Bitdefender

GravityZone

GHID DE INSTALARE

Bitdefender GravityZone
Ghid de Instalare

Publicat 2021.01.13

Termeni legali

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor

Cuprins

Prefață

Acest ghid este destinat administratorilor IT responsabili pentru instalarea protecției GravityZone la sediul organizației lor. Managerii IT în căutare de informații despre GravityZone pot găsi în acest ghid cerințele GravityZone și modulele de protecție disponibile.

Scopul acestui document este de a explica modul de instalare și configurare a soluției GravityZone și a agenților de securitate ai acesteia pe toate tipurile de stații de lucru din compania dumneavoastră.

1. Convenții utilizate în ghid

Convenții tipografice

Acest ghid folosește mai multe stiluri de text pentru o lizibilitate îmbunătățită. Aflați mai multe despre aspectul și însemnătatea acestora din tabelul de mai jos.

Aspect	Descriere
`mostră`	Numele de comenzi inline, sintaxele, căile și numele de fișiere, output-urile fișierelor de configurare și textele de intrare sunt tipărite cu caractere de tip `monospațiat`.
http://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
gravityzone-docs@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
„Prefață” (p. viii)	Acesta este un link intern, către o locație din document.
opțiune	Toate opțiunile produsului sunt tipărite cu caractere **bold**.
cuvânt cheie	Opțiunile de interfață, cuvintele cheie sau scurtăturile sunt evidențiate cu ajutorul caracterelor **aldine**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Notă

Nota nu este decât o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect asemănător.

Important

Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate informații importante, dar care nu sunt critice.

Avertisment

Este vorba de informații cruciale, cărora trebuie să le acordați o mare atenție. Dacă urmați indicațiile, nu se va întâmpla nimic rău. Este indicat să citiți și să înțelegeți despre ce este vorba, deoarece este descris ceva extrem de riscant.

1. DESPRE GRAVITYZONE

GravityZone este o soluție de securitate pentru companii, construită de la bun început pentru mediul de virtualizare și cloud pentru a oferi servicii de securitate pentru stațiile de lucru fizice, dispozitive mobile și mașinile virtuale din cloud-ul privat, public și serverele de e-mail Exchange.

GravityZone este un produs prevăzut cu o consolă de administrare unică, disponibilă în cloud, găzduită de Bitdefender, sau ca aplicație virtuală ce se instalează la sediul companiei și asigură un punct unic pentru configurarea, aplicarea și administrarea politicilor de securitate pentru un număr nelimitat de stații de lucru de orice tip, indiferent de locul în care se află.

GravityZone oferă mai multe niveluri de securitate pentru stațiile de lucru și pentru serverele de e-mail Microsoft Exchange: antimalware cu monitorizarea comportamentului, protecția contra amenințărilor în ziua zero, controlul aplicațiilor și sandboxing, firewall, controlul dispozitivelor, controlul conținutului, anti-phishing și antispam.

2. STRATURI DE PROTECȚIE GRAVITYZONE

GravityZone oferă următoarele straturi de protecție:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Anti-Exploit avansat
- Firewall
- Content Control
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Application Control
- Sandbox Analyzer
- Soluție EDR (Endpoint Detection and Response)
- Hypervisor Memory Introspection (HVI)
- Network Traffic Security Analytics (NTSA)
- Security for Storage
- Security for Mobile

2.1. Antimalware

Nivelul de protecție antimalware se bazează pe scanarea semnăturilor și analiza euristică (B-HAVE, ATC) împotriva: virușilor, troienilor, atacurilor de tip worm, spyware, adware, keylogger, rootkit și alte tipuri de software periculos

Tehnologia de scanare antimalware a Bitdefender se bazează pe următoarele tehnologii:

- În primul rând, se folosește o metodă de scanare tradițională acolo unde conținutul se potrivește cu baza de date de semnături. Baza de date de semnături conține modele de bytes specifice amenințărilor cunoscute și este actualizată în mod regulat de Bitdefender. Această metodă de scanare este eficientă împotriva amenințărilor confirmate care au fost cercetate și documentate. Cu toate acestea, indiferent cât de prompt este actualizată baza de date, există întotdeauna o fereastră de vulnerabilitate între momentul când se descoperă o nouă amenințare și momentul lansării unei remedieri..

- Împotriva amenințărilor noi și nedocumentate, se asigură un al doilea strat de protecție de către **B-HAVE**, motorul euristic al Bitdefender. Algoritmii euristici detectează programele malware pe baza caracteristicilor comportamentale. B-HAVE execută fișierele suspecte într-un mediu virtual pentru a testa impactul acestora asupra sistemului și pentru a se asigura că nu prezintă o amenințare. Dacă se detectează o amenințare, se blochează executarea programului.

Motoare de scanare

Bitdefender GravityZone poate configura automat motoarele de scanare la crearea pachetelor de agenți de securitate, în funcție de configurația endpointului.

Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

1. **Scanare locală**, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având conținutul de securitate stocat local.
2. **Scanarea hibrid cu motoare light (Cloud public)**, cu o amprentă medie, folosind scanarea în cloud și, parțial, conținut de securitate. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
3. **Scanarea centralizată în cloud-ul public sau privat**, cu o amprentă redusă care necesită un Security Server pentru scanare. În acest caz, nu se stochează local niciun conținut de securitate, iar scanarea este transferată către Security Server.

   Notă
   Există un set minim de motoare stocate local, care sunt necesare pentru despachetarea fișierelor arhivate.

4. **Scanare centralizată (cloud public sau privat cu Security Server) cu fallback* pe Scanare locală (motoare full)**
5. **Scanare centralizată (Scanare în cloud public sau privat cu Security Server) cu fallback* pe Scanare hibrid (cloud public cu motoare light)**

* Atunci când se folosește scanarea cu motoare duble, dacă primul motor este indisponibil, se va folosi motorul de rezervă (fallback). Consumul de resurse și gradul de utilizare a rețelei vor depinde de motoarele folosite.

2.2. Advanced Threat Control

Pentru amenințări care scapă chiar și de motorul euristic, este prezent un alt strat de protecție sub forma unei funcții Advanced Threat Control (ATC).

Advanced Threat Control monitorizează în mod continuu procesele în curs și cataloghează comportamentele suspecte, precum tentativele de: deghizare a tipului de proces, executare de cod în spațiul altui proces (furtul de memorie a procesului pentru escaladarea drepturilor), reproducerea, eliminarea fișierelor, ascunderea de aplicațiile de enumerare a proceselor etc. Fiecare comportament suspect duce la creșterea punctajului acordat proceselor. Atunci când se atinge un prag, se declanșează alarma.

2.3. HyperDetect

Bitdefender HyperDetect este un strat suplimentar de securitate conceput special pentru a detecta atacurile avansate și activitățile suspecte în faza de pre-execuție. HyperDetect conține modele de învățare automată (machine learning) și tehnologii de detectare a atacurilor ascunse pentru combaterea amenințărilor precum: atacuri de tip „zero-day", amenințări persistente avansate (APT), malware ascuns, atacuri fără fișiere (utilizarea necorespunzătoare a PowerShell, Windows Management Instrumentation etc.), furtul de date de autentificare, atacuri targetate, malware personalizat, atacuri bazate pe scripturi, exploit-uri, instrumente de hacking, trafic suspect în rețea, aplicații potențial nedorite (PUA), ransomware.

2.4. Anti-Exploit avansat

Având la bază tehnologia de învățare automată (machine learning), tehnologia proactivă de Anti-Exploit Avansat oprește atacurile de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive. Modulul Anti-exploit avansat depistează în timp real cele mai recente exploit-uri și diminuează vulnerabilitățile de corupere a memoriei care pot trece nedetectate de către alte soluții de securitate. Protejează aplicațiile utilizate cel mai frecvent, cum ar fi browser-ele, Microsoft Office sau Adobe Reader, precum și alte aplicații la care vă puteți gândi. Veghează asupra proceselor de sistem și protejează împotriva breșelor de securitate și a furturilor din procesele existente.

2.5. Firewall

Firewall-ul controlează accesul aplicațiilor la rețea și internet. Accesul este permis automat pentru o bază de date cuprinzătoare de aplicații cunoscute și sigure. În plus, firewall-ul poate proteja sistemul împotriva scanărilor de porturi, poate restricționa ICS și poate emite avertizări atunci când la o conexiune Wi-Fi se adaugă noi noduri.

2.6. Content Control

Modulul de control al conținutului susține aplicarea politicilor companiei privind traficul permis, accesul la internet, protecția datelor și controlul aplicațiilor. Administratorii pot defini opțiunile de scanare a traficului și excepțiile, pot stabili un program pentru accesul la internet, blocând anumite categorii web sau URL-uri, pot configura regulile de protecție a datelor și pot defini drepturile pentru utilizarea anumitor aplicații.

2.7. Network Attack Defense

Modulul de protecție Network Attack Defense se bazează pe o tehnologie Bitdefender ce vizează detectarea atacurilor din rețea concepute pentru a obține acces la endpoint-uri folosind tehnici specifice, cum ar fi: atacuri de tip „brute force”, exploit-uri la nivel de rețea, furt de parole, vectori de infectare drive-by-download, bot-uri și troieni.

2.8. Administrarea patch-urilor

Complet integrat în GravityZone, Patch Management menține actualizate sistemele de operare și aplicațiile software și oferă o imagine completă asupra stării de aplicare a patch-urilor pe stațiile de lucru administrate, cu sistem de operare Windows.

Modulul GravityZone Patch Management include mai multe funcții, cum ar fi scanarea la cerere / programată a patch-urilor, instalarea automată / manuală a patch-urilor sau raportarea patch-urilor absente.

Puteți afla mai multe despre distribuitorii autorizați și produsele compatibile cu GravityZone Patch Management din acest articol KB.

Notă
Patch Management este un add-on disponibil cu cheie de licență separată pentru toate pachetele GravityZone.

2.9. Device Control

Modulul Control dispozitiv împiedică scurgerile de date confidențiale și infecțiile cu malware folosind dispozitive externe atașate endpoint-ului, prin aplicarea unor reguli și excepții de blocare prin intermediul politicilor, pentru o gamă largă de tipuri de dispozitive (cum ar fi unități de stocare flash USB, dispozitive Bluetooth, CD/DVD playere, dispozitive de stocare etc.).

2.10. Full Disk Encryption

Acest strat de protecție vă permite să asigurați caracteristica Full Disk Encryption pe endpoint-uri, gestionând funcția BitLocker pe Windows și funcțiile FileVault și diskutil pe macOS. Puteți cripta și decripta volume boot și non-boot, cu doar câteva clicuri, în timp ce GravityZone gestionează întregul proces, cu intervenție minimă din partea utilizatorilor. În plus, GravityZone stochează codurile de recuperare necesare pentru a debloca volumele atunci când utilizatorii își uită parolele.

Notă
Full Disk Encryption este un add-on disponibil cu o cheie de licență separată pentru toate pachetele GravityZone disponibile.

2.11. Security for Exchange

Bitdefender Security for Exchange asigură protecție antimalware, antispam, antiphising, filtrare a conținutului și a fișierelor atașate, toate acestea complet integrate cu server-ul Microsoft Exchange, pentru a asigura un mediu securizat de comunicare prin mesaje și o productivitate sporită. Folosind tehnologiile antimalware și antispam premiate, aceasta protejează utilizatorii Exchange împotriva celor mai noi și mai sofisticate programe malware, precum și împotriva tentativelor de furt al datelor confidențiale sau valoroase ale utilizatorilor.

Important
Security for Exchange este proiectat pentru a proteja întreaga organizație Exchange de care aparține serverul Exchange protejat. Aceasta înseamnă că protejează toate căsuțele de e-mail active, inclusiv căsuțele de e-mail de tip user (utilizator) / room (cameră)/ equipment (echipament) / shared (partajat).

În plus față de protecția Microsoft Exchange, licența acoperă și modulele de protecție pentru stații de lucru instalate pe server.

2.12. Application Control

Modulul Control aplicații previne atacurile malware și de tip „ziua zero” și sporește securitatea fără a avea un impact asupra productivității. Modulul Control aplicații pune în aplicare politici flexibile de trecere în lista albă de aplicații, care identifică și previn instalarea și executarea oricăror aplicații nedorite, nesigure sau periculoase.

2.13. Sandbox Analyzer

Bitdefender Sandbox Analyzer oferă un nivel puternic de securitate împotriva amenințărilor avansate prin efectuarea unei analize automate și detaliate a fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender. Sandbox-ul utilizează o serie de tehnologii Bitdefender pentru a executa payload-uri într-un mediu virtual închis găzduit de Bitdefender sau instalat la nivel local, pentru a analiza comportamentul acestora și raporta orice schimbări subtile aduse sistemului, care semnalează intenții periculoase.

Sandbox Analyzer utilizează o serie de senzori pentru a detona conținut din endpoint-uri administrate, fluxuri ale traficului de endpoint rețea, carantină centralizată și servere ICAP (Internet Content Adaptation Protocol).

În plus, Sandbox Analyzer permite trimiterea manuală a mostrelor și prin API.

Notă
Această funcționalitate a modulului poate fi furnizată de Sandbox Analyzer Cloud și Sandbox Analyzer On-Premises. Sandbox Analyzer On-Premises este disponibil cu o cheie de licență separată.

2.14. Incidente

Caracteristica Incidente este o componentă de corelare a evenimentelor, capabilă să identifice amenințările avansate sau atacurile în curs de desfășurare. Ca parte a platformei noastre complete și integrate de protecție pentru endpoint-uri, caracteristica Incidente reunește informațiile despre dispozitive din întreaga rețea a companiei dumneavoastră. Această soluție vine în ajutorul eforturilor echipelor dumneavoastră responsabile cu răspunsul la incidente pentru a investiga și a reacționa la amenințări avansate.

Prin intermediul Bitdefender Endpoint Security Tools, puteți activa un modul de protecție numit Senzor de incidente pe endpoint-urile administrate, pentru a aduna date despre hardware și sistemul de operare. Respectând un cadru de lucru client-server, metadatele sunt colectate și procesate de ambele părți.

Această componentă aduce informații detaliate cu privire la incidentele detectate, o hartă interactivă a incidentelor, acțiuni de remediere și integrare cu Sandbox Analyzer și HyperDetect.

2.15. Hypervisor Memory Introspection (HVI)

Este cunoscut faptul că hackerii foarte bine organizați și orientați către profit caută vulnerabilități necunoscute (vulnerabilități de tip ziua zero) sau utilizează tehnici de exploatare concepute special, pentru utilizare unică (exploatări de tip ziua zero) și alte instrumente. De asemenea, hackerii folosesc tehnici avansate pentru a întârzia și structura succesiv sarcinile de atac în vederea mascării activității periculoase. Atacurile mai noi, orientate către profit, sunt concepute pentru a nu fi detectate și pentru a învinge instrumentele de securitate tradiționale.

Pentru mediile virtualizate, problema este acum soluționată, HVI protejând centre de date cu o densitate mare de mașini virtuale împotriva amenințărilor avansate și sofisticate, pe care motoarele pe bază de semnături nu le pot învinge. Aceasta susține o izolare puternică, asigurând detecția în timp real a atacurilor, blocându-le pe măsură ce apar și eliminând amenințările imediat.

Indiferent că mașina protejată este Windows sau Linux, server sau desktop, HVI oferă informații la un nivel imposibil de atins din sistemul de operare găzduit. Așa cum hypervisorul controlează accesul la hardware în numele fiecărei mașini virtuale găzduite, HVI cunoaște foarte bine memoria sistemelor găzduite atât în modul de utilizator, cât și în modul kernel. Rezultatul este că HVI are informații complete despre memoria sistemului găzduit și, prin urmare, deține întregul context. În același timp, HVI este izolată de sistemele găzduite protejate, așa cum este izolat și hypervisor-ul. Prin operarea la nivel de hypervisor și valorificarea funcționalităților acestuia, HVI depășește provocările tehnice ale securității tradiționale pentru a evidenția activități periculoase în centrele de date.

HVI identifică tehnicile de atac mai degrabă decât tiparele de atac. Astfel, această tehnologie poate identifica, raporta și preveni tehnicile de exploatare obișnuite. Kernel-ul este protejat împotriva tehnicilor rootkit folosite în timpul procesului de oprire a atacurilor pentru a împiedica detectarea. Procesele din modul de utilizator sunt protejate și împotriva injectării de cod, redirecționării funcțiilor și executării de cod din stivă sau segment.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

2.16. Network Traffic Security Analytics (NTSA)

Bitdefender Network Traffic Security Analytics (NTSA) este o soluție de securitate pentru rețea, care analizează traficul IPFIX pentru a depista prezenta oricărui comportament periculos sau a unor programe malware.

Bitdefender NTSA este menit să acționeze în completarea măsurilor dvs. de securitate existente, ca protecție complementară, capabilă să acopere punctele oarbe pe care soluțiile tradiționale nu le monitorizează.

Instrumentele tradiționale de securitate pentru rețea încearcă, în general, să prevină infectarea cu malware analizând traficul de intrare (prin sandbox, firewall-uri, antivirus etc.). Bitdefender NTSA se concentrează exclusiv pe monitorizarea traficului de ieșire din rețea pentru a depista eventualele semne de comportament rău-intenționat.

2.17. Security for Storage

GravityZone Security for Storage oferă protecție în timp real pentru principalele sisteme de partajare a fișierelor și stocare în rețea. Actualizările de sistem și ale algoritmului de detectare a amenințărilor se efectuează automat, fără niciun efort din partea dvs. și fără a determina întreruperea lucrului pentru utilizatorii finali.

Două sau mai multe GravityZone Security Server multi-platformă funcționează ca server ICAP, furnizând servicii antimalware către dispozitivele de tip NAS (Network-Attached Storage) și sistemele de partajare de fișiere în conformitate cu protocolul ICAP (Internet Content Adaptation Protocol, așa cum este acesta definit în RFC 3507).

Atunci când un utilizator solicită deschiderea, citirea, scrierea sau închiderea unui fișier de pe un laptop, o stație de lucru, un telefon mobil sau un alt dispozitiv, clientul ICAP (NAS sau sistem de partajare de fișiere) transmite o solicitare de scanare către Security Server și primește un verdict referitor la fișier. În funcție de rezultat, Security Server permite, respinge accesul sau șterge fișierul.

Notă
Acest modul este un add-on disponibil în baza unui cod de licență separat.

2.18. Security for Mobile

Combină securitatea la nivel de companie cu funcțiile de administrare și control al conformității din iPhone, iPad și dispozitivele Android oferind un software fiabil și o distribuire a actualizărilor prin intermediul magazinelor de aplicații Apple sau Android. Soluția a fost proiectată pentru a permite adoptarea controlată a inițiativelor de tip bring-your-own-device (BYOD) prin aplicarea unor politici de utilizare în mod consecvent pe toate dispozitivele mobile. Funcțiile de securitate includ blocarea ecranului, controlul autentificării, locația dispozitivului, ștergerea de la distanță, detecția dispozitivelor rootate sau decodate și a profilurilor de securitate. Pe dispozitivele Android, nivelul de securitate este îmbunătățit prin funcțiile de scanare în timp real și criptare pentru dispozitive de stocare mobile. Drept rezultat, dispozitivele mobile sunt controlate, iar informațiile confidențiale ale companiei existente pe acestea sunt protejate.

2.19. Disponibilitatea straturilor de protecție GravityZone

Disponibilitatea nivelurilor de protecție GravityZone diferă în funcție de sistemul de operare al stației de lucru. Pentru a afla mai multe, consultați articolul KB Disponibilitatea nivelurilor de protecție GravityZone.

3. ARHITECTURA GRAVITYZONE

Arhitectura unică a GravityZone permite soluției scalarea cu ușurință și în siguranță a unui număr nelimitat de sisteme. GravityZone poate fi configurat astfel încât să folosească mai multe aplicații virtuale și mai multe instanțe cu roluri specifice (Bază de date, Server de comunicații, Server de actualizări și Consolă web) pentru a asigura fiabilitatea și scalabilitatea.

Fiecare instanță a rolului poate fi instalată pe o altă aplicație. Funcțiile integrate de echilibrare a rolurilor se asigură că instalarea GravityZone protejează chiar și cele mai mari rețele corporative fără a cauza încetiniri sau blocaje. De asemenea, în locul funcțiilor de echilibrare integrate se poate folosi software-ul sau hardware-ul existent de echilibrare a sarcinilor, dacă acestea sunt prezente în rețea.

Livrat într-un container virtual, GravityZone poate fi importat pentru a rula pe orice platformă de virtualizare, inclusiv VMware, Citrix, Microsoft Hyper-V, Nutanix Prism, Microsoft Azure.

Integrarea cu VMware vCenter, Citrix XenServer, Microsoft Active Directory și Nutanix Prism Element si Microsoft Azure reduce efortul de instalare a protecției pentru stațiile de lucru fizice și virtuale.

Soluția GravityZone include următoarele componente:

- Aplicația virtuală GravityZone
- Security Server
- Pachet suplimentar HVI
- Agenți de securitate

3.1. VA GravityZone

Soluția locală a GravityZone este livrată sub forma unei aplicații virtuale (VA) Linux Ubuntu consolidate și auto-configurabile, integrate într-o imagine de mașină virtuală, ușor de instalat și configurat prin intermediul unei interfețe CLI (Command Line Interface). Aplicația virtuală este disponibilă în mai multe formate, compatibilă cu principalele platforme de virtualizare (OVA, XVA, VHD, OVF, RAW).

3.1.1. Baza de date GravityZone

Logica de bază a arhitecturii GravityZone. Bitdefender folosește o bază de date non-relațională MongoDB, ușor de scalat și reprodus.

3.1.2. Server de actualizări GravityZone

Serverul de actualizări joacă un rol important de actualizare a soluției GravityZone și a agenților pentru stațiile de lucru prin reproducerea și publicarea pachetelor necesare sau a fișierelor de instalare.

3.1.3. Serverul de comunicații GravityZone

Serverul de comunicații este legătura dintre agenții de securitate și baza de date, transferând politicile și sarcinile de securitate către stațiile de lucru protejate, precum și evenimentele raportate de agenții de securitate.

3.1.4. Serverul de incidente GravityZone

Serverul de incidente reprezintă legătura dintre agenții de securitate și baza de date, colectând date de pe endpoint-uri și generând incidente în funcție de amenințările detectate de tehnologiile de prevenție și algoritmii de învățare automată.

3.1.5. Consola web (GravityZone Control Center)

Soluțiile de securitate Bitdefender sunt gestionate dintr-un punct unic de administrare, consola web Control Center. Aceasta asigură administrarea și accesarea cu mai multă ușurință a stării de de securitate generale, a amenințărilor de securitate globale și a controlului asupra tuturor modulelor de securitate care protejează stațiile de lucru, serverele fizice sau virtualizate, precum și dispozitivele mobile. Bazată pe arhitectura Gravity, Control Center poate acoperi chiar și necesitățile celor mai mari organizații.

Control Center se integrează cu sistemele existente de administrare și monitorizare, pentru a facilita aplicarea automată a protecției pe stațiile de lucru, serverele sau dispozitivele mobile neadministrate care apar în Microsoft Active Directory, VMware vCenter, Nutanix Prism Element sau Citrix XenServer, sau care sunt detectate pur și simplu în rețea.

3.2. Security Server

Security Server este o mașină virtuală dedicată, care anulează duplicatele și centralizează majoritatea funcționalităților antimalware ale agenților de securitate, acționând ca server de scanare.

