musí být správně přeloženo na nakonfigurovanou IP adresu apliance. Proto musíte zajistit aby byla appliance nakonfigurována se správnou IP adresou.

Pro konfiguraci nastavení jména hosta (hostname):

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Vyberte z hlavního menu **Konfigurace nastavení jména hosta**.
3. Vložte jméno hosta od appliance a název Active Directory domény (pokud potřeba).
4. Vyberte **OK** pro uložení změn.

## Nakonfigurujte Nastavení Sítě

Můžete nakonfigurovat appliance tak aby získala síťová nastavení automaticky od DHCP serveru a nebo můžete nakonfigurovat síťová nastavení ručně. V případě že si vyberete použít DHCP, tak musíte nakonfigurovat DHCP Server tak aby pro appliance rezervoval konkrétní IP adresu.

Pro konfiguraci síťových nastavení:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Konfigurace síťových nastavení (Configure Network Settings)**.
3. Vyberte síťové rozhraní (interface) (standartně `eth0`).
4. Vyberte konfigurační metodu:
   - **Nastavit nastavení sítě ručně.** Musíte nastavit IP adresu, masku sítě, adresu brány a adresu DNS serveru.
   - **Získá síťová nastavení automaticky pomocí DHCP.** Použijte tuto volbu pouze když jste nakonfigurovali DHCP Server aby pro vaší appliance rezervoval konkrétní IP adresu.
5. Můžete si ověřit detaily stávající IP konfigurace nebo stav spojení výběrem odpovídajících opcí.

## Konfigurovat nastavení Proxy

Pokud navazuje vaše appliance spojení do Internetu skrze proxy server, tak musíte nakonfigurovat nastavení proxy.

**Poznámka**
Proxy nastavení mohou být také nakonfigurovány ze stránky Control Center, **Konfigurace > proxy**. Měníte-li nastavení proxy na jedné z lokací tak je také automaticky aktualizujete na dalších lokacích.

Pro konfiguraci proxy a nastavení:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Vyberte z hlavního menu **Konfigurace nastavení proxy**.
3. Vyberte **Konfigurace nastavení proxy**.
4. Zadejte adresu proxy serveru. Použijte následující syntaxi:
   - Pokud proxy server nevyžaduje autentizaci:

     `http(s)://<IP/hostname>:<port>`
   - Pokud proxy server vyžaduje autentizaci:

     `http(s)://<username>:<password>@<IP/hostname>:<port>`
5. Vyberte **OK** pro uložení změn.

Vyberte **Zobrazení informací proxy** abyste zkontrolovali nastavení proxy.

## MDM Komunikační Server

**Poznámka**
Tato konfigurace je potřeba pouze pro mobile device management, v případě že váš licenční klíč pokrývá službu Security for Mobile. Tato volba se objeví v menu po instalaci Role Komunikačního Serveru.

Ve standartním nastavení GravityZone, mobilní zařízení mohou být spravována pouze pokud jsou přímo připojená do firemní sítě (pomocí Wi-Fi nebo VPN). Tohle se stává, když začnete spravovat nové mobilní zařízení, která jsou standartně nakonfigurována na lokální adresu komunikačního serveru appliance.

Aby bylo možné spravovat mobilní zařízení přes internet , nezávisle na tom kde kde se nacházejí, musíte nakonfigurovat komunikační server s veřejně dostupnou adresou.

Aby bylo možné spravovat mobilní zařízení, když nejsou připojena na firemní síť, je potřeba mít k dispozici následující možnosti:

- Nastavte port forwarding na firemní bráně pro applianci na kteréběží role kommunikačního serveru.
- Přidejte další síťový adaptér do appliance na které běží role kommunikačního serveru a přiřaďte jí veřejnou IP adresu.

V obou případech musíte nakonfigurovat Communikační server s externí adresou za účelem správy mobilních zařízení:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Vyberte z hlavního menu **MDM Komunikační Server**.
3. Vyberte **Konfigurace externí adresy MDM Serveru**.
4. Zadejte externí adresu.

   Použijte následující syntaxi: `https://<IP/Domain>:<Port>`.

   - Pokud použijete port forwarding, tak musíte zadat veřejnou IP adresu nebo doménové jméno a pak port otevřený na bráně.
   - Pokud použijete veřejnou adresu komunikačního serveru, tak musíte zadat veřejnou adresu nebo doménové jméno a port komunikačního serveru. Standartní port je `8443`.
5. Vyberte **OK** pro uložení změn.
6. Vyberte **Zobrazit externí adresu MDM serveru** pro kontrolu nastavení.

## Pokročilá nastavení

Pokročilá nastavení zahrnují několik možností ručního nasazení, rozšíření prostředí a vylepšení zabezpečení:

- Nainstalovat/Odinstalovat Role
- Instalovat Security Server
- Nastavit nové heslo databáze

- Aktualizační server
- Konfigurovat Roli Balancer
- Balíček Replik
- Povolit zabezpečený cluster VPN
- Připojit k Existující Databázi
- Připojit ke stávající databázi (Zabezpečený VPN cluster)
- Zkontrolujte zabezpečený cluster VPN

Dostupnost možností se liší v závislosti na nainstalovaných rolích a povolených službách. Pokud například není v zařízení nainstalována role databázového serveru, můžete nainstalovat pouze role nebo se připojit k databázi GravityZone rozmístěné ve vaší síti. Po nainstalování role databázového serveru do zařízení nebudou dostupné možnosti připojení k jiné databázi.

### Nainstalovat/Odinstalovat Role

NaGravityZone appliance můžou běžet jedna, různé kombinace či všechny z těchto následujících rolí:

- **Databázový Server**
- **Aktualizační server**
- **Webová Konzole**
- **Komunikační server**
- **Server Incidentů**

Správné GravityZone nasazení vyžaduje aby běžela minimálně jedna instance z každé role. Proto tedy, v závislosti na tom jak preferujete rozmístit GravityZone role, budete nasazovat od jedné až po čtyřiGravityZone appliance. Roli Databázového Serveru musíte nainstalovat jako první. V případě vícero GravityZone appliances, nainstalujte nejprve roli Databázového Serveru na první appliance a pak konfigurujte všechny ostatní appliance tak že je připojíte do stávající databázové instance.

**Poznámka**

Můžete nainstalovat další instance jednotlivých rolí pomocí použití role balancerů. Další informace viz „Konfigurovat Roli Balancer“ (str. 114).

Pro instalaci rolí GravityZone:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Instalace/odinstalace (Install/Uninstall) rolí**.
4. Vyberte **Přidání nebo odebrání rolí (Add or remove roles)**.
5. Pokračujte podle aktuélní situace:
   - Pokud je tohle prvotní nasazení GravityZone appliance, stisklněte `Mezerník (Space)` a pak `Enter` pro instalaci role databázového serveru. Potvrďte váš výběr opakovaným stisknutím klávesy `Enter`. Nastavte heslo databáze a pak počkejte na dokončení instalace.
   - Pokud set již nasadili jinou appliance s rolí databázového serverutak vyberte **Zrušit (Cancel)** a vraťte se na menu **Přidat nebo odstranit role (Add or remove roles)**. Musíte pak vybrat **Konfigurace databázové adresy (Configure Database Address)** a zadejte následně adresu databázového serveru. Postarejte se o nastavení vlastního hesla databáze před použitím této možnosti. Pokud nevíte heslo databáze, tak nastavte nové výběrem **Pokročilá nastavení (Advanced Settings) > nastavte nové heslo (Set a new database password)** z hlavního menu.

     Použijte následující syntaxi: `http://<IP/Hostname>:<Port>`. Standartní port databáze je `27017`. Zadejte primární heslo databáze.
6. Pro instalaci dalších rolí vyberte **Přidání a odebrání rolí** z menu **Instalace/odinstalace rolí** a pak roli nainstalujte. Pro každou roli kterou chete nainstalovat nebo odinstalovat zmáčkněte `Mezerník (Space bar)` k vybrání či odebrání role anásledně zmáčkněte `Enter` pro zpracování požadavku. Musíte potvrdit výběr opakovaným stisknutím `Enter` a pak čekejte pro dokončení instalace.

**Poznámka**

Každá z rolí se nainstaluje standartně během několika minut. Během instalace se požadované soubory stahují z internetu. A proto může v případě pomalého internetového spojení zabrat instalace více času. Pokud instalace zamrzne, tak applianci nasaďte znova od začátku.

Můžete si zobrazit nainstalované role a jejich IP adresy, výběrem jedné z následujících možností z **Instalace/deinstalace rolí (Install/Uninstall Roles)** položky v menu:

- **Zobrazte lokálně nainstalované role (Show locally installed roles)**, abyste si zobrazili role instalované na této appliance.
- **Zobrazte si všechny nainstalované role (Show all installed roles)**, abyste si zobrazili všechny role nainstalované ve vašem GravityZone prostředí.

## Instalovat Security Server

**Poznámka**
Security Server bude k dispozici jen pokud to váš licenční klíč dovolí.

Můžete nainstalovat Security Server z GravityZone appliance konfigurační rozhraní (configuration interface), přímo na GravityZone appliance, nebo z Control Center jako samostatnou appliance. Výhody instalace Security Server z appliance jsou:

- Vhodnost GravityZone pro nasazení s jedinou appliance obashující všechna pravidla.
- Můžete si zobrazit a použítSecurity Server bez nutnosti integrace GravityZone s virtualizační platformou.
- Méně instalačních úloh nasazení k provedení.

Podmínky:

GravityZone appliance musí mít nainstalovanou roli Databázového Serveru, nebo musí být nakonfigurována tak, že se připojuje na existující databázový server.

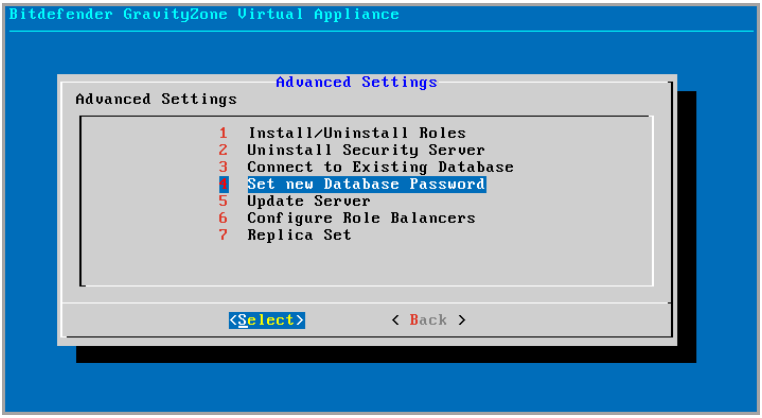
Abyste naistalovali Security Server z rozhraní appliance :

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Instalace (Install) Security Server**. Zobrazí se potvrzovací okno.
4. Stiskněte `Enter` pro pokračování a počkejte do té doby než se instalace dokončí.

**Poznámka**
Security Server lze odinstalovat pouze z **Pokročilá nastavení (Advanced Settings)** v menu rozhraní appliance.

## Nastavit nové heslo databáze

Při instalaci role databázového serveru musíte nastavit heslo pro ochranu databáze. V případě, že jej chcete změnit, zadejte nové z hlavní nabídky **Pokročilé nastavení > Nastavení nového hesla databáze** .




Rozhraní konzole zařízení: Možnost Nastavit nové heslo databáze

Při nastavování silného hesla postupujte podle pokynů.

## Konfigurace aktualizačního serveru (Configure Update Server)

GravityZone appliance je standartně nakonfigurována na stahování aktualizací z internetu. Pokud chcete, tak můžete nastavit nainstalované appliance aby se aktualizovaly z vašeho lokálního (firemního) Bitdefender aktualizačního serveru (update serveru) . Tedy z GravityZone appliance, která má nainsnalovanou roli aktualizačního serveru (Update Server role).

Pro nastavení adresy aktualizačního serveru (update serveru):

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Aktualizační server (Update Server)**.
4. Vyberte **Nastavení adresy aktualizačního serveru (Configure update address)**.

5. Vložte IP adresu nebo název hosta (hostname) appliance na které běží role aktualizačního serveru (Update Server role). Standartní port aktualizačního serveru (Update Server port) je `7074`.

## Konfigurovat Roli Balancer

Aby byla zajištěna spolehlivost a škálovatelnost, můžete nainstalovat několik instancí specifických rolí (Incident Server, Communication Server, Web Console).

Přičemž každá instance jednotlivé role je nainstalována na různé appliance.

Všechny instance jednotlivých rolí musí být zapojena k další pomocí role balanceru za účelem vyvažování zátěže.

GravityZone appliance obsahuje zabudované balancery, které můžete nainstalovat a používat. Pokud již máte ve vaší síti software nebo hardware pro rozložení zátěže, tak jej můžete použít místo zabudovaných balancerů.

Zabudovaná role balancerů nesmí být nainstalována dohromady s jinými rolemi na GravityZone appliance.

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Konfigurace role balancerů (Configure Role Balancers)**.
4. Vyberte vaši chtěnou volbu:
   - **Použít vnější balancery.** Vyberte tuhle volbu pokud vaše síťová infrastruktůra již obsahuje software nebo hardware balancery, které můžete používat. Musíte vložit adresu balanceru pro každou roli, kterou chcete balancovat. Použijte následující syntaxi:

     `http(s)://<IP/Hostname>:<Port>`.

   - **Použít vestavěné balancery.** Vyberte tuhle volbu pro instalaci a používání zabudovaného software balanceru.

     **Důležité**
     To install multiple instances of the Incidents Server role you may only use the built-in balancer.

5. Vyberte **OK** pro uložení změn.

### Balíček Replik

Pomocí této volby můžete zapnout funkci pro používání databázového replika setu (database replica set) namísto klasické jedno serverové instance (single-server database instance). Tento mechanizmus umožní vytváření vícero databázových instancí skrze distribuované GravityZone prostředí, abyste zajistili vysokou dostupnost databáze pro případ výpadku či chyby.

**Důležité**
Databázová replikace je dostupná pouze pro čistě nové instalace GravityZone appliance počínaje verzí 5.1.17-441.

### Konfigurace replika setu

Nejprve, musíte zapnout replika set na první instalované GravityZone applianci. Pak, budete moci přidávat další replika set členy nainstalováním role databázového serveru na dalších GravityZone instancích ve společném stejném prostředí.

**Důležité**

- Replika set potřebuje minimálně tři členy k tomu aby mohl fungovat.
- Můžete přidat až 7 instancí role databázového serveru jakožto replika set členů (limitace MongoDB).
- Je doporučeno používat lichý počet databázových instancí. Sudé číslo členů by jen konzumovalo zbytečně více zdrojů a mělo by přitom stejné výsledky.

Pro zapnutí databázové replikace ve vašem GravityZone prostředí:

1. Nainstalujte roli databázového serveru na první GravityZone applianci. Další informace viz „Nainstalovat/Odinstalovat Role“ (str. 110).
2. Nakonfigurujte ostatní appliance tak aby se napojili na první databázovou instanci. Další informace viz „Připojit k Existující Databázi“ (str. 117).
3. Přejděte do hlavního menu první appliance, vyberte **Pokročilá nastavení (Advanced Settings)** a následně vyberte **Replika Set** k jeho zapnutí. Zobrazí se potvrzovací okno.
4. Vyberte **Ano (Yes)** k potvrzení.
5. Nainstalujte roli Databázového Serveru na každou z dalších GravityZone appliancích.

Jakmile všechny výše popsané kroky dokončíte, tak všechny databázové instance začnou pracovat dohromady jako replika set:

- Primární instance je vybraná, jakožto jedinná, která může akceptovat operace pro zápis.
- Primární instance zapisuje všechny změny provedené v jejím data setu do logu.
- Druhotné instance replikují tento log a aplikují ty samé změny do jejich data setů.
- Jakmile se primární instance stane nedostupnou, replika set vybere jednu ze sekundárních instancí jako primární.
- Jakmile primární instance přestane komunikovat s ostatními členy setu na delší dobu než 10 sekund, replika set se pokusí vybrat dalšího člena aby se stal novým primárním.

### Odebírání členů z replika setu

Chcete-li odebrat členy sady replik, stačí vybrat z rozhraní konzoly zařízení (menu-based interface) **Instalovat/Odinstalovat role > Přidat nebo odebrat role** a zrušit výběr **Databázový server** .

**Poznámka**
Členy replika setu můžete odebrat jen pokud máte ve vaši síti minimálně 4 databázové instance nainstalované a zároveň dostupné.

## Povolit zabezpečený cluster VPN

Role GravityZone mají několik interních služeb, které mezi sebou komunikují výhradně. Pro bezpečnější prostředí můžete tyto služby izolovat vytvořením clusteru VPN pro ně. Buď jsou tyto služby na stejném zařízení nebo na více, budou pak komunikovat prostřednictvím zabezpečeného kanálu.

**Důležité**
- Tato funkce vyžaduje standardní nasazení GravityZone bez nainstalovaných vlastních nástrojů.
- Jakmile je cluster povolen, nemůžete jej deaktivovat.

Zabezpečení interních služeb na zařízeních:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte možnost Enable **Secure VPN Cluster** .

   Zpráva vás informuje o změnách, které budou provedeny.
4. Výběrem **Ano** potvrďte a pokračujte v instalaci VPN.

   Po dokončení se zobrazí potvrzovací zpráva.

Od této chvíle jsou všechny role v zařízení nainstalovány v zabezpečeném režimu a služby budou komunikovat prostřednictvím rozhraní VPN. Každá nová appliance, kterou přidáte do prostředí, se musí připojit ke clusteru VPN. Další informace viz „Připojit ke stávající databázi (Zabezpečený VPN cluster)“ (str. 118).

### Připojit k Existující Databázi

V distribuované architektuře GravityZone musíte nainstalovat roli databázového serveru do prvního zařízení a poté nakonfigurovat všechna další zařízení tak, aby se připojovala k existující instanci databáze. Tímto způsobem budou všechna zařízení sdílet stejnou databázi.

**Důležité**
Doporučuje se povolit zabezpečený cluster VPN a připojit se k databázi v takovém clusteru. Pro více informací, se obraťte na:

- „Povolit zabezpečený cluster VPN“ (str. 116)
- „Připojit ke stávající databázi (Zabezpečený VPN cluster)“ (str. 118)

Postup připojení zařízení k databázi GravityZone mimo zabezpečený cluster VPN:

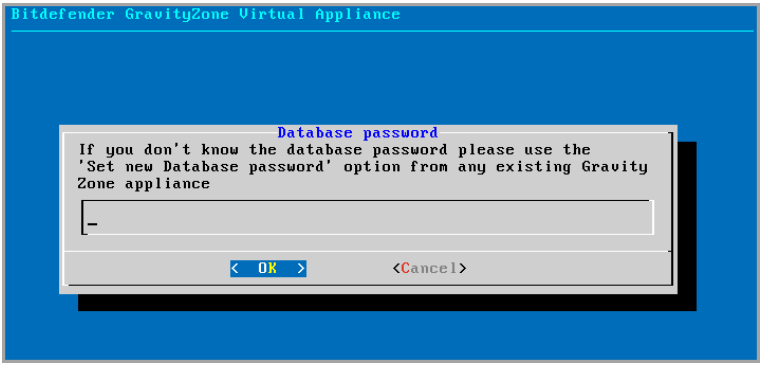
1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Připojit k stávající databázi (Connect to Existing Database)**.

**Poznámka**
Postarejte se o nastavení vlastního hesla databáze před použitím této možnosti. Pokud neznáte heslo k databázi, nastavte nové heslo přístupem do **Rozšířeného nastavení a Nastavení nového hesla databáze** z hlavní nabídky.

4. Vyberte **Konfigurace adresy databázového serveru (Configure Database Server address)**.
5. Vložte adresu databáze, použitím následující syntaxe:

   `<IP/Hostname>:<Port>`

   Specifikace portu není povinná a je volně volitelná. Standartní portem je `27017`.
6. Zadejte primární heslo databáze.




Rozhraní konzole appliance: vložte heslo databáze (enter database password)

7. Vyberte **OK** pro uložení změn.
8. Vyberte **Zobrazte adresu databázového serveru (Show Database Server address)** abyste se ujistili, že adresa byla správně nastavena.

## Připojit ke stávající databázi (Zabezpečený VPN cluster)

Tuto možnost použijte, pokud potřebujete rozšířit nasazení GravityZone o více zařízení a je povolen zabezpečený cluster VPN. Tímto způsobem nové zařízení bude sdílet stejnou databázi s existujícím nasazením v zabezpečeném režimu.

Další informace o zabezpečeném klastru VPN najdete na „Povolit zabezpečený cluster VPN“ (str. 116).

### Podmínky

Před pokračováním se ujistěte, že máte po ruce následující:

- IP adresa databázového serveru

- Heslo pro uživatele **bdadmin** v zařízení s rolí databázového serveru

### Připojte se k databázi

Postup připojení zařízení k databázi GravityZone v rámci zabezpečeného clusteru VPN:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu vyberte **Pokročilá nastavení (Advanced Settings)**.
3. Vyberte **Připojit k existující databázi (Secure VPN Cluster)** .

   Pokud nejsou splněny, budete informováni o požadavcích a alternativách.
4. Výběr potvrďte stisknutím **OK** a pokračujte.
5. Zadejte IP adresu databázového serveru v rámci zabezpečeného clusteru VPN.
6. Zadejte heslo pro uživatele **bdadmin** v zařízení s databázovým serverem.
7. Vyberte **OK** pro uložení změn a pokračujte.

Po dokončení procesu se zobrazí potvrzovací zpráva. Nové zařízení se stane členem klastru a bude bezpečně komunikovat s ostatními zařízeními. Všechna zařízení budou sdílet stejnou databázi.

## Zkontrolujte stav zabezpečeného clusteru VPN

Tato možnost je k dispozici pouze poté, co jste dříve povolili zabezpečený cluster VPN. Tuto možnost vyberte, chcete-li zkontrolovat, která zařízení ve vašem nasazení GravityZone ještě nezabezpečila své služby. Možná budete muset dále prozkoumat a zjistit, zda jsou zařízení online a přístupná.

## Nastavit Jazyk

Pro změnu nastavení jazyka v rozhraní appliance:

1. Vyberte **Konfigurace Jazyka (Configure Language)** v hlavním menu.
2. Vyberte jazyk z dostupných možností: Zobrazí se potvrzovací okno.

   **Poznámka**
   Případně budete muset listovat dolů abyste našli váš jazyk.

3. Vyberte **OK** pro uložení změn.

## 5.2. Správa Licencí

GravityZone je licencována jedním klíčem pro všechny bezpečnostní služby.

Kromě základních bezpečnostních služeb, GravityZone také poskytuje důležité ochranné funkce jako add-ony. Každý add-on je licencován jednotlivým klíčem a můžete jej použít pouze společně se základní platnou licencí. Pokud hlavní licence je neplatná, zobrazí se vám nastavení funkcí, ale nebudete jej moci používat.

Můžete si vybrat testovat GravityZone a rozhodnout se jestli je to to správné řešení pro vaší společnost. Pro aktivaci vašeho období hodnocení, musíte zadat trialový licenční klíč z registračního emailu do Control Center.

**Poznámka**
Control Center je dodávána bezplatně s kteroukoliv GravityZone bezpečnostní službou.

Pro pokračování využívání GravityZone po vypršení období trialu, musíte si koupit licenční klíč a použít jej k registraci produktu.

Pro koupi licence, kontaktuje Bitdefender prodejce nebo nás kontaktujte emailem na enterprisesales@bitdefender.com.

GravityZone licenční klíče mohou být spravovány ze záložky **Konfigurace > Licence** v Control Center. Pokud váš současný licenční klíč je skoro u konce platnosti, zobrazí se správa v konzoli informující vás, že potřebuje být obnoven. Pro zadání nové licence nebo zobrazení současné licence přejděte na záložky **Konfigurace > Licence**.

### 5.2.1. Hledání Prodejce

Naši prodejce vám pomohou pomocí všech informací, které potřebujete a pomohou vám vybrat nejlepší licenci pro vás.

Pro nalezení Bitdefender prodejce ve vaší zemi:

1. Přejděte na záložku Lokalizace Partnera na webu Bitdefender.
2. Vyberte zemi, ve které sídlíte pro zobrazení kontaktních informací dostupných partnerů Bitdefender.
3. Pokud nenajdete Bitdefender prodejce ve vaší zemi, nebojte se nás kontaktovat pomocí emailu na enterprisesales@bitdefender.com.

## 5.2.2. Zadávání Vašich Licenčních Klíčů

GravityZone registrace licence může být dokončena online nebo offline (pokud není internetové připojení k dispozici) V obou případech, musíte poskytnout platný licenční klíč.

Pro offline registraci, budete také potřebovat offline registrační kód spojený s licenčním kódem.

Pro změnu současného licenčního klíče nebo registraci add-onu:

1. Přihlašte se k Control Center použitím účtu administrátora společnosti.
2. Přejděte na záložku **Konfigurace > Licence**.
3. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky.
4. Vyberte typ registrace:
   - **Online**. V tomto případě, zadejte platný licenční klíč do pole **Licenční klíč**. Licenční klíč bude zkontrolován a ověřen online.
   - **Offline**, pokud není k dispozici připojení k internetu. V tomto případě, musíte poskytnout licenční kód a ještě registrační kód.