Există trei versiuni de Security Server, pentru fiecare tip de mediu de virtualizare:

- **Security Server for VMware NSX.** Această versiune se instalează automat pe fiecare gazdă din clusterul pe care a fost instalat Bitdefender.
- **Security Server pentru VMware vShield Endpoint.** Această versiune trebuie să fie instalată pe fiecare gazdă care necesită protecție.
- **Security Server Multi-platformă.** Această versiune este dedicată unor diferite tipuri de medii de virtualizare și trebuie să fie instalată pe una sau mai multe gazde astfel încât să acopere numărul de mașini virtuale protejate. Dacă folosiți HVI, trebuie să instalați un Security Server pee ficare gazdă pe care se află mașini virtuale care trebuie protejate.

3.3. Pachet suplimentar HVI

Pachetul HVI asigură legătura dintre hypervisor și Security Server de pe gazda respectivă. Astfel, Security Server poate monitoriza memoria utilizată pe gazda pe care este instalat, pe baza politicilor de securitate GravityZone.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

3.4. Agenți de securitate

Pentru a proteja rețeaua cu Bitdefender, trebuie să instalați agenții de securitate GravityZone corespunzători pe stațiile de lucru din rețea.

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

3.4.1. Bitdefender Endpoint Security Tools

GravityZone asigură protecția mașinilor Windows și Linux, fizice sau virtuale, cu Bitdefender Endpoint Security Tools, un agent de securitate inteligent, care ține cont de mediu și care se adaptează în funcție de tipul stației de lucru. Bitdefender Endpoint Security Tools poate fi instalat pe orice mașină, virtuală sau fizică, asigurând un sistem de scanare flexibil, fiind alegerea ideală pentru mediile mixte (fizice, virtuale și în cloud).

Pe lângă protecția sistemului de fișiere, Bitdefender Endpoint Security Tools include și protecția serverului e-mail pentru Serverele Microsoft Exchange.

Bitdefender Endpoint Security Tools folosește un singur model de politică pentru mașinile fizice și virtuale, precum și o singură sursă pentru kit-ul de instalare pentru toate mediile (fizice ori virtuale) care rulează sistemul de operare Windows.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Bitdefender Endpoint Security Tools:

- Antimalware
- Advanced Threat Control
- HyperDetect
- Firewall
- Content Control
- Network Attack Defense
- Administrarea patch-urilor
- Device Control
- Full Disk Encryption
- Security for Exchange
- Sandbox Analyzer
- Application Control

Roluri ale stațiilor de lucru

- Utilizator privilegiat
- Relay
- Server de cache pentru patch-uri
- Protecție Exchange

Utilizator privilegiat

Administratorii Control Center pot acorda drepturi de Utilizator privilegiat utilizatorilor de stații de lucru prin intermediul setărilor politicii de securitate. Modulul Utilizator privilegiat activează drepturile de administrare la nivel de utilizator, permițând utilizatorului stației de lucru să acceseze și să modifice setările de securitate prin intermediul unei console locale. Control Center primește o notificare atunci când o stație de lucru este în modul Utilizator privilegiat, iar administratorul Control Center poate suprascrie oricând setările de securitate locale.

Important
Acest modul este disponibil numai pentru sistemele de operare pentru desktop și server Windows suportate. Pentru mai multe informații, consultă capitolul „Sisteme de operare suportate” (p. 28).

Relay

Agenții pentru stațiile de lucru cu rol de Bitdefender Endpoint Security Tools Relay sunt folosiți ca servere de comunicații proxy și actualizări pentru alte stații de lucru din rețea. Agenții pentru stațiile de lucru cu rol de relay sunt necesari în special pentru organizațiile cu rețele izolate, unde întregul trafic se desfășoară printr-un singur punct de acces.

În companiile cu rețele mari distribuite, agenții de tip relay ajută la scăderea gradului de utilizare a lățimii de bandă, prevenind conectarea stațiilor de lucru protejate și a serverelor de securitate direct la aplicația GravityZone.

După ce în rețea a fost instalat un agent Bitdefender Endpoint Security Tools Relay, celelalte stații de lucru pot fi configurate prin intermediul politicii pentru a comunica cu Control Center prin agentul de tip relay.

Agenții Bitdefender Endpoint Security Tools Relay sunt utilizați în următoarele scopuri:

- Descoperirea tuturor stațiilor de lucru neprotejate din rețea.
- Instalarea agentului pentru stații de lucru în rețeaua locală.
- Actualizarea stațiilor de lucru protejate din rețea.
- Asigurarea comunicării între Control Center și stațiile de lucru conectate.
- Acționarea ca server proxy pentru stațiile de lucru protejate.
- Optimizarea traficului în rețea în timpul actualizărilor, instalărilor, scanărilor și al altor sarcini consumatoare de resurse.

Server de cache pentru patch-uri

Stațiile de lucru cu rol de releu pot funcționa și ca server de cache pentru patch-uri. Având activat acest rol, releele sunt folosite pentru stocarea patch-urilor descărcate de pe site-urile producătorilor de software și distribuirea lor pe stațiile de lucru din rețeaua dumneavoastră. De fiecare dată când o stație de lucru conține software cu patch-uri lipsă, acesta le ia de pe server și nu de pe site-ul producătorului, optimizând astfel traficul generat și gradul de ocupare a lățimii de bandă a rețelei.

Important
Acest rol suplimentar este disponibil cu un add-on Patch Management înregistrat.

Protecție Exchange

Bitdefender Endpoint Security Tools cu rolul de Exchange poate fi instalat pe serverele Microsoft Exchange cu scopul de a proteja utilizatorii Exchange de amenințările transmise prin e-mail.

Bitdefender Endpoint Security Tools cu rolul Exchange protejează atât serverul cât și soluția Microsoft Exchange.

3.4.2. Endpoint Security for Mac

Endpoint Security for Mac este un agent de securitate conceput pentru a proteja stațiile de lucru și laptopurile Macintosh cu tehnologie Intel. Technologia de scanare disponibilă este **Scanare localizată**, având conținut de securitate stocat local.

Straturi de protecție

Următoarele straturi de protecție sunt disponibile în cadrul Endpoint Security for Mac:

- Antimalware
- Advanced Threat Control
- Content Control
- Device Control
- Full Disk Encryption

3.4.3. GravityZone Mobile Client

GravityZone Mobile Client extinde politicile de securitate cu ușurință pe un număr nelimitat de dispozitive Android și iOS, protejându-le împotriva utilizării neautorizate, a riscurilor și pierderii de date confidențiale. Funcțiile de securitate includ blocarea ecranului, controlul autentificării, locația dispozitivului, ștergerea de la distanță, detecția dispozitivelor rootate sau decodate și a profilurilor de securitate. Pe dispozitivele Android, nivelul de securitate este îmbunătățit prin funcțiile de scanare în timp real și criptare pentru dispozitive de stocare mobile.

GravityZone Mobile Client este distribuit exclusiv prin Apple App Store și Google Play.

3.4.4. Bitdefender Tools (vShield)

Bitdefender Tools este un agent care necesită puțin spațiu pentru mediile virtuale VMware integrate cu terminalul vShield. Agentul de securitate se instalează pe

mașinile virtuale protejate cu Security Server, pentru a vă permite să profitați de funcțiile suplimentare pe care le oferă:

- Vă permite să rulați sarcinile Memory și Process Scan pe mașină.
- Informează utilizatorul cu privire la infestările detectate și măsurile luate pentru eliminarea acestora.
- Adaugă mai multe opțiuni pentru excepțiile la scanările antimalware.

3.5. Architectura Sandbox Analyzer

Bitdefender Sandbox Analyzer oferă un strat puternic de protecție împotriva amenințărilor avansate, efectuând analize automate în profunzime asupra fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender.

Sandbox Analyzer este disponibil în două variante:

- Sandbox Analyzer Cloud, găzduit de Bitdefender.
- Sandbox Analyzer On-Premises, disponibil ca aplicație virtuală care poate fi instalată local.

Sandbox Analyzer Cloud

Sandbox Analyzer Cloud conține următoarele componente:

- **Sandbox Analyzer Portal** – un server de comunicare găzduit, utilizat pentru administrarea solicitărilor dintre stațiile de lucru și clusterul sandbox Bitdefender.
- **Sandbox Analyzer Cluster** – infrastructura sandbox găzduită, unde are loc analiza comportamentală a mostrelor. La acest nivel, fișierele încărcate sunt detonate pe mașini virtuale cu sistem de operare Windows 7.

GravityZone Control Center operează ca o consolă de administrare și raportare, unde puteți configura politicile de securitate, vizualiza rapoarte și notificări.

Bitdefender Endpoint Security Tools, agentul de securitate instalat pe endpoint-uri, acționează ca senzor de alimentare pentru Sandbox Analyzer.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises este livrat sub forma unei aplicații virtuale Linux Ubuntu integrată într-o imagine de mașină virtulă, ușor de instalat și configurat prin intermediul unei interfețe CLI (command-line interface). Sandbox Analyzer On-Premises este disponibil în format OVA și poate fi instalat pe VMWare ESXi.

O instanță Sandbox Analyzer On-Premises conține următoarele componente:

- **Sandbox Manager**. Această componentă coordonează sandbox-ul. Sandbox Manager se conectează la hypervisor-ul ESXi prin API și utilizează resursele hardware ale acestuia pentru crearea și operarea mediului de analiză a malware-ului.
- **Mașini virtuale de detonare**. Această componentă este reprezentată de mașini virtuale utilizate de Sandbox Analyzer pentru a executa fișierele și a analiza comportamentele acestora. Mașinile virtuale de detonare pot rula pe sisteme de operare Windows 7 și Windows 10 64-bit.

GravityZoneControl Center operează ca o consolă de administrare și raportare pe care o puteți utiliza pentru configurarea politicilor de securitate și vizualizarea de rapoarte și notificări.

Sandbox Analyzer On-Premises operează următorii senzori de alimentare:

- **Senzor endpoint**. Bitdefender Endpoint Security Tools pentru Windows îndeplinește rolul de senzor de alimentare instalat pe endpoint-uri. Agentul Bitdefender utilizează tehnologii avansate de învățare automată (machine learning) și algoritmi neurali de rețea pentru detectarea conținutului suspect și trimiterea acestuia către Sandbox Analyzer, inclusiv obiecte din carantina centralizată.
- **Senzor rețea**. Aplicația virtuală de securitate pentru rețea (NSVA) este o aplicație virtuală care poate fi instalată în același mediu virtualizat ESXi ca și instanța Sandbox Analyzer. Senzorul de rețea extrage conținut din fluxurile de rețea și îl trimite către Sandbox Analyzer.
- **Senzor ICAP**. Fiind instalat pe dispozitive NAS (network attached storage) utilizând protocolul ICAP, Bitdefender Security Server suportă trimiterea de conținut către Sandbox Analyzer.

În afară de acești senzori, Sandbox Analyzer On-Premises suportă trimiterea manuală și prin API. Pentru detalii, consultați capitolul **Utilizarea Sandbox Analyzer** din Ghidul administratorului GravityZone.

4. CERINȚE

Toate soluțiile GravityZone sunt instalate și gestionate din Control Center.

4.1. Aplicația virtuală GravityZone

4.1.1. Formate și platforme de virtualizare compatibile

GravityZone este livrată ca și aplicație virtuală (VA). Este disponibilă în următoarele formate, compatibile cu majoritatea platformelor de virtualizare frecvent utilizate:

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

*Pachetele OVF și RAW sunt arhivate în format tar.bz2.

Pentru compatibilitatea cu platforma Oracle virtualBox, consultați acest articol KB.

Suport pentru alte formate și platforme de virtualizare disponibil la cerere.

4.1.2. Hardware

Cerințele hardware pentru aplicația virtuală GravityZone diferă în funcție de dimensiunea rețelei și de arhitectură aleasă. Pentru rețele de până la 3000 de terminale, puteți alege si instala toate rolurile GravityZone pe o singură aplicație, în timp ce pentru rețelele mai mari, trebuie să aveți în vedere distribuirea rolurilor între mai multe aplicații. Resursele necesare aplicației depind de rolurile pe care le instalați pe aceasta și de măsura în care utilizați sau nu Setul de replicare.

Notă
Setul de replicare este o funcție MongoDB care stochează replicările bazei de date și asigură redundanța și disponibilitatea crescută a datelor stocate. Pentru detalii, consultați Documentația MongoDB și „Gestionarea aplicației GravityZone” (p. 106).

Bitdefender HVI necesită, de asemenea, un volum semnificativ de resurse. Dacă utilizați acest serviciu, vă rugăm să consultați tabelele cu date specifice. Pentru informații privind cerințele complete ale serviciului, consultați „HVI” (p. 49).

Important
Măsurătorile sunt un rezultat al testelor interne ale Bitdefender, pornind de la o configurație GravityZone de bază și de la utilizarea regulată. Rezultatele pot diferi în funcție de configurația rețelei, de software-ul instalat, de numărul de evenimente generate, etc. Pentru metrica de scalabilitate personalizate, contactați Bitdefender.

vCPU

Tabelul de mai jos vă informează cu privire la numărul de vCPU necesar fiecărei aplicații virtuale.

Fiecare vCPU trebuie să aibă o capacitate de minim 2GHz.

Componentă	Numărul (maxim) de stații de lucru							
	250	500	1000	3000	5000	10000	25000	50000
Funcțiile de bază GravityZone								
Server de actualizări*	10	14	16	18	4	4	6	8
Consolă web**					6	10	12	12
Server de comunicații					6	10	12	18
Baza de date***					6	6	9	12
Server incidente					4	4	6	6
Total	**10**	**14**	**16**	**18**	**26**	**34**	**45**	**56**
GravityZone cu Bitdefender HVI								
Server de actualizări*	10	4	4	4	4	4	6	8
Consolă web**		6	8	8	10	10	12	12
Server de comunicații		6	8	8	10	10	16	20
Baza de date***		6	6	6	6	6	9	12
Server incidente		2	2	2	4	4	6	6
Total	**10**	**24**	**28**	**28**	**34**	**34**	**49**	**58**

* Recomandat dacă nu există Relee instalate.

** Pentru fiecare integrare activă, adăugați o vCPU pe aplicația virtuală cu rolul de Consolă web.
*** În cazul instalării distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

RAM (GB)

Componentă	Numărul (maxim) de stații de lucru							
	250	500	1000	3000	5000	10000	25000	50000
Funcțiile de bază GravityZone								
Server de actualizări	18	18	20	22	2	2	3	3
Consola web*					8	8	12	16
Server de comunicații					6	12	12	16
Baza de date**					8	10	12	12
Server incidente					2	2	4	4
Total	**18**	**18**	**20**	**22**	**26**	**34**	**43**	**51**
GravityZone cu Bitdefender HVI								
Server de actualizări	18	2	2	2	2	2	3	3
Consola web*		8	10	10	10	10	12	16
Server de comunicații		8	10	10	12	12	16	20
Baza de date**		8	8	8	8	12	12	12
Server incidente		2	2	2	2	2	4	4
Total	**18**	**28**	**32**	**32**	**36**	**40**	**47**	**55**

* Pentru fiecare integrare activă, adăugați un GB RAM pe aplicația virtuală cu rolul de Consolă web.
** În cazul unei instalări distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

Spațiu liber pe hard disk (GB)

Componentă	Numărul (maxim) de stații de lucru								
	250	250*	500	1000	3000	5000	10000	25000	50000
Funcțiile de bază GravityZone									
Server de actualizări	150	**190**	190	230	230	80	80	80	80
Consolă Web						80	80	80	80
Server de comunicații						80	80	80	80
Baza de date**						110	150	230	530
Total	**150**	**190**	**190**	**230**	**230**	**350**	**390**	**470**	**770**
GravityZone cu Bitdefender HVI									
Server de actualizări	150	190	80	80	80	80	80	80	80
Consolă Web			80	80	80	80	80	80	80
Server de comunicații			80	80	80	80	80	80	80
Baza de date**			110	110	130	130	190	330	730
Total	**150**	**190**	**350**	**350**	**370**	**370**	**430**	**570**	**970**

Important
Se recomandă utilizarea unor unități Solid-state (SSD).

* Spațiul suplimentar necesar pe SSD la alegerea instalării automate, deoarece instalează și Security Server. După finalizarea instalării, puteți dezinstala Security Server pentru a elibera spațiu pe disc.
** În cazul unei instalări distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

Notă
Este necesar pentru baza de date un spațiu suplimentar de cel puțin 30 GB, atunci când este instalat rolul de Server de incidente. Cantitatea de spațiu a fost deja adăugată rolului Bază de date, în tabelul de mai sus.

4.1.3. Conexiune Internet

Aplicația GravityZone necesită acces la Internet.

4.2. Control Center

Pentru a accesa consola web Control Center, sunt necesare:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 16+
- Rezoluție recomandată a ecranului: 1280 x 800 sau mai mare
- Calculatorul de pe care vă conectați trebuie să aibă conectivitate prin rețea la Control Center.

Avertisment
Control Center nu va funcționa/nu se va afișa corespunzător în Internet Explorer 9+ cu funcția Compatibility View activată, care este echivalentă cu utilizarea unei versiuni de browser incompatibile.

4.3. Protecția pentru endpoint-uri

Pentru a vă proteja rețeaua cu Bitdefender, este necesar să instalați agenții de securitate GravityZone pe stațiile de lucru din rețea. Pentru protecție optimizată, puteți instala, de asemenea, Security Server. În acest scop, aveți nevoie de un utilizator Control Center cu drepturi de administrator asupra serviciilor pe care trebuie să le instalați și asupra stațiilor de lucru din rețea pe care le administrați.

Cerințele pentru agentul de securitate sunt diferite, pornind de la existența rolurile existente pentru server, cum ar fi Releu, Protecția exchange sau Serverul de memorie cache pentru patch-uri. Pentru mai multe informații referitoare la rolurile agentului, consultați „Agenți de securitate” (p. 13).

4.3.1. Hardware

Agentul de securitate fără roluri

Uz procesor

Sistemele țintă	Tip CPU	Sisteme de operare (OS) compatibile
Stații de lucru	Procesoare compatibile cu Intel® Pentium, 2 GHz sau mai rapide	Sisteme de operare pentru desktop-urile care rulează Microsoft Windows.
	Intel® Core 2 Duo, 2 GHz sau mai rapid	macOS
Dispozitive inteligente	Procesoare compatibile cu Intel® Pentium, 800 MHZ sau mai rapide	OS incluse în Microsoft Windows
Servere	Cerințe minime: Procesoare compatibile Intel® Pentium, 2,4 GHz	OS Microsoft Windows Server și OS Linux
	Recomandat: CPU Intel® Xeon multi-core, 1,86 GHz sau mai rapidă	

Avertisment
Procesoarele ARM nu sunt compatibile în prezent.

Memorie RAM disponibilă

La instalare (MB)

SO	MOTOR SIMPLU					
	Scanare locală		Scanare hibrid		Scanare central.	
	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.
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

Pentru utilizare zilnică (MB)*

SO	Antivirus (motor simplu)			Module de protecție				
	Local	Hibrid	Centra-lizat	Scanare compor-tament	Firewall	Control conținut	Utilizator privilegiat	Server actualizări
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

* Evaluările acoperă utilizarea zilnică a clientului stației de lucru, fără a lua în considerare sarcinile suplimentare, cum ar fi scanările la cerere sau actualizările de produs.

Eliberează spațiu de pe disc

La instalare (MB)

SO	MOTOR SIMPLU						MOTOR DUBLU			
	Scanare locală		Scanare hibrid		Scanare central.		Scanare central. + locală		Scanare central. + hibrid	
	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.	Doar antiv.	Toate opț.
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Pentru utilizare zilnică (MB)*

SO	Antivirus (motor simplu)			Module de protecție				
	Local	Hibrid	Centra-lizat	Scanare compor-tament	Firewall	Control conținut	Utilizator privilegiat	Server actualizări
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

* Evaluările acoperă utilizarea zilnică a clientului stației de lucru, fără a lua în considerare sarcinile suplimentare, cum ar fi scanările la cerere sau actualizările de produs.

Agent de securitate cu rol de releu

Rolul de releu necesită resurse hardware suplimentare față de configurația de bază a agentului de securitate. Aceste cerințe trebuie să fie compatibile cu Serverul de actualizări și cu pachetele de instalare găzduite pe stația de lucru:

Număr de stații de lucru conectate	CPU compatibilă cu Serverul de actualizări	RAM	Spațiu liber pe hard disk pentru Serverul de actualizări
1-300	minim procesor Intel® Core™ i3 sau echivalent, 2 vCPU per nucleu	1.0 GB	10 GB
300-1000	minim procesor Intel® Core™ i5 sau echivalent, 4 vCPU per nucleu	1.0 GB	10 GB

Avertisment

- Procesoarele ARM nu sunt compatibile în prezent.
- Agenții de releu necesită discuri SSD, pentru a face față volumelor mari de operațiuni de citire/scriere.

Important

- Dacă doriți să salvați pachetele de instalare și actualizările pe o altă partiție decât cea pe care este instalat agentul, asigurați-vă că partițiile au spațiu liber suficient

pe hard disk (10 GB); în caz contrar, agentul va întrerupe instalarea. Acest lucru este necesar doar la instalare.

- Pe endpoint-urile Windows, este necesar ca link-urile din local spre local să fie activate.

Agent de securitate cu rol de protecție Exchange

În cazul Serverelor Exchange, carantina necesită spațiu suplimentar pe hard-disk, pe partiția pe care este instalat agentul de securitate.

Dimensiunea carantinei depinde de numărul de articole stocate și de dimensiunea acestora.

În mod implicit, agentul este instalat pe partiția sistemului.

Agent de securitate cu rol de server de memorie cache pentru patch-uri

Agentul cu rol de server de memorie cache pentru patch-uri trebuie să îndeplinească următoarele cerințe cumulate:

- Toate cerințele hardware pentru agentul simplu de securitate (fără roluri)
- Toate cerințele hardware ale rolului de Releu
- În plus, este necesar un spațiu liber pe hard disk de 100 GB pentru stocarea patch-urilor descărcate

Important
Dacă doriți să salvați patch-urile pe o altă partiție decât cea pe care este instalat agentul, asigurați-vă că ambele partiții au spațiu liber suficient pe hard disk (100 GB); în caz contrar, agentul va întrerupe instalarea. Acest lucru este necesar doar la instalare.

Cerințe pentru Mediile VMware vShield

Acestea sunt cerințele și amprenta Bitdefender Tools pentru sisteme integrate în medii VMware cu vShield Endpoint.

Platforma	RAM	Spațiu pe disc
Windows	6-16* MB (~ 10 MB pentru GUI)	24 MB
Linux	9-10 MB	10-11 MB

*5 MB dacă este activat Modul silențios și 10 MB dacă acesta este dezactivat. Dacă este activat Modul silențios, interfața grafică cu utilizatorul (GUI) Bitdefender Tools nu se încarcă automat la pornirea sistemului, eliberând resursele asociate.

4.3.2. Sisteme de operare suportate

Deskop Windows

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Actualizarea Windows 10 din 10 octombrie 2018 (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

Avertisment
(1) Asistența pentru platforma VMware vShield (versiunea fără agent) pentru Windows 8.1 (32/64 biți) este disponibilă începând cu VMware vSphere 5.5 – ESXi build 1892794 și versiunile ulterioare.
(2) În VMware NSX, sunt compatibile versiunile sistemelor de operare începând cu vSphere 5.5 Patch 2.
(3) În VMware NSX, sunt compatibile versiunile sistemelor de operare începând cu vSphere 5.5.

Avertisment
Bitdefender nu oferă compatibilitate cu build-urile Windows Insider Program.

Tabletă Windows și programe incluse

- 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

Server Windows

- 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)]

Avertisment

(1) Platforma VMware vShield (versiunea fără agent) este compatibilă cu Windows Server 2012 R2 (64 biți) începând cu VMware vSphere 5.5 – ESXi build 1892794 și versiunile ulterioare.
(2) În VMware NSX, sunt compatibile versiunile sistemelor de operare începând cu vSphere 5.5 Patch 2.
(3) În VMware NSX, sunt compatibile versiunile sistemelor de operare începând cu vSphere 5.5.
(4) VMware NSX nu este compatibil cu versiunile Windows 2012 pe 32 de biți și cu Windows Server 2008 R2.

Linux

Important
Endpoint-urile Linux folosesc licențe din numărul de licențe destinate sistemelor de operare tip server.

- Ubuntu 14.04 LTS sau mai recent
- Red Hat Enterprise Linux / CentOS 6.0 sau mai recent(2)
- SUSE Linux Enterprise Server 11 SP4 sau mai recent
- OpenSUSE Leap 42.x
- Fedora 25 sau mai recent(1)
- Debian 8.0 sau mai recent
- Oracle Linux 6.3 sau superior
- Amazon Linux AMI 2016.09 sau mai recent
- Amazon Linux 2

Avertisment
(1) Pe Fedora 28 și versiunile ulterioare, Bitdefender Endpoint Security Tools are nevoie de instalarea manuală a pachetului `libnsl`, prin executarea următoarei comenzi:

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

(2) Pentru instalările minime ale CentOS, Bitdefender Endpoint Security Tools are nevoie de instalarea manuală a pachetului `libnsl`, prin executarea următoarei comenzi:

```
sudo yum install libnsl
```

Cerințe preliminare privind Active Directory

La integrarea endpoint-urilor Linux cu un domeniu Active Directory prin System Security Services Daemon (SSSD), asigurați-vă că instrumentele **ldbsearch, krb5-user,** și **krb5-config** sunt instalate și că kerberos este configurat corespunzător.

```
/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
        }
```

Notă
Toate înregistrările sunt sensibile la grafia cu majuscule sau minuscule.

Compatibilitate cu scanarea la accesare

Scanarea la accesare este disponibilă pentru toate sistemele de operare găzduite acceptate. Pe sistemele Linux, asistența pentru scanarea la accesare este asigurată în următoarele situații:

Versiuni kernel	Distribuții Linux	Cerințe privind scanarea la accesare
2.6.38 sau mai recent*	Red Hat Enterprise Linux / CentOS 6.0 sau mai recent Ubuntu 14.04 sau mai recent SUSE Linux Enterprise Server 11 SP4 sau mai recent OpenSUSE Leap 42.x Fedora 25 sau mai recent Debian 9.0 sau mai recent Oracle Linux 6.3 sau superior Amazon Linux AMI 2016.09 sau mai recent	Trebuie să fie activată funcția (opțiunea kernel) **Fanotify**.
2.6.38 sau peste	Debian 8	**Fanotify** trebuie să fie activată și setată pe modul de aplicare, iar apoi trebuie recompilat pachetul kernel. Pentru detalii, consultați acest articol KB.

Versiuni kernel	Distribuții Linux	Cerințe privind scanarea la accesare
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender oferă asistență prin **DazukoFS** cu modulele pentru kernel precompilate.
Toate celelalte tipuri de kernel	Toate celelalte sisteme suportate	Modulul **DazukoFS** trebuie să fie compilat manual. Pentru mai multe detalii, vă rugăm consultați „Compilarea manuală a modulului DazukoFS” (p. 154).

* Cu anumite limitări, descrise mai jos.

Limitări privind scanarea la accesare

Versiuni kernel	Distribuții Linux	Detalii
2.6.38 sau peste	Toate sistemele compatibile	Scanarea la accesare monitorizează locațiile partajate în rețea numai în următoarele condiții: • Funcția **Fanotify** este activată atât pe sistemele de la distanță, cât și pe cele locale. • Partajarea se bazează pe sisteme de fișiere CIFS și NFS. **Notă** Scanarea la accesare nu scanează locații partajate în rețea montate prin SSH sau FTP.
Toate kernel-urile	Toate sistemele compatibile	Scanarea la accesare nu este suportată pe sistemele cu **DazukoFS** în cazul locațiilor partajate în rețea montate pe căi protejate deja de modulul de scanare la accesare.

Asistență Detecție și răspuns pentru stațiile de lucru (EDR - Endpoint Detection and Response)

Accesați această pagină web pentru o listă completă și actualizată a versiunilor de kernel și distribuții Linux care sunt compatibile cu Senzorul EDR.

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)

Modulul Control conținut nu este compatibil cu macOS Big Sur (11.0).

4.3.3. Sisteme de fișiere acceptate

Bitdefender se instalează pe și protejează următoarele sisteme de fișiere:

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

Notă
Opțiunea de scanare la accesare nu este disponibilă pentru NFS și CIFS/SMB.

4.3.4. Browsere compatibile

Securitatea pentru browser Endpoint este testată pentru compatibilitatea cu următoarele browsere:

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

4.3.5. Platforme de virtualizare suportate

Security for Virtualized Environments oferă asistență implicită pentru următoarele platforme de virtualizare:

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

  Notă
  Funcționalitatea de Gestionare a volumului de lucru în vSphere 7.0 nu este compatibilă.

- 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 (inclusiv Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp and 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 sau Windows Server 2008 R2, 2012, 2012 R2 (inclusiv Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (inclusiv KVM Hypervisor)
- Oracle VM 3.0
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism cu AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism cu AOS 5.6, 5.11 STS
- Nutanix Prism cu AHV 20170830.115, 20170830.301 și 20170830.395 Community Edition
- Nutanix Prism versiunea 2018.01.31 (Community Edition)

Notă
Suport pentru alte platforme de virtualizare disponibil la cerere.

Cerințe privind integrarea cu VMware NSX-V

- ESXi 5.5 sau mai recent pentru fiecare server
- vCenter Server 5.5 sau mai recent
- NSX Manager 6.2.4 sau mai recent
- VMware Tools 9.1.0 sau mai recent, cu agentul Guest Introspection.
  - Pentru mașinile virtuale Windows, consultați următorul articol din documentația VMware.
  - Pentru mașinile virtuale Linux, consultați următorul articol din documentația VMware.

Notă
VMware recomandă utilizarea următoarelor versiuni VMware Tools:
- 10.0.8 sau mai recent, pentru remedierea funcționării îngreunate a mașinilor virtuale după efectuarea upgrade-ului pentru VMware Tools în NSX / vCloud Networking and Security (Articol din baza de cunoștințe VMware 2144236).
- 10.0.9 sau mai recent pentru asistență Windows 10.

Important
Se recomandă să actualizați toate produsele VMware cu cel mai recent patch.

Cerințe de integrare cu VMware NSX-T Data Center

- VMware NSX-T Manager 2.4, 2.5 sau 3.0
- ESXi compatibil cu versiunea NSX-T Manager
- vCenter Server și vSphere compatibile cu versiunea NSX-T Manager
- Instrumente VMware cu agent Guest Introspection, cu impact redus asupra resurselor, compatibile cu versiunea NSX-T Manager

Pentru mai multe detalii de compatibilitate, consultați următoarele pagini web VMware:

- Ghid de compatibilitate VMware – GravityZone vs. NSX-T Manager
- Matrici de interoperabilitate pentru produsele VMware - NSX-T Data Center vs. VMware vCenter și VMware Tools

Cerințe privind integrarea cu Nutanix Prism Element

- Datele de autentificare ale unui utilizator Nutanix Prism Element cu drepturi de administrator (Cluster Admin sau User Admin)
- Nutanix Prism cu AOS 5.5, 5.10, 5.15 LTS
- Nutanix Prism cu AOS 5.6, 5.11 STS
- Nutanix Prism cu AHV 20170830.115, 20170830.301 și 20170830.395 Community Edition
- Nutanix Prism versiunea 2018.01.31 (Community Edition)

Platforme găzduite în cloud compatibile

Alături de mediile locale de virtualizare, GravityZone se poate integra și cu următoarele platforme găzduite în cloud:

- **Amazon EC2**

  În calitate de client Amazon EC2, puteți integra inventarul de instanțe EC2 grupate după Regiuni și Zone de disponibilitate cu inventarul de rețele GravityZone.

- **Microsoft Azure**

  În calitate de client Microsoft Azure, puteți integra mașinile virtuale Microsoft Azure grupate pe Regiuni și Zone de disponibilitate cu inventarul de rețea GravityZone.

Compatibilitate cu Tehnologii de virtualizare a desktopurilor și aplicațiilor

GravityZone este compatibilă cu următoarele tehnologii de virtualizare, începând cu Bitdefender Endpoint Security Tools versiunea 6.6.16.226:

- **VMware:**

  VMware V-App (aceeași versiune cu vCenter Server)

  VMware ThinApp 5.2.6

  VMware AppVolumes 2.180

  Important
  Nu se recomandă instalarea în Application Stack sau Writable Volumes.

- **Microsoft:**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix:**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

  Important
  Atribuiți politici pe baza regulilor utilizatorilor, astfel încât modulul Control dispozitiv să nu împiedice crearea sistemelor de operare și a nivelurilor de platformă.
  Este posibil să fie necesar să configurați regulile firewall-ului GravityZone astfel încât să permită traficul de rețea pentru fiecare dintre aceste aplicații. Pentru informații suplimentare,consultați Documentația de produs pentru Citrix App Layering.

Instrumente pentru administrarea platformelor de virtualizare suportate

În prezent, Control Center se integrează cu următoarele instrumente pentru administrarea platformelor de virtualizare:

- VMware vCenter Server
- Citrix XenServer
- Nutanix Prism Element

Pentru a configura integrarea, trebuie să furnizați numele de utilizator și parola unui administrator.

4.3.6. Security Server

Security Server este o mașină virtuală preconfigurată care rulează pe un Server Ubuntu cu următoarele versiuni:

- 16.04 (VMware NSX și multi-platformă)
- 12.04 LTS (VMware vShield)

Memorie și CPU

Alocarea resurselor memoriei și CPU pentru Security Server depinde de numărul și tipul de mașini virtuale care rulează pe sistemul gazdă. Tabelul următor include resursele recomandate care trebuie alocate:

Număr de MV protejate	RAM	CPU
1-50 MV	2 GB	2 CPU
51-100 MV	2 GB	4 CPU
101-200 MV	4 GB	6 CPU

Security Server pentru NSX este furnizat cu o configurație hardware predefinită (CPU și RAM), pe care o puteți ajusta în VMware vSphere Web Client oprind mașina, modificând setările acesteia și apoi pornind-o din nou. Pentru informații detaliate, consultați capitolul „Instalarea Security Server pentru VMware NSX” (p. 124).

Spațiu HDD

Mediu	Atribuire spațiu HDD
VMware NSX-V / NSX-T	40 GB
VMware cu vShield Endpoint	40 GB
Altul(a)	16 GB

Distribuția Security Server pe sistemele gazdă

Mediu	Security Server vs. sisteme gazdă
VMware NSX-V / NSX-T	Security Server se instalează automat pe fiecare gazdă ESXi din clusterul care trebuie protejat la momentul instalării serviciului Bitdefender.
VMware cu vShield Endpoint	Security Server trebuie să fie instalat pe fiecare gazdă ESXi, pentru asigurarea protecției.
Altul(a)	Deși nu este obligatorie, Bitdefender recomandă instalarea Security Server pe fiecare gazdă fizică, pentru performanțe superioare.

Latența rețelei

Latența comunicării dintre Security Server și endpoint-urile protejate trebuie să fie mai mică de 50 ms.

Nivelul de încărcare al modulului Protecție spațiu de stocare

Impactul Protecției spațiului de stocare asupra Security Server la scanarea a 20 GB este următorul:

Starea modulului de Protecție a dispozitivelor de stocare	Resursele Security Server	Încărcarea Security Server	Timpul de transfer (mm:ss)
Dezactivat (inițial)	N/A	N/A	10:10
Activat	4 vCPU 4 GB RAM	Normal	10:30
Activat	2 vCPU 2 GB RAM	Greu	11:23

Notă
Aceste rezultate sunt obținute pentru o serie de fișiere diferite (.exe, .txt, .doc, .eml, .pdf, .zip etc.), cu dimensiuni cuprinse între 10 KB și 200 MB. Durata de transfer corespunde unui volum de date de 20 GB din 46.500 fișiere.

4.3.7. Utilizarea pentru trafic

- **Traficul de actualizare a produselor între clientul stației de lucru și serverul de actualizări**

  Fiecare update periodic de Bitdefender Endpoint Security Tools generează următorul trafic de download pe fiecare stație de lucru protejată:

  - Pe SO Windows: ~20 MB
  - Pe SO Linux: ~26 MB
  - Pe macOS: ~25 MB

- **Traficul de actualizări de conținut de securitate descărcate între stația de lucru client și Serverul de actualizări (MB/zi)**

Tipul serverului de actualizări	Tipul motorului de scanare		
	Local	Hibrid	Central.
Relay	65	58	55
Serverul public de actualizări Bitdefender	3	3.5	3

- **Traficul de Scanare centralizată între clientul stației de lucru și Security Server**

Obiecte scanate	Tip Trafic		Descărcare (MB)	Încărcare (MB)
Fișiere*	Prima scanare		27	841
	Scanare cache		13	382
Site-uri internet**	Prima scanare	Trafic internet	621	N/A
		Security Server	54	1050
	Scanare cache	Trafic internet	654	N/A
		Security Server	0.2	0.5

* Datele furnizate au fost măsurate pentru 3,49 GB de fișiere(6.658 de fișiere), din care 1,16 GB sunt fișiere Portable Executable (PE).

** Datele furnizate au fost evaluate pentru cele mai importante 500 de site-uri.

- **Trafic de scanare hibrid între clientul stației de lucru și Serviciile Cloud Bitdefender**

Obiecte scanate	Tip Trafic	Descărcare (MB)	Încărcare (MB)
Fișiere*	Prima scanare	1.7	0.6
	Scanare cache	0.6	0.3
Trafic internet**	Trafic internet	650	N/A
	Servicii Cloud Bitdefender	2.6	2.7

* Datele furnizate au fost măsurate pentru 3,49 GB de fișiere(6.658 de fișiere), din care 1,16 GB sunt fișiere Portable Executable (PE).

** Datele furnizate au fost evaluate pentru cele mai importante 500 de site-uri.

- **Traficul dintre clienții Bitdefender Endpoint Security Tools Relay și serverul de actualizări pentru descărcarea conținutului de securitate**

  Clienții cu rol Bitdefender Endpoint Security Tools Relay descarcă ~16 MB / zi* de pe serverul de actualizări.

  * Disponibil pentru clienții Bitdefender Endpoint Security Tools începând de la versiunea 6.2.3.569.

- **Traficul dintre clienții stației de lucru și consola internet Control Center**

  Între clienții stații de lucru și consola internet Control Center se generează un trafic mediu de 618 KB / zi.

4.4. Protecție Exchange

Security for Exchange este oferit prin Bitdefender Endpoint Security Tools, care poate proteja atât sistemul de fișiere cât și serverul de e-mail Microsoft Exchange.

4.4.1. Medii compatibile Microsoft Exchange

Security for Exchange suportă următoarele versiuni și roluri Microsoft Exchange:

- Exchange Server 2019 cu rol de Edge Transport sau Mailbox
- Exchange Server 2016 cu rol de Edge Transport sau Mailbox
- Exchange Server 2013 cu rol de Edge Transport sau Mailbox
- Exchange Server 2010 cu rol de Edge Transport, Hub Transport sau Mailbox
- Exchange Server 2007 cu rol de Edge Transport, Hub Transport sau Mailbox

Security for Exchange este compatibil cu grupurile Database Availability Groups (DAG) Microsoft Exchange.

4.4.2. Cerințe de sistem

Security for Exchange este compatibil cu orice server fizic sau virtual de 64 de biți (Intel sau AMD) ce rulează o versiune și un rol compatibil Microsoft Exchange Server. Pentru detalii cu privire la cerințele de sistem pentru Bitdefender Endpoint Security Tools, consultați „Agentul de securitate fără roluri” (p. 24).

Disponibilitatea recomandată a resurselor serverului:

- Memorie RAM disponibilă: 1 GB
- Spațiu liber pe hard disk: 1 GB

4.4.3. Alte cerințe software

- Pentru Microsoft Exchange Server 2013 cu Service Pack 1: KB2938053 de la Microsoft.
- Pentru Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 sau mai nou

4.5. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises are următoarele cerințe:

- Hypervisorul ESXi (platforma de virtualizare pe care va rula mediul).
- Aplicația virtuală Sandbox Analyzer (aplicația de administrare care va controla detonarea mașinilor virtuale).
- Aplicația virtuală de securitate pentru rețea (NSVA) (o mașină virtuală care încorporează un senzor de rețea capabil să extragă payloadul din traficul de rețea).
- Conectivitate la o GravityZone Control Center existentă, utilizată pentru gestionarea la nivel înalt a mediului sandbox.
- Conexiune la internet pentru descărcarea aplicației virtuale Sandbox Analyzer, cu o lățime de bandă minimă de 5 MBps.

> **Important**
> Asigurați-vă că nu există alte aplicații sau procese care ar putea bloca conexiunea la internet în timpul descărcării și instalării Sandbox Analyzer.

4.5.1. ESXi Hypervisor

Aplicația virtuală Sandbox Analyzer este disponibilă în format OVA, implementabil pe un singur sistem gazdă fizic, care rulează hipervizorul VMware ESXi (versiunea 6.5 sau 6.7).

Cerințe de hardware pentru sistemul gazdă fizic

- CPU: numărul total de nuclee ale procesorului (luând în considerare hyperthreadingul) poate fi extrapolat prin utilizarea calculului prezentat în secțiunea „Cerințe pentru sistemul gazdă fizic și scalarea hardware” (p. 46).

- RAM: cantitatea totală de memorie RAM necesară pentru sistemul gazdă fizic poate fi extrapolată utilizând calculul prezentat în secțiunea „Cerințe pentru sistemul gazdă fizic și scalarea hardware” (p. 46).
- Spațiul pe disc: cel puțin 1 TB de spațiu de stocare SSD (adecvat pentru mediul de detonare cu 8 mașini virtuale, scalabil cu cel puțin 50 GB pentru fiecare mașină virtuală suplimentară pentru detonare).
- Rețea: o placă de rețea (NIC) dedicată.

  Acest card NIC poate fi împărțit în două carduri virtuale NIC, având următoarele caracteristici:

  – O placă de rețea (NIC) pentru interfața de administrare.

  – O placă de rețea (NIC) pentru rețeaua de detonare.

  Notă
  Se recomandă să utilizați plăci de rețea (NIC) fizice dedicate, cu aceleași mapări ca vNIC-urile menționate mai sus, dacă configurația hardware permite acest lucru.

Cerințe software

Versiuni compatibile ale serverului ESXi: 6.5 sau mai recent, VMFS versiunea 5.

Configurare suplimentară pe sistemul gazdă ESXi:

- SSH activat la pornire.
- Serviciul NTP trebuie să fie configurat și activ.
- Opțiunea **pornire/oprire cu sistemul gazdă** trebuie să fie activată.

Notă
Sandbox Analyzer este compatibil cu versiunea de evaluare a hypervisorului VMWare ESXi. Totuși, pentru efectuarea instalărilor, se recomandă rularea unei versiuni licențiate pentru ESXi.

4.5.2. Aplicația virtuală Sandbox Analyzer

Aplicația virtuală Sandbox Analyzer asigură scalabilitate realmente nelimitată, atâta timp cât resursele existente de hardware sunt disponibile.

Din numărul total al resurselor ESXi disponibile, Sandbox Analyzer împarte capacitățile CPU și RAM între Sandbox Manager și mașinile virtuale de detonare.

Cerințe minime de sistem pentru Sandbox Manager

- 6 vCPUs
- 20 GB memorie RAM
- 600 GB spațiu de disc

Sandbox Manager are trei carduri interne virtuale NIC, distribuite după cum urmează:

- O placă de rețea (NIC) pentru comunicarea cu consola de administrare (GravityZone Control Center)
- O placă de rețea (NIC) pentru conectivitatea la internet.
- O placă de rețea (NIC) pentru comunicarea cu mașinile virtuale de detonare.

Notă
Pentru realizarea comunicării, atât placa de rețea virtuală (vNIC) pentru administrarea ESXi, cât și placa de rețea virtuală (vNIC) pentru pentru administrarea Sandbox Manager trebuie să fie în aceeași rețea.

Mașini virtuale de detonare

Cerințe de sistem

- 4 vCPU (overprovisioned în raport de 4:1, consultați „Cerințe pentru sistemul gazdă fizic și scalarea hardware” (p. 46))
- 3 GB memorie RAM
- 50 GB spațiu de disc

Sandbox Analyzer On-Premises oferă suport pentru imaginile personalizate de mașini virtuale. Acest lucru permite detonarea mostrelor într-un mediu de rulare care imită un mediu real de producție.

Pentru crearea unei imagini de mașină virtuală trebuie îndeplinite următoarele condiții:

- Imaginea de mașină virtuală trebuie să fie în format VMDK, versiunea 5.
- Sistemele de operare suportate pentru construirea mașinilor virtuale de detonare:
  - Windows 7 64-bit (orice nivel de patch-uri)
  - Windows 10 64-bit (orice nivel de patch-uri)

Important

- Sistemul de operare trebuie să fie instalat pe a doua partiție din tabelul de partiții și montat pe unitatea C: (configurația implicită de instalare Windows).
- Contul local „Administrator" trebuie să fie activat și să aibă un câmp necompletat pentru introducerea parolei (dezactivare parolă).
- Înainte de a exporta o imagine de mașină virtuală, este necesar să licențiați corect sistemul de operare și tot software-ul instalat în imaginea de mașină virtuală.

Software imagine de mașină virtuală

Sandbox Analyzer suportă detonarea pentru o serie de formaturi și tipuri de fișiere. Pentru detalii, consultați „Obiecte Sandbox Analyzer " (p. 219).

Pentru raporturi concludente, asigurați-vă că aveți instalat în imaginea personalizată software-ul care poate deschide un anumit tip de fișier pe care vreți să îl detonați. Pentru detalii, consultați „Aplicații recomandate pentru mașinile virtuale de detonare" (p. 220).

4.5.3. Aplicație virtuală de securitate pentru rețea

Aplicația virtuală de securitate pentru rețea (NSVA) controlează senzorul de rețea, care extrage payload-uri din fluxurile de rețea și le trimite către Sandbox Analyzer. Cerințele minime de hardware sunt următoarele:

- 4 vCPUs
- 4 GB memorie RAM
- 1 TB spațiu de disc
- 2 plăci de rețea virtuale (vNIC)

4.5.4. Cerințe pentru sistemul gazdă fizic și scalarea hardware

Algoritmul de scalare al mediului Sandbox Analyzer are în vedere următoarea formulă, unde „K" este egal cu numărul de sloturi de detonare (sau mașini virtuale de detonare):

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

În mod similar, algoritmul de scalare pentru sistemul gazdă este următorul:

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

Principala diferență dintre resursele Sandbox Analyzer VA și resursele ESXi este dată de resursele alocate fiecărei mașini virtuale de detonare.