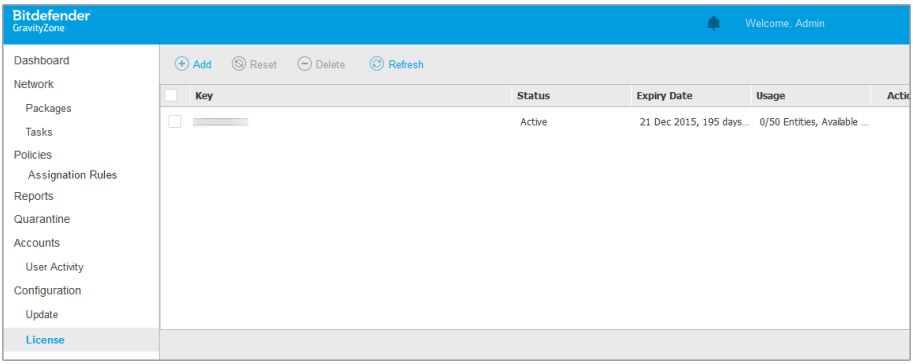
   Pokud licenční klíč není platný, chyba ověření se zobrazí jako tooltip přes pole **Licenční klíč**.
5. Klikněte na tlačítko **Přidat**. Licenční klíč bude přidán do záložky **Licence**, kde si můžete zkontrolovat její detaily.
6. Kliknutím na tlačítko **Uložit** aplikujete změny. Control Center se restartuje a vy se budete muset znovu přihlásit pro zobrazení změn.

**Poznámka**
Můžete použít add-ony tak dlouho jak kompatibilní základní licence je platná. V opačném případě sice uvidíte tyto rozšířené funkcionality, ale nebudete je moci používat.

## 5.2.3. Kontrolování Detailů Současné Licence

Pro zobrazení detailů vaší licence:

1. Přihlašte se k Control Center použitím účtu administrátora společnosti.
2. Přejděte na záložku **Konfigurace > Licence**.




Záložka Licence

3. V tabulce, si můžete zobrazit detaily o existujících licenčních klíčích.
   - Licenční klíč
   - Stav Licenčního klíče
   - Datum vypršení a zbývající čas licence

     **Důležité**
     Když licence vyprší, moduly ochrany instalovaného agenta budou vypnuty. Jako výsledek, zařízení nejsou chráněna a nemůžete provést žádnou úlohu skenu. Kterýkoli nově nainstalovaný agent vstoupí do trialu.

   - Počet využití licence

## 5.2.4. Resetování počtu využití licence

Můžete najít informace o vašem počtu využití licenčního klíče na záložce **Licence** pod sloupcem **Využití**.

Pokud chcete aktualizovat informace o využití, klikněte na licenci a klikněte na tlačítko **Resetovat** v horní části tabulky.

## 5.2.5. Zadejte licenční klíče

Na stránce **Licence (License)** si můžete vybrat jestli chcete neplatné licenční klíče smazat .

**Varování**
Smazáním licenčního klíče odeberete odpovídající službu z Control Center. Nebudete schopni instalovat a spravovat ochranu nabízenou touto službou na koncových bodech ve vaší síti. Nicméně, koncové body zůstanou chráněny po celou dobu platnosti licenčního klíče.
Když vložíte nový platný klíč obsahující již předtím smazanou službu, tak bude v Control Center znova zapnuta veškerá funkcionalita této služby.

Pro smazání licenčního klíče:

1. Přihlašte se k Control Center použitím účtu administrátora společnosti.
2. Přejděte na záložku **Konfigurace > Licence**.
3. Vyberte si licenční klíč, který chcete odebrat a klikněte na tlačítko ⊖ **Odstranit (Delete)** v horní části tabulky.

## 5.3. Instalace Ochrany na Koncová Zařízení

Závisí na konfiguraci strojů a na síťovém prostředí, může si vybrat instalaci pouze bezpečnostních agentů nebo také použít Security Server. V druhém případě, musíte první nainstalovat Security Server a poté bezpečnostní agenty.

Je doporučeno používat Security Server pro ochranu virtualizovaných prostředích jako jsou Nutanix, VMware or Citrix Xen, a nebo b případě pokud mají chráněné fyzické stroje málo hardwarových zdrojů.

**Důležité**
Pouze Bitdefender Endpoint Security Tools a Bitdefender Tools podporují spojení na Security Server. Další informace viz „Architektura GravityZone “ (str. 11).

### 5.3.1. Instalace Security Server

Security Server je dedikovaný virtuální stroj, který deduplikuje a centralizuje většinu antimalware funkcionalit klientů antimalware, funguje jako skenovací server.

Security Server nasazení je specifické pro prostředí do kterého se instaluje. Installační procesy jsou popsané níže:

- Security Server pro VMware NSX
- Security Server Multi-Platform nebo pro VMware vShield
- Security Server pro Amazon EC2
- Security Server pro Microsoft Azure

## Instalace Security Server pro VMware NSX

Do VMware NSX prostředí, musíte nasadit Bitdefender službu na každém chráněném clusteru. Za tímto účelem vytvořená speciální appliance bude automaticky nasazena na všech hostech v clusteru. Všechny virtuální stroje na hostu jsou automaticky připojeny pomocí funkce introspekce hostovaných strojů (Guest Introspection) k instanci Security Serveru nainstalovaných na tomto hostu.

Nasazení Security Serveru by se mělo provádět výhradně pomocí webového klienta vSphere (vSphere Web Client).

Pro instalaci Bitdefender služby:

1. Přihlašte se do vSphere Web Client.
2. Přejděte na **Síť (Network) &Bezpečnost (Security) > Instalace (Installation)** a klikněte na štítek **Nasazení služby (Service Deployments)**.
3. Klikněte na tlačítko **Nové nasazení služby (New service deployment)** (ikona znaku plus +). Otevře se konfigurační okno.
4. Vyberte **Introspekce hostů (Guest Introspection)** a klikněte na **Další (Next)**.
5. Vyberte si datacenterum a clustery na kterých chcete nasadit službu, pak klikněte ns **Další (Next)**.
6. Vyberte síť pro ukládání a správu (storage and management network), klikněte na **Další (Next)** a pak na **Dokončit (Finish)**.
7. Opakujte kroky od 3 do 6, tentokráte výběrem **Bitdefender** služby.

   Než začnete s instalací, tak se nejprve ujistěte, že máte síťové spojení mezi vybranou sítí a GravityZone Control Center.

   Jakmile je Bitdefender servis nainsntalován, tak začne automaticky nasazovat Security Server na všech ESXi hostech ve vybraných clustrech.

**Varování**
Proto aby služby fungovaly správně, je velmi důležité je nainstalovat ve správném pořadí, nejprve introspekci hosta a následně pak Bitdefender, a ne obě najednou.

**Poznámka**
Pro více informací k partnerským službám pro NSX, si přečtěte VMware NSX Documentation Center.
Pokud si vyberete**Specifikovaný na hostu (Specified on host)** pro ukládání a síťovou správu, zkontrolujte si že VM Agent je nastavený na hostech pro obě varianty Introspekce na hostu (Guest Introspection) a Bitdefender služby (services).

Security Server má specifické požadavky které závisí na počtu virtuálních strojů, které jím mají být chráněny. Pro standartní nastavení konfigurace hardware Security Serveru:

1. Přihlašte se do VMware vSphere Webového klienta.
2. Přejděte do **Hosty a Clustery (Hosts and Clusters)**.
3. Vyberte si cluster kde je Security Server nasazený a pak si vyberte si štítek **Související objekty (Related Objects) > Virtuální stroje (Virtual Machines)**.
4. Vypněte si **Bitdefender** aplianci.
5. Klikněte pravým tlačítkem na jméno appliance a pak vyberte v kontextovém menu **Editovat nastavení (Edit Settings..)**.
6. Ve štítku **Virtuální hardware (Virtual Hardware)**, nastavte hodnoty CPU a RAM tak aby splňovaly vaše požadavky a pak klikněte na **OK** pro uložení změn.
7. Zapněte si znova applianci.

**Poznámka**
Chcete-li upgradovat z VMware vShield na NSX, přečtěte si tento článek KB.

## Instalace Security Serveru pro Multi-Platformy nebo pro VMware vShield

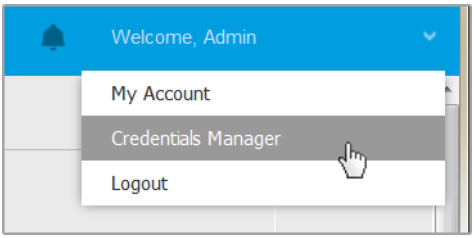
1. Připojte se k virtualizační platformě
2. Nainstalujte Security Server na hostech

### Připojte se do Virtualizační Platformy

K přístupu do virtualizované infrastruktůry integované s Control Center, musíte zadat všechny vaše uživatelské přístupové údaje pro každý dostupný systém virtualizačních serverů. Control Center používá vaše přihlašovací údaje pro připojení se k virtualizované infrastruktuře, a zobrazuje pouze zdroje, ke kterým máte přístup (jak je definováno v vCenter Server).

Pro specifikaci přístupových údajů za účelem spojení se systémy virtualizačních serverů:

1. Klikněte na vámi vybrané jméno ve v pravém horním rohu stránky a vyberte si **Správce přihlašovacích údajů (Credentials Manager)**.




Síť (Network) > Balíčky (Packages) menu

2. Přejděte na štítek **Virtuální Prostředí (Virtual Environment)**.
3. Vyspecifikujte potřebné autentizační přístupové údaje.
   a. Vyberte server z odpovídajícího menu.

      **Poznámka**
      Pokud nabídka není k dispozici, tak buď ještě nebyla nastavena žádná integrace, nebo již byla nastavena všechna potřebná pověření.

   b. Zadejte své uživatelské jméno a heslo a definující popis.
   c. Klikněte na tlačítko ⊕ **Přidat**. Nová sada přístupových údajů se vám zobrazí v tabulce.

**Poznámka**
Pokud jste si ještě nevyspecifikovali vaše autentizační přístupové údaje, tak budete vyzváni k jejich zadání jakmile se pokusíte prohlížet inventář jakéhokoliv vCenter Server systému. Jakmile zadáte svá pověření, uloží se do Správce pověření a příště je už zadávat nemusíte.

## Instalace Security Serveru na Hostech

Musíte nainstalovat Security Servery na hostech následovně:

- Ve VMware prostředích s vShield Koncovým bodem, musíte nainstalovat za tímto účelem vytvořenou applianci na každém hostu aby byl chráněn. Všechny virtuální stroje na hostech jsou automaticky připojeny pomocí vShield koncového bodu k instanci Security Serveru nainstalované na tomto hostu.
- V Citrix prostředích, musíte nainstalovat Security Server pomocí vzdálené instalační úlohy, na každém hostu, kterého chcete chránit pomocí HVI.

- V Nutanix Prism Element prostředích, musíte nainstalovat Security Server na každém hostu, pomocí vzdálené instalační úlohy.
- Ve všech ostatních prostředích, musíte nainstalovat Security Server na jeden nebo více hostů podle toho jaký počet virtuálních strojů má být chráněn. Musíte zvážit počet chráněných virtuálních strojů, dostupné zdroje pro Security Server na hostech, stejně jako síťové připojení mezi Security Server a chráněnými virtuálními stroji. Bezpečnostní agent nainstalovaný na virtuálních strojích se připojí k Security Server pomocí TCP/IP, s použitím detailů nastavených při instalaci nebo skrze politiku.

Pokud je Control Center integrována s vCenter Server, XenServer and Nutanix Prism Element, tak můžete automaticky nasadit Security Server na hosty přímo z Control Center. Také si můžete stáhnout Security Server balíčky pro samostatnou (standalone) instalaci z Control Center.

**Poznámka**
Pro VMware prostředí s vShield koncovým bodem (Endppoint),můžete nasadit Security Server na hostech exklusivně pomocí instalačních úloh.

### Místní Instalace

Na všech virtualizovaných prostředích které nejsou integrované sControl Center, musíte nainstalovat Security Server na hostech manuálně, použitím instalačního balíčku. Balíček Security Server je dostupný ke stažení z Control Center v několika různých formátech, kompatibilní s hlavními virtualizačními platformami.

### Stažení Instalačních Balíčků Security Server

Pro stažení instalačních balíčků Security Server:

1. Přejděte na záložku **Síť > Balíčky**.
2. Vyberte Výchozí Balíček Security Server.
3. Klikněte na tlačítko **Stáhnout** v horní části tabulky a vyberte typ balíčku z menu.
4. Uložte vybraný balíček na příslušné místo.

### Nasazení Security Server Instalačních Balíčků

Jakmile máte instalační baliček, nasaďte jej na hosta pomocí vašeho preferovaného nástroje pro nasazení na virtuální stroje.

Po nasazení, nastavte Security Server následovně:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client). Alternativně, se můžete připojit k applianci pomocí SSH.
2. Přihlašte se pomocích výchozích přihlašovacích údajů.
   - Uživatelské jméno: `root`
   - Heslo: `sve`
3. Spusťte příkaz `sva-setup`. Následně budete přistupovat ke konfiguračnímu rozhraní appliance.

   Security Server konfigurační rozhraní (hlavní menu)

   Pro navigování v možnostech a menu, použijte `Tab` a šipky. Pro vybrání určité možnosti, stiskněte `Enter`.
4. Nastavte nastavení sítě.

   Security Server používá protokol TCP/IP pro komunikaci s ostatními komponenty GravityZone. Můžete nastavit, aby appliance automaticky získala síťové nastavení z DHCP serveru nebo síťové nastavení provést ručně, jak je vysvětleno zde:

   a. Z hlavního menu, vyberte **Konfigurace sítě**.

   b. Vyberte síťové rozhraní.

   c. Vyberte konfigurační režim IP:

      - **DHCP**, pokud chcete aby Security Server získal automaticky nastavení síťe od DHCP serveru.
      - **Statické**, pokud nemáte DHCP server nebo máte IP rezervovanou pro applianci v DHCP serveru. V tomto případě, musíte ručně nastavit nastavení sítě.

        i. Zadejte hostname, IP adresu, masku sítě, gateway a DNS servery do příslušných polí.

        ii. Vyberte **OK** pro uložení změn.

**Poznámka**
Pokud jste připojen k applianci pomocí SSH klienta, změna nastavení sítě okamžitě zruší vaší relaci.

5. Konfigurace nastavení proxy.

   Pokud proxy server je používán v síti, musíte poskytnout její detaily, tak aby Security Server mohl komunikovat s GravityZone Control Center.

   **Poznámka**
   Podporovaná je pouze proxy se základním ověřením.

   a. Z hlavního menu, vyberte **Konfigurace Internetové proxy**.
   b. Zadejte hostname, uživatelské jméno, heslo a doménu do příslušných polí.
   c. Vyberte **OK** pro uložení změn.
6. Konfigurujte adresu Komunikačního Serveru.
   a. Z hlavního menu, vyberte **Nastavení Komunikačního serveru**.
   b. Zadejte adresu komunikačního serveru (Communication Server), včetně čísla 8443, použitím následujícího formátu:

      `https://Communication-Server-IP:8443`

      Alternativně, můžete použít jméno hosta místo IP adresy komunikačního serveru.
   c. Vyberte **OK** pro uložení změn.

### Vzdálená Instalace

Control Center vám umožňuje vzdáleně nainstalovat Security Server na viditelných hostech použitím installačních úloh.

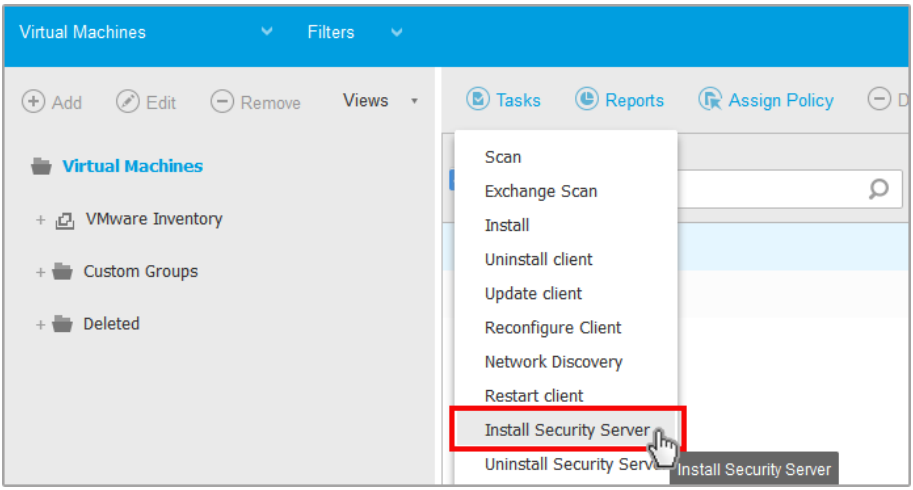
Pro instalaci Security Serveru vzdáleně na jednom nebo více hostech:

1. Jděte do záložky **Síť**.
2. Vyberte **Virtuální stroje** z možnosti zobrazení.
3. Prohlédněte si VMware, Citrix nebo Nutanix inventář a vyberte si označovací rámečky odpovídající požadovaným hostům nebo kontejnerům (Nutanix Prism, vCenter Server, XenServer nebo datacenter). Pro rychlý výběr, si můžete přímo

vybrat (root) kořenový kontejner (Nutanix inventář, VMware inventář nebo Citrix inventář). Budete moci zvolit hostitele jednotlivě z instalačního průvodce.

**Poznámka**
Nemůžete vybírat hostitele z různých složek.

4. Klikněte na tlačítko **Úlohy** v horní části tabulky a z menu vyberte **Aktualizovat Security Server**. Zobrazí se okno **Instalace Security Server**.




Instalace Security Server z menu úloh

5. Vyberte hostitele, na které chcete instalovat Security Servery.
6. Vyberte konfigurační nastavení, která chcete použít.

**Důležité**
Používání obecných nastavení při zavádění několika Security Serverů současně vyžaduje od hostitelů, aby sdíleli tu samou paměť, měli IP adresy přiřazené DHCP serverem, a byli součástí té samé sítě.

Pokud si vyberete konfiguraci každého Security Serveru jinak, tak budete mít možnost si vydefinovat nastavení, která chcete pro každého hosta zvlášť v dalším následném kroku pomocníka instalace. Kroky popsané níže aplikujte v

případě když použijete volbu **Konfigurovat každý (Configure each) Security Server**.

7. Klikněte **Další**.
8. Zadejte definující jméno pro Security Server.
9. Pro VMware prostředí si vyberte kontejner, do kterého chcete zahrnout Security Server z menu **Nasadit Kontejner (Deploy Container)** menu.
10. Vyberte cílovou paměť.
11. Vyberte typ zásobování disku. Doporučujeme používat zásobování tlustého disku.

    **Důležité**
    Pokud použijete zásobování tenkého disku a místo na disku v datovém úložišti dojde, Security Server zamrzne a hostitel tím pádem zůstane nechráněný.

12. Nastavte paměť a přidělování zdrojů pevnému disku na základě poměru konsolidace na hostiteli. Zvolte **Nízké**, **Střední** nebo **Vysoké** pro načtení doporučeného nastavení přidělování zdrojů, nebo **Ručně** pro nastavení přidělování zdrojů ručně.
13. Chcete nastavit administrativní heslo pro Security Server konzoli. Nastavení hesla pro správu přepíše výchozí kořenové heslo ("sve").
14. Nastavte časovou zónu zařízení.
15. Vyberte typ síťové konfigurace pro síť Bitdefender. IP adresa Security Server se nesmí změnit, protože ji agenti Linux používají ke komunikaci.

    Pokud zvolíte DHCP, ujistěte se, že jste nastavili DHCP server tak, aby rezervoval IP adresu zařízení.

    Pokud vyberete statický, musíte zadat IP adresu, masku podsítě, bránu a informace o DNS.
16. Vyberte síť vShield a zadejte pověření pro vShield. Výchozí štítek pro síť vShield je `vmservice-vshield-pg`.
17. Klikněte na tlačítko **Save**.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

**Poznámka**
Chcete-li upgradovat z VMware vShield na NSX, přečtěte si tento článek KB .

**Důležité**
Instalace Security Serveru na Nutanix pomocí vzdálené úlohy může selhat pokud je Prism Element cluster registrovaný do Prism Central nebo i z jiného důvodu. V těchto situacích, je doporučeno provést manuální nasazeníSecurity Serveru. Pro více informací čtěte KB article.

## Instalace Security Serveru pro Amazon EC2

Můžete použít Security Server k ochraně vašich Amazon EC2 instancí následovně:

- Nakonfigurujte Security Server nainstalovaný ve vaší lokální síti pro komunikaci s Amazon EC2 instancemi. Takto, budete schopni použít vaše lokální zdroje, buď fyzické nebo virtuální, také k ochraně Amazon EC2 inventáře.
- Nainstalujte jednu nebo vícero Security Server instancí ve vašem Amazon EC2 prostředí, podle vašich potřeb. V tomto případě, následujte proces popsaný zde v Článku znalostní databáze (KB article).

  **Důležité**
  - Aby fungovala komunikace mezi vašemi EC2 stroji a mezi instancemi Security Serverů nainstalovanými ve vašem Amazon EC2 inventáři, musíte správně nakonfigurovat Amazon VPC (Virtual Private Cloud) a také Amazon VPN spojení. Pro více informací, si přečtěte Dokumentaci Amazon VPC.
  - Doporučujeme nainstalovat Security Server ve stejném Amazon EC2 regionu spolu s instancemi které chcete chránit.

Výchozí režim skenování pro instance EC2 je Local Scan (zabezpečený obsah je uložen na nainstalovaném bezpečnostním agentovi a skenování je spuštěno lokálně na počítači). Pokud chcete skenovat instance EC2 pomocí Security Server, musíte nakonfigurovat instalační balíček agenta zabezpečení a příslušné politiky.

## Instalace Security Serveru pro Microsoft Azure

Můžete použít Security Server k ochraně vašich Microsoft Azure virtuálních strojů následovně:

- Nakonfigurujte Security Server nainstalovaný ve vaší lokální síti pro komunikaci s Microsoft Azure virtuálními stroji. Takto, budete schopni použít vaše lokální zdroje, buď fyzické nebo virtuální, také k ochraně Microsoft Azure inventáře.

- Nainstalujte jednu nebo vícero Security Server instancí ve vašem Microsoft Azure prostředí, podle vašich potřeb. V tomto případě, následujte proces popsaný zde v Článku znalostní databáze (KB article).

  **Důležité**

  - Pro správou komunikaci mezi vašimi Microsoft Azure virtuálními stroji a Security Server instancemi nainstalovanými ve vašem Microsoft Azure inventáři, musíte správně nakonfigurovat subnet vaši virtuální sítě. Pro detaily, si přečtěte Dokumentaci pro Microsoft Azure virtuální sítě.
  - Doporučujeme instalaci Security Serveru ve stejném Microsoft Azure regionu spolu s virtuálními stroji, které chcete chránit.

Výchozí režim skenování pro virtuální počítače Microsoft Azure je lokální sken (všechny signatury jsou uloženy v nainstalovaném bezpečnostním agentovi a skenování je spuštěno lokálně na zařízení). Chcete-li skenovat virtuální počítače Microsoft Azure pomocí Security Server, musíte nakonfigurovat instalační balíček bezpečnostního agenta a příslušné politiky.

## 5.3.2. Instalace Bezpečnostních Agentů

Pro ochranu vašich fyzických a virtuálních zařízení, musíte nainstalovat bezpečnostního agenta na každého z nich. Kromě spravování ochrany na místním zařízení, bezpečnostní agent také komunikuje s Control Center pro získání příkazů administrátora a k odeslání výsledků akcí.

Informace o dostupných bezpečnostních agentech, naleznete zde „Bezpečnostní agenty“ (str. 13).

Na stroje s Windows a Linux, bezpečnostní agent může mít dvě role a můžete je nainstalovat následovné:

1. Jako jednoduchého bezpečnostního agenta pro vaše zařízení.
2. Jako Relay, fungující jako bezpečnostní agent a také jako komunikační, proxy a aktualizační server pro ostatní zařízení v síti.

Můžete instalovat bezpečnostní agenty na fyzické a virtuální zařízení spuštěním instalačních balíčků lokálně nebo spuštěním úlohy vzdálené instalace z Control Center.

Je velmi důležité pozorně číst a postupovat podle instrukcí pro přípravu instalace.

V normálním režimu, bezpečnostní agenti, mají minimální uživatelské rozhraní. Umožňuje to uživatelům pouze zkontrolovat stav ochrany a spustit základní bezpečnostní úlohy (aktualizace a skeny), bez poskytnutí přístupu k nastavení.

Pokud povolil síťový administrátor pomocí instalačního balíčku a bezpečnostní politiky, bezpečnostní agent může být spuštěn v Režim Power User na zařízeních Windows, a umožnit koncovým uživatelům zobrazit a upravit nastavení politiky. Přesto, Control Center administrátor může vždy kontrolovat, které nastavení politiky je aplikováno, přepínat režim Power User.

Standartně zobrazovaný jazyk uživatelského rozhraní na chráněných koncových bodech Windows se nastavuje v čase instalace podle jazyku vašeho GravityZone účtu.

Na Mac systémech se nastavuje zobrazovací jazyk uživatelského rozhraní (user interface language) podle nastaveného jazyku na operačním systému v času instalace. Na Linuxech, bezpečnostní agent nemá lokalizované uživatelské rozhraní (user interface).

Pro instalaci uživatelského rozhraní na jiný jazyk na jednotlivých koncových bodech kde běží Windows, můžete vytvořit instalační balíček a nastavit preferovaný jazyk v jeho volbách konfigurace. Tato možnost není dostupná pro Macy a Linuxové koncové body. Pro více informací o vytváření instalačních balíčků, obraťte se zde „Vytváření Instalačních Balíčků“ (str. 137).

## Příprava na Instalaci

Před instalací, následujte tyto přípravné kroky, aby jste se ujistili, že půjde hladce:

1. Ujistěte se že cílová zařízení splňují minimální systémová požadavky. Pro některá zařízení, budete muset nainstalovat nejnovější dostupné servisní balíčky operačního systému nebo uvolnit místo na disku Zkompilujte seznam koncových bodů, které nesplňují potřebné požadavky, abyste je mohli vyloučit ze správy.
2. Odinstalace (ne pouze vypnutí) kteréhokoliv existujícího antimalware nebo Internet security software z cílových koncových bodů. Spuštění bezpečnostního agenta zároveň s ostatním bezpečnostním software na zařízení, může mít vliv na jejich provoz a způsobit velké problémy se systémem.

   Mnoho z nekompatibilních bezpečnostních programů je automaticky detekováno a odebráno při instalaci.

   Pokud se chcete dozvědět o tom více a pokud chcete zjistit, který bezpečnostní software třetích stran je detekován pomocí Bitdefender Endpoint Security Tools

klienta na stávajících operačních systémech Windows, tak si přečtěte tento Článek znalostní databáze (KB article).

**Důležité**
Pokud chcete zavést bezpečnostního agenta na počítač s Bitdefender Antivirus pro Mac 5.X, musíte tento odstranit ručně. Pro návod při postupu se podívejte na tento KB článek.

3. Instalace vyžaduje administrátorské oprávnění a přístup k Internetu. Pokud jsou cílené koncové body součástí Active Directory domény, tak byste měli použít pro vzdálenou instalaci přístupové údaje doménového administrátora. Jinak, se ujistěte, že máte veškeré nutné přístupové údaje k dispozici pro všechny koncové body.
4. Koncová zařízení musí mít síťové připojení k applianci GravityZone.
5. Doporučujeme použít statickou IP adresu pro server relaye. Pokud jste nenastavili statickou IP, použijte hostname stroje.
6. Při nasazování agenta skrze relay Linuxu, musí být splněny následující podmínky:
   - Relay musí mít nainstalovaný balíček Samba (`smbclient`) , verzi 4.1.0 nebo novější, `net` aby mohl zavádět agenty Windows.

     **Poznámka**
     Příkaz `net` binární/příkaz je obvykle dodáván s balíčky samba-client a / nebo samba-common. Na některých distribucích systému Linux (například CentOS 7.4) je příkaz `net` instalován pouze při instalaci úplné sady Samba (Common + Client + Server). Ujistěte se, že váš koncový bod přenosu má k dispozici příkaz `net`.

   - Cílové koncové body Windows musí mít zapnuté Administrative Share a Network Share.
   - Cílené koncové body s OS Linux a Mac musí mít povolené SSH.
7. Počínaje macOS High Sierra (10.13), ihned po instalaci Endpoint Security for Mac manuálně nebo vzdáleně, jsou uživatelé vyzváni k povolení Bitdefender rozšíření jádra (kernel extensions) na jejich počítačích. Dokud uživatel nepovolí Bitdefender rozšíření jádra (kernel extensions), tak nebudou některé Endpoint Security for Mac funkce fungovat. Pro zamezení uživatelské intervence, si můžete před povolit Bitdefender rozšíření jádra (kernel extensions) pomocí funkce whitelistingu skrze Mobile Device Management (MDM) nástroj.

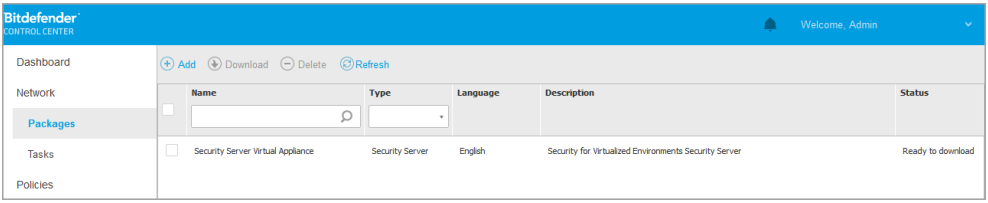
8. Když nasazujete agenta v Amazon EC2 inventáři, nakonfigurujte si bezpečnostní skupiny asociované s instancemi které chcete chránit v Amazon EC2 **Přístrojová deska (Dashboard) > Síť (Network) & Bezpečnost (Security)** následovně:
   - Pro vzdálenou installaci, povolte SSH* přístup z EC2 instance.
   - Pro lokální instalaci, povolte SSH* a RDP (Remote Desktop Protocol) přístup z počítače ze kterého se připojujete.

   * Pro vzdálenou instalaci na Linuxových instancích musíte povolit SSH přihlášení použitím jména uživatele a hesla (username and password).
9. Když nasazujete agenta v Microsoft Azure inventáři:
   - Cílový virtuální stroj musí být ve stejné virtuální síti spolu s GravityZone appliancí.
   - Cílový virtuální stroj musí být ve stejné virtuální síti spolu s Relay, která komunikuje s GravityZone appliancí, přičemž ta je v jiné síti.

## Místní Instalace

Jeden způsob jak nainstalovat bezpečnostního agenta na zařízení je lokálně spustit instalační balíček.

Můžete vytvořit a spravovat instalační balíčky v záložce **Síť > Balíčky**.




Záložka Balíčky

Jakmile je první klient nainstalován, bude použit k nalezení ostatních zařízení v síti, na základě mechanizmu Objevování v Síti. Pro detailní informace o objevování v síti, se obraťte na „Jak funguje síťové rozpoznávání “ (str. 154).

Pro lokální instalaci bezpečnostního agenta na zařízení, postupujte takto:

1. Vytvořit instalační balíček podle vašich potřeb.

**Poznámka**
Tento krok není povinný pokud již instalační balíček byl vytvořen pro síť pod vaším účtem.

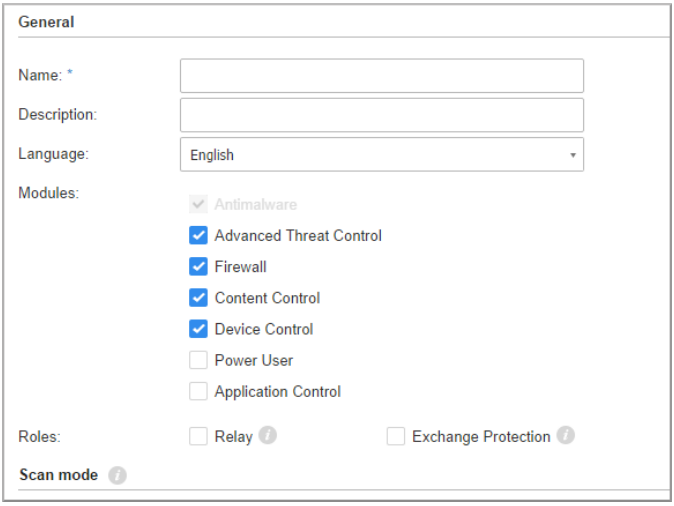
2. Stáhnout instalační balíček na cílové zařízení.

   Alternativně můžete odeslat odkaz ke stažení instalačního balíčku emailem několika uživatelům ve vaší síti.
3. Spustit instalační balíček na cílovém zařízení.

## Vytváření Instalačních Balíčků

Pro vytvoření instalačního balíčku:

1. Připojte a přihlaste se do Control Center.
2. Přejděte na záložku **Síť > Balíčky**.
3. Klikněte na tlačítko ⊕ **Přidat** v horní části tabulky. Zobrazí se konfigurační okno.




Vytvoření Balíčků - Možnosti

4. Zadejte výstižný název a popis pro instalační balíček, který chcete vytvořit.
5. Z pole **Jazyk**, vyberte požadovaný jazyk pro rozhraní klienta.

**Poznámka**
Tato volba je dostupná pouze pro operační systémy Windows.

6. Vyberte ochranné moduly, které chcete nainstalovat.

**Poznámka**
Nainstalují se pouze moduly, které jsou v daném operačním systému podporované. Další informace viz „Bezpečnostní agenty“ (str. 13).

7. Vyberte roli cílového zařízení:
   - **Relay**, pro vytvoření balíčku pro zařízení s rolí Relaye. Další informace viz „Relay“ (str. 15)
   - **Cache server pro správu záplat a aktualizací (Patch Management Cache Server)**, abyste Relay či internímu serveru umožnili distribuci aktualizací a záplat pro software. Tato role se zobrazuje jakmile je Relay role vybrána. Další informace viz „Patch Caching Server“ (str. 15)
   - **Ochrana Exchange**, pro nainstalování modulů ochrany pro Servery Microsoft Exchange, zahrnující antimalware, anitspam, filtrování obsahu a příloh pro provoz Exchange mailů a antimalware skenování na vyžádání databází Exchange. Další informace viz „Instalace Ochrany Exchange (Exchange Protection)“ (str. 166).
8. **Odinstalace předchozího řešení** . Doporučuje se ponechat toto zaškrtávací políčko zaškrtnuté pro automatické odebrání nekompatibilního bezpečnostního softwaru během instalace agenta Bitdefender na koncovém bodě. Pokud zrušíte výběr této možnosti, agent Bitdefender se nainstaluje vedle stávajícího bezpečnostního řešení. Později můžete ručně na vlastní nebezpečí odstranit dříve nainstalované bezpečnostní řešení,

**Důležité**
Souběžné spuštění agenta Bitdefender s jiným bezpečnostním softwarem na koncovém bodě může mít vliv na jejich provoz a způsobit závažné problémy se systémem.

9. **Režim Skenu**. Vyberte skenovací technologii, která nejlépe sedí pro vaše síťové prostředí a vaše zdroje zařízení. Můžete definovat režim skenu vybráním z následujících typů:

- **Automatické**. V tomto případě bezpečnostní agent automaticky detekuje konfiguraci zařízení a přizpůsobí technologii skenování odpovídajícím způsobem:
  - Centrální Sken ve Veřejném nebo Soukromém Cloudu (pomocí Security Server) se záložním Hybridním skenováním (Light Enginy), pro fyzické počítače s malým výkonem hardware a pro virtuální stroje. Tento případ vyžaduje nejméně jeden nasazený Security Server v síti.
  - Lokální Sken (s Full Enginy) pro fyzické počítače s vysokým výkonem hardware.
  - Lokální sken pro EC2 instance a Microsoft Azure virtuální stroje.

  **Poznámka**
  Za počítače s nízkým výkonem jsou považovány počítače, které mají CPU frekvenci nižší než 1.5 Ghz nebo paměť RAM menší než 1GB.

- **Vlastní**. V tomto případě, můžete konfigurovat režim skenu vybráním mezi několika skenovacími technologiemi pro fyzické a virtuální stroje:
  - Centrální sken ve veřejném a nebo privátním Cloudu (spolu s Security Serverem), který může podle nastavení v politikách spadnout (fallback*) na lokální sken (s plnohodnotnými stroji (enginy)) nebo na Hybridní Sken (s lehkými stroji (enginy)
  - Hybridní Sken (s lehkými agenty)
  - Lokální Sken (s Full Enginy)

  Výchozí režim skenování pro instance EC2 je Local Scan (zabezpečený obsah je uložen na nainstalovaném bezpečnostním agentovi a skenování je spuštěno lokálně na počítači). Pokud chcete skenovat instance EC2 pomocí Security Server, musíte nakonfigurovat instalační balíček agenta zabezpečení a příslušné politiky.

  Výchozí režim skenování pro virtuální počítače Microsoft Azure je lokální sken (všechny signatury jsou uloženy v nainstalovaném bezpečnostním agentovi a skenování je spuštěno lokálně na zařízení). Chcete-li skenovat virtuální počítače Microsoft Azure pomocí Security Server, musíte nakonfigurovat instalační balíček bezpečnostního agenta a příslušné politiky.

* V případě skenování pomocí dvou strojů najednou, pokud je jeden z nich nedostupný, bude použit záložní. Spotřeba zdrojů a využití sítě bude založena na využití enginů.

Pro více informací ohledně dostupných skenovacích technologií, se obraťte na„Skenovací nástroje“ (str. 3)

10. **Zavést vShield na koncový bod, když je zjištěno prostředí VMware integrované s vShieldem**. Tato volba se může použít když je instalační balíček nasazen z VMware prostředí integrovaného s vShield. V tomto případě, VMware vShield Endpoint bude nainstalován na cílovém stroji namísto Bitdefender bezpečnostního agenta.

   **Důležité**
   Tato volba je pouze vhodná pro vzdálené nasazení a ne lokální instalace. Když instalujete lokálně ve VMware prostředích integrovaných s vShieldem, tak máte možnost si stáhnout Integrovaný vShield balíček (vShield-Integrated package).

11. Při úpravě skenovacích enginů používajících Veřejné nebo Soukromé skenovací Cloudy (Security Server), musíte vybrat lokálně nainstalovaný Security Servery, které chcete použít a konfigurovat jejich prioritu v sekci **Přiřazení Security Server**:

    a. Klikněte na seznam Security Server v hlavičce tabulky. Zobrazí se seznam zjištěných Security Serverů.

    b. Zvolte jednotku.

    c. Klikněte na tlačítko ⊕ **Přidat** v hlavičce sloupce **Akce**.

       Security Server je přidán na seznam.

    d. Postupujte stejným způsobem pro přidání více bezpečnostních serverů, pokud jsou dostupné. V tomto případě, můžete nastavit jejich prioritu použitím šipek ⌃ nahoru a ⌄ dolů dostupných na pravé straně každé entity. Pokud první Security Server není dostupný, další bude využit a tak dále.

    e. Pro smazání jedné entity ze seznamu, klikněte na příslušné tlačítko ⊗ **Smazat** navrchu tabulky.

    Můžete si vybrat šifrované připojení k Security Server vybráním možnosti **Použít SSL**.

12. **Smíšené**. Můžete konfigurovat následující možnosti na několika typech souborů z cílových zařízení:

- **Odeslat výpisy o pádu**. Zvolte tuto možnost, aby v případě selhání bezpečnostního agenta byla odeslala výpisy o pádu do laboratoří společnosti Bitdefender. Výpisy o pádu pomohou našim technikům při zjišťování příčiny problému a při zabraňování v jeho opětovném výskytu. Nebudou odeslány žádné osobní informace.
- **Odeslat soubory karantény do Bitdefender Labs každé (hodiny)**. Ve výchozím nastavení jsou soubory karantény do Laboratoří společnosti Bitdefender automaticky odesílány každou hodinu. Můžete upravit časové intervaly, kdy mají být soubory karantény odeslány. Vzorky souborů budou analyzovány pracovníky výzkumu malwaru společnosti Bitdefender. Pokud je přítomnost malwaru potvrzena, je vydána signatura umožňující odstranění malwaru.
- **Odeslat podezřelé spustitelné soubory do Bitdefender**. Zvolte tuto možnost, aby podezřele vyhlížející soubory nebo soubory vykazující podezřelé chování byly odesílány do Laboratoří společnosti Bitdefender na analýzu.

13. Vyberte **Skenovat před instalací**, pokud se chcete ujistit, že jsou stroje čisté před instalací klienta na ně. Provede se rychlý sken v cloudu na cílových strojích před startem instalace.
14. Bitdefender Endpoint Security Tools je nainstalován ve výchozím instalačním adresáři. Vyberte **Použít vlastní instalační cestu** , chcete-li nainstalovat agenta Bitdefender na jiném místě. Pokud určitá složka neexistuje, vytvoří se při instalaci.
    - Ve Windows je výchozí cesta `C:\Program Files\`. Chcete-li nainstalovat Bitdefender Endpoint Security Tools do vlastního umístění, použijte při zadávání cesty konvence Windows. Například, `D:\folder`.
    - V systému Linux je Bitdefender Endpoint Security Tools ve výchozím nastavení nainstalován do složky `/opt` . Chcete-li agenta Bitdefender nainstalovat do vlastního umístění, použijte při zadávání cesty konvence Linux. Například `/folder` .

      Bitdefender Endpoint Security Tools nepodporuje instalaci do následujících vlastních cest:
      – Jakákoli cesta, která nezačíná lomítkem (/). Jedinou výjimkou je umístění Windows `%PROGRAMFILES%` , které agent zabezpečení interpretuje jako výchozí složku Linux `/opt` .
      – Jakákoli cesta, která je v `/tmp` nebo `/proc`.

- Jakákoli cesta, která obsahuje následující speciální znaky: `$, !, *, ?, ", ', `, \, (, ), [, ], {, }`.
- Specifikátor `systemd` (%).

V systému Linux vyžaduje instalace do vlastní cesty glibc 2.21 nebo vyšší.

**Důležité**
Při použití vlastní cesty se ujistěte, že máte pro každý operační systém správný instalační balíček.

15. Pokud chcete, můžete nastavit heslo a zabránit uživatelům před odebráním ochrany. Vyberte **Nastavit heslo pro odinstalaci** a zadejte požadované heslo do příslušných polí.
16. Pokud cílová zařízení jsou v Síťovém Inventáři pod **Vlastní Skupiny**, můžete je přesunout do určitých složek okamžitě po dokončení nasazení bezpečnostního agenta.

    Vyberte **Použít vlastní složku** a vyberte složku v příslušné tabulce.
17. V sekci **Zavaděč** nastavte relay, ke kterému se budou počítače připojovat při instalaci a aktualizacích klienta:
    - **Zařízení GravityZone**, když se koncové body připojují přímo k zařízení GravityZone.

      V tomto případě, můžete také určit:
      - Vlastní Komunikační server, zadáním jeho IP nebo jméno hostitele, pokud je třeba.
      - Nastavení proxy, pokud cílové koncové body komunikují se zařízením GravityZone prostřednictvím proxy. V tomto případě zvolte **Použít proxy pro komunikaci** a zadejte požadované nastavení proxy do polí níže.
    - **Endpoint Security Relay**, pokud chcete připojit koncové body k relay klientovi nainstalovanému ve vaší síti. Všechny stroje s funkcí relay, nalezené ve vaší síti, budou uvedeny v níže zobrazené tabulce. Zvolte požadovaný stroj s relay. Připojené koncové body budou komunikovat s Control Center pouze prostřednictvím zvoleného relaye.

      **Důležité**
      Port 7074 musí být otevřený pro nasazení skrze Bitdefender Endpoint Security Tools Relay ,aby fungoval.

18. Klikněte na tlačítko **Save**.

Nově vytvořený balíček bude přidán do seznamu balíčků.

**Poznámka**
Nastavení nakonfigurovaná během instalačního procesu budou okamžitě aplikována na koncové body ihned po dokončení instalace. Jakmile je politika aplikována na klientovi, nastavení nakonfigurovaná uvnitř politik budou vynucena a nahradí některá nastavení v instalačních balíčcích (jako například nastavení kommunikačních serverů nebo nastavení proxy)

## Stahování instalačních balíčků

K stažení instalačních balíčků bezpečnostních agentů:

1. Přihlašte se do Control Center z koncového bodu na kterém chcete ochranu nainstalovat.
2. Přejděte na záložku **Síť > Balíčky**.
3. Vyberte instalační balíček který chcete stáhnout.
4. Klikněte na **Download** tlačítko na vrchní straně tabulky a vyberte následně typ instalace který chcete použít. Dva druhy instalačních souborů jsou k dispozici:
   - **Downloader**. Downloader nejprve stáhne plnohodnotnou instalační sadu z Bitdefender cloudových serverů a následně zahájí instalační proces. Díky velmi malé velikosti můžou běžet jak na 32 tak i na 64-bitových systémech (což umožňuje jednoduchou distribuci) Na druhé straně to potřebuje aktivní internetové spojení.
   - **Full kit**. Full kity (plné instalační sady) jsou větší velikosti a musí být spouštěny na specifickém druhu operačního systému.

     Full kit (úplná instalační sada) se používá pro instalaci na koncových bodech s žádným nebo pomalým internetovým spojením. Stáhněte tento soubor na koncový bod s internetovým připojením, a pak následně přeneste tento soubor pomocí extérního disku či uložiště nebo síťového sdíleného disku či úložiště.

     **Poznámka**
     Dostupné verze full kitů (plných instalačních sad):
     - **Windows OS:** 32-bitové a 64-bitové systémy

- **Linux OS:** 32-bitové a 64-bitové systémy
- **macOS:** pouze 64-bitové systémy

Uliště se, že používáte správnou verzi pro systém na který instalujete.

5. Uložte soubor na koncový bod.

**Varování**

- Název staženého spustitelného souboru Downloaderu musí být přejmenován, jinak nebude možné stáhnout instalační soubory z Bitdefender serveru.

6. Navíc, pokud jste již vybrali Downloader, tak můžete vytvořit MSI balíček pro Windows koncové body. Pro více informací, si přečtěte this KB article.

## Pošlete odkaz pro stažení instalačních souborů emailem.

Možná budete potřebovat rychle informovat ostatní uživatele, že je instalační balíček je dostupný ke stažení. V tomto případě, proveďte následující kroky popsané níže:

1. Přejděte na záložku **Síť > Balíčky**.
2. Vyberte instalační balíček který chcete.
3. Klikněte na **Pošlete odkazy k stažení** tlačítko na vrchní straně tabulky. Zobrazí se konfigurační okno.
4. Zadejte emailové adresy všech uživatelů, kteří mají dostat odkaz ke stažení instalačních souborů. Zmáčkněte `Enter` po zadání každé emailové adresy.

   Ubezpečte se prosím zda je každá vložená emailová adresa platná.
5. Pokud se chcete podívat na odkazy pro stahování předtím než je pošlete emailem tak klikněte na **Installation links** tlačítko.
6. Klikněte na **Send**. Email obsahující odkaz na instalaci bude odeslán na každou specifikovanou emailovou adresu.

## Probíhá instalace balíčků

Aby instalace fungovala, je nutné aby byla spuštěna pod administrátorkýma právama.

Balíček se nainstaluje různě podle každého druhu operačního sytému viz níže:

- Na Windows a macOS operačních systémech:

1. Stáhněte si instalační soubor přímo na cílových koncových bodech z Control Center nebo jej zkopírujte ze sdíleného síťového disku.
2. Pokud jste si stáhli full kit (úplný instalační balíček), tak extrahujte soubory přímo z archivu.
3. Spusťe spustitelný soubor.
4. Postupujte podle návodu na obrazovce.

**Poznámka**
Na macOS, po instalaci Endpoint Security for Maca, jsou uživatelé na jejich počítačích vyzváni povolit Bitdefender rozšíření jádra (kernel extensions). Dokud uživatelé nepovolí Bitdefender rozšíření jádra (kernel extensions), tak některé funkce bezpečnostního klienta nebudou fungovat. Pro detaily, se obraťte se na tento KB článek.

- Na linuxových operačních systémech:
  1. Připojte a přihlaste se do Control Center.
  2. Stáhněte si nebo zkopírujte si instalační soubor do cílového koncového bodu.
  3. Pokud jste si stáhli full kit (úplný instalační balíček), tak extrahujte soubory přímo z archivu.
  4. Získejte rootovská práva spuštěním `sudo su` příkazu.
  5. Změňte práva pro instalační soubor tak abyste jej mohli spustit:

     ```
     # chmod +x installer
     ```

  6. Spusťte instalační soubor:

     ```
     # ./installer
     ```

  7. Pro kontrolu zda byl agent nainstalován na koncovém bodě, spusťte tento příkaz:

     ```
     $ service bd status
     ```

Jakmile byl bezpečnostní agent nainstalován, koncový bod se ukáže jakožto spravovaný v Control Center (**Network** page) během několika minut.

**Důležité**

Pokud požíváte VMware Horizon View Persona Management, tak doporučujeme nakonfigurovat Active Directory skupinové politiky (Group Policy) aby exkludovaly následující Bitdefender procesy (bez úplné cesty):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Tyto výjimky jsou platné dokud je na koncovém bodu nainstalovaný bezpečnostní agent. Pro dalsší detaily, se podívejte na Stránku dokumentace VMware Horizon.

## Vzdálená Instalace

Control Center vám umožňuje vzdáleně instalovat bezpečnostního agenta na zařízení z integrovaných prostředí s Control Center a další zařízení detekované v zařízení v síti použitím instalačních úloh. V prostředích VMware, vzdálená instalace spoléhá na VMware Tools, kdežto v Citrix XenServer prostředích a Nutanix Prism Element prostředích, to závisí na administrativních sdíleních Windows a SSH.