Prin urmare, un mediu de detonare tipic (8 VM) ar avea următoarele cerințe:

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

> **Notă**
> Fiecare mașină virtuală de detonare are nevoie de 1 vCPU alocat pentru Sandbox Analyzer VA și 1 vCPU pentru mașina virtuală de detonare. Mașina virtuală de detonare va fi prevăzută cu 4 vCPU, dar acestea vor fi overprovisioned într-un raport de 4:1, fiind astfel nevoie de 1 singur vCPU pentru sistemul gazdă ESXi.

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

> **Notă**
> Memoria RAM este utilizată în raport de 1:1 de Sandbox Analyzer VA, mașinile virtuale de detonare și sistemul gazdă ESXi. Astfel, fiecare mașină virtuală de detonare va necesita 5 GB RAM de la sistemul gazdă ESXi, din care 2 GB vor fi alocați pentri Sandbox Analyzer VA și 3 GB vor fi alocați pentru mașina virtuală de detonare în sine.

Sistemul gazdă fizic rezultat necesită, în scenariul menționat mai sus, cel puțin 22 de nuclee CPU (inclusiv hyperthreading) și cel puțin 60 GB de RAM, cu un spațiu suplimentar de 10-20% din memoria RAM rezervat pentru hypervisorul în sine.

De obicei, durează nouă minute pentru executa detonarea unei mostre și pentru a genera raportul de detonare, iar această operațiune folosește toate resursele alocate. Se recomandă să vă proiectați mediul de sandboxing pornind de la capacitatea de detonare (fișiere/oră) și apoi să transformați această valoare în resurse necesare la nivel de sistem gazdă și mașină virtuală.

4.5.5. Cerințe de comunicații pentru Sandbox Analyzer

Componentele Sandbox Analyzer On-Premises folosesc anumite porturi de comunicații legate de anumite interfețe de rețea pentru a comunica între ele și/sau cu serverele publice ale Bitdefender.

Mediul de sandboxing necesită trei interfețe de rețea:

- **eth0 – Interfața rețelei de administrare**. Se conectează la GravityZone și la sistemul gazdă ESXi.

  Se recomandă conectarea eth0 la aceeași rețea la care este conectată și interfața de administrare ESXi. De asemenea, se recomandă maparea acestuia la un adaptor fizic dedicat.

  Următorul tabel descrie cerințele de comunicație în rețea pentru eth0:

Direcție	Porturi de comunicație (pe TCP)	Sursă/destinație
La ieșire	8443	Serverul de comunicații GravityZone
	443	Aplicația virtuală GravityZone
	80	Aplicația virtuală GravityZone
	22	Gazdă ESXi
	443	API-ul sistemului gazdă ESXi
La intrare	8443	Oricare

- **eth1 – Rețeaua de detonare**. Nu necesită nicio operațiune de configurare. Procesul de instalare creează resursele virtuale necesare.
- **eth2 – Rețeaua de acces la internet**. Se recomandă să aveți o conexiune la internet nerestricționată și nefiltrată.

  Se recomandă ca rețeaua de administrare și rețeaua de acces la internet să fie atribuite unor subrețele diferite.

Aplicația virtuală GravityZone necesită acces la aplicația virtuală Sandbox Analyzer pe portul 443 (pe TCP) pentru a vizualiza și descărca rapoartele Sandbox Analyzer.

Aplicația virtuală GravityZone necesită conectivitate la aplicația virtuală Sandbox Analyzer pe portul 443 (pe TCP) pentru a solicita starea mostrelor detonate.

4.6. HVI

HVI operează cu ajutorul a două componente: Security Server și Pachet suplimentar HVI. Aceste produse trebuie instalate pe gazdele din mediul virtualizat unde se află mașinile virtuale pe care doriți să le protejați.

Notă
Este posibil ca serviciul HVI pentru soluția dvs. GravityZone să fie disponibil cu un cod de licență separat.

Înainte de a instala HVI pe gazde, asigurați-vă că sunt îndeplinite următoarele cerințe:

Platforme de virtualizare suportate

- Citrix XenServer 7.1 Enterprise Edition sau o versiune mai recentă, cu cele mai noi patch-uri

  Important
  Pentru orice versiune XenServer, începând cu versiunea 7.1, care a ajuns la sfârșitul perioadei de asistență, Bitdefender oferă suport HVI pentru încă două luni. La expirarea acestei perioade, vă recomandăm să faceți actualizarea la o versiune XenServer suportată de Citrix. Pentru informații suplimentare, accesați Citrix Legacy Products Matrix și Citrix Product Matrix.

- Citrix Hypervisor 8.0 Enterprise Edition sau o versiune mai nouă, cu ultimele patch-uri de securitate

  Avertisment
  Pentru Citrix Hypervisor 8.0 este necesar să instalați patch-ul XS80E004.

Mașini virtuale găzduite suportate

Mașinile virtuale pe care doriți să le protejați cu HVI trebuie să îndeplinească următoarele condiții:

1. Mașinile sunt în modul de virtualizare HVM, ceea ce înseamnă că sunt complet virtualizate.
2. Mașinile rulează un sistem de operare compatibil:

- **Sisteme de operare Windows Desktop (32-bit and 64-bit)**
  - Windows 10 May 2020 Update (20H1)
  - Windows 10 November 2019 Update (19H2)
  - Windows 10 May 2019 Update (19H1)
  - Actualizarea Windows 10 din 10 octombrie 2018 (Redstone 5)
  - Actualizarea Windows 10 din 10 aprilie 2018 (Redstone 4)
  - Windows 10 Fall Creators Update (Redstone 3)
  - Actualizare Windows 10 Creators (Restone 2)
  - Windows 10 Anniversary Update (Redstone 1)
  - Windows 10 November Update (Threshold 2)
  - Windows 10
  - Windows 8.1
  - Windows 8
  - Windows 7
- **Sisteme de operare Windows Server (64-bit)**
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012/ Windows Server 2012 R2
  - Windows Server 2008 R2
- **Sisteme de operare Linux (64-bit)**

Distribuție	Versiune	Versiune kernel
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

Distribuție	Versiune	Versiune kernel
Ubuntu	14.04 LTS	3.13.139 sau mai recent
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	Înainte de 7.5	4.1 (UEK/RHCK)
Oracle Linux	7.5 sau mai recent	4.14 (UEK/RHCK)

Cerințe hardware pentru VA GravityZone

- **vCPU necesar**

  Tabelul de mai jos vă informează cu privire la numărul de vCPU necesar fiecărei aplicații virtuale.

  Fiecare vCPU trebuie să aibă o capacitate de minim 2GHz.

Componentă	Numărul (maxim) de stații de lucru							
	250	500	1000	3000	5000	10000	25000	50000
Server de actualizări*	10	4	4	4	4	4	6	8
Consolă web**		6	8	8	10	10	12	12
Server de comunicații		6	8	8	10	10	16	20

Componentă	Numărul (maxim) de stații de lucru								
	250	500	1000	3000	5000	10000	25000	50000	
Baza de date***		6	6	6	6	6	9	12	
Total		**10**	**24**	**28**	**28**	**34**	**34**	**49**	**58**

* Recomandat dacă nu există Relee instalate.
** Pentru fiecare integrare activă, adăugați o vCPU pe aplicația virtuală cu rolul de Consolă web.
*** În cazul instalării distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

- **Spațiu disponibil pe RAM necesar (GB)**

Componentă	Numărul (maxim) de stații de lucru								
	250	500	1000	3000	5000	10000	25000	50000	
Server de actualizări		2	2	2	2	2	3	3	
Consola web*		8	10	10	10	10	12	16	
Server de comunicații	18	8	10	10	12	12	16	20	
Baza de date**		8	8	8	8	12	12	12	
Total		**18**	**28**	**32**	**32**	**36**	**40**	**47**	**55**

* Pentru fiecare integrare activă, adăugați un GB RAM pe aplicația virtuală cu rolul de Consolă web.
** În cazul unei instalări distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

- **Spațiu necesar pe hard disk (GB)**

Server de actualizări	150	190	80	80	80	80	80	80	80
Consolă Web			80	80	80	80	80	80	80
Server de comunicații			80	80	80	80	80	80	80
Baza de date**			110	110	130	130	190	330	730

Total	**150**	**190**	**350**	**350**	**370**	**370**	**430**	**570**	**970**

* Spațiul suplimentar necesar pe SSD la alegerea instalării automate, deoarece instalează și Security Server. După finalizarea instalării, puteți dezinstala Security Server pentru a elibera spațiu pe disc.
** În cazul unei instalări distribuite a rolurilor, alături de Setul de replicare: pentru fiecare instanță suplimentară a Bazei de date, adăugați numărul specificat la total.

Notă
Este necesar pentru baza de date un spațiu suplimentar de cel puțin 30 GB, atunci când este instalat rolul de Server de incidente. Cantitatea de spațiu a fost deja adăugată rolului Bază de date, în tabelul de mai sus.

Cerințe hardware pentru gazde

- **Microarhitectura CPU:**
  - Orice procesor Intel® Sandy Bridge sau mai recent, ce suportă tehnologia de virtualizare Intel®.
  - Extensiile VT-x sau VT-d trebuie să fie activate în BIOS.
- **Spațiu liber pe hard disk:** În afară de spațiul necesar pentru Security Server, HVI necesită încă 9 MB pentru pachetul suplimentar pe fiecare gazdă.

Cerințe Security Server

Alocarea resurselor memoriei și CPU pentru Security Server depinde de numărul și tipul de MV care rulează pe gazdă. Tabelul următor include resursele recomandate care trebuie alocate:

Număr de MV protejate	RAM	CPU
1-50 MV	6 GB	4 CPU
51-100 MV	8 GB	6 CPU
101-200 MV	16 GB	8 CPU

Spațiu liber pe hard disk: Este necesar să aveți un spațiu pe disc de 8 GB pe fiecare gazdă pentru Security Server.

Pentru o performanță optimă într-un mediu XenAPP, scalați resursele Security Server pe baza configurației dumneavoastră, după cum urmează:

Număr de 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

Cerințe pentru mașinile virtuale gazdă

În cazul unei instalări obișnuite, pentru o performanță și o rată de consolidare MV optime, se recomandă să aveți minim următoarea configurație hardware pentru mașinile virtuale gazdă:

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

4.7. Full Disk Encryption

GravityZone Full Disk Encryption vă permite să operați BitLocker pe endpoint-urile Windows și FileVault și utilitarul diskutil de tip linie de comandă pe endpoint-urile macOS prin intermediul Control Center.

Pentru a asigura protecția datelor, acest modul asigură criptarea integrală a unității de disc pentru volumele boot și non-boot, pe discuri fixe, și stochează cheile de recuperare în cazul în care utilizatorii își uită parola.

Modulul de criptare folosește resursele hardware existente din mediul dumneavoastră GravityZone.

În ceea ce privește software-ul, cerințele sunt aproximativ aceleași ca și pentru BitLocker, FileVault și utilitarul diskutil de tip linie de comandă, majoritatea limitărilor referindu-se la aceste instrumente.

Pe Windows

Modulul de criptare GravityZone suportă BitLocker, începând cu versiunea 1.2, pe mașinile cu sau fără cip TPM (Trusted Platform Module).

GravityZone suportă BitLocker pe stațiile de lucru care rulează următoarele sisteme de operare:

- 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 (cu TPM)
- Windows 7 Enterprise (cu TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (cu TPM)

*BitLocker nu este inclus în aceste sisteme de operare și trebuie instalat separat Pentru mai multe informații despre instalarea BitLocker pe Windows Server, consultați aceste articole KB furnizate de 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

Important
GravityZone nu suportă criptarea pe Windows 7 și Windows 2008 R2 fără TPM.

Pentru cerințe detaliate referitoare la BitLocker, consultați acest articol KB furnizat de Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Pe Mac

GravityZone suportă FileVault și diskutil pe stațiile de lucru macOS care rulează următoarele sisteme de operare:

- 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. Protecție spațiu de stocare

Soluții compatibile de stocare și partajare de fișiere:

- Sisteme de tip NAS (network-attached storage) și SAN (storage-area network) conforme cu ICAP (Internet Content Adaptation Protocol) de la Dell®, EMC®, IBM®, Hitachi®, HPE®, Oracle® și alți producători
- Nutanix® Files 3.x până la 3.6.2
- Citrix® ShareFile

4.9. Protecție pentru telefonul mobil

4.9.1. Platforme acceptate

Security for Mobile suportă următoarele tipuri de dispozitive mobile și sisteme de operare:

- Dispozitive Apple iPhone și tablete iPad (iOS 8.1+)
- Smartphone-uri și tablete Android (4.2+)

4.9.2. Cerințe de conectivitate

Dispozitivele mobile trebuie să aibă o conexiune de date celulare sau Wi-Fi activă și conectivitate la Serverul de comunicare.

4.9.3. Notificări Push

Security for Mobile folosește notificări de tip push pentru a avertiza clienții mobili în momentul în care sunt disponibile actualizări și opțiuni de politică. Notificările de tip push sunt transmise de Serverul de comunicații prin serviciul oferit de producătorul sistemului de operare:

- Serviciul Firebase Cloud Messaging (FCM) pentru dispozitivele Android. Pentru ca FCM să funcționeze, sunt necesare următoarele:
  - Google Play Store trebuie să fie instalat.
  - Dispozitive cu sistem de operare Android 4.2 sau mai recent.
  - Pentru a transmite notificări push, trebuie să fie deschise o serie de porturi.
- Serviciul de notificări push Apple (APN) pentru dispozitive iOS. Pentru informații suplimentare, consultați acest articol Apple KB.

Puteți verifica dacă notificările push pe mobil funcționează corect în secțiunea **Verificare notificări push pentru mobil** din **Configurare > Diverse**.

Pentru a afla mai multe cu privire la fluxul de lucru pentru Administrarea dispozitivelor mobile GravityZone, consultați acest articol KB.

4.9.4. Certificate de administrare iOS

Pentru a configura infrastructura pentru administrarea dispozitivelor mobile iOS, trebuie să furnizați o serie de certificate de securitate.

Pentru mai multe informații, consultați capitolul „Certificate” (p. 98).

4.10. Porturile de comunicare GravityZone

GravityZone este o soluție distribuită, ceea ce înseamnă că toate componentele sale comunică între ele utilizând rețeaua locală sau internetul. Fiecare componentă utilizează o serie de porturi pentru a comunica cu celelalte. Este necesar să vă asigurați că aceste porturi sunt deschise pentru GravityZone.

Pentru informații detaliate privind porturile GravityZone, consultați acest articol KB.

5. INSTALAREA PROTECȚIEI

GravityZone este o soluție de tip client-server. Pentru a vă proteja rețeaua cu Bitdefender, este necesar să configurați rolurile de server GravityZone, să vă înregistrați licența, să configurați pachetele de instalare și să le instalați pe endpoint-uri prin intermediul agenților de securitate. Unele straturi de protecție necesită instalarea și configurarea unor componente suplimentare.

5.1. Instalarea și configurarea GravityZone

Pentru a vă asigura că instalarea se efectuează fără probleme, parcurgeți pașii următori:

1. Pregătirea pentru instalare
2. Instalarea și configurarea GravityZone
3. Conectați-vă la Control Center și configurați primul cont de utilizator
4. Configurarea setărilor Control Center

5.1.1. Pregătirea pentru instalare

Pentru instalare, aveți nevoie de o imagine a aplicației virtuale GravityZone. După ce instalați și configurați aplicația GravityZone, puteți instala clientul sau descărca de la distanță pachetele de instalare necesare pentru toate componentele de securitate ale interfeței web Control Center.

Imaginea aplicației GravityZone este disponibilă în mai multe formate diferite, compatibile cu principalele platforme de virtualizare. Puteți obține cheia de licență transmițând o solicitare pe site-ul Solicitare de ofertă produse pentru companii Bitdefender.

Pentru instalare și configurarea inițială, trebuie să aveți la dispoziție următoarele:

- Denumiri DNS sau adrese IP fixe (prin configurare statică sau prin rezervare DHCP) pentru aplicațiile GravityZone
- Numele de utilizator și parola unui administrator de domeniu
- Detalii privind Serverul vCenter, vShield Manager, XenServer (nume de gazdă sau adresă IP, port de comunicare, numele de utilizator și parola administratorului)

- Cheile de licență (verificați e-mail-ul de înregistrare folosit pentru achiziție sau pentru versiunea de evaluare.)
- Setările serverului pentru e-mail-urile transmise
- Dacă este cazul, setările serverului proxy
- Certificate de securitate

5.1.2. Instalați GravityZone

O instalare GravityZone constă într-una sau mai multe aplicații care rulează cu rol de server. Numărul de aplicații depinde de diverse criterii, cum ar fi: dimensiunea și modul de proiectare al infrastructurii rețelei dumneavoastră sau caracteristicile GravityZone pe care le veți folosi. Rolurile de server sunt de trei tipuri: de bază, auxiliare și opționale

Important
Rolurile auxiliar și opțional sunt disponibile numai pentru anumite soluții GravityZone.

Rolul GravityZone	Tipul rolului	Instalare
Server de baze de date Update Server Consolă Web Server de comunicații	De bază (obligatoriu)	Cel puțin o instanță a fiecărui rol. O aplicație GravityZone poate rula unul, mai multe sau toate aceste roluri.
	Auxiliar	O singură aplicație pentru fiecare rol
Security Server	Opțional	Recomandat numai pentru rețele mici sau când resursele sunt reduse. În caz contrar, instalați un Security Server individual din Control Center, după finalizarea instalării GravityZone.
Server incidente	Necesar	Poate fi configurat atât în aplicațiile complete, cât și în cele distribuite. Utilizați software-ul încorporat de echilibrare a sarcinilor de lucru atunci când instalați mai multe instanțe.

În funcție de modul în care să distribuiți rolurile GravityZone, veți instala una sau mai multe aplicații GravityZone. Serverul de baze de date este primul care va fi instalat.

Într-un scenariu cu mai multe aplicații GravityZone, veți instala Serverul de baze de date pe prima aplicație și veți configura toate celelalte aplicații pentru a se conecta la instanța de bază de date existentă.

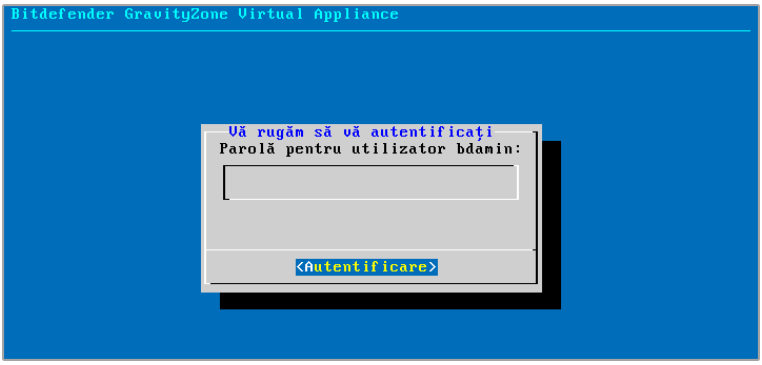
Puteți instala mai multe instanțe ale rolurilor Server de baze de date, Consolă web și Server de comunicații. În acest caz, veți utiliza funcția Set de replici pentru serverul de baze de date și veți încărca elementele de echilibrare pentru Consola web și Serverul de comunicații în aplicațiile GravityZone.

Pentru a instala și configura GravityZone:

1. Descărcați imaginea aplicației virtuale GravityZone de pe site-ul Bitdefender (link-ul este furnizat în e-mail-ul de confirmare a înregistrării sau achiziției).
2. Importați imaginea aplicației virtuale GravityZone în mediul dumneavoastră virtualizat.
3. Porniți aplicația.
4. Din instrumentul pentru administrarea platformei de virtualizare, accesați interfața consolei aplicației GravityZone.
5. Configurați parola pentru `bdadmin`, administratorul de sistem încorporat.

Interfața consolei aplicației: introduceți parola nouă

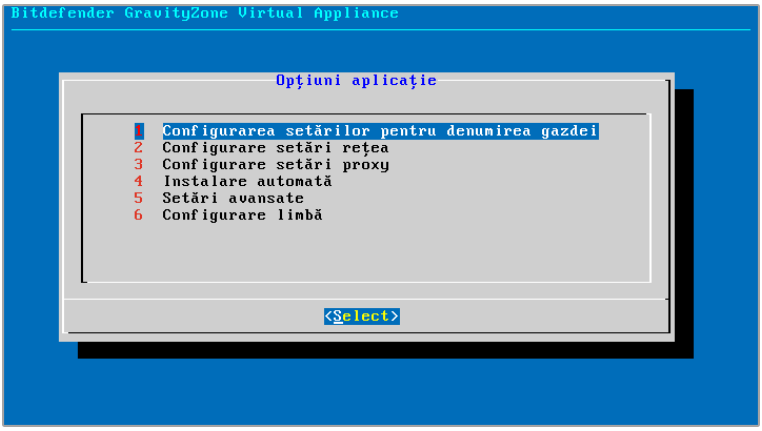
6. Autentificați-vă cu parola pe care tocmai ați configurat-o.



Interfață consolă aplicație: autentificare

Veți accesa interfața de configurare a aplicației.

Utilizați tastele săgeți și tasta Tab pentru a naviga prin meniuri și opțiuni. Apăsați Enter pentru a selecta o anumită opțiune.



Interfață consolă aplicație: meniul principal

7. Dacă aveți nevoie să schimbați limba interfeței, selectați opțiunea **Configurare limbă**. Pentru detalii referitoare la configurare, consultați „Configurare limbă” (p. 68).
8. Configurați numele de gazdă al aplicației.

9. Configurați setările rețelei.
10. Configurați setările proxy. (dacă este necesar)
11. Instalați rolurile de server GravityZone. Aveți la dispoziție două opțiuni:
    - Instalare automată. Selectați această opțiune dacă aveți nevoie să instalați o singură aplicație GravityZone în rețeaua dumneavoastră.
    - Setări avansate. Selectați această opțiune dacă trebuie să instalați GravityZone manual sau pe o arhitectură distribuită.

După ce ați instalat și configurat aplicația GravityZone, puteți edita setările aplicației în orice moment, folosind interfața de configurare. Pentru informații suplimentare referitoare la configurarea aplicației GravityZone, consultați „Gestionarea aplicației GravityZone” (p. 106).

Configurarea setărilor pentru denumirea gazdei

Comunicarea cu rolurile GravityZone se realizează folosind adresa IP sau denumirea DNS a aplicației pe care sunt instalate. În mod implicit, componentele GravityZone comunică prin intermediul adresei IP. Dacă doriți să permiteți comunicarea prin denumirile DNS, trebuie să configurați aplicațiile GravityZone cu o denumire DNS și să vă asigurați că aceasta corespunde adresei IP configurate a aplicației.

Cerințe preliminare:

- Configurați înregistrare DNS pe serverul DNS.
- Denumirea DNS trebuie să corespundă adresei IP configurate a aplicației. Prin urmare, trebuie să vă asigurați că aplicația este configurată cu adresa IP corespunzătoare.