Jakmile je bezpečnostní agent nainstalován na zařízení, může to zabrat pár minut pro zbytek síťových zařízení, aby byli viditelné v Control Center.

Bitdefender Endpoint Security Tools zahrnuje mechanizmus automatického objevování v síti, který umožňuje detekování zařízení, která nejsou v Active Directory. Detekovaná zařízení jsou zobrazena jako **nespravovaná** v záložce **Síť**, v zobrazení **Počítače**, pod **Vlastní Skupiny**. Control Center automaticky odebere Active Directory zařízení ze seznamu detekovaných zařízení.

Za účelem zapnutí funkce síťového rozpoznání, musíte mít nejprve Bitdefender Endpoint Security Tools klienta již nainstalovaného nejméně na jednom z koncových bodů v též síti. Tento koncový bod bude použit k proskenování sítě a instalaci Bitdefender Endpoint Security Tools klienta na nechráněných koncových bodech.

Pro detailní informace o objevování v síti, se obraťte na „Jak funguje síťové rozpoznávání “ (str. 154).

## Požadavky pro vzdálenou instalaci

Aby mohla vzdálená instalace fungovat:

- Na Windows:
  - Musí být zapnuté `admin$` administrativní sdílení (Administrative share). Nakonfigurujte každou cílovou pracovní stanici, tak aby nepoužívala pokročilé sdílení souborů (advanced file sharing).
  - Nakonfigurjte řízení účtů uživatelů (User Account Control (UAC)) podle závislosti na operačním systému běžícího na cílových bodech. Pokud koncové body jsou součásti Active Directory domény, tak můžete použít skupinové politiky (group policy) ke konfiguraci řízení účtů uživatelů (User Account Control). Pro detaily, se obraťte se na tento KB článek.
  - Vypněte Windows Firewall nebo nakonfigurujte ho tak aby byl povolen provoz pro sdílení souborů a tiskáren (File and Printer Sharing protocol).

  **Poznámka**
  Vzdálená instalace funguje pouze na moderních operačních systémech, počínaje Windows 7 / Windows Server 2008 R2, pro které Bitdefender dodává plnohodnotnou podporu. Další informace viz „Podporované Operační Systémy“ (str. 29).

- Na Linux OS: musí být zapnutý SSH.
- Na macOS: musí být povolené vzdálené přihlášení (remote login) a sdílení souborů (file sharing) .

## Běží úlohy vzdálené instalace

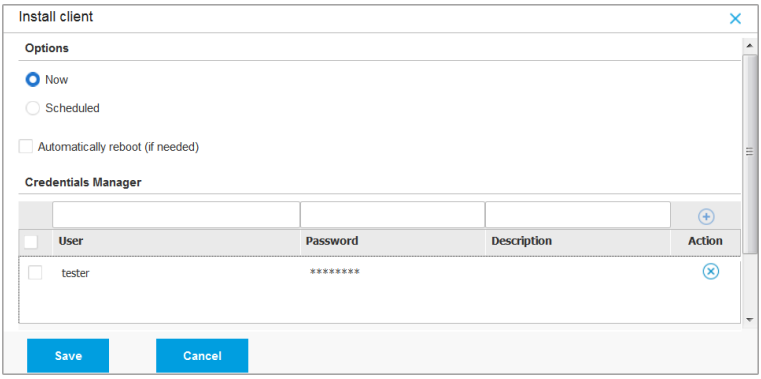
Pro spuštění instalační úlohy na dálku:

1. Připojte a přihlaste se do Control Center.
2. Jděte do záložky **Síť**.
3. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
4. Vyberte požadovanou skupinu v levém panelu. Všechny dostupné jednotky ve vybrané skupině jsou zobrazeny v pravém panelu tabulky.

**Poznámka**
Případně můžete také použít filtry a zobrazit pouze nespravované koncové body. Klikněte na nabídku **Filtry** a zvolte následující možnosti: **Nespravované** z karty **Zabezpečení** a **Všechny položky rekurzivně** z karty **Hloubka**.

5. Vyberte jednotky (koncové body nebo skupiny koncových bodů), na které si přejete nainstalovat zabezpečení.
6. Klikněte na tlačítko **Úlohy** nahoře od tabulky a vyberte **Instalovat**.

   Zobrazí se průvodce **Instalačním klientem**.




Instalace Bitdefender Endpoint Security Tools z Nabídky úloh

7. V sekci **Možnosti** nastavte čas instalace:
   - **Nyní**, čímž spustíte okamžité zavádění.
   - **Plánovaný**, čímž nastavíte interval opakování zavádění. V tomto případě zvolte svůj požadovaný časový interval (každou hodinu, den nebo týden) a nastavte ho dle svých potřeb.

     **Poznámka**
     Například, když je na cílovém stroji nutné před instalací klienta nejprve provést určité operace (jako je odinstalace jiného softwaru a restartování OS), můžete zavedení nastavit tak, aby se spustilo každé 2 hodiny. Úloha se na každém koncovém bodě spustí každé 2 hodiny, dokud zavedení neproběhne úspěšně.

8. Pokud chcete, aby se koncové body automaticky restartovaly pro dokončení instalace, zvolte **Restartovat automaticky (je-li potřeba)**.
9. V sekci **Správce pověření** upřesněte administrativní pověření nezbytné pro vzdálenou autentizaci na cílových koncových bodech. Pověření můžete přidat zadáním uživatelského jména a hesla pro každý cílový operační systém.

   **Důležité**
   Pro stanice Windows 8.1 musíte poskytnout oprávnění zabudovaného administrátorského účtu, nebo účtu administrátora domény. Více informací naleznete v tomto KB článku.

   Pro přidání požadovaných oprávnění OS:

   a. Zadejte uživatelské jméno a heslo účtu administrátora do příslušných polí v záhlaví tabulky.

      Pokud jsou počítače v doméně, stačí zadat pověření administrátora domény.

      Při zadávání jména uživatelského účtu použijte konvence systému Windows:

      - Pro stroje s Active Directory použijte tyto syntaxe: `username@domain.com` a `domain\username`. Abyste si mohli být jisti, že pověření budou fungovat, zadejte je v obou tvarech (`username@domain.com` a `domain\username`).
      - Pro stroje Pracovní skupiny stačí zadat pouze uživatelské jméno bez jména pracovní skupiny.

      Můžete také přidat popis, který vám usnadní identifikaci jednotlivých účtů.

   b. Klikněte na tlačítko ⊕ **Přidat**. Účet je přidán do seznamu oprávnění.

      **Poznámka**
      Zadaná pověření jsou automaticky uložena do vašeho Správce pověření, takže je příště už nemusíte zadávat. Do Správce pověření vstoupíte tak, že ukážete myší na vaše uživatelské jméno v pravém horním rohu konzole.

      **Důležité**
      Pokud jsou poskytnutá pověření neplatná, zavedení klienta na odpovídajících koncových bodech selže. Pokud jsou pověření na cílových koncových bodech změněna, ujistěte se, že jste aktualizovali zadaná pověření OS ve Správci pověření.

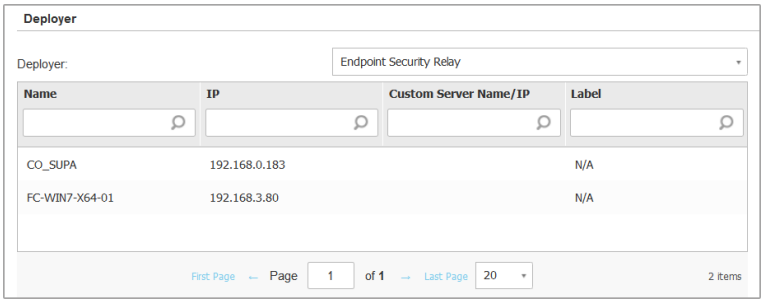
10. Označte zaškrtávací pole odpovídající účtům, které chcete použít.

> **Poznámka**
> Pokud nezvolíte žádná pověření, zobrazí se okno s varováním. Tento krok je povinný pro vzdálenou instalaci bezpečnostního agenta na koncové body.

11. V sekci **Zavaděč** nastavte relay, ke kterému se budou počítače připojovat při instalaci a aktualizacích klienta:
    - **Zařízení GravityZone**, když se koncové body připojují přímo k zařízení GravityZone.

      V tomto případě můžete určit také:
      - Vlastní Komunikační server, zadáním jeho IP nebo jméno hostitele, pokud je třeba.
      - Nastavení proxy, pokud cílové koncové body komunikují se zařízením GravityZone prostřednictvím proxy. V tomto případě zvolte **Použít proxy pro komunikaci** a zadejte požadované nastavení proxy do polí níže.
    - **Endpoint Security Relay**, pokud chcete připojit koncové body k relay klientovi nainstalovanému ve vaší síti. Všechny stroje s funkcí relay, nalezené ve vaší síti, budou uvedeny v níže zobrazené tabulce. Zvolte požadovaný stroj s relay. Připojené koncové body budou komunikovat s Control Center pouze prostřednictvím zvoleného relaye.

> **Důležité**
> Aby zavedení prostřednictvím relay agenta fungovalo, port 7074 musí být otevřený.



12. Použijte sekci **Další cíle**, pokud chcete zavést klienta na konkrétní stroje ve vaší síti, které se nezobrazují v síťovým inventáři. Rozbalte sekci a zadejte IP adresy nebo jména hostitelů těchto strojů do určeného pole, oddělených čárkou. Můžete přidat tolik IP adres, kolik potřebujete.
13. Pro aktuální zavedení musíte zvolit jeden instalační balíček. Klikněte na seznam **Použít balíček** a zvolte požadovaný instalační balíček. Zde naleznete všechny instalační balíčky, které byly dříve vytvořeny pro váš účet a také výchozí instalační balíčky, dostupné v Control Center.
14. Pokud potřebujete, můžete upravit některá nastavení zvoleného balíčku kliknutím na tlačítko **Upravit** vedle pole **Použít balíček**.

    Nastavení instalačního balíčku se zobrazí níže a vy budete moci provést požadované změny. Pro další detailnější informace jak připravovat či upravovat instalační balíčky, se podívejte na „Vytváření Instalačních Balíčků“ (str. 137).

    Pokud si přejete uložit změny jako nový balíček, vyberte možnost **Uložit jako balíček**, umístěnou ve spodní části seznamu nastavení balíčku, a zadejte název nového instalačního balíčku.
15. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

**Důležité**

Pokud požíváte VMware Horizon View Persona Management, tak doporučujeme nakonfigurovat Active Directory skupinové politiky (Group Policy) aby exkludovaly následující Bitdefender procesy (bez úplné cesty):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Tyto výjimky jsou platné dokud je na koncovém bodu nainstalovaný bezpečnostní agent. Pro dalsší detaily, se podívejte na Stránku dokumentace VMware Horizon.

## Příprava linux systému pro on-access skenování

Bitdefender Endpoint Security Tools for Linux obsahuje on-access skenovací schopnosti, které fungují společně se specifickými linuxovými distribucemi a verzemi jádra. Pro více informací, čtěte system requirements.

Dále se dozvíte jak manuálně zkompilovat DazukoFS module.

### Manuálně zkompilujte DazukoFS module

Následujte níže uvedené kroky pro kompilaci DazukoFS pro danou verzi jádra systému a poté nahrajte modul:

1. Stáhněte patřičné soubory hlaviček jádra (kernel headers)
   - Na **Ubuntu** systémech, spusťte tento příkaz:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - Na **RHEL/CentOS** systémech, spusťte tento příkaz:

     ```
     $ sudo yum install kernel-devel kernel-headers-`uname -r`
     ```

2. Na **Ubuntu** systémech, potřebujete `build-essential`:

   ```
   $ sudo apt-get install build-essential
   ```

3. Zkopírujte a extrahujte DazukoFS zdrojový kód do preferovaného adresáře:

   ```
   # mkdir temp
   # cd temp
   # cp /opt/BitDefender/share/modules/dazukofs/dazukofs-source.tar.gz
   # tar -xzvf dazukofs-source.tar.gz
   # cd dazukofs-3.1.4
   ```

4. Zkompilujte modul:

   ```
   # make
   ```

5. Nainstalujte a nahrajte modul:

```
# make dazukofs_install
```

### Požadavky na používání on-access skenování s DazukoFS

Proto aby DazukoFS a on-access skenování fungovalo společně, musí být splněna následující série podmínek. Prosím zkontrolujte jestli veškeré hlášky uvedené níže souhlasí pro váš Linux systém a následujte pokyny a doporučení za účelem vyhnutí se chybám.

- SELinux politika musí být vypnuta nebo nastavena na **permissive** mód. Zkontrolujte a upravte SELinux nastavení, editujte `/etc/selinux/config` soubor.
- Bitdefender Endpoint Security Tools klient je exklusivně kompatibilní s DazukoFS verzí zahrnuté v instalačním balíčku. Pokud je DazukoFS již ninstalován v systému, odeberte ho před instalací Bitdefender Endpoint Security Tools klienta.
- DazukoFS podporuje jen vybrané určité verze jádra. Pokud DazukoFS balíček dodaný s Bitdefender Endpoint Security Tools klientem není kompatibilní s verzí jádra systému, tak nebude možné tento modul nahrát. V případě, když nemůžete aktualizovat jádro na podporovanou verzi a nebo rekompilovat DazukoFS modul pro Vaší verzi jádra. Naleznete DazukoFS balíček v Bitdefender Endpoint Security Tools instalačním adresáři:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Když sdílíte soubory používáním dedikovaných serverů jakožto NFS, UNFSv3 or Samba, must spustit Služby v následujícím pořadí:

  1. Povolte on-access skenování pomocí politiky z Control Center.

     Pro více informací, se obraťte na GravityZone Příručku Administrátora.

  2. Spusťte službu pro sdílení síťových disků (network sharing service).

     Pro NFS:

     ```
     # service nfs start
     ```

     Pro UNFSv3:

```
# service unfs3 start
```

Pro Samba:

```
# service smbd start
```

**Důležité**
V případě NFS služby, DazukoFS je komatibilní pouze s NFS uživatelským serverem (NFS user server).

## Jak funguje síťové rozpoznávání

Mimo integrace s Active Directory, GravityZone také obsahuje automatický rozpoznávací síťový mechanizmus vytvořený za účelem detekce počítačů v pracovní skupině (workgroup computers).

GravityZone používá a spoléhá se na **Microsoft Computer Browser** službu a **NBTscan** nástroj za účelem provedení síťového rozpoznávání (network discovery).

Vyhledávací služba počítačů (The Computer Browser service) je síťová technologie používaná počítači s Windows OS ke správě a uchovávání doménových seznamů, pracovních skupin a počítačů v nich a také za účelem dodávání těchto seznamů klientským počítačům na jejich vyžádání. Počítače odhalené v síti pomocí vyhledávací služby počítačů (Computer Browser service) si můžete zobrazit pomocí spuštění následujícího příkazu **net view** v okně příkazového řádku.


příkaz Net view

NBTscan nástroj skenuje počítačovou síť pomocí NetBIOS. Dotazuje se každého koncového bodu v síti a získává informace jakožto IP adresy, NetBIOS jméno počítače a MAC adresy.

Abyste mohli zapnout a využít automatické síťové rozpoznávání (network discovery),tak musíte již mít Bitdefender Endpoint Security Tools Relay nainstalovaného na nejméně jednom počítači v síti. Tento počítač bude pak použit k následnému proskenování sítě.

**Důležité**

Control Center nepoužívá informace o síti ze služby Active Directory ani z funkce mapy sítě. Síťová mapa (network map) staví na jiné technologii síťového rozpoznávání: Link Layer Topology Discovery (LLTD) protokolu.

Control Center není aktivně zapojená v provozování služby vyhledávání počítačů (Computer Browser service). Bitdefender Endpoint Security Tools se pouze dotazuje služby vyhledávání počítačů (Computer Browser service) za účelem získání seznamu pracovních stanic a serverů momentálně viditelných na síti , známý jako seznam prohlížených (browse list) a následně ho zašle do Control Center. Control Center zpracovává seznam prohlížených viditelných stanic (browse list), přidává nově rozpoznané počítače do vlastniho **Unmanaged Computers** seznamu. Předem rozpoznané počítače nejsou smazány po novém dotazu pro síťové rozpoznání, takže musíte manuálně & vymazat počítače které nejsou nadále připojeny v síti.

Prvotní dotaz na seznam rozpoznaných (browse list) je přenesen pomocí prvního Bitdefender Endpoint Security Tools klienta nainstalovaného v síti.

- Pokud je nainstalovaná role relay na skupinovém počítači, pouze počítače z této skupiny budou viditelné v Control Center.
- Pokud je nainstalovaná role relay na doménovém počítači, pouze počítače z této domény budou viditelné v Control Center. Počítače z jiných domén mohou být rozpoznány, pokud existuje důvěrný vztah s doménou, kde je relay nainstalována.

Následné dotazy k síťovému rozpoznání jsou prováděny každou hodinu. Pro každý nový dotaz, Control Center rozděluje prostor spravovaných počítačů do viditelných oblastí a pak určí jednu konkrétní relay pro každou jednotlivou oblast aby pro ní následně prováděla pravidelné rozpoznávací úlohy. Viditelná oblast je skupinou počítačů které sami sebe rozpoznávají. Normálně je viditelná oblast definována pracovní skupinou nebo doménou, ale to závisí na topologii a konfiguraci sítě. V některých případech, viditelná oblast obsahuje vícero domén a pracovních skupin.

V případě že vybraná relay selže v provedení dotazu, Control Center počká na další naplánovaný dotaz, beztoho aniž by vybrala jinou relay pro další pokus.

Za účelem úplné viditelnosti celé sítě, relay role musí být nainstalovány minimálně na jednom počítači v každé doméně a v každé pracovní skupině. Ideálně, Bitdefender Endpoint Security Tools klient musí bet nainstalován minimálně na jednom počítači v každé jednotlivé podsíti.

## Více o Microsoft službě k rozpoznávání počitačů.

Stručné fakta o službě k rozpoznávání počitačů.

- Pracuje nezávisle na Active Directory.
- Běží exkluzivně přes IPv4 sítě and funguje nezávisle uvnitř hranic LAN skupin (pracovních skupin nebo domén). Seznam rozpoznaných (browse list) je vytvářen a udržován pro každou LAN skupinu.
- Typicky používá bezspojové serverové vysílání (broadcasty) ke komunikaci mezi koncovými body.
- Používá NetBIOS přes TCP/IP (NetBT).
- Potřebuje NetBIOS službu pro rozpoznání jmen (name resolution). Doporučuje se mít funkční Windows Internet Name Service (WINS) infrastruktůru v síti.
- Není zapnutá automaticky ve Windows Serverech 2008 a 2008 R2.

Pro podrobnější informace ohledně služby k rozpoznávání počitačů, si přečtěte článek Computer Browser Service Technical Reference na Microsoft Technetu.

## Podmínky pro síťové rozpoznávání

K úspěšnému rozpoznání všech počítačů (serverů a pracovních stanic) které budou spravovány z Control Center, následující podmínky musí být splněny:

- Počítače musí být součástí pracovni skupiny nebo domény a připojeny pomocí IPv4 v lokální síti. Služba k rozpoznání počítačů nefunguje přez IPv6 sítě.
- Několik počítačů v každé LAN skupině (pracovní skupině nebo doméně) musí mít zapnutou službu k rozpoznání počítačů (Computer Browser service). Primární doménový kontroler musí mít také spuštěnou službu (Computer Browser service).
- NetBIOS přez TCP/IP (NetBT) musí být zapnutý na počítačích. Lokální firewall musí mít povolený NetBT provoz.

- okud používáte relay Linux pro nalezení dalších koncových bodů s Linux nebo Mac, musíte na koncové body buď nainstalovat Samba, nebo je propojit v Active Directory a použít DHCP. Tímto na nich bude NetBIOS automaticky nastaven.
- Služba pro sdílení souborů musí být zapnuta na počítačích. Lokální firewall musí umožnit a povolit sdílení souborů.
- Windows Internet Name Service (WINS) infrastruktůra musí být nastavená a správně pracovat.
- Musí být povoleno zjišťování sítě ( **Ovládací panely > Centrum sítí a sdílení > Změnit pokročilé nastavení sdílení** ).

  Chcete-li tuto funkci povolit, musí být spuštěny následující služby:
  - DNS Client
  - Funkce Discovery Resource Publication
  - SSDP Discovery
  - UPnP Device Host
- V prostředích s vicero doménami se doporučuje nastavit důvěryhodný vztah mezi doménami, tak aby počítače mohly přistupovat k seznamům rozpoznaných počítačů (browse lists) z jiných domén.

Počítače z kterých se Bitdefender Endpoint Security Tools klient dotazuje služby k rozpoznání počítačů (Computer Browser service) musí být schopné zjistit NetBIOS jména.

**Poznámka**
Síťový rozpoznávácí mechanizmus funguje pro všechny operační systémy, včetně Windows Embedded verzí, pokud jsou splněny všechny potřebné podmínky.

## 5.4. Instalace EDR

Tento modul je standardně dodáván s instalační sadou Bitdefender Endpoint Security Tools a vyžaduje aktivaci senzoru incidentů, když poprvé zadáte licenční klíč.

Před instalací se ujistěte, že cílové koncové body splňují minimální požadavky . Minimální požadavky na incidenty odpovídají požadavkům bezpečnostního agenta.

Abyste chránili koncové body pomocí EDR, tak si můžete vybrat ze dvou možností:

- Nainstaluje bezpečnostní agenty s EDR Senzorem jakmile vložíte váš licenční klíč. Viz Aktivace vaší licence .

- Použijte úlohu **Rekonfigurovat (Reconfigure)**.

**Důležité**
The Incidents Sensor no longer provides support for Internet Explorer.

Další informace si přečtěte v GravityZone příručce Administrátora.

## 5.5. Instalace Sandbox Analyzer On-Premises

Aby proběhla instalace hladce, proveďte následující kroky:

1. Připravte se na Instalaci
2. Nasadit virtuální zařízení Sandbox Analyzer
3. Nasazení síťového zabezpečení virtuálních strojů

### 5.5.1. Připravte se na Instalaci

Před instalací Sandbox Analyzer On-Premises se ujistěte, že:

- Hypervisor VMware ESXi je nainstalován a nakonfigurován. Podrobnosti naleznete v dokumentaci vSphere Instalace a nastavení , část 2: „Instalace a nastavení ESXi“.
- Virtuální zařízení Bitdefender GravityZone je nasazeno a nakonfigurováno.

**Poznámka**
Pokud jde o hypervizora VMware ESXi, ujistěte se, že:

- ESXi version je 6.5 nebo novější.
- VMFS datastore verze je 5.
- SSH je povoleno v **zásadách spuštění** s konfigurací **Start and stop s hostitelem** .
- Služba NTP je aktivní a nakonfigurovaná.

Licenční klíč Sandbox Analyzer On-Premises řídí počet maximálních souběžných detonací. Protože každá detonace vyžaduje spuštěnou instanci virtuálního stroje, počet souběžných detonací se odráží v počtu vytvořených virtuálních strojů. Podrobnosti o přidávání licenčních klíčů v GravityZone Control Center viz „Zadávání Vašich Licenčních Klíčů“ (str. 121).

## 5.5.2. Nasadit virtuální zařízení Sandbox Analyzer

Nasazení virtuálního zařízení Sandbox Analyzer:

1. Přihlaste se do GravityZone Control Center.
2. Přejděte na záložku **Síť > Balíčky**.
3. Vyberte políčko z tabulky **Sandbox Analyzer** .
4. Klikněte na tlačítko **Stáhnout** v levé horní části stránky. Vyberte možnost **Security Appliance (ESXi standalone)** .
5. Pomocí nástroje pro správu virtualizace (například klienta vSphere) importujte stažený soubor OVA do Vašeho virtuálního prostředí.

   **Poznámka**
   Při nasazování souboru OVA nakonfigurujte sítě takto:

   - **Bitdefender Síť** - Toto je síť, kde jsou umístěny další komponenty Bitdefender (rozhraní `eth0` ). Sandbox Analyzer a zařízení GGravityZone musí být ve stejné síti a musí komunikovat prostřednictvím `eth0` .
   - **Soukromá detonační síť** - Sandbox Analyzer používá tuto síť pro interní komunikaci (rozhraní `eth1` ). Tato síť musí být izolována od ostatních segmentů sítě.
   - **Síť s přístupem na internet** - Sandbox Analyzer používá tuto síť k získání nejnovějších aktualizací (rozhraní `eth2` ). Rozhraní `eth2` by nemělo mít stejnou IP nebo síť jako `eth0` .

6. Nastartujte appliance.
7. Z nástroje pro správu virtualizace otevřete rozhraní konzoly virtuálního zařízení Sandbox Analyzer.
8. Po zobrazení výzvy k zadání pověření použijte `root` pro uživatelské jméno `sve` pro zadání hesla.
9. Otevřete konfigurační nabídku spuštěním následujícího příkazu:

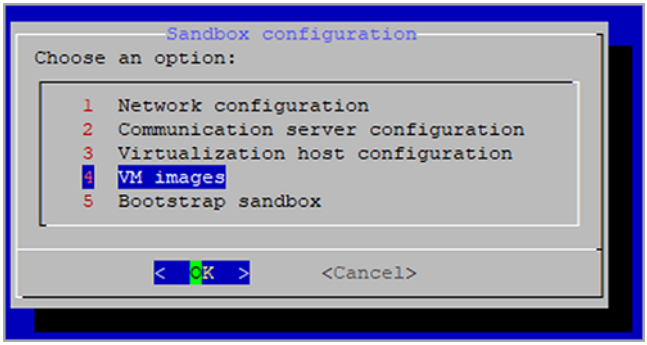
   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

10. V nabídce **Konfigurace karantény** proveďte následující nastavení:

a. **Konfigurace sítě** . Tuto možnost vyberte, chcete-li nakonfigurovat správu NIC. Sandbox Analyzer použije toto síťové rozhraní ke komunikaci s GravityZone.

   IP adresu lze zadat ručně nebo automaticky prostřednictvím DHCP.

   > **Poznámka**
   > Pokud je zařízení GravityZone v jiné síti než `eth0` , musíte do **konfigurace sítě přidat statickou routu. > BitDefender Network > routy** , aby Sandbox Analyzer správně fungoval.




Konzola analyzátoru karantény

b. **konfigurace internet proxy**. Aby instalace proběhla úspěšně, Sandbox Analyzer vyžaduje připojení k internetu. Pokud tomu tak je, můžete nakonfigurovat Sandbox Analyzer tak, aby používal proxy server zadáním těchto údajů:

   - **Host** - IP nebo FQDN proxy serveru. Použijte následující syntaxi: `http://<IP/Hostname>:<Port>`.
   - **Uživatel a heslo** - musíte zadat heslo dvakrát.
   - **Doména** - v případě domény Active Directory.

c. **Konfigurace komunikačního serveru** . Zadejte buď adresu IP nebo název hostitele zařízení, na kterém je spuštěna role komunikačního serveru.

   Použijte následující syntaxi: `http://<IP/Hostname>:<Port>`. Standartní port je `8443`.

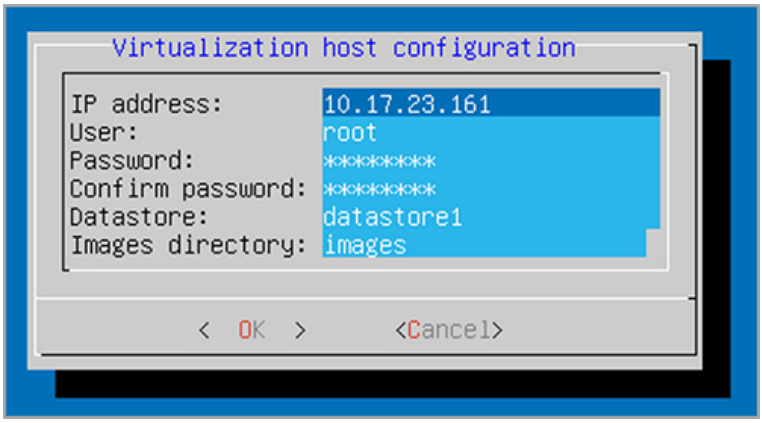
**Poznámka**
Jakmile je zadána adresa IP nebo název hostitele a konfigurace je uložena, bude instance Sandbox Analyzer viditelná v GravityZone Control Center, na stránce **Sandbox Analyzer > Infrastruktura** .

d. **Konfigurace virtualizovaného hostitele** . Sandbox Analyzer používá server ESXi k zajištění infrastruktury pro analýzu malwaru. Pomocí **Konfigurace virtualizovaného hostitele** připojíte zařízení Sandbox Analyzer k hostiteli ESXi poskytnutím následujících informací:

- The ESXi server IP asdresa
- Root přihlašovací údaje pro přístup k hostiteli ESXi.
- Datastore vyhrazeny pro Sandbox Analyzer.

  Zadejte název datového úložiště, jak je zobrazeno v ESXi.
- Název složky použité v datovém úložišti pro ukládání obrazů virtuálních strojů.

  Pokud tato složka neexistuje, musíte ji před uložením konfigurace Sandbox Analyzer vytvořit v datovém úložišti.




Konzole zařízení Sandbox Analyzer

e. **Obrazy VM**. Chcete-li vytvořit detonační virtuální stroje pro Sandbox Analyzer, musíte zkopírovat soubory VMDK obsahující požadované obrazy do složky

**Images** zadané v **Virtualized host configuration** . Pro každý obraz můžete v nabídce **obrazy VM** provést následující nastavení:

i. V nabídce **Konfigurace obrazu** zadejte název obrazu (jak bude zobrazen v GravityZone Control Center) a operační systém.

> **Poznámka**
> Složka obsahující obrazy VM se pravidelně prohledává a nové záznamy se hlásí do GravityZone. Tyto položky jsou viditelné v Control Center, na stránce **Sandbox Analyzer > Infrastructure > Image Management**.

V určitých situacích se při používání Sandbox Analyzer můžete setkat s problémy s detonačními virtuálními stroji. Chcete-li tyto problémy vyřešit, je třeba zakázat možnost anti-fingerprinting. Více informací naleznete na „Techniky Anti-fingerprinting “ (str. 162).

ii. V nabídce **DMZ hostitelé** můžete povolit názvy hostitelů, které služby a komponenty třetích stran zabudované ve virtuálních strojích vyžadují ke komunikaci se Správcem Sandbox. Podrobnosti viz „Hostitelé DMZ“ (str. 163)

iii. V nabídce **Vyčištění** můžete odstranit obrazy VM, které již nepotřebujete.

f. **Bootstrap sandbox**. Po přidání podrobností o konfiguraci Sandbox Analyzer pokračujte v instalaci výběrem této možnosti. Stav instalace se projeví v GravityZone Control Center, v **Sandbox Analyzer > na stránce Infrastruktura**

## Techniky Anti-fingerprinting

Ve výchozím nastavení bude během procesu vytváření obrazu analyzátor Sandbox umožňovat různé techniky anti-fingerprinting. Některé typy malwaru jsou schopny určit, zda se spouštějí v prostředí karantény, a pokud ano, nebudou aktivovat své škodlivé rutiny.

Účelem technik anti-fingerprinting je simulovat různé podmínky s cílem napodobit prostředí skutečného světa. V důsledku virtuálně eliminované kombinace implementovaného softwaru a konfigurace prostředí, kombinace, kterou nelze předvídat předem nebo kontrolovat, je možné, že určité techniky nebudou kompatibilní se softwarem nainstalovaným v golden image. Tyto vzácné situace poznáte podle následujících příznaků:

- Chyby během procesu vytváření obrazu.
- Chyby při pokusu o spuštění softwaru uvnitř obrazu.

- Chybové zprávy se vrátily při detonaci vzorků.
- Licencovaný software již nefunguje kvůli neplatným licenčním klíčům.

Rychlý lék na takové vzácné jevy spočívá v přestavbě obrazu s vypnutými technikami anti-fingerprinting. Udělejte to takto, postupujte podle níže uvedených kroků:

1. Přihlaste se do GravityZone Control Center a odstraňte image.
2. Přihlaste se k zařízení Sandbox Analyzer a spusťte konzolu zařízení Sandbox Analyzer spuštěním následujícího příkazu:

   ```
   /opt/bitdefender/bin/sandbox-setup
   ```

3. Jděte do **obrazy VM > Konfigurace obrazu**.
4. Vyberte obraz, který způsobuje problémy.
5. Přejděte na možnost **Anti-fingerprinting** .
6. Zrušte zaškrtnutí příslušného políčka, abyste zakázali techniky anti-fingerprinting.

### Hostitelé DMZ

Během procesu vytváření obrazu bude vytvořena virtuální infrastruktura, která usnadní komunikaci mezi správcem Sandbox a virtuálními stroji. Z hlediska sítě se to promítne do izolovaného síťového prostředí, které bude obsahovat veškerou potenciální komunikaci, kterou může detonovaný vzorek vytvořit.

Menu serverů DMZ umožňuje povolit názvy hostitelů, se kterými musí služby a komponenty třetích stran zabudované ve virtuálních strojích komunikovat, aby správně fungovaly.

Příkladem této situace by byly licenční servery KMS používané licencováním systému Windows, pokud se na dodávané virtuální počítače použije hromadná licence.

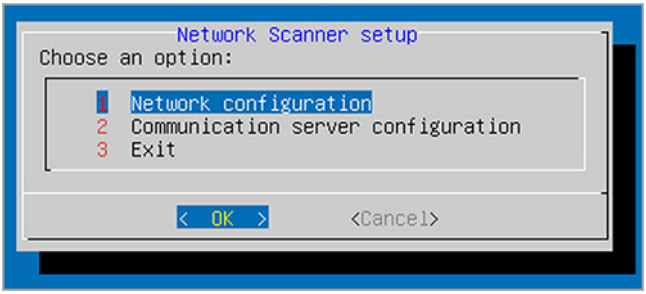
## 5.5.3. Nasazení síťového zabezpečení virtuálních strojů

Tato část popisuje, jak nasadit Network Security Virtual Appliance, Sandbox Analyzer, komponentu která zachycuje síťový provoz a odesílá podezřelé vzorky k analýze chování.

Nasazení Network Security Virtual Appliance:

1. Přihlaste se do GravityZone Control Center.
2. Přejděte na záložku **Síť > Balíčky**.
3. Zaškrtněte políčko tabulce **Network Security Virtual Appliance** .
4. Klikněte na tlačítko **Stáhnout** v levé horní části stránky a vyberte možnost **(VMware OVA)** .
5. Pomocí nástroje pro správu virtualizace (například klienta vSphere) importujte stažený soubor OVA do Vašeho virtuálního prostředí.
6. V průvodci nasazením vyberte kartu síťového rozhraní (NIC) použitou pro komunikaci s GravityZone a NIC použitou pro zachycení provozu.
7. Nastartujte appliance.
8. Z virtualizačního nástroje pro správu vašeho prostředí se připojte do konzole GravityZone SVE SVA Network Security Virtual Appliance.
9. Po zobrazení výzvy k zadání pověření použijte `root` pro uživatelské jméno `sve` pro zadání hesla.
10. Otevřete konfigurační nabídku spuštěním následujícího příkazu:

```
/opt/bitdefender/bin/nsva-setup
```




Konzole pro síťové zabezpečení

11. Přejděte do nastavení **Konfigurace komunikačního serveru** .
12. Zadejte IP adresu nebo název hostitele a port komunikačního serveru GravityZone.

Použijte následující syntaxi: `http://<IP/Hostname>:<Port>`. Standartní port je `8443`.

13. Uložte konfiguraci.

### Konfigurace síťového senzoru k detonaci souborů pcap

Síťový senzor může extrahovat obsah ze souborů zachycených na síti (pcap) a automaticky jej odeslat k detonaci do instance Sandbox Analyzer.

K detonaci obsahu ze souborů pcap:

1. Přihlaste se do virtuálního zařízení Network Security.
2. Po zobrazení výzvy k zadání pověření použijte `root` pro uživatelské jméno `sve` pro zadání hesla.
3. Spusťte následující příkaz:

```
/opt/bitdefender/bin/scan-pcap <local pcap path>
```

Ve výše uvedeném příkazu `<místní cesta pcap>` představuje místo, kam se soubor pcap nahraje do virtuálního zařízení zabezpečení sítě.

Další podrobnosti o používání síťového senzoru naleznete v kapitole **Zásady > Sandbox Analyzer** z Příručky správce GravityZone.

## 5.6. Instalace šifrování celých disků (Full Disk Encryption)

GravityZone Full Disk Encryption přichází jako služba, která vyžaduje aktivaci na základě licenčního klíče. Pro provedení tohoto, musíte přejít do **Konfigurace > Licence** a zadat licenční klíč.

Pro další podrobné informace ohledně licenčních klíáčů, si přečtěte „Správa Licencí“ (str. 120).

Bitdefender bezpešnostní agenti podporující šifrování celých disků (Full Disk Encryption) počínaje verzemi 6.2.22.916 na Windows a 4.0.0173876 na MacOS. K tomu abyste zjistili zda jsou agenti zcela kompatibilní s tímto modulem , máte následující dvě možnosti:

- Nainstalovat bezpečnostní agenty spolu s obsaženým šifrovacím modulem.
- Použijte **Reconfigure** úlohu.

Pro podrobnou infomaci jak se používá šifrování celých disků (Full Disk Encryption) ve Vaší síti, si přečtěte **Security Policies > Encryption** kapitolu v GravityZone Příručce Administrátora.

## 5.7. Instalace Ochrany Exchange (Exchange Protection)

Security for Exchange v sobě nese automaticky integraci pro Exchange Servery, v závislosti podle role serveru. Pouze kompatibilní funkce jsou nainstalovány pro každou roli, jak je popsáno níže:

| Funkce | Microsoft Exchange 2019/2016/2013 | | Microsoft Exchange 2010/2007 | | |
|---|---|---|---|---|---|
| | Edge | Mailbox | Edge | Hub | Mailbox |
| **Úroveň přepravy** | | | | | |
| Filtrování Antimalware | x | x | x | x | |
| Filtrování Antispam | x | x | x | x | |
| Filtrování obsahu | x | x | x | x | |
| Filtrování příloh | x | x | x | x | |
| **Exchange Store** | | | | | |
| Skenování antimalware na vyžádání (On-demand) | | x | | | x |

### 5.7.1. Příprava na Instalaci

Než nainstalujete Security for Exchange, ujistěte se jestli jsou všechny požadavky splněny, jinak se Bitdefender Endpoint Security Tools klient může nainstalovat bez modulu pro ochranu Exchange (Exchange Protection module).

Aby mohl modul pro ochranu Exchange (Exchange Protection module) běžet hladce a abyste zamezili konfliktům a nechtěným výsledkům, odstraňte jakékoliv agenty pro antimalware a emailovou filtraci.

Bitdefender Endpoint Security Tools klient automaticky rozpozná a odstraní většinu antimalware produktů a vypne antimalware agenta zabudovaného v Exchange Serveru od verze 2013. Kompletní seznam rozpoznaných bezpečnostních software a další informace nalezntete, v tomto KB článku.

Můžete manuálně kdykoliv znovu zapnout zabudovaného Exchange antimalware agenta, ovšem tento postup není doporučen.

### 5.7.2. Instalace ochrany na Exchange Serverech

K ochraně Exchange Serverů mmusíte nainstalovat Bitdefender Endpoint Security Tools klienta s rolí Ochrana pro Exchange (Exchange Protection role) na každém z nich.

Máte několik možností jak nasadit Bitdefender Endpoint Security Tools klienta na Exchange Serverech:

- Lokální instalace, skrze stáhnutí a spuštění instalačního balíčku na serveru.
- Vzdálená instalace, pomocí spuštění **Install** úlohy.
- Vzdáleně, spuštěním **Rekonfigurace Klienta** úlohy, pokud Bitdefender Endpoint Security Tools klient již nabízí ochranu na daném serveru.

Za účelem detailních instalačních kroků čtěte „Instalace Bezpečnostních Agentů“ (str. 133).

## 5.8. Instalace HVI

**Poznámka**
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

Abyste mohli používat HVI na virtuálních strojích z vašich Xen hostů, tak musíte provést následující kroky:

1. Zkontrolujte si předem požadavky pro instalaci
2. Instalovat Security Server
3. Instalovat Doplňkový balíček HVI

### Podmínky

- XenServer je integrován s GravityZone.
- XenCenter musí být nainstalovaný na vašem stroji.

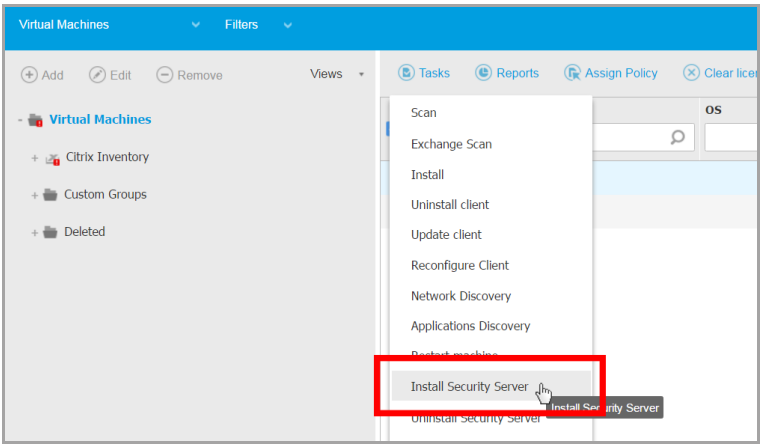
# Instalace Security Server

Pro instalaci Security Serveru na jednom nebo vícero hostech:

1. Jděte do záložky **Síť**.
2. Vyberte **Virtuální stroje** z možnosti zobrazení.
3. Prohlédněte si Citrix inventář a označte si v označovacích rámečcích adekvátní požadované hosty. Pro rychlý výběr, můžete vybrat přímo kořenový (root) kontejner v(Citrix Inventáři). Budete moci zvolit hostitele jednotlivě z instalačního průvodce.

   **Poznámka**
   Nemůžete vybírat hostitele z různých složek.

4. Klikněte na tlačítko **Úlohy** v horní části tabulky a z menu vyberte **Aktualizovat Security Server**. Zobrazí se okno **Instalace Security Server**.




Instalace Security Server

5. Vyberte hostitele, na které chcete instalovat Security Servery.
6. Vyberte konfigurační nastavení, která chcete použít.

**Důležité**
Používání obecných nastavení při zavádění několika Security Serverů současně vyžaduje od hostitelů, aby sdíleli tu samou paměť, měli IP adresy přiřazené DHCP serverem, a byli součástí té samé sítě.

Pokud si vyberete konfiguraci každého Security Serveru jinak, tak budete mít možnost si vydefinovat nastavení, která chcete pro každého hosta zvlášť v dalším následném kroku pomocníka instalace. Kroky popsané níže aplikujte v případě když použijete volbu **Konfigurovat každý (Configure each) Security Server**.

7. Klikněte **Další**.

**Poznámka**
V závislosti na vašem předešlém výběru, některé volby zde popsané nemusí být aplikovatelné pro vaši situaci.

8. Zadejte definující jméno pro Security Server.
9. Vyberte si kontejner ve kterém chcete zahrnout Security Server z menu **Kontejner (Container)**.
10. Vyberte cílovou paměť.
11. Vyberte typ zásobování disku. Doporučujeme používat zásobování tlustého disku.

**Důležité**
Pokud použijete zásobování tenkého disku a místo na disku v datovém úložišti dojde, Security Server zamrzne a hostitel tím pádem zůstane nechráněný.

12. Nastavte paměť a přidělování zdrojů pevnému disku na základě poměru konsolidace na hostiteli. Zvolte **Nízké**, **Střední** nebo **Vysoké** pro načtení doporučeného nastavení přidělování zdrojů, nebo **Ručně** pro nastavení přidělování zdrojů ručně.
13. Nastavte časovou zónu zařízení.
14. Nastavte administrativní heslo pro konzoli Security Serveru. Nastavení hesla pro správu přepíše výchozí kořenové heslo ("sve").
15. Vyberte typ síťové konfigurace pro síť Bitdefender. IP adresa Security Server se nesmí změnit, protože ji agenti Linux používají ke komunikaci.

Pokud zvolíte DHCP, ujistěte se, že jste nastavili DHCP server tak, aby rezervoval IP adresu zařízení.

Pokud vyberete statický, musíte zadat IP adresu, masku podsítě, bránu a informace o DNS.

16. Klikněte na tlačítko **Save**.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

## Instalovat Doplňkový balíček HVI

1. Přejděte na stránku **Konfigurace > Aktualizace**.
2. Vyberte Doplňkový balíček HVI ze seznamu **Komponentů** a klikněte na tlačítko **Stáhnout** v horní části tabulky.
3. Přejděte na stránku **Síť** a v nastavení zobrazení vyberte **Virtuální zařízení**.
4. Z menu **Zobrazení** v levém panelu vyberte **Server**.
5. Vyberte jednoho nebo více hostitelů Xen ze síťového inventáře. Dostupné hostostitele můžete snadno prohlížet zvolením možnosti **Druh (Type) > Hostitelé (Hosts)** v nabídce **Filtry (Filters)**.
6. Klikněte na tlačítko **Úlohy** na pravé liště a vyberte **Instalovat Doplňkový balíček HVI**. Otevře se instalační okno.
7. Naplánujte, kdy má být instalační úloha spuštěna. Můžete si zvolit, zda chcete spustit úlohu okamžitě po jejím uložení, nebo v konkrétním čase. V případě, že instalaci nelze dokončit v určený čas, úloha bude automaticky opakována podle nastavených parametrů pro opakování. Například, pokud vyberete více hostitelů a jeden hostitel je v době, kdy má instalace balíčku proběhnout nedostupný, úloha se spustí znovu v určeném čase.
8. Hostitel musí být restartován pro aplikování změn a dokončení instalace. Pokud chcete, aby se hostitel sám restartoval, zvolte **Restartovat automaticky hostitele (Automatically reboot host)**.
9. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

## 5.9. Instalace Ochrany Storage (Storage Protection)

Security for Storage je Bitdefender (NAS) a systémy pro sdílení souborů, které jsou kompatibilní s protokolem Internet Content Adaptation Protocol (ICAP). Podporované systémy pro sdílení souborů viz „Ochrana Úložiště“ (str. 55).

Chcete-li použít Security for Storage s řešením GravityZone:

1. Nainstalujte a nakonfigurujte alespoň dva Security Server ve vašem prostředí, aby fungovaly jako servery ICAP. Bitdefender Security Server analyzuje soubory, posílá verdikty do systémů úložišť a v případě potřeby provede příslušné kroky. V případě přetížení přesměruje první Security Server přebytek dat na druhý.

   **Poznámka**
   Dle osvědčených postupů nainstalujte vyhrazené Security Server pro ochranu úložiště, odděleně od Security Server použitého pro jiné role, jako je antimalwarové skenování.

   Podrobnosti o postupu instalace Security Server naleznete v této příručce v kapitole **Instalace Security Server**.

2. Konfigurace modulu **Ochrana úložiště (Storage Protection)** z nastavení politik služby GravityZone.

   Podrobnosti naleznete v kapitole **Bezpečnostní politiky >Politiky pro počítače a virtuální počítače > Ochrana úložiště(Storage Protection)** v příručce administrátora GravityZone.

Podrobnosti o konfiguraci a správě serverů ICAP v určitém zařízení NAS nebo v systému sdílení souborů naleznete v dokumentaci k této konkrétní platformě.

## 5.10. Instalace ochrany mobilních zařízení (Mobile Devices Protection)

Security for Mobile je řešení pro správu mobilních zařízení (mobile device management) vytvořené pro iPhone, iPad a Android zařízení. Pro kompletní seznam podporovaných verzí operačních systémů, zkontrolujte systémové požadavky (system requirements).

Pro správu Security for Mobile z Control Center, musíte přidat mobilní zařízení do Active Directory nebo do vlastních uživatelů, a pak nainstalovat GravityZone Mobile Client aplikaci na zařízeních. Poté co nastavíte službu, tak si můžete spustit administrativní úlohy na mobilních zařízeních.

Než začnete, tak se ujistěte, že jste správně nastavili Nastavení veřejné (externí) IP adresy pro komunikační server.

Pro instalaci Security for Mobile:

1. Pokud nemáte integraci s Active Directory, tak musíte vytvořit uživatele pro vlastníky mobilních zařízení.
2. Přidejte zařízení k uživatelům.
3. Nainstalujte GravityZone Mobile Client na zařízeních a aktivujte je.

### 5.10.1. Nakonfigurujte si externí adresu pro kommunikační server

Ve standartním nastavení GravityZone, mobilní zařízení mohou být spravována pouze pokud jsou přímo připojená do firemní sítě (pomocí Wi-Fi nebo VPN). Tohle se stává, když začnete spravovat nové mobilní zařízení, která jsou standartně nakonfigurována na lokální adresu komunikačního serveru appliance.

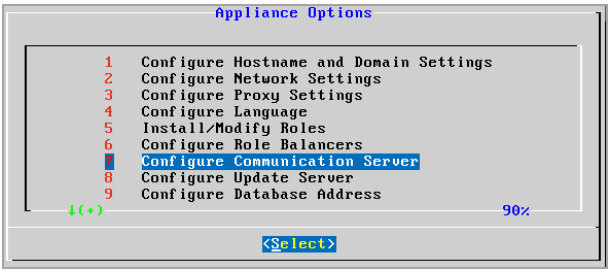
Aby bylo možné spravovat mobilní zařízení přes internet , nezávisle na tom kde kde se nacházejí, musíte nakonfigurovat komunikační server s veřejně dostupnou adresou.

Aby bylo možné spravovat mobilní zařízení, když nejsou připojena na firemní síť, je potřeba mít k dispozici následující možnosti:

- Nastavte port forwarding na firemní bráně pro applianci na kteréběží role kommunikačního serveru.
- Přidejte další síťový adaptér do appliance na které běží role kommunikačního serveru a přiřaďte jí veřejnou IP adresu.