Pentru a configura setările pentru denumirea gazdei:

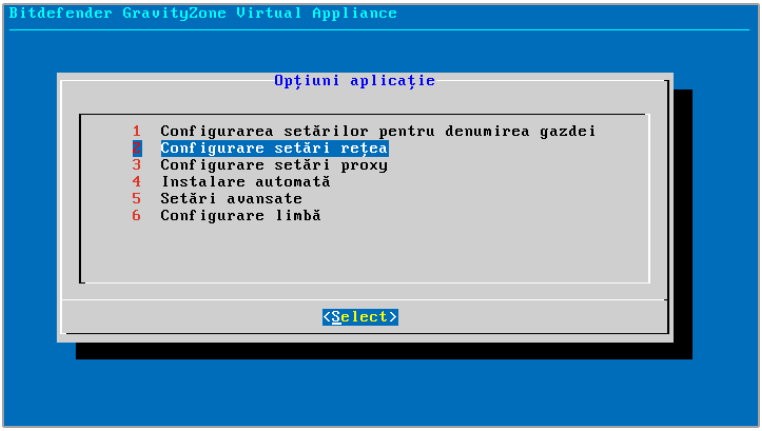
1. Din meniul principal, selectați **Configurarea setărilor pentru denumirea gazdei**.
2. Introduceți denumirea gazdei aplicației și numele de domeniu Active Directory (dacă este necesar).
3. Selectați **OK** pentru a salva modificările.

Configurare setări rețea

Puteți configura aplicația pentru a obține automat setările rețelei de la serverul DHCP sau puteți configura manual setările rețelei. Dacă optați pentru utilizarea

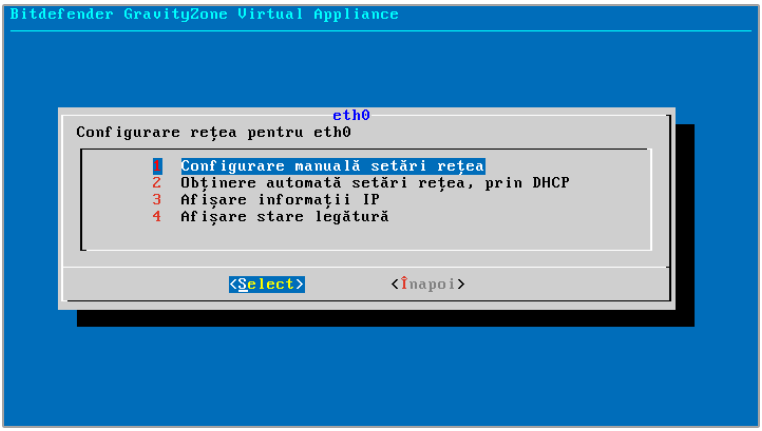
DHCP, trebuie să configurați Serverul DHCP pentru rezervarea unei anumite adrese IP pentru aplicație.

1. Din meniul principal, selectați **Configurare setări rețea**.



Interfață consolă aplicație: opțiune setări rețea

2. Selectați interfața de rețea.
3. Selectați metoda de configurare:
   - **Configurare manuală setări rețea.** Trebuie să specificați adresa IP, masca de rețea, adresa portului și adresele serverului DNS.
   - **Obținere automată setări rețea, prin DHCP.** Utilizați această opțiune numai dacă ați configurat Serverul DHCP pentru rezervarea unei anumite adrese IP pentru aplicație.



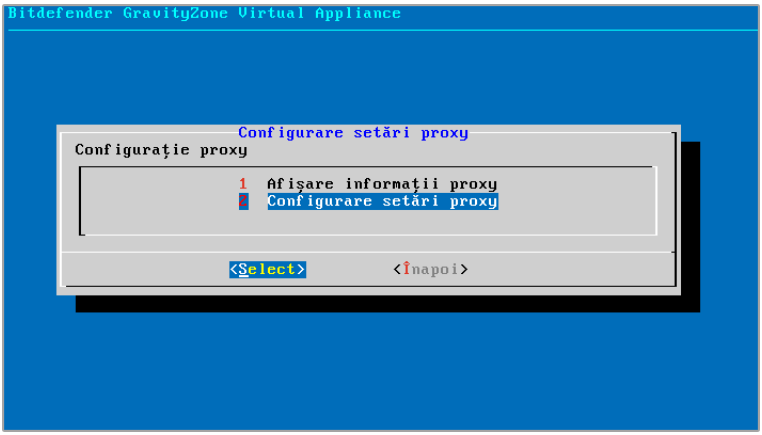
Interfață consolă aplicație: configurare rețea

4. Puteți verifica detaliile configurației IP curente sau starea legăturii selectând opțiunile corespunzătoare.

Configurare setări proxy

În cazul în care doriți ca aplicația să se conecteze la Internet printr-un server proxy, trebuie să configurați setările proxy.

1. Din meniul principal, selectați **Configurare setări proxy**.
2. Selectați **Afișare informații proxy** pentru a verifica dacă este activat proxy-ul.
3. Selectați **OK** pentru a reveni la ecranul anterior..
4. Selectați din nou **Configurare stări proxy**.



Interfață consolă aplicație: configurare setări proxy

5. Introduceți adresa serverului proxy. Utilizați următoarea sintaxă:
   - Dacă serverul proxy nu necesită autentificare:
     `http(s)://<IP/hostname>:<port>`
   - Dacă serverul proxy necesită autentificare:
     `http(s)://<username>:<password>@<IP/hostname>:<port>`
6. Selectați **OK** pentru a salva modificările.

Instalare automată

În timpul instalării automate, toate rolurile de bază se instalează pe aceeași aplicație. Pentru o instalare distribuită GravityZone, consultați „Setări avansate” (p. 66).

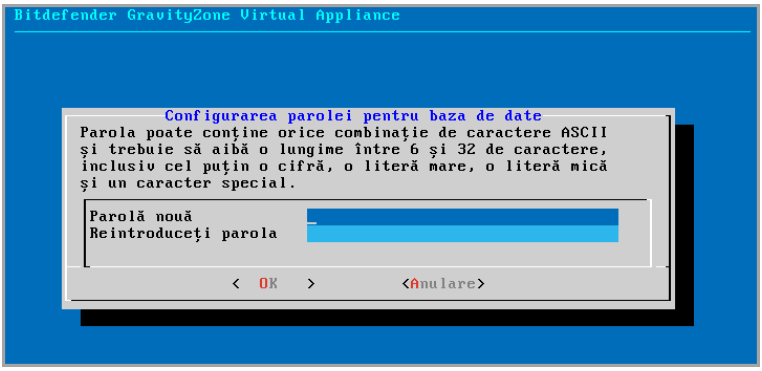
Important
Instalarea automată va determina și instalarea Security Server, încorporat în aplicația GravityZone. Pentru informații despre Security Server, consultați „Arhitectura GravityZone” (p. 11).
Opțiunea de a instala rolurile automat este disponibilă numai în momentul configurării inițiale a GravityZone.

Pentru a instala rolurile automat:

1. Din meniul principal, selectați **Instalare automată**.

2. Pentru a continua, citiți și acceptați Acordul de licență pentru utilizatorul final.
3. Confirmați rolurile ce urmează a fi instalate.
4. Setați parola pentru Serverul de baze de date.

   Parola poate conține orice combinație de caractere ASCII și trebuie să aibă o lungime între 6 și 32 de caractere, inclusiv cel puțin o cifră, o literă mare, o literă mică și un caracter special.



Interfață consolă aplicație: configurare parolă pentru baza de date

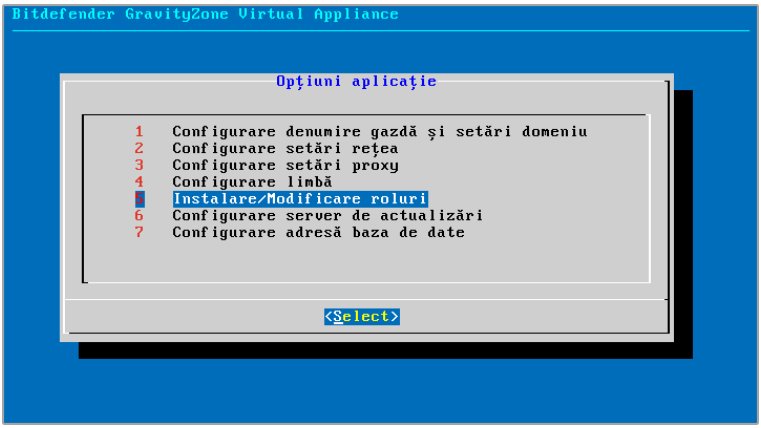
5. Așteptați până când procesul de instalare este finalizat.

Setări avansate

Folosiți această opțiune pentru a instala numai o parte sau toate rolurile GravityZone, individual, sau pentru a vă extinde infrastructura GravityZone. Puteți instala rolurile pe una sau mai multe aplicații. Această metodă de instalare este necesară atunci când se testează actualizările sau pe arhitecturile distribuite GravityZone pentru a scala GravityZone în rețele extinse și pentru a asigura un nivel ridicat de disponibilitate a serviciilor GravityZone.

Pentru a instala rolurile în mod individual:

1. Din meniul principal, selectați **Setări avansate**.



Interfață consolă aplicație: instalare roluri

2. Selectați **Instalare/Dezinstalare roluri** pentru a instala aplicația într-un mediu GravityZone cu un singur server de baze de date.

   Notă
   Celelalte opțiuni vizează extinderea instalării GravityZone la o arhitectură distribuită. Pentru mai multe informații, consultați „Conectare la o bază de date existentă” (p. 117) sau „Conectare la baza de date existentă (Cluster VPN Securizat)” (p. 118).

3. Selectați **Adăugare sau ștergere roluri**. Va apărea un mesaj de confirmare.
4. Apăsați `Enter` pentru a continua.
5. Apăsați bara de `Spaţiu` și apoi tasta `Enter` pentru instalarea rolului de Server de baze de date. Trebuie să confirmați alegerea apăsând din nou `Enter`.
6. Setați parola pentru baza de date.

   Parola poate conține orice combinație de caractere ASCII și trebuie să aibă o lungime între 6 și 32 de caractere, inclusiv cel puțin o cifră, o literă mare, o literă mică și un caracter special.
7. Apăsați `Enter` și așteptați finalizarea instalării.

8. Instalați celelalte roluri selectând **Adăugare sau ștergere roluri** din meniul **Instalare/Dezinstalare roluri** și apoi rolurile pe care doriți să le instalați.
   a. Selectați **Adăugare sau ștergere roluri** din meniu **Instalare/dezinstalare roluri**.
   b. Citiți Contractul de licență pentru utilizatorul final. Apăsați `Enter` pentru acceptare și continuare.

      Notă
      Acest lucru este necesar o singură dată, după instalarea Serverului de baze de date.

   c. Selectați rolurile ce urmează a fi instalate. Apăsați bara de `Spaţiu` pentru a selecta un rol și apăsați `Enter` pentru a continua.
   d. Apăsați `Enter` pentru confirmare și așteptați să se finalizeze instalarea.

Notă
Fiecare rol este în mod normal instalat în câteva minute. În timpul instalării, fișierele necesare sunt descărcate de pe Internet. Prin urmare, instalarea durează mai mult timp dacă conexiunea la Internet este lentă. Dacă instalarea stagnează, reluați configurarea aplicației.

Configurare limbă

Inițial, interfața de configurare a aplicației este în limba engleză.

Pentru a schimba limba interfeței:

1. Selectați **Configurare limbă** din meniul principal.
2. Selectați limba dintre opțiunile disponibile:. Va apărea un mesaj de confirmare.

   Notă
   Este posibil să fie nevoie să derulați lista pentru a ajunge la limba dorită.

3. Selectați **OK** pentru a salva modificările.

5.1.3. Configurarea inițială a Control Center

După ce ați instalat și configurat aplicația GravityZone, trebuie să accesați interfața web Control Center și să configurați contul de administrator al companiei.

1. În bara de adrese a browser-ului web, introduceți adresa IP sau numele de gazdă DNS al aplicației Control Center (folosind prefixul `https://`). Va apărea un asistent de configurare.
2. Introduceți cheia de licență necesară pentru validarea soluției GravityZone achiziționate. De asemenea, puteți introduce o cheie pentru add-on-ul GravityZone, dacă aveți una.

   Verificați e-mail-ul de înregistrare, de încercare sau de achiziție pentru a afla cheile de licență.

   a. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Va apărea o fereastră de configurare.

   b. Selectați tipul de înregistrare a licenței (online sau offline).

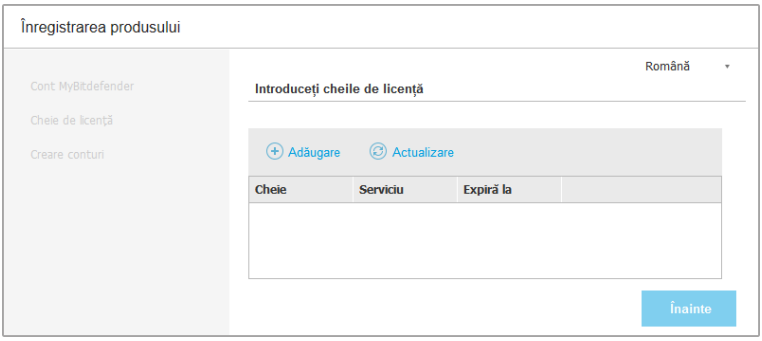
   c. Introduceți cheia de licență în câmpul **Cheie de licență**. Pentru înregistrare offline, vi se solicită, de asemenea, codul de înregistrare.

   d. Așteptați până la validarea cheii de licență. Dați clic pe **Adăugare** pentru a finaliza procesul.

   Cheia de licență și data de expirare a acesteia vor apărea în tabelul licenței.

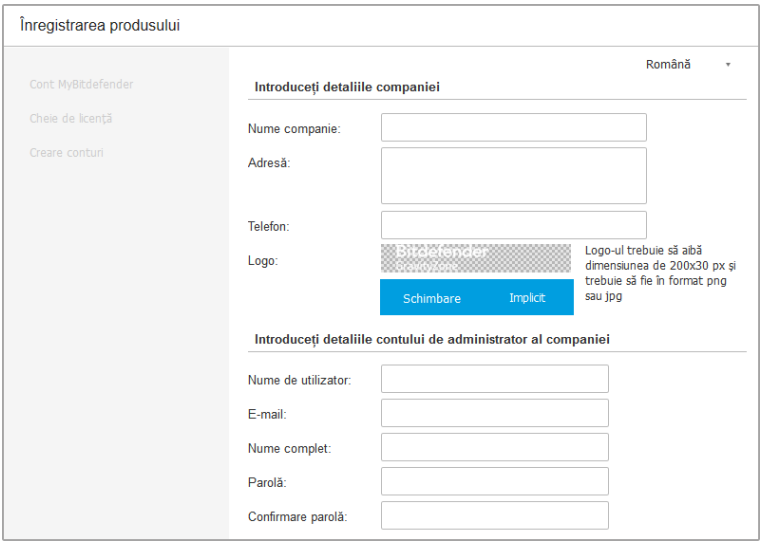
   Notă

   - La configurarea inițială, este necesar să furnizați o cheie de licență de bază validă pentru a începe utilizarea GravityZone. Apoi, puteți adăuga mai multe chei de licență pentru add-on-uri sau pentru a le modifica pe cele existente.
   - Puteți folosi add-on-urile cât timp este furnizată o licență de bază valabilă. În caz contrar, veți putea vizualiza caracteristicile, însă nu le veți putea folosi.



Configurare inițială - Specificați cheia de licență

3. Faceți clic pe **Înainte** pentru a continua.
4. Completați cu informații despre companie, cum ar fi denumirea companiei, adresa și numărul de telefon.
5. Puteți modifica sigla afișată în Control Center, în rapoartele companiei și notificările prin e-mail astfel:
   - Faceți clic pe **Schimbare** pentru a selecta sigla din calculatorul dumneavoastră. Formatul fișierului de tip imagine trebuie să fie .png sau .jpg, iar dimensiunea imaginii trebuie să fie de 200x30 pixeli.
   - Faceți clic pe **Implicit** pentru a șterge imaginea și a reseta la imaginea furnizată de Bitdefender.
6. Specificați detaliile necesare pentru contul de administrator al companiei dumneavoastră: nume de utilizator, adresă e-mail și parolă. Parola trebuie să includă cel puțin o literă mare, cel puțin o literă mică și cel puțin o cifră sau un caracter special.



Configurare inițială - Configurați-vă contul

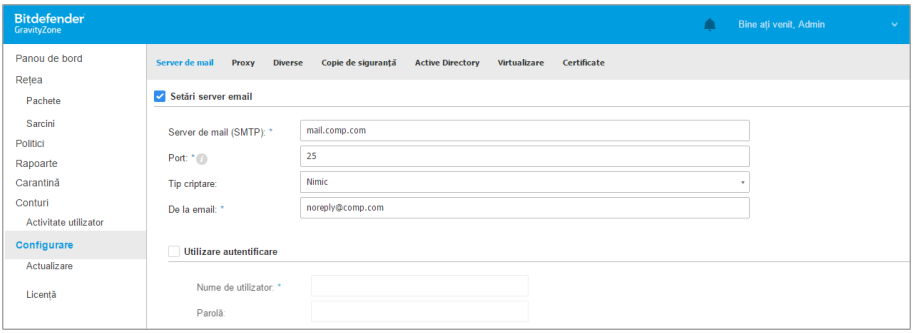
7. Dați clic pe **Creare cont**.

Va fi creat contul de administrator al companiei și vă veți autentifica imediat cu noul cont pe Bitdefender Control Center.

5.1.4. Configurare setări Control Center

După instalarea inițială, trebuie să configurați setările Control Center. În calitate de administrator al companiei, puteți face următoarele:

- Configurați mail-ul, serverul proxy și alte setări generale.
- Executați sau programați o copie de rezervă a bazei de date Control Center.
- Configurați integrarea cu Active Directory și instrumentele de administrare a platformei de virtualizare (vCenter Server, XenServer).
- Instalați certificatele de securitate.



Setări server de mail

Server de mail

Control Center necesită un server e-mail extern pentru transmiterea comunicărilor prin e-mail.

Notă
Se recomandă deschiderea unui cont e-mail dedicat care va fi utilizat de Control Center.

Pentru a permite Control Center să transmită e-mail-uri:

1. Mergeți la pagina **Configurare**.
2. Selectați secțiunea **Server de mail**.
3. Selectați **Setari server de mail** și configurați setările necesare:
   - **Server de mail (SMTP).** Introduceți adresa IP sau numele de domeniu al serverului de mail care va transmite e-mail-urile.
   - **Port.** Introduceți portul folosit pentru conectarea la serverul de mail.
   - **Tip criptare.** Dacă serverul de mail necesită o conexiune criptată, selectați tipul corespunzător din meniu (SSL, TLS sau STARTTLS)
   - **De la email.** Introduceți adresa e-mail care doriți să apară în câmpul De la din e-mail (adresa e-mail a expeditorului).
   - **Utilizare autentificare.** Selectați această casetă dacă serverul de mail necesită autentificare. Trebuie să specificați un nume de utilizator / o adresă e-mail și o parolă valabilă.

4. Faceți clic pe **Save**.

Control Center validează automat setările de mail în momentul în care le salvați. Dacă setările furnizate nu pot fi validate, un mesaj de eroare vă avertizează cu privire la setarea incorectă. Corectați setarea și încercați din nou.

Proxy

În cazul în care compania dumneavoastră dispune de o conexiune la Internet printr-un server proxy, trebuie să configurați setările proxy:

1. Mergeți la pagina **Configurare**.
2. Selectați secțiunea **Proxy**.
3. Selectați **Utilizează setări proxy** și configurați setările necesare:
   - **Adresă** - introduceți adresa IP a serverului proxy.
   - **Port** - introduceți portul folosit pentru conectarea la serverul proxy.
   - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
   - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.
4. Faceți clic pe **Save**.

Diverse

Din pagina **Configurare** > fila **Diverse**, puteți configura următoarele preferințe generale:

- **Dacă este necesară o imagine Security Server care nu este disponibilă.** Aplicația GravityZone nu include în mod implicit imaginile mașinii virtuale Security Server. Dacă un administrator încearcă să descarce o imagine Security Server sau să ruleze o sarcină de instalare Security Server, acțiunea va eșua. Puteți configura o sarcină automată pentru această situație, selectând una dintre opțiunile următoare:
  - **Descărcați imaginea automat**
  - **Informează administratorul și nu descărca**

  Notă

  Pentru a evita interferența cu activitatea administratorului, puteți descărca automat pachetele Security Server necesare de pe pagina **Actualizare** din

secțiunea **Actualizare produs**. Pentru mai multe informații, consultați capitolul „Descărcarea actualizărilor de produs” (p. 188).

- **Atunci când este nevoie de un kit indisponibil.** Puteți configura o sarcină automată pentru această situație, selectând una dintre opțiunile următoare:
  - **Descărcați pachetul automat**
  - **Informează administratorul și nu descărca**
- **Instalări simultane.** Administratorii pot instala componentele de securitate de la distanță, prin rularea sarcinilor de instalare. Folosiți această opțiune pentru a specifica numărul maxim de instalări simultane posibile.

  De exemplu, dacă numărul maxim de instalări simultane este setat pe 10 și o sarcină de instalare de la distanță a unui client este alocată unui număr de 100 de calculatoare, Control Center va transmite inițial 10 pachete de instalare prin rețea. În acest caz, instalarea clientului este efectuată simultan pe maximum 10 calculatoare, toate celelalte sarcini secundare fiind în stare de așteptare. Imediat ce a fost realizată o sarcină secundară, este expediat un nou pachet de instalare și așa mai departe.
- **Activați autentificarea de tip „two-factor” pentru toate conturile.** Autentificarea de tip „two-factor” (2FA) adaugă un strat suplimentar de securitate conturilor GravityZone, solicitând un cod de autentificare pe lângă datele de conectare la Control Center. Această funcție necesită descărcarea Google Authenticator, Microsoft Authenticator sau a altei aplicații de autentificare în doi pași de tip TOTP (Time-Based One-Time Password Algorithm) - compatibilă cu standardul RFC6238 - pe dispozitivul mobil al utilizatorului, apoi asocierea aplicației cu contul GravityZone și utilizarea acesteia la fiecare autentificare în Control Center. Aplicația de autentificare generează un cod de șase cifre la fiecare 30 de secunde. Pentru a finaliza conectarea la Control Center, după introducerea parolei, utilizatorul va trebui să introducă și codul de autentificare din șase cifre.

  Autentificarea în doi pași este activată implicit la crearea unei companii. După aceea, la autentificare, o fereastră de configurare le va solicita utilizatorilor să activeze această caracteristică. Utilizatorii vor avea opțiunea de a omite activarea funcției 2FA numai de trei ori. La cea de-a patra încercare de autentificare, nu mai este posibilă evitarea configurării autentificării în doi pași (2FA), iar utilizatorul nu se va mai putea autentifica.

  Dacă doriți să dezactivați funcționalitatea 2FA pentru toate conturile GravityZone din cadrul companiei dumneavoastră, nu trebuie decât să deselectați opțiunea.

Veți primi un mesaj de confirmare înainte ca modificările să fie aplicate. Din acest moment, utilizatorii vor avea în continuare funcția 2FA activată, însă nu o vor putea dezactiva din setările contului lor.

Notă

- Puteți vizualiza starea funcției 2FA pentru contul unui utilizator din pagina **Conturi**.
- Dacă un utilizator având autentificarea 2FA activată nu se poate conecta la GravityZone (din cauza unui dispozitiv nou sau a pierderii codului secret), puteți să resetați activarea autentificării de tip „two-factor" din pagina contului utilizatorului, accesând secțiunea **autentificare de tip „two-factor"**. Pentru detalii, consultați **Conturi utilizatori > Administrarea autentificării bifactoriale** din Ghidul administratorului.

- **Setări server NTP**. Serverul NTP se utilizează pentru sincronizarea intervalului dintre toate aplicațiile GravityZone. Se furnizează o adresă de server NTP implicit, pe care o puteți modifica în câmpul **NTP Server Address**.

  Notă
  Pentru ca aplicațiile GravityZone să comunice cu Serverul NTP, portul 123 (UDP) trebuie să fie deschis.