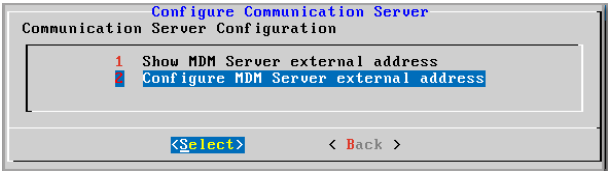
V obou případech musíte nakonfigurovat Communikační server s externí adresou za účelem správy mobilních zařízení:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).
2. Z hlavního menu, vybete **Konfigurace Komunikačního Serveru (Configure Communication Server)**.




Volby okna aplikací (Application Options window)

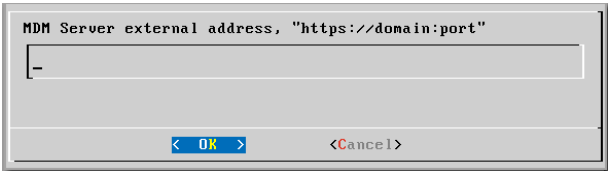
3. Vyberte **Konfigurace externí adresy MDM Serveru**.




Nakonfigurujte okno kommunikačního Serveru

4. Zadejte externí adresu.

   Použijte následující syntaxi: `https://<IP/Domain>:<Port>`.




Zadávací okno pro externí adresu MDM Serveru

- Pokud použijete port forwarding, tak musíte zadat veřejnou IP adresu nebo doménové jméno a pak port otevřený na bráně.
- Pokud použijete veřejnou adresu komunikačního serveru, tak musíte zadat veřejnou adresu nebo doménové jméno a port komunikačního serveru. Standartní port je `8443`.

5. Vyberte **OK** pro uložení změn.

## 5.10.2. Vytvářejte a organizujte vlastní uživatele

V situacích nesouvisejících s Active Directory musíte nejprve vytvořit vlastní uživatele, abyste získali prostředek pro identifikaci uživatelů mobilních zařízení. Specifikovaní uživatelé mobilních zařízení nejsu nijak provázáni s Active Directory nebo s jinými uživateli definovanými v Control Center.

### Přidávání vlastních uživatelů

Pro vytvoření vlastního uživatele:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. V okně na levé straně vyberte **Vlastní skupiny**.
4. Klikněte na **Přidat uživatele (Add User)** ikonu v nástrojové liště akcí. Zobrazí se konfigurační okno.
5. Určete požadované podrobnosti o uživateli:
   - Definující jméno (například celé jméno uživatele)
   - Emailová adresa uživatele

   **Důležité**
   - Ujistěte se, že zadáváte platnou emailovou adresu. Když přidáte zařízení, uživateli bude odeslán email s instrukcemi pro instalaci.
   - Každá emailová adresa může být registrována pouze pro jednoho uživatele.

6. Klikněte **OK**.

### Přidávání vlastních uživatelů

Pro organizování vlastních uživatelů:

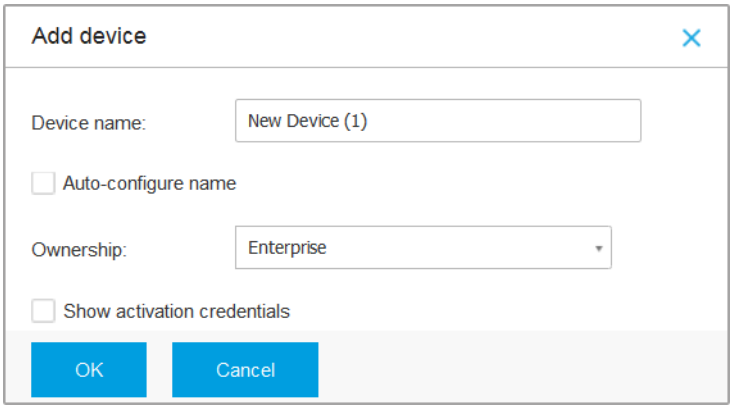
1. Vytvořte vlasní skupiny.
   a. Vyberte **Vlastní skupiny (Custom Groups)** v levém postraním panelu a klikněte na ikonu **Přidat (Add)** v nástrojové liště akcí (nad panelem).
   b. Zadejte působivé jméno pro skupinu a klikněte na **OK**. Nová skupina je zobrazena pod **Vlastními skupinami**.

2. Přesuňte uživatele do vhodných vlastních skupin.
   a. Vyberte uživatele v pravém postranním panelu.
   b. Přetáhněte a odložte váš výběr nad žádanou skupinou na levé straně panelu.

## 5.10.3. Přidejte zařízení k uživatelům

Pro přidání zařízení uživateli:

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Vyhledejte si užvatele v Active Directory složkách nebo ve vlastních skupinách.
4. Klikněte na the ⊕ **Přidat zařízení (Add Device)** ikonu na vrchní straně síťové tabulky. Zobrazí se konfigurační okno.




Přidat mobilní zařízení k uživateli

5. Zadejte pro zařízení definující jméno.
6. Pokud chcete, aby byl název zařízení generován automaticky, použijte volbu **Automatické nastavení jména**. Poté, co je přidáno, má zařízení obecné jméno. Jakmile je zařízení aktivováno, je automaticky přejmenováno podle odpovídajícího výrobce a informace o modelu.
7. Vyberte si druh vlastnictví zařízení buď firemní (Enterprise) nebo osobní (Personal).

8. Vyberte si volbu **Ukázat aktivační přístupové údaje (Show activation credentials)** poté klikněte na tlačítko **OK** když se chystáte nainstalovat GravityZone Mobile Client na uživatelském rozhraní.
9. Klikněte **OK**. Uživateli je okamžitě odeslán email s instrukcemi pro instalaci a podrobnosti pro aktivaci, které je potřeba nastavit na zařízení. Podrobnosti aktivace zahrnují aktivační token a adresu komunikačního serveru (a odpovídající QR kód).

**Poznámka**

- Můžete vidět detailní informace zařízení kdykoliv kliknete na jméno v Control Center.
- Můžete také přidat mobilní zařízení k výběru uživatelů a skupin. V tomto případě, vám konfigurační okno umožní pouze definování vlastníka zařízení. Mobilní zařízení vytvořená pomocí několikanásobného výběru obdrží automaticky generovaná obecná jména. Jakmile je zařízení spravováno, jeho jméno se automaticky změní, včetně názvu výrobce a popisu modelu.

## 5.10.4. Nainstalujte GravityZone Mobile Client na zařízeních

GravityZone Mobile Client aplikace je exklusivně distribuována skrze Apple App Store a Google Play.

Pro instalaci GravityZone Mobile Client na zařízení:

1. Hledejte v aplikacích na oficiálním app storu.
   - Google Play link
   - Apple App Store link
2. Stáhněte si a nainstalujte si aplikaci na zařízení.
3. Spusťte aplikaci a vytvořte požadovanou konfiguraci:
   a. Na Android zařízeních, klikněte na **Aktivovat (Activate)** pro zapnutí povolení pro GravityZone Mobile Client jako administrátor zařízení. Přečtěte si pozorně poskytnutou informaci.

**Poznámka**

- Úloha Uzamknout pro zařízení Android (7.0 a novější) prosadí heslo nastavené ve vaší konzoli GravityZone pouze v případě, že na zařízená není nastavena žádná ochrana pomocí zámku. V opačném případě budou

jako ochrana zařízení použita současná nastavení zámku obrazovky, jako je vzor, PIN, heslo, otisk prstu nebo Smart Lock.

- Úloha Odemknout je již nedostupná pro zařízení s Android (7.0 a novější).
- Z důvodu technických omezení nejsou úlohy uzamčení a vymazání v systému Android 11 k dispozici.

b. Vložte aktivační token a communikační adresu serveru nebo, alternativně, sken QR kód poslaný emailem.

c. Klikněte na **Důvěřovat (Trust)** když budete vyzváni pro akceptaci certifikátu komunikačního serveru. Touto cestou, GravityZone Mobile Client validuje komunikační server (Communication Server) a bude pak akceptovat oznámení pouze od něj, zabraňuje takto preventivně principiálně útokům skrze prostředníka.

d. Klikněte na **Aktivovat (Activate)**.

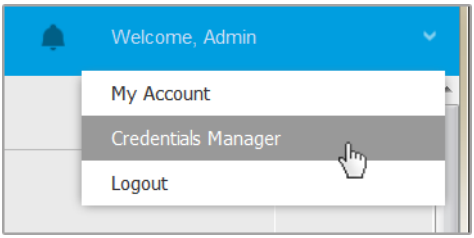
e. Na iOS zařízeních, jste vyzváni k instalaci MDM profilu. Pokud je vaše heslo chráněné, budete tázáni abyste ho poskytli. Také musíte povolit GravityZone zpřístupnit nastavení vašich zařízení, jinak se instalační proces vrací zpět k předešlému kroku. Následujte instrukce na obrazovce pro dokončení profilové instalace.

**Poznámka**
Uživatelé musí povolit umístění na pozadí zařízení, nejen při používání aplikace, aby funkce Locate fungovala správně.

## 5.11. Správce přihlašovacích údajů

Správce pověření vám pomáhá definovat pověření nezbytná pro přístup k dostupným inventářům vCenter Server a také pro autentizaci na dálku na různých operačních systémech ve vaší síti.

Pro otevření Správce pověření klikněte na své uživatelské jméno v pravém horním rohu stránky a zvolte **Správce pověření**.




Nabídka Správce pověření

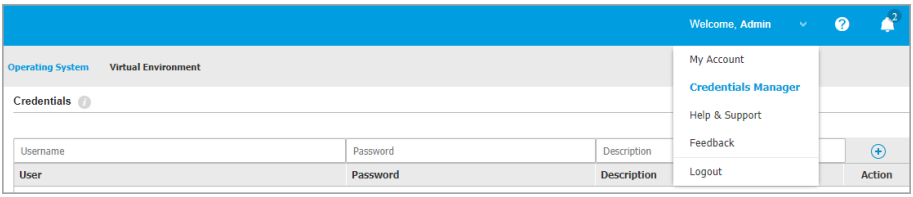
Okno **Správce pověření** obsahuje dvě karty:

- Operační systém
- Virtuální prostředí

## 5.11.1. Operační systém

Z karty **Operační systém** můžete spravovat administrátorská pověření potřebná pro vzdálenou autentizaci během instalačních úloh, poslaných na počítače a virtuální stroje ve vaší síti.

Pro přidání sady pověření:




Správce přihlašovacích údajů

1. Zadejte uživatelské jméno a heslo administrátorského účtu pro každý cílový operační systém do příslušných polí v horní části záhlaví tabulky. Můžete také přidat popis, který vám usnadní identifikaci jednotlivých účtů. Pokud jsou počítače v doméně, stačí zadat pověření administrátora domény.

   Při zadávání jména uživatelského účtu použijte konvence systému Windows:

- Pro stroje s Active Directory použijte tyto syntaxe: `username@domain.com` a `domain\username`. Abyste si mohli být jisti, že pověření budou fungovat, zadejte je v obou tvarech (`username@domain.com` a `domain\username`).
- Pro stroje Pracovní skupiny stačí zadat pouze uživatelské jméno bez jména pracovní skupiny.

2. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky. Nová sada pověření je přidána do tabulky.

> **Poznámka**
> Pokud jste neurčili autentifikační pověření, budete je muset zadat při spouštění instalační úlohy. Zadaná pověření jsou automaticky uložena do vašeho Správce pověření, takže je příště už nemusíte zadávat.

## 5.11.2. Virtuální prostředí

Z karty Virtuální prostředí můžete spravovat autentizační pověření pro dostupné systémy virtualizovaných serverů.

Pro přístup do virtualizované infrastruktůry integrované s Control Center, si musíte pro každý dostupný virtualizační serverový systém vytvořit uživatelské přístupové údaje. Control Center používá vaše přihlašovací údaje pro připojení se k virtualizované infrastruktuře, a zobrazuje pouze zdroje, ke kterým máte přístup (jak je definováno ve virtualizačním serveru).

Pro určení pověření nutných pro připojení se k virtualizovanému serveru:

1. Vyberte server z příslušné nabídky.

> **Poznámka**
> Pokud nabídka není k dispozici, tak buď ještě nebyla nastavena žádná integrace, nebo již byla nastavena všechna potřebná pověření.

2. Zadejte své uživatelské jméno a heslo a definující popis.
3. Klikněte na tlačítko ⊕ **Přidat**. Nová sada pověření je přidána do tabulky.

> **Poznámka**
> Pokud nenastavíte vaše autentizační pověření ve Správci pověření, budete je muset zadat ve chvíli, kdy se pokusíte prohlížet inventář jakéhokoli systému

virtualizovaných serverů. Jakmile zadáte svá pověření, uloží se do Správce pověření a příště je už zadávat nemusíte.

**Důležité**
Kdykoli změníte uživatelské heslo pro váš virtualizovaný serverový systém, nezapomeňte ho aktualizovat také ve Správci pověření.

## 5.11.3. Odstranění pověření ze Správce pověření

Pro odstranění starých pověření ze Správce pověření:

1. Ukažte na řádek v tabulce obsahující pověření, která chcete odstranit.
2. Klikněte na tlačítko ⊗ **Odstranit** na pravé straně odpovídajícího řádku tabulky. Zvolený účet bude odstraněn.

# 6. AKTUALIZUJE SE GRAVITYZONE

Bitdefender zveřejňuje všechny aktualizace obsahu produktů a zabezpečení prostřednictvím serverů Bitdefender na internetu. Všechny aktualizace jsou šifrované a digitálně podepsané, aby s nimi nemohlo být manipulováno.

GravityZone obsahuje roli aktualizačního serveru (Update Server roli), navrženou tak aby bylo možné distribuovat centrálně z jednoho bodu všechny aktualizace do vašeho GravityZone prostředí. Aktualizační server (Update Server) funguje jako prostředník, který zjišťuje zda se nacházejí nějaké aktualizace GravityZone na Bitdefender aktualizačních serverech dostupných na internetu a následně je stáhne k sobě a dává k dosppozici pro vaší lokální síť. GravityZone komponenty se mohou nakonfigurovat tak aby se automaticky aktualizovaly z lokálního aktualizačního serveru (update serveru) místo z internetu.

Jakmile je nová aktualizace k dispozici, tak GravityZone appliance, bezpečnostní BEST agent a nebo Security Server ověřuje digitální podpis aktualizace za účelem ověření její důvěryhodnosti a za účelem kontroly integrity obsahu aktualizačního balíčku. Poté je každý soubor aktualizace rozebrán a jeho verze je porovnána s nainstalovanou verzí. Novější soubory jsou staženy lokálně a porovnány s jejich MD5 hashem pro zajištění, že nejsou měněny.

Jakmile neprojde balíček ověřením, tak se aktualizační proces zastaví a vrátí se zpátky s chybovým hlášením. Jinak se nahlíží na aktualizaci jako na platnou a připravenou k instalaci.

Pro aktualizaci GravityZone appliancí nainstalovaných ve vašem prostředí a instalačních balíčků GravityZone komponentů, se přihlašte pod firemním administrátosrským účtem a přejděte na **Konfigurace (Configuration) > Aktualizace (Update)** stránku.

## 6.1. Aktualizace GravityZone Appliancí

Prostřednictvím aktualizací appliancí GravityZone , vydává Bitdefender nové funkce a vylepšení stávajících. Ty jsou viditelné v Control Center.

Před spuštěním aktualizace se doporučuje zkontrolovat následující:

- Aktualizační stav
- Jakékoli informace nebo varovné zprávy, které se mohou objevit.
- Log změn

Kontrolovat stav aktualizace:

1. Přejděte na stránku **Konfigurace > Aktualizace > rolí GravityZone**.
2. V sekci **Aktuální stav** se podívejte na zprávu, která ukazuje celkový stav nasazení. V případě, žeGravityZone potřebuje aktualizovat, bude k dispozici tlačítko **Update**
3. V sekci **Infrastruktura** zkontrolujte podrobnosti o každé roli GravityZone nasazené ve vaší síti. Protože role se aktualizují nezávisle, můžete pro každou roli zobrazit: název appliance, které je hostitelem, jeho IP adresu, aktuální verzi, nejnovější verzi a stav aktualizace.

Chcete-li zkontrolovat changelog:

1. Přejděte na stránku **Konfigurace > Aktualizace > rolí GravityZone**.
2. Klikněte na odkaz **Zobrazit seznam změn** . Vyskakovací okno zobrazuje seznam se všemi verzemi a změnami.

   Informace k novému vydání každého produktu jsou také publikovány na stránkách Bitdefender technické podpory (Support Center).

GravityZone můžete aktualizovat dvěma způsoby:

- Ručně
- Automaticky

### 6.1.1. Ruční aktualizace

Tuto metodu vyberte, chcete-li mít úplnou kontrolu, kdy se má aktualizace spustit.

Manuální aktualizace GravityZone:

1. Přejděte na stránku **Konfigurace > Aktualizace > rolí GravityZone**.
2. Klikněte na tlačítko **Aktualizovat** (je-li k dispozici).

   Aktualizace může chvíli trvat. Počkejte, dokud nebude dokončena.
3. Vymažte mezipaměť (cache) vašeho prohlížeče.

Během aktualizace Control Center odhlásí všechny uživatele a informuje je o probíhající aktualizaci. Budete mít možnost zobrazit podrobný průběh procesu aktualizace.

Po dokončení aktualizace se na stránce Control Center zobrazí přihlašovací stránka.

## 6.1.2. Automatická aktualizace

Automatickou instalací aktualizací jste si jisti, že GravityZone je vždy aktualizována nejnovějšími funkcemi a opravami zabezpečení.

GravityZone má dva typy automatických aktualizací:

- Aktualizace produktu
- Aktualizace softwaru třetích stran

### Aktualizace produktu

Tyto aktualizace přinášejí nové funkce v GravityZone a řeší problémy vyplývající z těchto funkcí.

Protože aktualizace jsou pro uživatele GravityZone rušivé, jsou navrženy tak, aby fungovaly na základě určeného plánu. Aktualizaci můžete naplánovat na vhodné hodiny. Ve výchozím nastavení jsou automatické aktualizace produktů zakázány.

Povolení a naplánování aktualizací produktů:

1. Přejděte na stránku **Konfigurace > Aktualizace > rolí GravityZone**
2. Zaškrtněte políčko **Povolit automatické aktualizace produktu GravityZone**.
3. Nastavte **Opakování (Recurrence)** na **Denně (Daily)**, **Týdně (Weekly)** (vyverte jeden nebo více dnů v týdnu) nebo **Měsíčně (Monthly)**.
4. Nastavte **Interval**. Můžete nastavit čas pro spuštění aktualizačního procesu na ihned jakmile se objeví nová verze.

GravityZone standardně zobrazuje varovnou zprávu všem uživatelům Control Center 30 minut před spuštěním automatické aktualizace. Chcete-li varování vypnout, zrušte zaškrtnutí políčka **Povolit před aktualizací upozornění na 30 minutové výpadky**.

### Aktualizace softwaru třetích stran

GravityZone virtuální appliance vloží řadu softwarových produktů poskytovaných jinými dodavateli. Cílem tohoto typu aktualizací je co nejrychleji patchovat takový software a snížit možná bezpečnostní rizika.

Tyto aktualizace běží bez nutnosti obsluhy a nepřerušují práci s Control Center.

Ve výchozím nastavení je tato možnost povolena. Chcete-li tuto možnost zakázat:

1. Přejděte na stránku **Konfigurace > Aktualizace > rolí GravityZone**

2. Zrušte zaškrtnutí políčka **Povolit automatické aktualizace zabezpečení pro komponenty třetích stran GravityZone**.

   Softwarové opravy(patche) třetích stran pak budou vydány s jednou z aktualizací produktu GravityZone.

## 6.2. Konfigurace aktualizačního (update) serveru

Standartně si stahuje aktualizační server (Update Server) aktualizace přímo z Internetu každou hodinu. Doporučuje se neměnit standartní nastavení aktualizačního serveru.

Pro zobrazejí a konfiguraci nastavení aktualizačního serveru (Update Server settings):

1. Přejděte na stránku **Aktualizace (Update)** v Control Center a klikněte na štítek **Komponenty (Components)**.
2. Klikněte na tlačítko **Nastavení (Settings)** nacházející se na horní levé polovině obrazovky pro zobrazení okna **Nastavení aktualizačního serveru (Update Server Settings)**.
3. Pod **Konfigurace aktualizačního serveru (Update Server Configuration)**, si můžete ověřit a nakonfigurovat hlavní nastavení.
   - **Adresy Balíčků.** Adresu od kud se budou balíčky ztahovat.
   - **Aktualizovat Adresu.** Aktuzalizační server (Update Server) je nastavený tak aby si ztahoval aktualizace z `upgrade.bitdefender.com:80`. Jedná se o standartní adresu která je automaticky překládána tak aby ukazovala na nejbližší server, který má uloženy Bitdefender aktualizace pro vaší oblast.
   - **Port.** Při konfiguraci GravityZone komponentů tak aby se aktualizovaly z aktualizačního serveru (z Update Serveru) musíte uvést port. Standartní port je `7074`.
   - **IP.** IP adresu aktualizačního serveru (Update Serveru).
   - **Období aktualizace (hodiny).** Pokud chcete zeměnit pravidelný čas aktualizací, tak zadejte novou hodnotu do tohoto pole. Standartní hodnota je 1.
4. Pokud můžete tak nastavte aktualizační server (Update Server) tak aby si sám stahoval automaticky Security Server a kity pro koncové body.

5. Aktualizační server (Update Server) může fungovat jako brána pro data posílané Bitdefender klienty produktů nainstalovaných v síti na Bitdefender servery. Tato data můžou obsahovat anonymizované reporty ohledně virových aktivit, reporty o funkčním selhání a data pro online registrace. Zapnutí role brány je užitečná pro řízení provozu a také pro síťe bez přístupu k internetu.

   **Poznámka**
   Přičemž můžete vypnout moduly produktů, které zasílají statistická data nebo data o selhání funkčnosti na Bitdefender Labs kdykoliv budete chtít. Můžete používat politiky pro vzdálenou správu těchto funkcí na počítačích a virtuálních strojích spravovaných skrze Control Center.

6. Klikněte na tlačítko **Save**.

## 6.3. Stahování produktových aktualizací

Infomace o stávajících komponentech GravityZone si můžete zobrazit na štítku **Komponenty (Components)**. Obsahuje dostupné informace o stávajících verzích, dále k novým aktualizacím (pokud nějaké existujou) a také informace k stavům vašich aktualizačních procesů.

Pro aktualizaci komponentů GravityZone:

1. Přejděte na stránku **Aktualizace (Update)** v Control Center a klikněte na štítek **Komponenty (Components)**.
2. Klikněte na komponent the který chcete updatovat v seznamu **Produktů (Product)**. Všechny dostupné verze budou zobrazovány v tabulce **Balíčky (Packages)**. Vyberte si pomocí zatrhávacího rámečeku odpovídající verzi kterou chcete stáhnout.

   **Poznámka**
   Nové balíčky budou ve stavu **Ne stáhnuté (Not downloaded)**. Jakmile Bitdefender vydá novou verzi, tak je nejstarší nestažená verze z tabulky odebrána.

3. Klikněte na **Akce (Actions)** nacházející se na vrchní straně tabulky a vyberte **Publikovat (Publish)**. Vybrané verze se automaticky stáhnou a status se adekvátně změní. Aktualizujte si obsah tabulky kliknutím na tlačítko **Aktualizace (Refresh)** a zkontrolujte odpovídající stav.

**Důležité**
GravityZone appliance neobsahuje standartně Security Server balíčky. Musíte si stáhnout manuálně Security Server balíčky potřebné pro vaše prostředí.

## 6.4. Offline Aktualizace Produktu

GravityZone používá ve výchozím stavu aktualizační systém připojená k internetu. Pro izolované sítě nabízí společnost Bitdefender alternativní způsob, jak zpřístupnit aktualizace komponent a obsahu zabezpečení offline.

### 6.4.1. Podmínky

Pro použití offline aktualizací, potřebujete:

- Instance GravityZone nainstalovaná v síti s přístupem do internetu (“online instance”). Online instance musí mít:
  - Přímý přístup do internetu
  - Přístup na portech 80 a 443. Pro více detailních informací o portech, které používá GravityZone , si přečtěte this KB article.
  - Pouze nainstalované role databázového a aktualizačního serveru (Database and Update Server roles)
- Jedna nebo více instancí GravityZone nainstalovaných v síti bez přístupu do internetu (“offline instances”)
- Obě GravityZone instance musí mít stejnou verzi appliance

### 6.4.2. Nastavení Online Instance GravityZone

Během této fáze, nasadíte instanci GravityZone do sítě s přístupem do internetu a následně ji nakonfigurujete tak aby fungovala jako offline aktualizační server (offline update server).

1. Nasaďte GravityZone na stroj s přístupem do internetu.
2. Nainstalujte pouze role databázového a aktualizačního serveru (Database and Update Server roles).
3. Spojte se se strojem pomocí TTY terminálu ve vašem virtuálním prostředí (nebo se spojte pomocí SSH).
4. Přihlašte se uživatelem `bdadmin` a pomocí hesla které jste k němu nastavili.