- **Activează Syslog**. Activând această funcție, veți permite GravityZone să trimită notificări către un server de autentificare ce folosește protocolul Syslog. Astfel, aveți posibilitatea de a monitoriza mai bine evenimentele GravityZone.

  Pentru a vizualiza și configura lista de notificări trimise către serverul Syslog, consultați capitolul **Notificări** din Ghidul administratorului GravityZone.

  Pentru a activa autentificarea pe un server Syslog de la distanță:

  1. Bifați caseta **Activare Syslog**.
  2. Introduceți numele serverului sau IP-ul, protocolul preferat și portul monitorizat de Syslog .
  3. Selectați în formatul în care doriți să trimiteți datele către serverul Syslog:
     - **Format JSON**. JSON este un format simplu de schimb de date, complet independent de orice limbaj de programare. JSON reprezintă datele în format text, care poate fi citit de o persoană. În formatul JSON, detaliile

fiecărui eveniment sunt structurate pe obiecte, fiecare obiect constând într-o combinație nume/valoare.

De exemplu:

```
{
    "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"
}
```

Pentru informații suplimentare, consultați www.json.org.

Acesta este formatul implicit în GravityZone.

– **Common Event Format (CEF)**. CEF este un standard deschis dezvoltat de ArcSight, care simplifică administrarea jurnalelor.

De exemplu:

```
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
```

Pentru informații suplimentare, consultați Standardul ArcSight de implementare a formatului CEF (Common Event Format).

În capitolul **Notificări** din Ghidul administratorului, puteți vizualiza tipurile de notificări disponibile pentru fiecare format.

4. Faceți clic pe butonul ⊕ **Adăugare** din coloana **Acțiune**.

Faceți clic pe **Salvare** pentru a aplica modificările.

Copie de siguranță

Pentru a vă asigura că toate datele Control Center sunt sigure, poate fi util să realizați o copie de siguranță a bazei de date GravityZone. Puteți executa oricâte copii de siguranță ale bazelor de date doriți sau puteți programa copii de siguranță periodice care să fie executate la un anumit interval.

Fiecare comandă de realizare a unei copii de rezervă a bazei de date creează un fișier `tgz` (fișier GZIP Compressed Tar Archive) în locația specificată în setările pentru realizarea copiilor de siguranță.

Dacă mai mulți administratori au drepturi de administrare asupra setărilor Control Center, puteți configura **Setările de notificare** pentru a vă alerta la fiecare finalizare a unei copieri de siguranță a bazei de date. Pentru informații suplimentare, consultați capitolul **Notificări** din Ghidul administratorilor GravityZone.

Crearea copiilor de siguranță ale bazelor de date

Pentru a executa o copie de rezervă a bazei de date:

1. Mergeți la pagina **Configurare** din Control Center și dați clic pe fila **Copie de siguranță**.
2. Faceți clic pe butonul **Creare copie de siguranță imediată** din partea de sus a tabelului. Va apărea o fereastră de configurare.
3. Selectați tipul de locație în care va fi salvată arhiva copiei de siguranță:
   - **Local**, pentru salvarea arhivei copiei de siguranță în aplicația GravityZone. În acest caz, trebuie să specificați calea către directorul specific din aplicația GravityZone în care va fi stocată arhiva.

     Aplicația GravityZone are o structură de directoare Linux. De exemplu, puteți opta pentru crearea copiei de rezervă în directorul `tmp`. În acest caz, introduceți `/tmp` în câmpul **Cale**.
   - **FTP**, pentru a salva arhiva de rezervă pe un server FTP. În acest caz, introduceți datele serverului FTP în câmpurile următoare.
   - **Rețea**, pentru a salva arhiva cu copiile de rezervă într-o locație partajată din rețea. În acest caz, introduceți calea în locația de rețea dorită (de exemplu, `\\calculator\folder`), numele de domeniu și datele de autentificare ale utilizatorului domeniului.

4. Faceți clic pe butonul **Testare setări**. Un mesaj text vă va informa dacă setările specificate sunt corecte sau nu.

   Pentru a crea o copie de rezervă, toate setările trebuie să fie corecte.

5. Faceți clic pe **Generare**. Se va deschide pagina **Copie de siguranță**. O nouă înregistrare a copiei de siguranță va fi inclusă în listă. Verificați **Starea** noii copii de rezervă. După finalizarea realizării copiei de rezervă, veți găsi arhiva `tgz` în locația specificată.

   Notă
   Lista disponibilă pe pagina **Copie de siguranță** conține jurnalele copiilor de siguranță create. Aceste jurnale nu oferă acces la arhivele copiilor de siguranță; acestea afișează doar detaliile copiilor de siguranță create.

Pentru a programa realizarea unei copii de siguranță a bazei de date:

1. Mergeți la pagina **Configurare** din Control Center și dați clic pe fila **Copie de siguranță**.
2. Faceți clic pe butonul **Setări copie de siguranță** din partea de sus a tabelului. Va apărea o fereastră de configurare.
3. Selectați **Copie de siguranță programată**.
4. Configurați intervalul de realizare a copiei de siguranță (zilnic, săptămânal sau lunar) și ora începerii.

   De exemplu, puteți programa realizarea copiilor de siguranță săptămânal, în fiecare vineri, la ora 22:00.

5. Configurați locația programată a copiei de siguranță.
6. Selectați tipul de locație în care va fi salvată arhiva copiei de siguranță:
   - **Local**, pentru salvarea arhivei copiei de siguranță în aplicația GravityZone. În acest caz, trebuie să specificați calea către directorul specific din aplicația GravityZone în care va fi stocată arhiva.

     Aplicația GravityZone are o structură de directoare Linux. De exemplu, puteți opta pentru crearea copiei de rezervă în directorul `tmp`. În acest caz, introduceți `/tmp` în câmpul **Cale**.

   - **FTP**, pentru a salva arhiva de rezervă pe un server FTP. În acest caz, introduceți datele serverului FTP în câmpurile următoare.

- **Rețea**, pentru a salva arhiva cu copiile de rezervă într-o locație partajată din rețea. În acest caz, introduceți calea în locația de rețea dorită (de exemplu, `\\calculator\folder`), numele de domeniu și datele de autentificare ale utilizatorului domeniului.

7. Faceți clic pe butonul **Testare setări**. Un mesaj text vă va informa dacă setările specificate sunt corecte sau nu.

   Pentru a crea o copie de rezervă, toate setările trebuie să fie corecte.

8. Faceți clic pe **Salvează** pentru a crea o copie de rezervă programată.

Restaurarea copiei de siguranță a unei baze de date

Atunci când din diverse motive, instanța dvs. GravityZone nu funcționează corect (actualizări nereușite, interfață deficientă, fișiere corupte, erori etc.), puteți restaura baza de date GravityZone folosind o copie de siguranță:

- Aceeași aplicație
- O imagine GravityZone nouă
- Funcția Replica Set

Alegeți opțiunea care se potrivește cel mai bine situației dvs. și începeți procedura de restaurare numai după ce ați citit cu atenție cerințele preliminare descrise în continuare.

Restaurarea bazei de date în aceeași aplicație virtuală (VA) GravityZone

Cerințe preliminare

- O conexiune SSH la aplicația GravityZone, folosind drepturile de **root**.

  Puteți folosi **putty** și datele de autentificare **bdadmin** pentru a vă conecta la aplicație prin SSH și apoi executați comanda sudo su pentru a comuta la contul **root**.

- Infrastructura GravityZone nu s-a modificat de la efectuarea backup-ului.
- Copia de siguranță este mai recentă decât 30 aprilie 2017, iar versiunea GravityZone este mai recentă decât 6.2.1-30. În caz contrar, contactați echipa de asistență tehnică.
- În arhitecturile distribuite, GravityZone nu a fost configurat pentru replicarea bazelor de date (Replica Set).

  Pentru a verifica configurația, urmați pașii de mai jos:

1. Deschideți fișierul `/etc/mongodb.conf`.
2. Asigurați-vă că `replSet` nu este configurat, după cum este ilustrat în exemplul de mai jos:

```
# replSet = setname
```

Notă
Pentru a restaura baza de date dacă funcția Replica Set este activată, consultați „Restaurarea bazei de date într-un mediu pe bazat pe Replica Set” (p. 84).

- Nu există procese CLI în derulare.

  Pentru a vă asigura că toate procesele CLI sunt oprite, executați următoarea comandă:

```
# killall -9 perl
```

- Pachetul **mongoconsole** este instalat în aplicație.

  Pentru a verifica dacă această condiție este îndeplinită, executați această comandă:

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

  Această comandă nu ar trebui să returneze erori. În caz contrar, executați comenzile:

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

Restaurarea bazei de date

1. Accesați locația care conține arhiva bazei de date:

```
# cd /director-cu-backup
```

, unde `directory-with-backup` este calea către locația fișierelor de backup.

De exemplu:

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

2. Restaurați baza de date.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_password
--authenticationDatabase admin --gzip --drop --archive < \
gz-backup-$AAAALLZZamprenta temporală
```

> **Important**
> Asigurați-vă că înlocuiți `GZ_db_password` cu parola efectivă a serverului de baze de date GravityZone și variabilele amprentei temporale din denumirea arhivei cu data efectivă.
> De exemplu, data efectivă ar trebui să arate astfel:
>
> ```
> gz-backup-2019-05-17(1495004926).tar.gz
> ```

3. Reporniți aplicațiile.

   Restaurarea bazei de date este acum finalizată.

Restaurarea bazei de date dintr-o aplicație virtuală (VA) GravityZone scoasă din uz

Cerințe preliminare

- O nouă instalare a aplicației virtuale (VA) GravityZone:
  - Folosind același IP ca aplicația anterioară
  - Având instalat DOAR rolul de Server de baze de date.

  Puteți descărca imaginea aplicației virtuale (VA) GravityZone de aici.
- O conexiune SSH la aplicația virtuală GravityZone, folosind drepturile de **root**.
- Infrastructura GravityZone nu s-a modificat de la efectuarea backup-ului.
- Backup-ul este mai recent decât 30 aprilie 2017.

- În arhitecturile distribuite, GravityZone nu a fost configurat pentru replicarea bazelor de date (Replica Set).

  Dacă folosiți Replica Set în mediul GravityZone, aveți de asemenea rolul de Server de baze de date instalat și pe alte instanțe ale aplicației.

  Pentru a restaura baza de date dacă funcția Replica Set este activată, consultați „Restaurarea bazei de date într-un mediu pe bazat pe Replica Set” (p. 84).

Restaurarea bazei de date

1. Conectați-vă la aplicația GravityZone prin intermediul SSH și comutați la **root**.
2. Opriți VASync:

   ```
   # stop vasync
   ```

3. Opriți CLI:

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

4. Accesați locația unde se află copia de siguranță:

   ```
   # cd /director-cu-backup
   ```

   , unde `directory-with-backup` este calea către locația fișierelor de backup.

   De exemplu:

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

5. Restaurați baza de date.

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

Important
Asigurați-vă că înlocuiți `GZ_db_password` cu parola efectivă a serverului de baze de date GravityZone și variabilele amprentei temporale din denumirea arhivei cu data efectivă.
De exemplu, data efectivă ar trebui să arate astfel:

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

6. Restaurați ID-ul anterior al aplicației:

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

Important
Asigurați-vă că înlocuiți `GZ_db_password` cu parola efectivă a serverului de baze de date GravityZone.

7. Ștergeți trimiterea la rolurile vechi.

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

Important
Asigurați-vă că înlocuiți `GZ_db_password` cu parola efectivă a serverului de baze de date GravityZone.

8. Porniți VASync:

```
# start vasync
```

9. Porniți CLI:

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

10. Instalați celelalte roluri.

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

Observați că schema bazei de date a fost actualizată la cea mai recentă versiune:

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

11. Reporniți aplicația.

Restaurarea bazei de date este acum finalizată.

Restaurarea bazei de date într-un mediu pe bazat pe Replica Set

Dacă ați instalat baza de date într-un mediu pe bazat pe Replica Set, puteți găsi procedura oficială de restaurare în manualul online mongoDB (disponibil doar în limba engleză).

Notă
Procedura necesită cunoștințe tehnice avansate și trebuie efectuată numai de către un specialist instruit. Dacă întâmpinați dificultăți, vă rugăm să contactați echipa de Suport tehnic care vă va ajuta să restaurați baza de date.

Active Directory

Prin integrarea Active Directory, puteți importa în Control Center inventarul existent din sistemul Active Directory local și din sistemul Active Directory găzduit în

Microsoft Azure, simplificând configurarea, administrarea, monitorizarea și raportarea securității. De asemenea, utilizatorilor Active Directory li se pot aloca roluri de utilizator diferite în Control Center.

Pentru integrarea și sincronizarea GravityZone cu un domeniu Active Directory:

1. Accesați pagina **Configurare > Active Directory > Domenii** și selectați ⊕ **Adăugare**.
2. Configurați setările necesare:
   - Interval sincronizare (ore)
   - Denumirea de domeniu Active Directory (inclusiv extensia domeniului)
   - Numele de utilizator și parola unui administrator de domeniu
   - Locația din Inventarul de rețea în care să se afișeze endpoint-urile AD:
     - Mențineți structura AD și ignorați unitățile organizaționale goale
     - Ignorați structura AD, importați în Grupuri personalizate
     - Mențineți structura AD cu unitățile organizaționale selectate
   - Controlerele de domeniu cu care se sincronizează Control Center. Extindeți secțiunea **Solicită controler domeniu** și alegeți controlerele din tabel.
3. Faceți clic pe **Save**.

Important
Ori de câte ori se schimbă parola, nu uitați să o actualizați și în Control Center.

Drepturi de acces

Folosind regulile de acces, puteți permite GravityZone Control Center accesul la utilizatorii Active Directory (AD), pe baza regulilor de acces. Pentru a integra și sincroniza domeniile AD, consultați secțiunea Active Directory. Pentru mai informații suplimentare despre administrarea conturilor de utilizator prin intermediul regulilor de acces, consultați capitolul **Conturile de utilizator** din Ghidul de instalare GravityZone.

Furnizori de servicii de virtualizare

GravityZone poate fi integrat în prezent în VMware vCenter Server, Citrix XenServer, Nutanix Prism Element, Amazon EC2 și Microsoft Azure.

- „Integrare cu vCenter Server” (p. 86)
- „Integrare cu XenServer” (p. 89)

- „Integrarea cu Nutanix Prism Element” (p. 90)
- „Integrarea cu Amazon EC2” (p. 91)
- „Integrarea cu Microsoft Azure” (p. 92)
- „Administrarea integrărilor cu platforma” (p. 93)

Important
La fiecare configurare a unei noi integrări cu un nou sistem vCenter Server, XenServer, Nutanix Prism Element sau Microsoft Azure, nu uitați să verificați și să actualizați drepturile de acces pentru utilizatorii existenți.

Integrare cu vCenter Server

Puteți integra GravityZone cu unul sau mai multe sisteme Server vCenter. Sistemele Server vCenter în Linked Mode trebuie adăugate separat la Control Center.

Pentru a configura integrarea cu un Server vCenter:

1. Accesați pagina **Configurare** din Control Center și navigați la **Furnizori de servicii de virtualizare > Platforme de administrare**.
2. Dați clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați **Server vCenter** din meniu. Va apărea o fereastră de configurare.
3. Specificați detaliile Serverului vCenter.
   - Denumirea sistemului Serverului vCenter este în Control Center
   - Denumirea gazdei sau adresa IP a sistemului Serverului vCenter
   - Portul Serverului vCenter (implicit 443)
4. Specificați datele care vor fi utilizate pentru autentificarea la Serverul vCenter. Puteți alege să utilizați datele furnizate pentru integrarea cu Active Directory sau un alt set de date de autentificare. Utilizatorul ale cărui date le furnizați trebuie să aibă drepturi de administrator de nivel principal pe Serverul vCenter.
5. Selectați platforma VMware instalată în mediul dvs. și configurați setările în mod corespunzător:
   - **Niciuna**. Selectați această opțiune pentru NSX-T sau dacă nu este instalată nicio platformă VMware specifică și selectați **Salvare**. Pentru integrare este necesară acceptarea certificatului de securitate autosemnat.

     Pentru a configura integrarea cu NSX-T Manager și pentru a aplica protecția la nivel de endpoint pe mașinile dumneavoastră virtuale prin intermediul

politicii GravityZone Guest Introspection, consultați următorul articol din baza de cunoștințe (KB).

- **vShield**. Specificați detaliile sistemului Manager vShield integrat cu Serverul vCenter.
  - Denumirea gazdei sau adresa IP a sistemului Manager vShield
  - Portul Manager vShield (implicit 443)
- **NSX-V**. Specificați detaliile Managerului NSX integrat cu Serverul vCenter.

  Notă
  Pentru a face upgrade de la VMWare vShield la NSX, consultați acest articol KB.

  - Numele gazdei sau adresa IP a Managerului NSX
  - Port Manager NSX (implicit 443)
  - Numele de utilizator și parola folosite pentru autentificare pe Managerul NSX.

    Aceste date de autentificare vor fi salvate pe entitatea protejată, nu în Managerul de date de autentificare.
  - Bifați caseta **Etichetează la identificarea virușilor** pentru a folosi etichetele de securitat NSX implicite la identificarea programelor periculoase pe mașina virtuală.

    O mașină poate fi marcată cu trei tipuri diferite de etichete de securitate, în funcție de nivelul de risc al amenințării:

    - `ANTI_VIRUS.VirusFound.threat=redus`, se aplică atunci când Bitdefender identifică un program malware cu risc redus, pe care îl poate șterge.
    - `ANTI_VIRUS.VirusFound.threat=mediu`, se aplică în cazul în care Bitdefender nu poate șterge fișierele infectate, dar le dezinfectează.
    - `ANTI_VIRUS.VirusFound.threat=ridicat`, e aplică în cazul în care Bitdefender nu poate șterge și nu poate dezinfecta fișierele infectate, dar blochează accesul la acestea.

    Dacă se identifică amenințări cu niveluri diferite de risc pe aceeași mașină, vor fi aplicate toate etichetele asociate. De exemplu, o mașină

pe care se identifică programe periculoase cu nivel ridicat și redus de risc vor avea ambele etichete de securitate.

> **Notă**
> Etichetele de securitate se găsesc în VMware vSphere, la **Rețea & securitate > Administratori NSX >** `Administrator NSX` **> Administrare > Etichete de securitate**.
> Deși puteți crea oricât de multe etichete doriți, numai cele trei etichete menționate funcționează cu Bitdefender.

6. **Restricționați atribuirea politicii din modul de vizualizare rețea**. Folosiți această opțiune pentru a controla dreptul administratorilor de rețea de a modifica politicile mașinilor virtuale prin intermediul vizualizării **Calculatoare și mașini virtuale** din pagina **Rețea**. Atunci când este selectată această opțiune, administratorii pot modifica politicile mașinilor virtuale numai din modul de vizualizare **Mașini virtuale** al inventarului rețelei.
7. Faceți clic pe **Save**. Vi se va solicita să acceptați certificatele de securitate pentru vCenter Server și NSX Manager. Aceste certificate asigură o comunicare securizată între componentele GravityZone și VMware, eliminând riscul atacurilor prin intermediari.

   Puteți verifica dacă ați instalat certificatele corecte comparând informațiile din browser-ul site-ului pentru fiecare componentă VMware cu informațiile despre certificat afișate în Control Center.
8. Selectați casetele de bifare pentru a accepta utilizarea certificatelor.
9. Faceți clic pe **Save**. Veți putea vizualiza Serverul vCenter în lista integrărilor active.
10. Dacă utilizați platforma NSX-V:
    a. Mergeți la secțiunea **Actualizare > Componente**.
    b. Descărcați și apoi publicați pachetul **Security Server (VMware cu NSX)**. Pentru mai multe informații cu privire la actualizarea componentelor GravityZone, consultați „Actualizare GravityZone” (p. 184).
    c. Mergeți la fila **Configurare > Furnizori de virtualizare**.
    d. În coloana **Acțiune**, faceți clic pe butonul **Înregistrare** afferent vCenter înregistrat cu NSX pentru a înregistra serviciul Bitdefender cu Managerul NSX VMware.

Avertisment
Dacă certificatul de securitate a expirat, iar vCenter încearcă să se sincronizeze, se va afișa o fereastră derulantă în care vi se va solicita să îl actualizați. Accesați fereastra de configurare a integrării cu vCenter Server integration, faceți clic pe **Salvare**, acceptați noile certificate și apoi faceți din nou clic pe **Salvare**.

După înregistrare, Bitdefender adaugă în consola VMware vSphere:
- Serviciul Bitdefender
- Manager servicii Bitdefender
- Trei profiluri de servicii implicite noi pentru modurile de scanare permisiv, normal și agresiv.

Notă
Puteți vizualiza aceste profiluri de servicii și pe pagina **Politici** din Control Center. Faceți clic pe butonul **Coloane** din colțul din dreapta al ferestrei pentru informații suplimentare.

La final, veți putea vedea dacă Serverul vCenter se sincronizează. Așteptați câtva minute până la încheierea sincronizării.

Integrare cu XenServer

Puteți integra GravityZone cu unul sau mai multe sisteme XenServer.

Pentru a configura integrarea cu XenServer:

1. Mergeți la pagina **Configurație** din Control Center și faceți clic pe fila **Furnizori virtualizare**.
2. Dați clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați **XenServer** din meniu. Va apărea o fereastră de configurare.
3. Specificați detaliile XenServer.
   - Denumirea sistemului XenServer în Control Center
   - Denumirea gazdei sau adresa IP a sistemului XenServer
   - Portul XenServer (implicit 443)
4. Specificați datele care urmează să fie folosite pentru autentificarea la XenServer. Puteți alege să utilizați datele furnizate pentru integrarea cu Active Directory sau un alt set de date de autentificare.
5. **Restricționați atribuirea politicii din modul de vizualizare rețea**. Folosiți această opțiune pentru a controla dreptul administratorilor de rețea de a modifica

politicile mașinilor virtuale prin intermediul vizualizării **Calculatoare și mașini virtuale** din pagina **Rețea**. Atunci când este selectată această opțiune, administratorii pot modifica politicile mașinilor virtuale numai din modul de vizualizare **Mașini virtuale** al inventarului rețelei.

6. Faceți clic pe **Save**. Veți putea vizualiza Serverul vCenter Server în lista integrărilor active și veți vedea dacă se sincronizează. Așteptați câtva minute până la încheierea sincronizării.

Integrarea cu Nutanix Prism Element

Puteți integra GravityZone cu unul sau mai multe clustere Nutanix Prism Element, indiferent dacă sunt sau nu înregistrate în Nutanix Prism Central.

Pentru a configura integrarea cu Nutanix Prism Element:

1. Mergeți la pagina **Configurație** din Control Center și faceți clic pe fila **Furnizori virtualizare**.
2. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați **Nutanix Prism Element** din meniu. Va apărea o fereastră de configurare.
3. Specificați detaliile Nutanix Prism Element:
   - Denumirea Nutanix Prism Element în Control Center.
   - Adresa IP a unei mașini virtuale de tip controller (Controller Virtual Machine - CVM) din clusterul Nutanix Prism Element sau adresa IP de tip „Cluster Virtual IP”.
   - Portul Nutanix Prism Element (implicit: 9440).
4. Specificați datele de conectare care vor fi utilizate pentru autentificarea în Nutanix Prism Element.

   Important
   Utilizatorul ale cărui date de autentificare le furnizați trebuie să aibă drepturi de tip Cluster Admin sau User Admin în Nutanix Prism Element.

5. **Restricționați atribuirea politicii din modul de vizualizare rețea**. Folosiți această opțiune pentru a controla dreptul administratorilor de rețea de a modifica politicile mașinilor virtuale prin intermediul vizualizării **Computere și mașini virtuale** din pagina **Rețea**. Atunci când este selectată această opțiune,

administratorii pot modifica politicile mașinilor virtuale numai din modul de vizualizare Mașini virtuale al inventarului rețelei.

6. Faceți clic pe **Save**. Vi se va solicita să acceptați certificatele de securitate pentru Nutanix Prism. Aceste certificate asigură o comunicare securizată între GravityZone și Nutanix Prism Element, eliminând riscul atacurilor prin intermediari.

   Puteți verifica dacă ați instalat certificatele corecte comparând informațiile despre site din browser pentru fiecare cluster Nutanix Prism Element sau CVM cu informațiile despre certificat afișate în Control Center.

7. Selectați casetele de bifare pentru a accepta utilizarea certificatelor.

8. Faceți clic pe **Save**.

   Dacă ați introdus un IP CVM pentru a configura integrarea, vi se va solicita într-o nouă fereastră să specificați dacă doriți să folosiți IP-ul virtual a cluster-ului în locul IP-ului CVM:

   a. Dați clic pe **Da** pentru a utiliza IP-ul virtual al cluster-ului în vederea integrării. IP-ul virtual al cluster-ului va înlocui IP-ul CVM în detaliile Nutanix Prism Element.

   b. Dați clic pe **Nu** pentru a folosi în continuare IP-ul CVM.

      Notă
      Conform celor mai bune practici, se recomandă să utilizați IP-ul virtual al cluster-ului în locul IP-ului CVM. Astfel, integrarea rămâne activă chiar și atunci când un anumit sistem gazdă devine indisponibil.

   c. În fereastra **Adăugare Nutanix Prism Element**, dați clic pe **Salvare**.

Veți putea vizualiza Nutanix Prism Element în lista integrărilor active. Așteptați câteva minute până la finalizarea sincronizării.

Integrarea cu Amazon EC2

Puteți integra GravityZone cu inventarul Amazon EC2 și vă puteți proteja instanțele EC2 găzduite în cloud-ul Amazon.

Cerințe preliminare:

- Codurile de acces și cele secrete pentru un cont AWS valabil
- Contul AWS trebuie să includă următoarele permisiuni:

- `IAMReadOnlyAccess`
- `AmazonEC2ReadOnly` pentru toate regiunile AWS

Puteți crea mai multe integrări cu Amazon EC2. Pentru fiecare integrare, trebuie să furnizați un cont de utilizator AWS valabil.

Notă
Nu puteți adăuga mai multe integrări folosind datele de autentificare ale rolurilor IAM create pentru același cont AWS.

Pentru a integrare cu Amazon EC2:

1. Mergeți la pagina **Configurație** din Control Center și faceți clic pe fila **Furnizori virtualizare**.
2. Faceți clic pe butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați **Integrare cu Amazon EC2** din meniu. Va apărea o fereastră de configurare.
3. Specificați detaliile integrării cu Amazon EC2:
   - Numele integrării. Dacă adăugați mai multe integrări cu Amazon EC2, le puteți identifica după nume.
   - Codurile de acces și cele secrete pentru contul de utilizator AWS.
4. **Restricționați atribuirea politicii din modul de vizualizare rețea**. Folosiți această opțiune pentru a controla dreptul administratorilor de rețea de a modifica politicile mașinilor virtuale prin intermediul vizualizării **Calculatoare și mașini virtuale** din pagina **Rețea**. Atunci când este selectată această opțiune, administratorii pot modifica politicile mașinilor virtuale numai din modul de vizualizare **Mașini virtuale** al inventarului rețelei.
5. Faceți clic pe **Save**. Dacă datele de autentificare furnizate sunt corecte, integrarea va fi creată și adăugată în tabel.

Așteptați câteva momente până când GravityZone se sincronizează cu inventarul Amazon EC2.

Integrarea cu Microsoft Azure

Puteți integra GravityZone în Microsoft Azure și vă puteți proteja mașinile virtuale găzduite în cloud-ul Microsoft.

Cerințe preliminare:

- Aplicația Azure cu drepturi de citire
- ID Active Directory
- ID aplicație
- Cod de siguranță aplicație

Pentru mai multe detalii referitoare la obținerea datelor de autentificare necesare și configurarea aplicației Azure, consultați acest articol din Baza de cunoștințe.

Puteți crea mai multe integrări Microsoft Azure. Pentru fiecare integrare, trebuie să aveți un ID Active Directory valid.

Pentru a configura integrarea cu Microsoft Azure:

1. Mergeți la pagina **Configurație** din Control Center și faceți clic pe fila **Furnizori virtualizare**.
2. Accesați butonul ⊕ **Adăugare** din partea de sus a tabelului și selectați **AzureIntegration** din meniu. Va apărea o fereastră de configurare.
3. Specificați detaliile integrării cu Azure:
   - **Numele integrării.**. Dacă adăugați mai multe integrări cu Azure, le puteți identifica după nume.
   - **ID Active Directory**. Fiecare instanță Azure Active Directory are un cod unic de identificare, disponibil în detaliile contului Microsoft Azure.
   - **ID aplicație**. Fiecare aplicație Azure are un cod unic de identificare, disponibil în detaliile aplicației.
   - **Cod de siguranță aplicație**. Codul secret al aplicației este reprezentat de valoarea afișată atunci când este salvată o cheie în setările aplicației Azure.
4. Selectați opțiunea **Restricționarea atribuirii politicii din fereastra de rețea** pentru a modifica politica doar din fereastra **Mașini virtuale**. Dacă este deselectată, puteți modifica politica din fereastra **Computere și mașini virtuale**.
5. Faceți clic pe **Save**. Dacă datele de autentificare furnizate sunt corecte, integrarea va fi creată și adăugată în tabel.

Așteptați câteva momente până când GravityZone se sincronizează cu inventarul Microsoft Azure.

Administrarea integrărilor cu platforma

Pentru a edita sau actualiza integrarea cu o platformă:

1. În Control Center, mergeți la fila **Configurare > Furnizori de virtualizare**.

2. Faceți clic pe butonul **Editare** din coloana **Acțiune**.
3. Configurați setările regulii după cum este nevoie. Pentru mai multe informații, consultați una dintre următoarele secțiuni, după caz:
   - „Integrare cu vCenter Server” (p. 86)
   - „Integrare cu XenServer” (p. 89)
   - „Integrarea cu Nutanix Prism Element” (p. 90)
   - „Integrarea cu Amazon EC2” (p. 91)
   - „Integrarea cu Microsoft Azure” (p. 92)
4. Faceți clic pe **Save**. Așteptați câteva minute până când serverul reia sincronizarea.

Integrările Nutanix Prism Element, Amazon EC2 și Microsoft Azure sunt sincronizate în mod automat o dată la 15 minute. Puteți sincroniza manual o integrare în orice moment, după cum urmează:

1. În Control Center, mergeți la fila **Configurare > Furnizori de virtualizare**.
2. Faceți clic pe butonul **Resincronizare inventar** din rubrica **Acțiune**.
3. Faceți clic pe **Da** pentru a confirma acțiunea.

Butonul **Resincronizare inventar** este util cu precădere atunci când starea integrării se modifică și trebuie sincronizată, ca în următoarele situații:

- Pentru integrarea Nutanix Prism Element:
  - Utilizatorul nu mai are drepturi de administrator asupra inventarului.
  - Utilizatorul nu mai este valabil (parolă modificată sau ștearsă)
  - Certificatul de securitate nu mai este valabil.
  - Intervine o eroare de conexiune.
  - Se adaugă sau se elimină un sistem gazdă în/din cluster-ul Nutanix Prism Element.
- Pentru integrarea Microsoft Azure:
  - Se adaugă sau se elimină un abonament în/din Microsoft Azure.
  - Se adaugă sau se elimină mașini virtuale în/din inventarul Microsoft Azure.

De asemenea, puteți sincroniza integrarea dând clic pe butonul **Modificare** și apoi pe **Salvare**.

Pentru a elimina o integrare vShield, XenServer, Nutanix Prism Element, Amazon EC2 sau Microsoft Azure:

1. În Control Center, mergeți la fila **Configurare > Furnizori de virtualizare**.
2. Faceți clic pe butonul ⊗ **Ștergere** din coloana **Acțiunee**, corespunzător integrării pe care doriți să o ștergeți.
3. Faceți clic pe **Da** pentru a confirma acțiunea.

Pentru a șterge o integrare NSX:

1. Autentificați-vă pe consola VMware vSphere și ștergeți toate politicile Bitdefender și Security Server.
2. În Control Center, mergeți la fila **Configurare > Furnizori de virtualizare**.
3. În coloana **Acțiune**, corespunzătoare integrării pe care doriți să o ștergeți, faceți clic pe ⊗ **Anulare înregistrare** și apoi pe ⊗ **Ștergere**.
4. Faceți clic pe **Da** pentru a confirma acțiunea.

Pentru a vă asigura că sunt afișate cele mai recente informații, faceți clic pe butonul **Reîmprospătare** din partea de sus a tabelului.

Furnizori de servicii de securitate

GravityZone Security for Virtualized Environments se integrează cu VMware NSX-T Data Center prin NSX-T Manager.

Integrarea cu NSX-T Manager

NSX-T Manager este planul de administrare al serverelor dumneavoastră vCenter, integrat cu un centru de date NSX-T. Pentru ca integrarea să funcționeze, este necesar să configurați integrarea serverelor vCenter asociate cu NSX-T Manager. Pentru informații suplimentare, consultați secțiunea Integrarea cu vCenter Server.

Pentru a configura integrarea cu NSX-T Manager:

1. În Control Center, navigați la **Configurare > Furnizori de servicii de virtualizare > Furnizori de securitate**.
2. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Va apărea o fereastră de configurare.
3. Specificați detaliile integrării cu NSX-T:
   - Numele integrării NSX-T.

- Denumirea gazdei sau adresa IP a sistemului vCenter Server asociat.
- Portul NSX-T (implicit 433).

4. Specificați datele care urmează să fie folosite pentru autentificarea la vCenter Server. Puteți alege să utilizați datele furnizate pentru integrarea cu Active Directory sau un alt set de date de autentificare. Utilizatorul ale cărui date le furnizați trebuie să aibă drepturi de administrator de nivel principal pe Serverul vCenter.
5. Faceți clic pe **Save**.

   Control Center este acum integrată cu NSX-T. Pentru a aplica protecția la nivel de endpoint pe mașinile dumneavoastră virtuale prin intermediul politicii GravityZone Guest Introspection, consultați articolul din baza de cunoștințe (KB) intitulat Configurarea și aplicarea protecției la nivel de endpoint pe mașinile virtuale gazdă VMware NSX prin intermediul politicii GravityZone Guest Introspection.

Notă
GravityZone poate fi utilizat numai pentru a proteja sistemul vCenter Server asociat.

NTSA

În cadrul acestei secțiuni, puteți configura integrarea cu Bitdefender Network Traffic Security Analytics, o soluție de securitate pentru companii ce detectează cu precizie breșele de securitate a datelor și oferă informații detaliate cu privire la atacurile avansate analizând traficul din rețea. Pentru a afla mai multe despre această soluție, consultați Documentația Bitdefender NTSA.

Important
Secțiunea integrării cu NTSA este disponibilă numai după introducerea unei licențe NTSA valide în pagina **Configurare > Licență**.

Pentru a configura integrarea cu NTSA, este necesar să aveți instalată soluția NTSA în mediul dumneavoastră și să dispuneți de datele de autentificare pentru accesarea consolei web NTSA.

În timpul integrării, vi se va solicita să furnizați adresa consolei web NTSA (adresa IP sau numele de gazdă) și un cod (cheie de asociere) generat în consola web NTSA, după cum se explică mai jos.

Configurarea integrării cu NTSA

1. Conectați-vă la GravityZone Control Center.
2. Accesați pagina **Configurare** și selectați fila NTSA.
3. Activați opțiunea **Integrare cu Network Traffic Security Analytics (NTSA)**.
4. Introduceți următoarele date:
   - Adresa consolei web NTSA (adresa IP / nume gazdă).
   - Portul utilizat de GravityZone pentru a comunica cu NTSA (443 în mod implicit).
   - Cheia de asociere (codul) generat de consola web NTSA, după cum urmează:
     a. Autentificați-vă în consola web NTSA și accesați pagina **Licențiere**.
     b. Selectați opțiunea **Integrarea cu GravityZone**.
     c. Selectați opțiunea **Generează o cheie de asociere**. Cheia va apărea automat.
     d. Utilizați butonul **Copiere în clipboard** pentru a prelua cheia de asociere.
     e. Faceți clic pe **OK** pentru confirmare.
5. Verificați dacă amprenta afișată a gazdei corespunde codului hash al certificatului SSL din aplicația NTSA, apoi activați opțiunea **Accept certificatul**.
6. Faceți clic pe **Save**.

După ce configurarea s-a finalizat cu succes, integrarea va fi afișată ca fiind **Sincronizată**. Integrarea cu NTSA poate avea următoarele stări:

- **Nu este cazul**: integrarea încă nu a fost configurată.
- **Sincronizată**: integrarea este configurată și activată.
- **Cod incorect**: cheia de asociere din consola web NTSA nu este validă.
- **Eroare de conexiune**: nu se poate stabili conexiunea la consola web NTSA folosind adresa specificată (adresă IP incorectă / nume gazdă incorect).
- **Eroare de certificat**: amprenta actuală a certificatului SSL din aplicația NTSA nu se potrivește cu amprenta acceptată inițial.
- **Eroare necunoscută**: există o eroare necunoscută de comunicație.

Câmpul **Ultima modificare de stare** afișează data și ora ultimei modificări reușite a setărilor de integrare sau când s-a modificat starea integrării.

Odată ce integrarea cu NTSA a fost configurată, puteți dezactiva/activa integrarea utilizând caseta disponibilă în partea de sus a paginii **NTSA**.

Asocierea conturilor GravityZone și NTSA

După configurarea integrării, conturile dumneavoastră GravityZone și NTSA vor fi conectate și veți putea naviga cu ușurință la consola web NTSA, după cum urmează:

1. În GravityZone Control Center, apăsați pe butonul **NTSA** poziționat în colțul din stânga jos al ferestrei.
2. Se va face redirecționarea către pagina de autentificare a consolei web NTSA. După introducerea datelor dumneavoastră de autentificare pentru NTSA, puteți începe să navigați prin consola web NTSA.

   Este necesar să introduceți datele dumneavoastră de autentificare pentru NTSA numai prima dată. După aceea, veți avea automat acces la consola web NTSA făcând clic pe butonul **NTSA**, fără să vi se solicite să vă autentificați.

Ștergere integrării cu NTSA

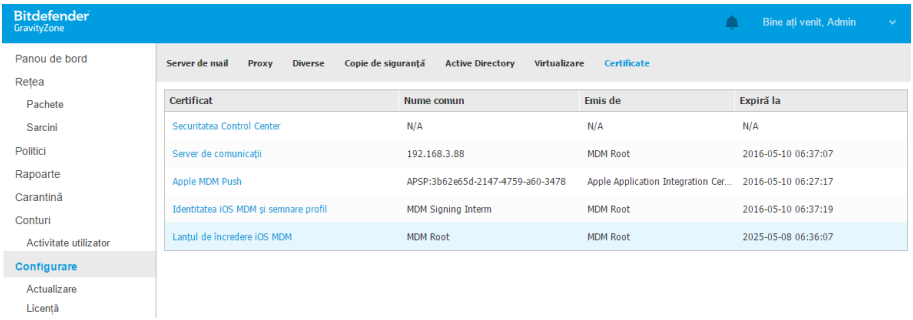
Ștergerea cheii de licență NTSA din pagina **Configurare > Licență** va determina, de asemenea, ștergerea integrării cu NTSA.

Notă
Se va elimina asocierea dintre conturile dumneavoastră NTSA și GravityZone în următoarele situații:

- Cheia de licență NTSA a fost ștearsă.
- Parola dumneavoastră NTSA a fost modificată.
- Parola GravityZone a fost modificată.
- Setările de integrare cu NTSA au fost modificate.

Certificate

Pentru o funcționare corectă a configurației GravityZone și într-o manieră sigură, trebuie să creați și să adăugați o serie de certificate de securitate în Control Center.



Pagina Certificate

Control Center suportă următoarele formate de certificat:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)

Notă
Următoarele certificate sunt necesare exclusiv pentru administrarea securității pe dispozitivele Apple iOS:

- Certificat server de comunicații
- Certificat de Server de incidente
- Certificatul Apple MDM Push
- Certificat de identitate iOS MDM și de semnare a profilului
- Certificat lanț de încredere iOS MDM

Dacă nu doriți să rulați aplicația de administrare a dispozitivelor mobile iOS, nu trebuie să furnizați aceste certificate.

Certificat de securitate Control Center

Certificatul de securitate Control Center este necesar pentru identificarea consolei Control Center ca și website de încredere în browser-ul web. În mod implicit, Control Center folosește un certificat SSL semnat de Bitdefender. Acest certificat încorporat nu este recunoscut de browser-ele web și atrage avertismente de securitate. Pentru a evita avertismentele de securitate ale browser-ului, adăugați un certificat SSL

semnat de către compania dumneavoastră sau de o Autoritate de certificare (CA) externă.

Pentru a adăuga sau înlocui certificatul Control Center:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe denumirea certificatului.
3. Selectați tipul de certificat (cu cod privat separat sau încorporat).
4. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
5. Pentru certificatele cu cheie privată separată, faceți clic pe butonul **Adăugare** de lângă câmpul **Cheie privată** și încărcați codul privat.
6. În cazul în care certificatul este protejat cu parolă, introduceți parola în câmpul corespunzător.
7. Faceți clic pe **Save**.

Certificat de securitate pentru comunicații între stația de lucru și Security Server

Acest certificat asigură o conexiune sigură între agenții de securitate și Security Server (multi-platformă) atribuit de aceștia.

În timpul instalării, Security Server generează un certificat auto-semnat implicit. Puteți înlocui acest certificat încorporat adăugând unul la alegere din Control Center.

Pentru a adăuga sau înlocui un Certificat de comunicații între stația de lucru și Security Server:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe denumirea certificatului.
3. Selectați tipul de certificat (cu cod privat separat sau încorporat).
4. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
5. Pentru certificatele cu cheie privată separată, faceți clic pe butonul **Adăugare** de lângă câmpul **Cheie privată** și încărcați codul privat.
6. În cazul în care certificatul este protejat cu parolă, introduceți parola în câmpul corespunzător.

7. Faceți clic pe **Save**. Este posibil să se afișeze un mesaj de avertizare dacă certificatul este auto-semnat sau expirat. Dacă este expirat, vă rugăm să vă reînnoiți certificatul.
8. Dați clic pe **Da** pentru a continua încărcarea certificatului. Imediat după finalizarea încărcării, Control Center trimite certificatul de securitate către Security Server.

Dacă este nevoie, puteți reveni la certificatul încorporat inițial al fiecărui Security Server, după cum urmează:

1. Dați clic pe numele certificatului din pagina **Certificate**.
2. Selectați **Niciun certificat (utilizare certificat implicit)** la tipul certificatului.
3. Faceți clic pe **Save**.

Certificat server de comunicații

Certificatul Serverului de comunicații este utilizat pentru securizarea interacțiunii dintre Serverul de comunicații și dispozitivele mobile iOS.

Cerințe:

- Acest certificat SSL poate fi semnat de compania dumneavoastră sau de o Autoritate de certificare externă.

  Avertisment
  Acest certificat poate fi invalidat dacă nu este emis de o autoritate de certificare publică/sigură (de exemplu, certificate auto-semnate).

- Denumirea comună a certificatului trebuie să corespundă exact denumirii de domeniu sau adresei IP utilizate de clienții mobili pentru a se conecta la Serverul de comunicații. Acesta este configurat ca și adresă MDM externă în interfața de configurare a consolei aplicației GravityZone.
- Clienții mobili trebuie să confirme acest certificat. În acest scop, trebuie să adăugați și iOS MDM Trust Chain.

Pentru a adăuga sau înlocui certificatul Serverului de comunicații:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe denumirea certificatului.
3. Selectați tipul de certificat (cu cod privat separat sau încorporat).

4. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
5. Pentru certificatele cu cheie privată separată, faceți clic pe butonul **Adăugare** de lângă câmpul **Cheie privată** și încărcați codul privat.
6. În cazul în care certificatul este protejat cu parolă, introduceți parola în câmpul corespunzător.
7. Faceți clic pe **Save**.

Certificat de Server de incidente

Pentru a adăuga sau înlocui certificatul de Server de incidente:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe denumirea certificatului.
3. Selectați tipul de certificat (cu cod privat separat sau încorporat).
4. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
5. Pentru certificatele cu cheie privată separată, faceți clic pe butonul **Adăugare** de lângă câmpul **Cheie privată** și încărcați codul privat.
6. În cazul în care certificatul este protejat cu parolă, introduceți parola în câmpul corespunzător.
7. Faceți clic pe **Save**.

Certificatul Apple MDM Push

Apple solicită un certificat MDM Push pentru asigurarea unei comunicări securizate între Serverul de comunicații și serviciul de Notificări Push Apple (APN) la transmiterea notificărilor de tip push. Notificările de tip push sunt utilizate pentru solicitarea conectării dispozitivelor la Serverul de comunicații când sunt disponibile opțiuni noi sau modificări de politică.

Apple emite acest certificat direct companiei, însă Solicitarea de semnare a certificatului (CSR) trebuie să fie semnată de Bitdefender. Centrul de control oferă un asistent care vă ajută să obțineți cu ușurință certificatul Apple MDM Push.

Important

- Pentru obținerea și administrarea certificatului, aveți nevoie de un ID Apple. Dacă nu aveți un ID Apple, îl puteți crea accesând pagina ID-ul meu Apple. La crearea ID-ului Apple, folosiți o adresă de e-mail generică și nu adresa de serviciu, deoarece veți avea nevoie de aceasta la reînnoirea certificatului.
- Site-ul Apple nu funcționează corect în browserul Internet Explorer. Vă recomandăm să utilizați cele mai recente versiuni de Safari sau Chrome.
- Certificatul Apple MDM Push este valabil timp de un an. Atunci când certificatul se apropie de data de expirare, trebuie să-l reînnoiți și să importați certificatul reînnoit în Control Center. Dacă lăsați certificatul să expire, trebuie să creați unul nou și să vă reactivați toate dispozitivele.

Adăugarea unui certificat Apple MDM Push

Pentru a obține certificatul Apple MDM Push și pentru a-l importa în Control Center:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe numele certificatului și urmați instrucțiunile asistentului de configurare, după cum este descris mai jos:

   Pasul 1 - Obținere solicitare de semnare a certificatului semnată de Bitdefender

   Selectați opțiunea corespunzătoare:

   - **Trebuie să generez o solicitare de semnare a certificatului semnată de Bitdefender** (recomandat)
     a. Introduceți numele companiei, numele dvs. complet și adresa de e-mail în câmpurile corespunzătoare.
     b. Faceți clic pe **Generare** pentru a descărca fișierul CSR semnat de Bitdefender.
   - **Am deja o solicitare de semnare a certificatului și trebuie să obțin semnătura Bitdefender**
     a. Încărcați fișierul CSR și cheia privată asociată făcând clic pe butonul **Adăugare** din dreptul câmpurilor corespunzătoare.

        Serverul de comunicații necesită o cheie privată la autentificarea pe serverele APN.
     b. Specificați parola care protejează cheia privată, dacă există.
     c. Faceți clic pe butonul **Semnare** pentru a descărca fișierul CSR semnat de Bitdefender.

Pasul 2 - Solicitare certificat push de la Apple

a. Faceți clic pe link-ul **Portal Certificate Push Apple** și autentificați-vă folosind ID-ul Apple și parola dvs.
b. Faceți clic pe butonul **Create a Certificate** și acceptați Condițiile de utilizare.
c. Faceți clic pe **Choose file**, selectați fișierul CSR și apoi faceți clic pe **Upload**.

> **Notă**
> Este posibil ca butonul **Choose file** să poarte altă denumire, precum **Choose** sau **Browse**, în funcție de browserul folosit.

d. Din pagina de confirmare, faceți clic pe butonul **Download** pentru a obține certificatul MDM Push.
e. Reveniți la asistentul de configurare din Control Center.

Pasul 3 - Importare certificat push Apple

Faceți clic pe butonul **Adăugare certificat** și încărcați fișierul certificatului din calculator.

Puteți verifica detaliile certificatului în câmpul de mai jos.

3. Faceți clic pe **Save**.

Reînnoirea certificatului Apple MDM Push

Pentru a reînnoi certificatul Apple MDM și pentru a-l actualiza în Control Center:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe numele certificatului pentru a deschide asistentul de import.
3. Obțineți o Solicitare de semnare a certificatului semnată de Bitdefender. Procedura este aceeași ca și în cazul obținerii unui nou certificat.
4. Faceți clic pe link-ul **Portal Certificate Push Apple** și autentificați-vă folosind același ID Apple utilizat pentru crearea certificatului.
5. Localizați certificatul MDM Push pentru Bitdefender și faceți clic pe butonul **Renew** corespunzător.
6. Faceți clic pe **Choose file**, selectați fișierul CSR și apoi faceți clic pe **Upload**.
7. Faceți clic pe **Download** pentru a salva certificatul pe calculatorul dumneavoastră.
8. Reveniți la Control Center și importați noul certificat push Apple.
9. Faceți clic pe **Save**.

Certificat de identitate iOS MDM și de semnare a profilului

Certificatul de identitate iOS MDM și de semnare a profilului este utilizat de Serverul de comunicații pentru semnarea certificatelor de identitate și configurarea profilelor transmise către dispozitivele mobile.

Cerințe:

- Trebuie să fie un certificat Intermediar sau Final, semnat de către companie sau de o Autoritate externă de certificare.
- Clienții mobili trebuie să confirme acest certificat. În acest scop, trebuie să adăugați și iOS MDM Trust Chain.

Pentru a adăuga sau înlocui un certificat de identitate iOS MDM și de semnare a profilului:

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.
2. Faceți clic pe denumirea certificatului.
3. Selectați tipul de certificat (cu cod privat separat sau încorporat).
4. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
5. Pentru certificatele cu cheie privată separată, faceți clic pe butonul **Adăugare** de lângă câmpul **Cheie privată** și încărcați codul privat.
6. În cazul în care certificatul este protejat cu parolă, introduceți parola în câmpul corespunzător.
7. Faceți clic pe **Save**.

Certificat lanț de încredere iOS MDM

Certificatele de tip „lanț de încredere iOS MDM" sunt necesare pe telefoanele mobile pentru asigurarea faptului că acestea confirmă certificatul Serverului de comunicații și certificatul de identitate iOS MDM și de semnare a profilului. Serverul de comunicații transmite acest certificat aparatelor mobile în timpul activării.

Lanțul de încredere iOS MDM trebuie să includă toate certificatele intermediare până la cel principal aferente companiei sau certificatele intermediare emise de către Autoritatea de certificare.

Pentru a adăuga sau înlocui certificatele de tip „lanț de încredere iOS MDM":

1. Mergeți la pagina **Configurare** și dați clic pe fila **Certificate**.

2. Faceți clic pe denumirea certificatului.
3. Faceți clic pe butonul **Adăugare** de lângă câmpul **Certificate** și încărcați certificatul.
4. Faceți clic pe **Save**.

Depozit

Această filă include informații despre produs și actualizările agentului de securitate, inclusiv versiunile de produs stocate pe serverul de actualizări și versiunile disponibile în locația oficială de tip repository a Bitdefender, ciclurile de actualizări, data și ora actualizării și ultima verificare pentru versiuni noi.

Notă
Versiunile produsului nu sunt disponibile pentru serverele de securitate.

5.1.5. Gestionarea aplicației GravityZone

Aplicația GravityZone este furnizată cu o interfață de configurare de bază, disponibilă din instrumentul de administrare folosit pentru administrarea mediului virtualizat în care ați instalat aplicația.

Acestea sunt principalele opțiuni disponibile după prima instalare a aplicației GravityZone:

- Configurarea setărilor pentru denumirea gazdei
- Configurare setări rețea
- Configurare setări proxy
- Server de comunicații MDM
- Setări avansate
- Configurare limbă

Utilizați tastele săgeți și tasta `Tab` pentru a naviga prin meniuri și opțiuni. Apăsați `Enter` pentru a selecta o anumită opțiune.

Configurarea denumirii gazdei și setări

Comunicarea cu rolurile GravityZone se realizează folosind adresa IP sau denumirea DNS a aplicației pe care sunt instalate. În mod implicit, componentele GravityZone comunică prin intermediul adresei IP. Dacă doriți să permiteți comunicarea prin

denumirile DNS, trebuie să configurați aplicațiile GravityZone cu o denumire DNS și să vă asigurați că aceasta corespunde adresei IP configurate a aplicației.

Cerințe preliminare:

- Configurați înregistrare DNS pe serverul DNS.
- Denumirea DNS trebuie să corespundă adresei IP configurate a aplicației. Prin urmare, trebuie să vă asigurați că aplicația este configurată cu adresa IP corespunzătoare.

Pentru a configura setările pentru denumirea gazdei:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Configurarea setărilor pentru denumirea gazdei**.
3. Introduceți denumirea gazdei aplicației și numele de domeniu Active Directory (dacă este necesar).
4. Selectați **OK** pentru a salva modificările.

Configurare setări rețea

Puteți configura aplicația pentru a obține automat setările rețelei de la serverul DHCP sau puteți configura manual setările rețelei. Dacă optați pentru utilizarea DHCP, trebuie să configurați Serverul DHCP pentru rezervarea unei anumite adrese IP pentru aplicație.

Pentru configurarea setărilor de rețea:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Configurare setări rețea**.
3. Selectați interfața rețelei (implicit, `eth0`).
4. Selectați metoda de configurare:
   - **Configurare manuală setări rețea.** Trebuie să specificați adresa IP, masca de rețea, adresa portului și adresele serverului DNS.
   - **Obținere automată setări rețea, prin DHCP.** Utilizați această opțiune numai dacă ați configurat Serverul DHCP pentru rezervarea unei anumite adrese IP pentru aplicație.

5. Puteți verifica detaliile configurației IP curente sau starea legăturii selectând opțiunile corespunzătoare.

Configurare setări proxy

În cazul în care dispozitivul dispune de o conexiune la Internet printr-un server proxy, trebuie să configurați setările proxy.

Notă
Setările serverului proxy pot fi configurate și din Control Center, pagina **Configurare > Proxy**. Modificarea setărilor serverului proxy dintr-o locație le actualizează automat și în alte locații.

Pentru a configura setările proxy:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Configurare setări proxy**.
3. Selectați **Configurare stări proxy**.
4. Introduceți adresa serverului proxy. Utilizați următoarea sintaxă:
   - Dacă serverul proxy nu necesită autentificare:
     `http(s)://<IP/hostname>:<port>`
   - Dacă serverul proxy necesită autentificare:
     `http(s)://<username>:<password>@<IP/hostname>:<port>`
5. Selectați **OK** pentru a salva modificările.

Selectați **Afișare informații proxy** pentru a verifica setările proxy.

Server de comunicații MDM

Notă
Această configurație este necesară numai pentru administrarea dispozitivelor mobile în cazul în care cheia de licență include serviciul Security for Mobile. Opțiunea apare în meniu după instalarea rolului de server de comunicații.

În configurația implicită GravityZone, dispozitivele mobile pot fi administrate numai dacă sunt direct conectate la rețeaua companiei (prin Wi-Fi sau VPN). Acest lucru

se întâmplă deoarece la înregistrarea dispozitivelor mobile, acestea sunt configurate pentru a se conecta la adresa locală a aplicației Serverului de comunicații.

Pentru a putea administra dispozitivele prin Internet, indiferent de locația acestora, trebuie să configurați Serverul de comunicații cu o adresă ce poate fi accesată public.

Pentru a putea administra dispozitivele mobile atunci când nu sunt conectate la rețeaua companiei, sunt disponibile următoarele opțiuni:

- Configurați redirecționarea portului pe gateway-ul companiei pentru aplicația care îndeplinește rolul de Server de comunicații.
- Adăugați un adaptor de rețea suplimentar care îndeplinește rolul de Server de comunicații și alocați-i o adresă IP publică.

În ambele cazuri, trebuie să configurați Serverul de comunicații cu adresa externă care va fi utilizată pentru administrarea dispozitivului mobil:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Server de comunicații MDM**.
3. Selectați **Configurare adresă externă Server MDM**.
4. Introduceți adresa externă.

   Utilizați următoarea sintaxă: `https://<IP/Domain>:<Port>`.

   - Dacă utilizați opțiunea de redirecționare a portului, trebuie să introduceți adresa IP publică sau numele de domeniu și portul deschis pe portal.
   - Dacă folosiți o adresă publică pentru Serverul de comunicații, trebuie să introduceți adresa IP publică sau numele de domeniu și portul Serverului de comunicații. Portul implicit este 8443.
5. Selectați **OK** pentru a salva modificările.
6. Selectați **Afișare adresă externă server MDM** pentru a verifica setările.

Setări avansate

Setările avansate acoperă diferite opțiuni de instalare manuală, extensii de mediu și îmbunătățiri privind securitatea:

- Instalare/dezinstalare roluri

- Instalarea Security Server
- Stabilire parolă nouă pentru baza de date
- Server de actualizări
- Configurare elemente echilibrare roluri
- Set de duplicate
- Activare Cluster VPN Securizat
- Conectare la o bază de date existentă
- Conectare la baza de date existentă (Cluster VPN Securizat)
- Verificare cluster securizat VPN

Disponibilitatea opțiunilor variază în funcție de rolurile instalate și de serviciile activate. Spre exemplu, dacă rolul de Server de baze de date nu este instalat pe aplicație, puteți instala doar roluri sau vă puteți conecta doar la o bază de date GravityZone instalată în rețeaua dvs. După instalarea rolului de Server de baze de date pe aplicație, opțiunile de conectare la o altă bază de date nu mai sunt disponibile.

Instalare/dezinstalare roluri

Aplicația GravityZone poate rula una, mai multe sau toate rolurile următoare:

- **Server de baze de date**
- **Server de actualizări**
- **Consolă Web**
- **Server de comunicații**
- **Server incidente**

O configurare GravityZone necesită rularea unei instanțe a fiecărui rol. Prin urmare, în funcție de modul în care preferați să distribuiți rolurile GravityZone, veți instala una până la patru aplicații GravityZone. Rolul de Server de baze de date este primul care va fi instalat. Într-un scenariu cu mai multe aplicații GravityZone, veți instala Serverul de baze de date pe prima aplicație și veți configura toate celelalte aplicații pentru a se conecta la instanța de bază de date existentă.

Notă

Puteți instala instanțe suplimentare ale rolurilor specifice, folosind elementele de echilibrare a rolurilor. Pentru mai multe informații, consultați capitolul „Configurare elemente echilibrare roluri” (p. 114).

Pentru a instala rolurile GravityZone:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Instalare/dezinstalare roluri**.
4. Selectați **Adăugare sau ștergere roluri**.
5. Continuați în funcție de situația actuală:
   - Dacă aceasta este configurarea inițială a aplicației GravityZone, apăsați bara de `Spațiu` și apoi apăsați `Enter` pentru instalarea rolului de Server de bază de date. Trebuie să confirmați alegerea apăsând din nou `Enter`. Configurați parola pentru baza de date și apoi așteptați finalizarea instalării.
   - Dacă ați instalat deja o altă aplicație cu rol de Server de bază de date, selectați **Anulare** și reveniți la meniul **Adăugare sau ștergere roluri**. Apoi, trebuie să selectați **Configurare adresă bază de date** și să introduceți adresa serverului de bază de date. Asigurați-vă că setați o parolă pentru baza de date înainte de a accesa această opțiune. Dacă nu cunoașteți parola pentru baza de date, configurați una nouă selectând **Setări avansate > Setare parolă nouă pentru baza de date** din meniul principal.

     Utilizați următoarea sintaxă: `http://<IP/Hostname>:<Port>`. Portul implicit al bazei de date este 27017. Introduceți parola primară pentru baza de date.
6. Instalați celelalte roluri selectând **Adăugare sau ștergere roluri** din meniul **Instalare/Dezinstalare roluri** și apoi rolurile pe care doriți să le instalați. Pentru fiecare rol pe care doriți să-l instalați sau dezinstalați, apăsați bara de `Spațiu` pentru a selecta sau deselecta rolul și apoi apăsați `Enter` pentru continuare. Trebuie să confirmați selecția apăsând `Enter` din nou și apoi să așteptați până la finalizarea instalării.

Notă

Fiecare rol este în mod normal instalat în câteva minute. În timpul instalării, fișierele necesare sunt descărcate de pe Internet. Prin urmare, instalarea durează mai mult timp dacă conexiunea la Internet este lentă. Dacă instalarea stagnează, reluați configurarea aplicației.

Puteți vizualiza rolurile instalate și IP-urile aferente selectând din meniul **Instala/dezinstalare roluri** una dintre opțiunile următoare:

- **Afișare roluri instalate local**, pentru a vizualiza doar rolurile instalate pe aplicația respectivă.
- **Afișare toate rolurile instalate**, pentru a vizualiza toate rolurile instalate în mediul dumneavoastră GravityZone.

Instalarea Security Server

Notă
Security Server va putea fi utilizat numai dacă licența dumneavoastră permite acest lucru.

Puteți instala Security Server din interfața de configurare a aplicației GravityZone, direct în aplicația GravityZone, sau din Control Center ca aplicație independentă. Avantajele instalării Security Server din aplicație sunt următoarele:

- Adecvat pentru configurări GravityZone cu o singură aplicație având toate rolurile.
- Puteți vizualiza și utiliza Security Server fără să fie necesar să integrați GravityZone cu o platformă de virtualizare.
- Mai puține operațiuni de configurare de efectuat.

Cerințe preliminare:

Aplicația GravityZone trebuie să aibă instalat rolul de Server de baze de date, sau trebuie să fie configurată pentru a se conecta la o bază de date existentă.

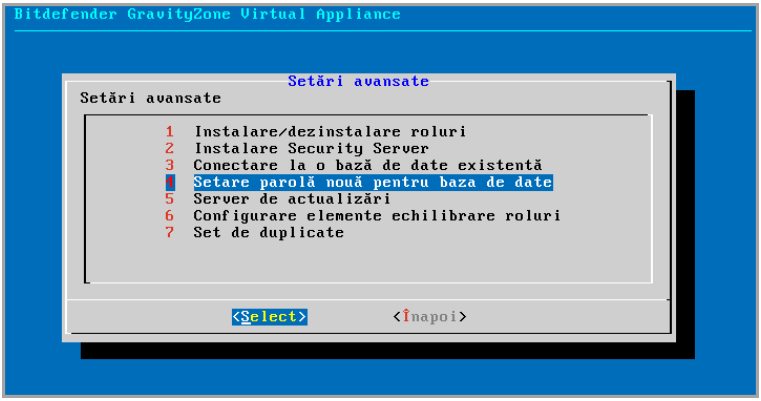
Pentru a instala Security Server din interfața aplicației:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Instalare Security Server**. Va apărea un mesaj de confirmare.
4. Apăsați `Enter` pentru confirmare și așteptați finalizarea instalării.

Notă
Puteți dezinstala acest Security Server numai din meniul **Setări avansate** din interfața aplicației.

Stabilire parolă nouă pentru baza de date

La instalarea rolului de Server de baze de date, vi se solicită să configurați o parolă pentru protejarea bazei de date. Dacă doriți să o modificați, configurați o altă parolă accesând **Setări avansate >; Stabilire parolă nouă pentru baza de date** din meniul principal.



Interfață consolă aplicație: Opțiunea Configurare parolă nouă pentru baza de date

Urmați liniile directoare pentru configurarea unei parole puternice.

Configurare server de actualizări

Aplicația GravityZone este, în mod implicit, configurată pentru preluarea actualizărilor de pe Internet. Dacă preferați, puteți configura aplicațiile instalate să se actualizeze de la serverul local de actualizări Bitdefender (aplicația GravityZone cu rolul de Server de actualizări instalat).

Pentru a configura adresa serverului de actualizări:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Server de actualizări**.
4. Selectați **Configurare adresă actualizări**.

5. Introduceți adresa IP sau numele gazdei aplicației care îndeplinește rolul de Server de actualizări. Portul implicit al Serverului de actualizări este 7074.

Configurare elemente echilibrare roluri

Pentru a asigura fiabilitatea și scalabilitatea, puteți instala mai multe instanțe ale rolurilor specifice (Server de incidente, Server de comunicații, Consolă web).

Fiecare instanță a rolului este instalată pe o altă aplicație.

Toate instanțele anumitor roluri trebuie să fie conectate cu celelalte roluri, prin elementul de echilibrare roluri.

Aplicația GravityZone include elemente de echilibrare încorporate pe care le puteți instala și utiliza. Dacă aveți deja un software sau hardware de echilibrare în rețea, puteți opta pentru utilizarea acestora în locul elementelor de echilibrare încorporate.

Elementele de echilibrare a rolurilor încorporate nu pot fi instalate alături de roluri pe o aplicație GravityZone.

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Configurare elemente de echilibrare a rolurilor**.
4. Selectați opțiunea dorită:
   - **Utilizare elemente de echilibrare externe.** Selectați această opțiune dacă infrastructura rețelei include deja un software sau hardware de echilibrare pe care îl puteți folosi. Trebuie să introduceți adresa elementului de echilibrare pentru fiecare rol vizat. Utilizați următoarea sintaxă:

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

   - **Utilizarea elementelor de echilibrare încorporate.** Selectați această opțiune pentru instalarea și folosirea software-ului de echilibrare încorporat.

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

5. Selectați **OK** pentru a salva modificările.

Set de duplicate

Cu ajutorul acestei opțiuni puteți activa utilizarea unui set de replici al bazei de date în locul folosirii unei instanțe de bază de date cu un singur server. Acest mecanism permite crearea mai multor instanțe de baze de date într-un mediu GravityZone distribuit, asigurând un nivel ridicat de disponibilitate a bazei de date în cazul apariției unei erori.

Important
Replicarea bazelor de date este disponibilă doar pentru instalări noi ale aplicației GravityZone începând cu versiunea 5.1.17-441.

Configurarea Setului de replici

Mai întâi trebuie să activați Setul de replici în prima aplicație GravityZone instalată. Apoi veți putea adăuga membri ai setului de replici instalând rolul de bază de date pe celelalte instanțe GravityZone din același mediu.

Important

- Replica Set necesită cel puțin trei membri pentru a funcționa.
- Puteți adăuga până la șapte instanțe de roluri de baze de date ca membri ai setului de replici (limitare MongoDB).
- Se recomandă să folosiți un număr impar de instanțe ale bazei de date. Un număr par de membri va consuma mai multe resurse pentru aceleași rezultate.

Pentru activarea replicării bazelor de date în mediul dumneavoastră GravityZone:

1. Instalați rolul Server de baze de date pe prima aplicație GravityZone. Pentru mai multe informații, consultați capitolul „Instalare/dezinstalare roluri” (p. 110).
2. Configurați celelalte aplicații pentru conectarea la prima instanță de bază de date. Pentru mai multe informații, consultați capitolul „Conectare la o bază de date existentă” (p. 117).
3. Mergeți la meniul principal al primei aplicații, selectați **Setări avansate** și apoi selectați **Set de duplicate** pentru activare. Va apărea un mesaj de confirmare.
4. Selectați **Da** pentru confirmare.
5. Instalați rolul de server baze de date pe fiecare dintre celelalte aplicații GravityZone.

Imediat ce pașii de mai sus au fost îndepliniți, toate instanțele de baze de date vor începe să funcționeze ca set de replici:

- Se alege o instanță principală, care va fi singura care va accepta operațiunile de scriere.
- Instanța principală înregistrează într-un jurnal toate modificările efectuate asupra setului său de date.
- Instanțele secundare duplică acest jurnal și aplică aceleași modificări asupra seturilor lor de date.
- Atunci când instanța principală devine indisponibilă, setul de replici va alege una dintre instanțele secundare ca fiind cea principală.
- Atunci când o instanță principală nu comunică cu ceilalți membri ai setului pentru o perioadă de timp mai mare de 10 secunde, setul de replici va încerca să selecteze un alt membru care să devină noua instanță principală.

Ștergerea de membri din setul de replici

Pentru a șterge membri din setul de duplicate, selectați din interfața consolei aplicației respective (interfața pe bază de meniu) **Instalare/Dezinstalare roluri > Adăugare sau ștergere roluri** și deselectați **Server de baze de date**.

Notă
Puteți șterge un membru al setului de replici numai dacă au fost instalate în rețea cel puțin patru instanțe de baze de date.

Activare Cluster VPN Securizat

Rolurile GravityZone au diferite servicii interne, care comunică doar între ele. Pentru un mediu mai sigur, puteți izola aceste servicii prin crearea unui cluster VPN pentru acestea. Fie că aceste servicii rulează pe o aplicație, fie că rulează pe mai multe aplicații, vor comunica printr-un canal securizat.

Important
- Această caracteristică necesită o instalare standard GravityZone, fără niciun instrument personalizat instalat.
- După activarea cluster-ului nu îl veți putea dezactiva.

Pentru securizarea serviciilor interne pe aplicații:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați Activare **Cluster VPN securizat**.

   Va apărea un mesaj de informare cu privire la modificările care vor fi aduse.
4. Selectați **Da** pentru a confirma și pentru a continua cu instalarea VPN.

   După finalizare va fi afișat un mesaj de confirmare.

De acum înainte, toate rolurile de pe aplicație sunt instalate în modul securizat și serviciile vor comunica prin interfața VPN. Orice nouă aplicație adăugată mediului trebuie să fie inclusă în cluster-ul VPN. Pentru mai multe informații, consultați capitolul „Conectare la baza de date existentă (Cluster VPN Securizat)” (p. 118).

Conectare la o bază de date existentă

În arhitectura distribuită GravityZone, este necesar să instalați rolul de Server de baze de date pe prima aplicație și să configurați toate celelalte aplicații pentru a se conecta la instanța de bază de date existentă. Astfel, toate aplicațiile vor împărți aceeași bază de date.

Important
Se recomandă activarea Cluster-ului VPN securizat și conectarea la o bază de date dintr-un astfel de cluster. Pentru mai multe informații, consultați capitolul :

- „Activare Cluster VPN Securizat” (p. 116)
- „Conectare la baza de date existentă (Cluster VPN Securizat)” (p. 118)

Pentru conectarea aplicației la o bază de date GravityZone din afara unui Cluster VPN securizat:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Conectare la o bază de date existentă**.