5. Spusťte příkaz `sudo su`pro získání práv **root**.
6. Spusťte následující příkazy pro offline instalaci `gzou-mirror` package:

```
# apt update # gzcli update # apt install gzou-mirror
```

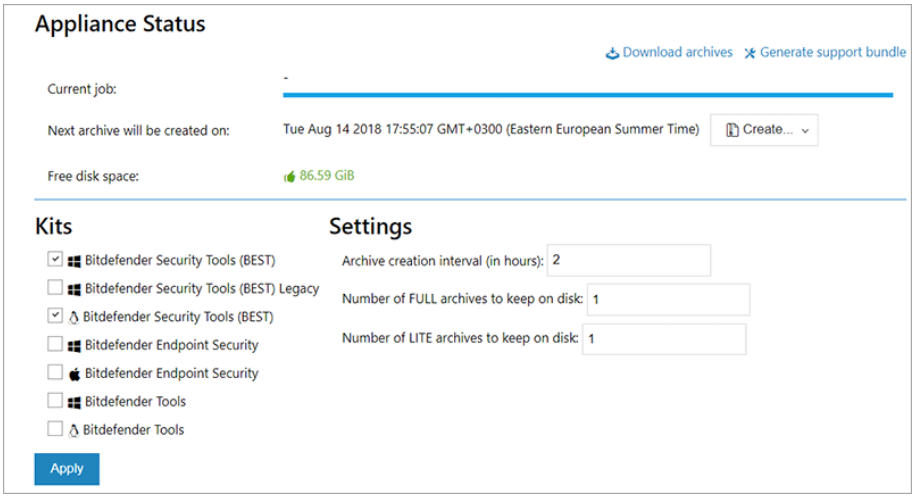
`gzou-mirror` má následující role:

- Nakonfigurujte aktualizační server (Update Server) tak aby generoval automaticky offline aktualizační archivy (offline update archives).
- Nastavte webovou službu (web service) na online instancích, která poskytuje konfigurace a volby stahování (download options) pro offline aktualizační archivy (offline update archives).

### 6.4.3. Konfigurace a stahování prvotních aktualizačních souborů

Během této fáze, budete konfigurovat nastavení aktualizačního archivu (update archive settings) pomocí webové služby (web service) nainstalované na online instanci, a pak následně vytvářet soubory archivu potřebné pro nastavení offline instance. Pak si budete muset stáhnout aktualizační soubory (update files) a umístit je na přenositelné úložné zařízení (USB klíč).

1. Přistupujte na webovou sloužbu (web service) skrze URL adresu tohoto formuláře: `https://Online-Instance-Update-Server-IP-or-Hostname`, pomocí uživatelského jména `bdadmin` a hesla které jste pro něj nastavili.




Online instance - Webové služby (Web Service)

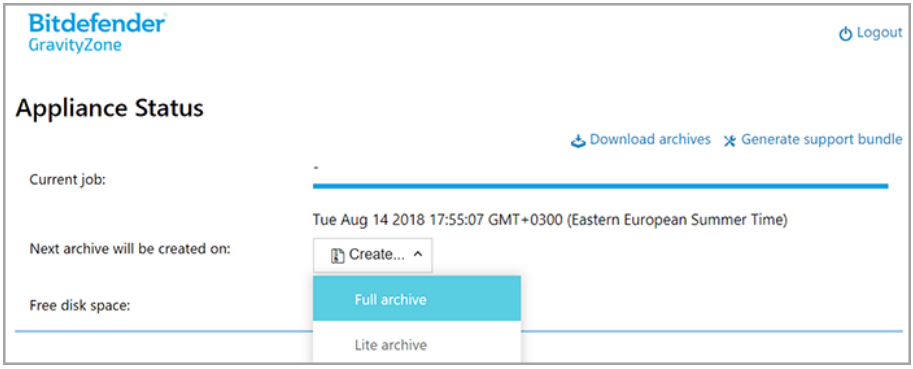
2. Nakonfigurujte následovně offline aktualizační archive (offline update archive) takto:
   - Pod **Instalační balíčky (Kits)**: si vyberte instalační balíčky (kity) koncových agentů, které chcete zahrnout v offline aktualizačním archivu (offline update archive).
   - Pod **Nastavení (Settings)**, editujte vaše předvolby aktualizací archivu (update archive preferences).

     Naplánovaná úloha (CRON job) nainstalovaná na online instanci bude každou minutu zjišťovat jestli nejsou nové soubory pro aktualizaci k dispozici a jestli je volná kapacita na disku větší než 10GB. Každou časovou periodu podle nastavení ve volbě **Interval pro vytvoření archivu (v hodinách) (Archive creation interval (in hours))**, se spustí CRON úloha a vytvoří následující soubory:
     - **Úplný archiv (produkt + bezpečnostní obsah)**, jakmile jsou nové aktualizační soubory dostupné
     - **Lite archiv** (pouze bezpečnostní obsah), pokud neexistují žádné nové aktualizační soubory

     Archivy se vytvoří v následující lokaci:

```
https://Online-Instance-Update-Server-IP-or-Hostname/snapshots
```

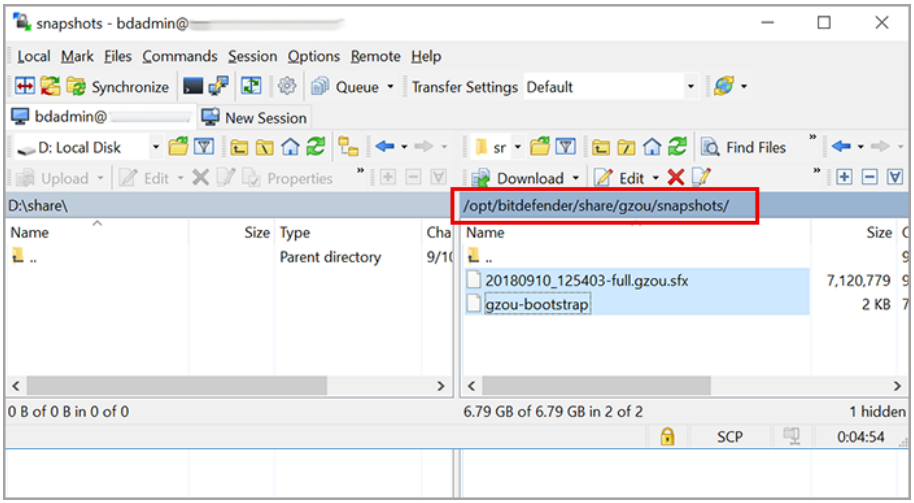
3. Klikněte na **Vytvořit (Create) > Úplný (Full)** archiv, za účelem vytvoření prvotního úplného archivu. Počkejte než se archiv vytvoří.




Online instance - Webová služba (Web Service): Vytvoření archivu

4. Stáhněte si úplný aktualizační archiv (Full update archive) a `gzou-bootstrap` soubor z online instance. Máte několik možností na výběr:
   - Skrze webovou službu (web service): klikněte na **Stáhnout archivy (Download archives)** pro přístup na stránku obsahující odkazy na aktualizační soubory (update files). Klikněte na úplná aktualizace archivu (full update archive) a `gzou-bootstrap` odkazy souborů pro jejich stažení na váš koncový bod.
   - Vyberte si vašeho preferovaného SCP/SCTP klienta (WinSCP, například) pro vytvoření SCP spojení (session) s online instancí a transfer výše uvedených souborů do jakékoliv lokace ve vaší online síti. Standardní cesta k online instanci je:

     ```
     /opt/bitdefender/share/gzou/snapshots
     ```




Přenos aktualizačních souborů (update files) použitím SCP

- Pomocí SAMBA sdílení (share). Použijte pouze pro čtení (read-only) SAMBA sdílení (share) k získání offline aktualizačních archivů (update archives) z následující lokace:

  `\\Online-Instance-Update-Server-IP-or-Hostname\gzou-snapshots`

  **Poznámka**
  Přístupové údaje pro přístup na SAMBA sdílení (share), pokud vyžadovány, tak jsou totožné s přístupovými údaji pro online instanci (`bdadmin` uživatel a heslo).

## 6.4.4. Nastavením Offline Instance GravityZone

Během tohoto kroku, budete nasazovat a konfigurovat offline instanci pro příjem aktualizací (updates) skrze archivy generované online instancí. Pokud není uvedeno jinak, všechny příkazy musí být spuštěny jako **root**.

1. Nasazení GravityZone na stroj z izolovaného prostředí.
2. Nainstalujte pouze role databázového a aktualizačního serveru (Database and Update Server roles).

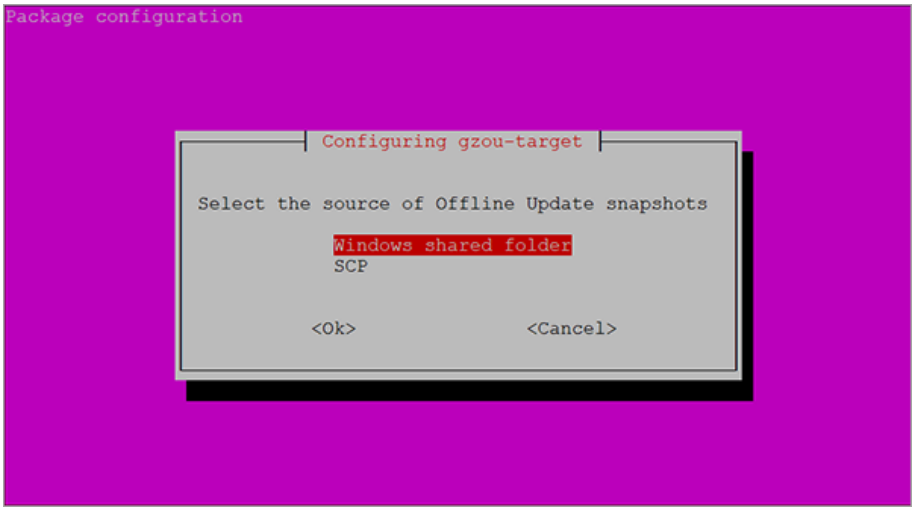
3. Přeneste aktualizační archive a `gzou-bootstrap` soubor staženy z online instance do `/home/bdadmin adresáře (directory)` na offline instanci použitím přenositelného úložného zařízení (USB disku).

   **Důležité**
   Proto aby offline aktualizace fungovala, se ujistěte jestli:
   - Jsou aktualizační archiv (update archive) a `gzou-bootstrap` ve stejné složce.
   - Je aktualizační archive (update archive) **Úplný (full)** archiv.

4. Spusťte `gzou-bootstrap` soubor následovně:
   a. Spojte se se strojem pomocí TTY terminálu ve vašem virtuálním prostředí (nebo se spojte pomocí SSH).
   b. Přetransformovat `gzou-bootstrap` do spustitelné formy:

   ```
   #
   chmod +x gzou-bootstrap
   ```

   c. Spusťte: `./gzou-bootstrap`
5. Vyberte si metodu přenosu aktualizačních archivů (update archives) do offline instance:
   - Vyberte si **Windows sdílenou složku (shared folder)** (Samba sdílení). V tomto případě, si budete muset vyspecifikovat cestu ke Windows sdílení (share) z izolované sítě, kam se má offline instance automaticky připojovat k získávání aktualizačních archivů (update archives). Zadejte přístupové údaje potřebné k přístupu na specifikovanou lokaci.
   - Vyberte si SCP pokud budete přenášet soubory manuálně do složky `/opt/bitdefender/share/gzou/snapshots/` na offline instanci pomocí SCP.




Offline GravityZone Instance - Konfigurace módu přenosu aktualizačního souboru

**Poznámka**
Pokud chcete později změnit metodu přenosu:

a. Přihlašte se na offline instanci pomocí TTY terminálu ve vašem virtuálním prostředí (nebo se připojte na ni pomocí SSH).
b. Přihlašte se uživatelem `bdadmin` a pomocí hesla které jste k němu nastavili.
c. Spusťte příkaz `sudo su`pro získání práv roota.
d. Spusťte:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Objeví se vám konfigurační dialog, kde můžete provést změny které chcete.

6. Přejděte do offline módu GravityZone v konzoli a pomocí příkazové řádky nainstalujte chybějící role.
7. Přihlašte se offline na konzoli z vašeho prohlížeče a vložte váš licenční klíč (v offline modu).

### 6.4.5. Používání offline aktualizací

Jakmile jste nastavili GravityZone instance, pokračujte následnými kroky k aktualizaci vaší offline instalace:

1. Stáhněte si nejnovější offline aktualizační archiv (update archive) z online instance do vašeho preferovaného síťového sdílení (network share). Více informací naleznete na „Konfigurace a stahování prvotních aktualizačních souborů“ (str. 187).
2. Použijte USB disk k přenosu aktualizovaného (update) archivu do nakonfigurovaného Samba sdílení z izolované sítě. Více informací naleznete na „Nastavením Offline Instance GravityZone“ (str. 190).

   Soubory budou automaticky staženy do následujícího adresáře na offline instanci:

   ```
   /opt/bitdefender/share/gzou/snapshots/
   ```

### 6.4.6. Pomocí webové konzole

Přihlašte se do webové konzole zadáním IP adresy/názvu hosta appliance ve vašem prohlížeči. Můžete editovat dostupné volby:

- Ovládací Panel (Control Center)
- Obecná nastavení

#### Ovládací Panel (Control Center)

**Stav Appliance (Appliance Status)** zobrazí stav poslední provedené úlohy (typ archivu, datum a čas), a informace o dalším naplánované úloze.

Můžete si vybrat:

- **Vytvořte archiv bezpečnostního obsahu**
- **Vytvořit úplný archiv**

V části **Vytvořené archivy** si můžete stáhnout bezpečnostní obsah a plné archivy.

Vyberte si archiv(y) z dostupného seznamu a klikněte na tlačítko **Stáhnout(Download)**.

Můžete také vidět dostupné místo na diskovém úložišti appliance.

## Obecná nastavení

Můžete si vydefinovat plán pro stahování GravityZone kitů.

1. Klikněte na tlačítko **Editace nastavení (Edit Settings)**.
2. Vyberte si jeden nebo více kitů ze seznamu **Dostupné kity (Available Kits)**.
3. V sekci **Schedule** můžete definovat interval pro vytvoření archivů a také počet archivů, které se mají uchovávat na disku.
4. Klikněte na tlačítko **Aplikovat(Apply)** pro uložení a provedení změn.

# 7. ODINSTALACE OCHRANY

Můžete odinstalovat a reinstalovat GravityZone komponenty v případech když potřebujete použít licenční klíč pro jiný stroj, za účelem vyřešení chyb a nebo když provádíte upgrade.

Za účelem řádné odinstalace Bitdefender ochrany z koncových bodů ve Vaší síti, postupujte podle instrukcí popsaných v této kapitole.

- Odinstalace ochrany koncových bodů
- Odinstalace HVI
- Odinstalace ochrany Exchange (Exchange Protection)
- Odinstalace ochrany koncových bodů
- Odinstalace serverových rolí GravityZone

## 7.1. Odinstalace ochrany koncových bodů

Pro bezpečné odstranění Bitdefender ochrany, musíte nejprve odisntalovat bezpečnostní agenty, a pak Security Server, pokud potřeba. Pokud chcete odinstalovat pouze Security Server, ujistěte se nejprve zda jsou jeho agenti připojeni na jiný Security Server.

- Odinstalace bezežnostních agentů
- Odinstalace Security Server

### 7.1.1. Odinstalace bezežnostních agentů

Máte dvě možnosti jak odinstalovat bezpečnostní agenty:

- vzdáleně v Control Center
- Manuálně přímo na cílovém stroji

**Varování**
Bezpečnostní agenti a Bezpečnostní Servery jsou nezbytní pro udržení zařízení v bezpečí od jakékoli hrozby, jejich odinstalováním můžete síť entity dostat do nebezpečí.

#### Vzdálená deinstalace

Pro odinstalaci Bitdefender ochrany ze spravovaného koncového bodu vzdáleně:

1. Přejděte na **Network** stránku.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Všechny počítače z vybraného kontejneru jsou zobrazeny v pravém panelu.
4. Vyberte si koncový bod, ze kterého chcete odinstalovat Bitdefender bezpečnostního agenta.
5. Klikněte na **Úlohy (Tasks)** na Horní straně tabulky at the a vyberte **Odinstalace klienta (Uninstall client)**. Zobrazí se konfigurační okno.
6. V **Odinstalace agenta (Uninstall agent)** okně úloh si můžete vybrat jestli si chcete ponechat soubory v kartanténě a nebo jestli je chcete smazat.

   Pro prostředí integrované skrze VMware vShield, musíte vybrat potřebná přístupová data (heslo a uživatele)pro každý jednotlivý stroj, neboť v jiném případě skončí odinstalace chybovou hláškou. Vyberte **Vyberte přístupová data pro integraci s vShield (Use credentials for vShield integration)**, pak přidejte potřebná přístupová data do tabulky správce přístupových údajů zobrazené níže.
7. Kliknutím na **Uložit** vytvoříte úlohu. Potvrzovací zpráva se zobrazuje.

Můžete se podívat na a spravovat úlohy v **Sítě (Network) > Tasks (Úlohy)**.

Pokud chcete přeinstalovat bezpečnostní agenty, obraťte se na „Instalace Ochrany na Koncová Zařízení“ (str. 123).

## Lokální odinstalace

Abyste mohli manuélně odinstalovat Bitdefender bezpečnostního agenta z Windows stroje:

1. Záleží na Vašem operačním systému:
   - Ve Windows 7,přejděte na **Start > Control Panel > Uninstall a program** pod **Programs** kategorie.
   - Ve Windows 8, přejděte na **Settings > Control Panel > Uninstall a program** pod **Program** kategorie
   - Ve Windows 8.1, klikněte pravým tlačítkem myši na **Start** tlačítko, a pak vyberte **Control Panel > Programs & features**.
   - Ve Windows 10, přejděte na **Start > Settings > System > Apps & features**.

2. Vyberte Bitdefender agenta ze seznamu programů.
3. Klikněte na **Uninstall**.
4. Vložte Bitdefender heslo, pokud je zapnuté v bezpečnostní politice. Během odinstalace, můžete pozorovat pokrok této úlohy.

Pro manuální odinstalaci Bitdefender bezpečnostního agenta z Linuxového stroje:

1. Otevřete terminál
2. Získejte práva roota použitím `su` or `sudo su` příkazu.
3. Navigujte použitím příkazu `cd` do následující cesty: `/opt/BitDefender/bin`
4. Spusťe skript:

```
# ./remove-sve-client
```

5. Abyste mohli pokračovat vložte Bitdefender heslo, pokud je zapnuté v bezpečnostní politice.

Pro manuální odinstalaci Bitdefender agenta z MacOS:

1. Přejděte na **Finder > Applications**.
2. Otevřete Bitdefender složku.
3. Dvojitý-Klik na **Bitdefender Mac Uninstall**.
4. V potvrzovacím okně, klikněte na obojí **Check** a **Uninstall** abyste mohli pokračovat.

Pokud chcete přeinstalovat bezpečnostní agenty, obraťte se na „Instalace Ochrany na Koncová Zařízení“ (str. 123).

## 7.1.2. Odinstalace Security Server

Security Server můžete odinstalovat stejným způsobem, jak byl nainstalován, buď z Control Center, nebo z rozhraní nabídky virtuálního zařízení GravityZone.

Pro odinstalaci Security Server v Control Center:

1. Jděte do záložky **Síť**.
2. Vyberte **Virtuální stroje** z možnosti zobrazení.

3. Vyberte datové centrum nebo složku, která obsahuje hostitele, na kterém je Security Server nainstalovaný. Koncové body se zobrazují na pravé straně tabulky.
4. Označte pole odpovídající hostiteli, na kterém je Security Server nainstalovaný.
5. V **Tasks** menu, vyberte **Uninstall Security Server**.
6. Vložte přístupové údaje vShield (pokud je potřeba) a klikněte na **Ano (Yes)** pro vytvoření úlohy.

Můžete se podívat na a spravovat úlohy v **Sítě (Network) > Tasks (Úlohy)**.

Když Security Server je nainstalován na stejné virtuální applianci stejně jako ostatní GravityZone role, můžete je odstranit pomocí použití příkazové řádky (command-line interface ) přímo na applianci. Postupujte následovně:

1. Přistupujte ke konzoli appliance z vašeho nástroje pro správu virtualizace (například, vSphere Client).

   Použijte směrová tlačítka a `Tab` tlačítko k navigaci skrze nabídku menu a možností (options). Stiskněte `Enter` pro vybrání specifické možnosti funkce.
2. V **Appliance Options** menu, běžte na **Advanced Settings**.
3. Vyberte **Odinstalace Security Serveru**. Zobrazí se potvrzovací okno.
4. Stiskněte `Y` key, nebo stiskněte `Enter` přičemž vybráním **Yes** možnosti výběru budete pokračovat. Čekejte než se odinstalace dokončí.

## 7.2. Odinstalace HVI

Pro odinstalaci HVI z hostitele, postačí odinstalovat HVI dodatkový rozšiřující balíček (Supplemental Pack). Nadále budete moci používat Security Server jakožto skenovací server, pokud máte k dispozici platný licenční klíč proSecurity for Virtualized Environments.

Pokud chcete úplně odstranit Bitdefender, tak musíte odinstalovat oba, jak HVI Dodatkový rozšiřující balíček (Supplemental Pack) tak i samotný Security Server.

**Poznámka**
Modul HVI je možné zpřístupnit pro vaše řešení GravityZone pomocí samostatného licenčního klíče.

## Odinstalovat Doplňkový balíček HVI

Máte dvě možnosti jak odstranit Dodatkový rozšiřující balíček (Supplemental Pack):

- Vzdáleně z Control Center, spuštěním odinstalační úlohy.
- Vzdáleně z XenCenter, spuštěním pár příkazů na cílovém hostitelském stroji.

Pro odebrání HVI balíčku (packu) použijte Control Center:

1. Přihlaste se do Control Center.
2. Přejděte na stránku **Síť** a v nastavení zobrazení vyberte **Virtuální zařízení**.
3. Z menu **Zobrazení** v levém panelu vyberte **Server**.
4. Vyberte jednoho nebo více hostitelů Xen ze síťového inventáře. Dostupné hostitele můžete snadno prohlížet zvolením možnosti **Typ > Hostitelé** v nabídce **Filtry**.
5. Klikněte na tlačítko **Úlohy** na pravé liště a vyberte **odinstalovat Doplňkový balíček HVI**. Otevře se konfigurační okno.
6. Naplánujte, kdy chcete balíček odstranit. Můžete si zvolit, zda chcete spustit úlohu okamžitě po jejím uložení, nebo v konkrétním čase. V případě, že odstranění nelze dokončit v určený čas, úloha bude automaticky opakována podle nastavených parametrů pro opakování. Například, pokud vyberete více hostitelů a jeden hostitel je v době, kdy má odstranění balíčku proběhnout nedostupný, úloha se spustí znovu v určeném čase.
7. Hostitel musí být restartován pro dokončení odstraňování. Pokud chcete, aby se hostitel sám restartoval, zvolte **Restartovat automaticky (je-li potřeba)**.
8. Klikněte na tlačítko **Save**. Zobrazí se potvrzovací okno.

   Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

Pro odstranění HVI balíčku (packu) použitím XenCenteru:

1. Přihlašte se do XenCenteru.
2. Otevřete konzoli Xen hostitele.
3. Zadejte heslo pro XenServer hostitele.
4. Spusťe následující příkazy:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-r
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # služba (s
```

## Odinstalace Security Server

Pro odinstalaci Security Serveru z jednoho nebo z vícero hostitelů:

1. Přihlaste se do Control Center.
2. Jděte do záložky **Síť**.
3. Vyberte **Virtuální stroje** z možnosti zobrazení.
4. Prohlédněte si Citrix inventář a označte si v označovacích rámečcích adekvátní požadované hosty. Pro rychlý výběr, můžete filtrovat síťový inventář pro zobrazení pouze Security Serverů.
5. Click the **Tasks** button at the upper side of the table and choose **OdinstalovatSecurity Server** from the menu. Zobrazí se potvrzovací okno. Pokračujte kliknutím na **Ano (Yes)**.

Úlohu můžete prohlížet a spravovat na stránce **Síť > Úlohy**.

# 7.3. Odinstalace ochrany Exchange (Exchange Protection)

Můžete odstranit Exchange Ochranu z kteréhokoliv Microsoft Exchange Serveru s Bitdefender Endpoint Security Tools klientem na kterém je tato role již nainstalována. Můžete provést odinstalaci z Control Center.

1. Jděte do záložky **Síť**.
2. Vyberte **Počítače a Virtuální Stroje** z možnosti zobrazení.
3. Zvolte požadovaný kontejner z levého panelu. Entity se zobrazí v pravém poli tabulky.
4. Vyberte koncový bod z kterého chcete odinstalovat ochranu exchange (Exchange Protection).
5. Klikněte na **Rekonfigurace klienta (Reconfigure Client)** v **úlohy(Tasks)** v menu, ve vrchní části pole tabulky. Zobrazí se konfigurační okno.
6. Ve sekci **Všeobecné(General)** odznačte (vymažte zatržítko) pro **Ochranu Exchange (Exchange Protection)** check box.

**Varování**
Ujistěte se, zda jste vybrali v konfiguračním okně všechny ostatní role , které jsou aktivní na koncovém bodu. jinak budou také odinstalovány.

7. Kliknutím na **Uložit** vytvoříte úlohu.

Můžete se podívat na a spravovat úlohy v **Sítě (Network) > Tasks (Úlohy)**.

Pokud chcete reinstalovat ochranu Exchange (Exchange Protection), podívejte se na „Instalace Ochrany Exchange (Exchange Protection)“ (str. 166).

## 7.4. Odinstalace Sandbox Analyzer On-Premises

K odinstalaci Sandbox Analyzer On-Premises:

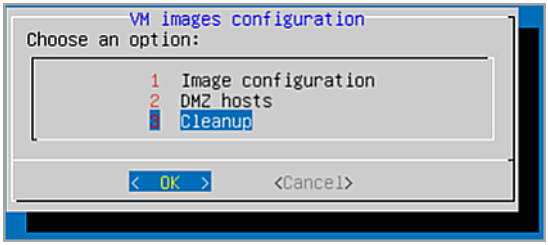
1. Odeberte obrazy virtuálního počítače (VM) z konzoly zařízení Sandbox Analyzer.
   a. Přihlaste se do rozhraní zařízení Sandbox Analyzer.

      Použijte směrová tlačítka a `Tab` tlačítko k navigaci skrze nabídku menu a možností (options).

      Stiskněte `Enter` pro vybrání specifické možnosti funkce.

   b. V nabídce **Konfigurace karantény** přejděte na možnost **Obrazy VM** .

   c. V nabídce **Konfigurace obrazů VM** přejděte na možnost **Vyčištění** .




Konzola zařízení Sandbox Analyzer - Konfigurace karantény - Vyčištění

   d. Zkontrolujte, zda chcete odebrat nainstalované obrazy virtuálního počítače.

      Počkejte na dokončení této akce. Během této akce budou také vymazána data spojená s obrazy virtuálního stroje.

2. Odstranit virtuální zařízení Sandbox Analyzer:

a. Vypnout virtuální zařízení Sandbox Analyzer.
b. Odstraňte zařízení z inventáře ESXi.

## 7.5. Odinstalace ochrany koncových bodů

Když chcete odebrat Bitdefender ochranu z mobilního zařízení, tak to potřebujete provést z obou jak Control Center tak i ze zařízení.

Když smažete zařízení z Control Center:

- GravityZone mobilní klient je odpojen, ale ne odstaněn ze zařízení.
- Všechny výpisy týkající se odstraněného zařízení jsou stále dostupné.
- Vaše osobní informace a aplikace nejsou nijak ovlivněny.
- Pro zařízení iOS je odstraněn profil MDM. Pokud zařízení není připojeno k internetu, profil MDM zůstane nainstalovaný tak dlouho, dokud není nové připojení k dispozici.

**Varování**

- Smazaná mobilní zařízení není možné obnovit.
- Ujistěte se, že cílové zařízení není zamčené před tím než ho smažete. Pokud omylem odstraníte uzamčené zařízení, musíte ho pro jeho odemčení obnovit do továrního nastavení.

1. Jděte do záložky **Síť**.
2. Z nastavení zobrazení vyberte **Mobilní zařízení**.
3. Klikněte na **Filtry (Filters)** na vrchní straně síťového panelu a pak vyberte **Zařízení (Devices)** z kategorie **Náhled (View)**. Klikněte na tlačítko **Save**.
4. Zvolte požadovaný kontejner z levého panelu. Všechna zařízení jsou zobrazena na pravé straně tabulky.
5. Vyberte označovací rámeček zařízení, na kterém chcete odstranit ochranu.
6. Klikněte na ⊖ **Smazat** v horní části tabulky.

V dalším kroku, musíte odinstalovat software ze zařízení.

Pro odinstalaci Bitdefender ochrany z Android zařízení:

1. Přejděte na **Bezpečnost (Security) > Správci zařízení (Device Administrators)**.

2. Odznačte GravityZone zaškrtávací rámeček. Zobrazí se potvrzovací okno.
3. Klikněte na **Deaktivovat (Deactivate)**. Upozornění je zobrazeno, informující vás, že funkce ochrany proti krádeži (anti-theft features) už nebudou fungovat a že ztratíte přístup ke korporátním datům a sítím.
4. Odinstalujte mobilního klienta GravityZone stejně jako kteroukoliv jinou aplikaci.

Pro odinstalaci Bitdefender ochrany z iOS zařízení:

1. Přejděte na Bitdefender GravityZone mobile client ikonu a držte jej. minimálně 5 do -ti sekund.
2. Vyberte si v přiložených kroužcích jakmile se zobrazí. Aplikace je smazána.

Pokud chcete znovu nainstalovat ochranu mobilů, podívejte se do„Instalace ochrany mobilních zařízení (Mobile Devices Protection)“ (str. 171)

## 7.6. Odinstalace GravityZone virtual appliance rolí

Role virtuálního zařízení GravityZone můžete odinstalovat prostřednictvím rozhraní založeného na nabídce. Ikdyž odeberete jednu z nich , vaše síť je nadále chráněná. I přesto, ale potřebujete minimálně jednu instanci z každé role GravityZone , aby fungovala správně.

V případě jedné appliance s všemi GravityZone rolemi, když odbíráte jednu roli, koncové body zůstávají nadále chráněny, ikdyž některé z funkcí mohou být nedostupné, v závislosti na každé jednotlibé roli.

V případě vícero GravityZone appliancí, můžete bezpečně odinstalovat roi dokud existuje dostupná jiná instance se stejnou rolí ve vaší síti. Díky designu, vícero instancí comunikačnío serveru a webové konzole správy (Communication Server and Web Console ) mohou být nainstalovány na různých appliancích a spojeny pomocí role balanceru. Jakmile odinstalujete instanci jedné specifické role, tak její funkce je přebrána jinou dostupnou instancí.

Pokud je potřeba, tak můžete odinstalovat komunikační server z jedné appliance , přičemž můžete přiřadit její funkci jiné instanci téže role. Pro hladkou migraci, následujte tyto kroky:

1. V Control Center, přejděte na stránku **Politiky (Policies)**.
2. Vyberte existující politiku nebo klikněte na **Přidat (Add)** abyste přidali novou.
3. Pod sekcí **Všeobecné (General)**, přejděte na **Kommunikace (Communication)**.

4. V tabulce **Přiřazení komunikace s koncovým bodem** klikněte na pole **Název**. Zobrazí se seznam zjištěných komunikačních serverů.
5. Vyberte kommunikační server (communication server) od kterého chcete aby navázal vztah s koncobvými body.
6. Klikněte na tlačítko ⊕ **Přidat** v pravé části tabulky. Pokud máte v seznamu více jak jeden Komunikační server (communication server), tak můžete nakonfigurovat jejich prioritu posunem šipek nahoru a dolů na správné straně každé entity.
7. Klikněte **Uložit (Save)** pro vytvoření politiky. Koncové body budou komunikovat s Control Center skrze specifikovaný komunikační server (communication server).
8. V příkazové řádce (command-line interface) od GravityZone , odinstalujte starou roli komunikačního serveru (Communication Server role).

**Varování**
Pokud odinstalujete starý komunikační server (Communication Server) beztoho aniž byste nastavili politiku, tak bude komunikace navždy ztracena a vy budete muset reinstalovat všechny bezpečnostní agenty.

Pro odinstalaci GravityZone virtual appliance rolí:

1. Přihlašte se do konzole rozhraní vašeho nástroje správy virtualizovaného prostředí (Například do vSphere klienta). Použijte směrová tlačítka a `Tab` tlačítko k navigaci skrze nabídku menu a možností (options). Stiskněte `Enter` pro vybrání specifické možnosti funkce.
2. Vyberte **Pokročilá nastavení (Avanced Settings)**.
3. Vyberte **Instalace/odinstalace (Install/Uninstall) rolí**.
4. Běžte do **Přidat nebo odstranit role (Add or remove roles)**.
5. Použitím `Mezerníku (Space)`, odznačte jakoukoliv roli kterou chcete odinstalovat, pak stiskněte `Enter`. Potvrzovací okno se zobrazí, informující vás o tom, že role bude odebrána.
6. Stiskněte `Enter` pro pokračování a počkejte než se odinstalace dokončí.

Pokud chcete roli znova nainstalovat podívejte se na „Nainstalovat/Odinstalovat Role“ (str. 110).

# 8. ODBORNÁ POMOC

Bitdefender poskytuje svým zákazníkům bezkonkurenčně rychlou a přesnou podporu. Pokud se setkáte s jakýmkoli problémem nebo máte dotaz ohledně čehokoli na vašem produktu Bitdefender, přejděte na naše online Centrum podpory. Dodá vám několik zdrojů, kde můžete rychle najít řešení nebo odpověď. Nebo, pokud vám to tak vyhovuje lépe, můžete kontaktovat Tým péče o zákazníky Bitdefender. Naši zástupci podpory pohotově zodpoví vaše dotazy a poskytnou vám potřebnou pomoc.

**Poznámka**
Informace o našich poskytovaných službách podpory a zásadách podpory naleznete v Centru podpory.

## 8.1. Bitdefender Centrum Podpory

Bitdefender Centrum podpory je místo, kde naleznete všechnu pomoc s vaším produktem Bitdefender, kterou potřebujete.

Můžete použít několik zdrojů pro rychlé nalezení řešení nebo odpovědi:

- Články Knowledge Base
- Bitdefender Fórum Podpory
- Dokumentace produktu

Můžete také použít svůj oblíbený vyhledávač k nalezení dalších informací o počítačovém zabezpečení, produktech Bitdefender a společnosti.

### Články Knowledge Base

Bitdefender Knowledge Base je online úložiště informací o produktech Bitdefender. Uchovává v snadno přístupném formátu zprávy o výsledcích probíhající technické podpory a činnostech opravy chyb týmů podpory a vývoje produktu Bitdefender, spolu s obecnějšími články o virové prevenci, správě řešení produktů Bitdefender s podrobnými vysvětleními a mnoha dalšími články.

Bitdefender Knowledge Base je přístupná veřejnosti a lze ji volně prohledávat. Rozsáhlé informace, které obsahuje, jsou dalším prostředkem poskytování potřebných technických znalostí zákazníkům produktu Bitdefender. Všechny platné žádosti o informace nebo hlášení chyb od klientů produktu Bitdefender se časem dostanou do Bitdefender Knowledge Base jako hlášení o opravách chyb, taháky

pro obcházení problémů nebo informativní články doplňující soubory nápovědy produktu.

Bitdefender Knowledge Base pro obchodní produkty je kdykoli dostupná na http://support.bitdef.cz/.

### Bitdefender Fórum Podpory

Fórum podpory produktu Bitdefender poskytuje uživatelům produktu Bitdefender snadný způsob, jak získat pomoc a pomoci ostatním. Můžete vložit jakýkoliv problém nebo otázku ohledně vašeho produktu Bitdefender.

Technici podpory produktu Bitdefender sledují nové příspěvky a fóru, aby vám pomohli. Odpověď nebo řešení můžete rovněž získat od zkušenějšího uživatele produktu Bitdefender.

Před zveřejněním problému nebo otázky prohledejte fórum, jestli se na něm nenachází podobné nebo související téma.

Fórum podpory produktu Bitdefender je k dispozici na adrese https://forum.bitdefender.com v 5 různých jazycích: v angličtině, němčině, francouzštině, španělštině a rumunštině. Klikněte na odkaz **Business Protection** pro přístup k sekci věnované obchodním produktům.

### Dokumentace produktu

Dokumentace produktu je ten nejkompletnější zdroj informací o vašem produktu.

Nejsnadnější způsob získání dokumentace je na stránce **Pomoc & Podpora** v Control Center. Klikněte na své uživatelské jméno v pravém horním rohu konzole, zvolte **Pomoc & Podpora** a poté odkaz průvodce, který vás zajímá. Průvodce se otevře v nové kartě vašeho prohlížeče.

## 8.2. Žádost o podporu

Můžete požádat o podporu pomocí online supportniho centra. Vyplňte Kontaktní formulář (contact form) a potvrďte zaslání.

## 8.3. Používání Nástroje podpory

Nástroj podpory GravityZone je navržen pro pomáhání uživatelům a podporujícím technikům ve snadném získání informací potřebných k odstraňování problémů. Spusťte Nástroj podpory na postižených počítačích a odešlete výsledný archiv s informacemi o odstraňování problémů zástupci podpory společnosti Bitdefender

## 8.3.1. Používání Nástroje podpory na operačních systémech Windows

### Spuštění aplikace Nástroj podpory

Chcete-li vygenerovat protokol o postižených počítačích, použijte jednu z těchto metod:

- Příkazový Řádek

  V případě problémů s BEST nainstalovaným v počítači.

- Problém s instalací

  Pro situace, kdy BEST není v počítači nainstalována a instalace selže.

### Metoda příkazového řádku

Pomocí příkazového řádku můžete sbírat protokoly přímo z postiženého počítače. Tato metoda je užitečná v situacích, kdy nemáte přístup do GravityZone Control Center nebo počítač nekomunikuje s konzolí.

1. Otevřete příkazový řádek s oprávněními pro správu.
2. Přejděte do složky pro instalaci produktu. Výchozí cesta je:

   `C:\Program Files\Bitdefender\Endpoint Security`

3. Zhromažďujte a ukládejte protokoly spuštěním tohoto příkazu:

   ```
   Product.Support.Tool.exe collect
   ```

   Protokoly jsou uloženy ve výchozím nastavení v `C:\Windows\Temp`.

   Volitelné, pokud chcete protokol nástrojů podpory uložit do vlastního umístění, zadejte vlastní cestu :

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Například:

   ```
   Product.Support.Tool.exe collect path="D:\Test"
   ```

Během provádění příkazu můžete na obrazovce sledovat průběh. Po dokončení procesu se na výstupu zobrazí název archivu obsahujícího protokoly a jeho umístění.

Chcete-li protokoly odeslat do Bitdefender Enterprise Support `C:\Windows\Temp` nebo vlastního umístění a najděte soubor archivu s názvem `ST_[název_počítače]_[aktuální datum]` . Připojte archiv k vašemu supportnímu ticketu pro další odstranění problémů.

### Problém s instalací

1. Chcete-li stáhnout nástroj BEST Support Tool, klikněte zde .
2. Spusťte spustitelný soubor jako správce. Zobrazí se okno.
3. Vyberte umístění pro uložení archivu protokolů.

   Během shromažďování protokolů si na obrazovce všimnete ukazatele průběhu. Po dokončení procesu zobrazí výstup název archivu a jeho umístění.

Chcete-li protokoly odeslat na podporu společnosti Bitdefender Enterprise Support, přejděte do vybraného umístění a najděte soubor archivu s názvem `ST_[computername]_[currentdate]`. Připojte archiv k vašemu supportnímu ticketu pro další odstranění problémů.

## 8.3.2. Používání Nástroje podpory na operačních systémech Linux

Pro operační systémy Linux je Nástroj podpory integrovaný s bezpečnostním agentem Bitdefender.

Pro sbírání systémových informací Linux pomocí Nástroje podpory, zadejte následující příkaz:

```
# /opt/BitDefender/bin/bdconfigure
```

pomocí těchto dostupných možností:

- `--help` pro seznam všech příkazů Nástroje podpory
- `enablelogs` pro zapnutí protokolů produktu a komunikačních modulů (všechny služby se automaticky restartují)

- `disablelogs` pro zakázání protokolů produktu a komunikačních modulů (všechny služby se automaticky restartují)
- `deliverall` pro vytvoření:
  - Archiv obsahující protokoly produktu a komunikačního modulu, doručený do složky `/tmp` v následujícím formátu `bitdefender_machineName_timeStamp.tar.gz`.

    Poté, co je archiv vytvořen:

    1. Budete dotázáni, zda si přejete zakázat protokoly. Pokud je třeba, služby se automaticky restartují.
    2. Budete dotázáni, zda si přejete odstranit protokoly.
- `deliverall -default` doručí ty samé informace jako předchozí možnost, ale na protokolech budou provedena výchozí opatření bez dotazování se uživatele (protokoly budou vypnuty a odstraněny).

Můžete spustit také příkaz `/bdconfigure` přímo z balíčku BEST (plný nebo downloader), aniž byste měli produkt nainstalovaný.

Pro nahlášení problému s GravityZone, který ovlivňuje vaše systémy Linux, postupujte dle následujících kroků pomocí dříve popsaných možností:

1. Povolte protokoly produktu a komunikačního modulu.
2. Pokusit se o opětovné vyvolání problému.
3. Zakázat protokoly.
4. Vytvořte protokolový archiv.
5. Otevřete emailový lístek podpory pomocí formuláře dostupného na stránce **Pomoc & Podpora** v Control Center s popisem problému a připojeným protokolovým archivem.

Nástroj podpory pro Linux poskytuje následující informace:

- Složky `etc`, `var/log`, `/var/crash` (pokud dostupná) a `var/epag` z `/opt/BitDefender`, obsahující protokoly a nastavení Bitdefender.
- Soubor `/var/log/BitDefender/bdinstall.log`, obsahující instalační informace
- Soubor `network.txt`, ve kterém jsou uvedeny informace o nastavení sítě / připojení stroje

- Soubor `product.txt`, včetně obsahu všech souborů `update.txt` z `/opt/BitDefender/var/lib/scan` a kompletní rekurzivní seznam všech souborů z `/opt/BitDefender`
- Soubor `system.txt`, obsahující obecné systémové informace (distribuce a kernelové verze, dostupná RAM a volné místo na pevném disku)
- Soubor `users.txt` s uživatelskými informacemi
- Další informace ohledně produktu související se systémem, jako jsou externí připojení procesů a využití CPU
- Systémové protokoly

### 8.3.3. Používání Nástroje podpory na operačních systémech Mac

Při posílání žádosti Týmu technické podpory Bitdefender je nutné uvést následující:

- Podrobný popis problému, se kterým jste se setkali.
- Screenshot (pokud proveditelný) přesně té chybové zprávy, která se vám zobrazuje.
- Protokol Nástroje podpory.

Pro sběr systémových informací Mac pomocí Nástroje podpory:

1. Stáhněte ZIP archiv obsahující Nástroj podpory.
2. Z archivu extrahujte soubor **BDProfiler.tool**.
3. Otevřete okno Terminálu.
4. Přejděte do umístění souboru **BDProfiler.tool**.
   Například:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. K souboru přidejte práva pro spuštění:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Spusťte nástroj.

   Například:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Až budete vyzváni k zadání hesla administrátora, stiskněte `Y` a zadejte heslo.

   Počkejte pár minut, než nástroj dokončí generování protokolu. Výsledný soubor archivu (**Bitdefenderprofile_output.zip**) naleznete na své Ploše.

## 8.4. Kontaktní informace

Účinná komunikace je klíčem k úspěšnému obchodu. Za uplynulých 18 let si Bitdefender vybudoval nezpochybnitelnou pověst díky neustálému usilování o lepší komunikaci s cílem překonat očekávání našich klientů a partnerů. V případě dotazů nás bez váhání kontaktujte.

### 8.4.1. Webové adresy

Prodejní oddělení: enterprisesales@bitdefender.com
Centrum podpory:http://support.bitdef.cz/
Dokumentace: gravityzone-docs@bitdefender.com
Lokální distributoři :http://www.bitdefender.com/partners
Partner Program: partners@bitdefender.com
Mediální vztahy: pr@bitdefender.com
Viry: virus_submission@bitdefender.com
Spam: spam_submission@bitdefender.com
Oznámení zneužívání produktu: abuse@bitdefender.com
Webová stránka: http://www.bitdefender.com

### 8.4.2. Lokální distributoři

Lokální distributoři produktu Bitdefender jsou připraveni zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech.

Chcete-li najít distributora produktu Bitdefender ve vaší zemi:

1. Přejděte na web http://www.bitdefender.com/partners.
2. Jděte na **Partner Locator**.

3. Informace o kontaktech na lokální Bitdefender distributory by se měla automaticky zobrazit. Pokud se tak nestane, vyberte zemi ve které se nacházíte a zobrazte si informace.
4. Pokud nenajdete distributora produktu Bitdefender ve vaší zemi, kontaktujte nás emailem na adrese enterprisesales@bitdefender.com.

### 8.4.3. Bitdefender Kanceláře

Pobočky produktu Bitdefender jsou připraveny zodpovědět jakékoli dotazy ohledně své oblasti působnosti jak v komerčních, tak v obecných záležitostech. Jejich příslušné adresy a kontakty jsou uvedeny níže.

#### Spojené státy

**Bitdefender, LLC**
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (prodej&technická podpora): 1-954-776-6262
Prodej: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrum podpory: http://www.bitdefender.com/support/business.html

#### Francie

**Bitdefender**
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
Email: b2b@bitdefender.fr
Web: http://www.bitdefender.fr
Centrum podpory: http://www.bitdefender.fr/support/business.html

#### Španělsko

**Bitdefender España, S.L.U.**
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España

Fax: (+34) 93 217 91 28
Telefon (pobočka a prodej): (+34) 93 218 96 15
Telefon (technická podpora): (+34) 93 502 69 10
Prodej: comercial@bitdefender.es
Web: http://www.bitdefender.es
Centrum podpory: http://www.bitdefender.es/support/business.html

## Německo

**Bitdefender GmbH**
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (pobočka a prodej): +49 (0) 2304 94 51 60
Telefon (technická podpora): +49 (0) 2304 99 93 004
Prodej: firmenkunden@bitdefender.de
Web: http://www.bitdefender.de
Centrum podpory: http://www.bitdefender.de/support/business.html

## Velká Británie a Irsko

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (prodej&technická podpora): (+44) 203 695 3415
Email: info@bitdefender.co.uk
Prodej: sales@bitdefender.co.uk
Web: http://www.bitdefender.co.uk
Centrum podpory: http://www.bitdefender.co.uk/support/business.html

## Rumunsko

**BITDEFENDER SRL**
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (prodej&technická podpora): +40 21 2063470

Prodej: sales@bitdefender.ro
Web: http://www.bitdefender.ro
Centrum podpory: http://www.bitdefender.ro/support/business.html

## Spojené arabské emiráty

**Bitdefender FZ-LLC**
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (prodej&technická podpora): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Prodej: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrum podpory: http://www.bitdefender.com/support/business.html

# A. Dodatky

## A.1. Podporované typy souborů

Antimalwarové skenovací nástroje obsažené v bezpečnostních řešeních společnosti Bitdefender jsou schopné skenovat všechny typy souborů, které by mohly obsahovat hrozby. Seznamy níže zahrnují nejběžnější typy souborů, které jsou analyzovány.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo

## A.2. Objekty Sandbox Analyzeru

### A.2.1. Podporované typy souborů a přípony pro ruční odesílání

Následující přípony souborů jsou podporovány a mohou být ručně spuštěny v Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archiv), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, soubory MZ/PE (spustitelné), PDF, PEF (spustitelné), PIF (spustitelné), RTF, SCR, URL (binární), VBE, VBS, WSF, WSH, WSH-VBS, XHTML..

Sandbox Analyzer dokáže rozpoznat výše zmíněné typy souborů také, když jsou součástí archivů těchto typů: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, komprimovaný archiv LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (vícesvazkový), ZOO, XZ.

### A.2.2. Typy souborů podporované předfiltrováním obsahu při automatickém odesílání

Předběžné filtrování obsahu určí konkrétní typ souboru kombinací, která zahrnuje obsah a příponu objektu. To znamená, že spustitelný soubor, který má příponu .tmp, bude rozpoznán jako aplikace a pokud bude shledán podezřelým, bude odeslán do Sandbox Analyzer.

- Aplikace - soubory ve formátu PE32, včetně, ale bez omezení na následující přípony: exe, dll, com.
- Dokumenty - soubory ve formátu dokumentu, včetně následujících přípon: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm , dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.

- Skripty: `ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.`
- Archivy: `zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.`
- E-maily (uložené v systému souborů): `eml, tnef.`

### A.2.3. Výchozí vyloučení při automatickém odesílání

`asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.`

### A.2.4. Doporučené použití pro detonační VMs

Sandbox Analyzer On-Premises vyžaduje, aby byly na detonační virtuální stroje nainstalovány určité aplikace, aby otevřely odeslané vzorky.

| Aplikace | Soubory |
|---|---|
| Microsoft Office suite | xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx |
| Adobe Flash Player | swf |
| Adobe Acrobat Reader | pdf |
| Výchozí nastavení systému Windows | bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif |
| 7zip<br>WinZip<br>WinRAR | 7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue |
| Google Chrome<br>Internet Explorer | html, url |
| Python | py, pyc, pyp |
| Mozilla Thunderbird<br>Microsoft Outlook | eml |

## A.3. Jádra podporovaná senzorem Incidenty

Senzor Incidenty podporuje následující jádra: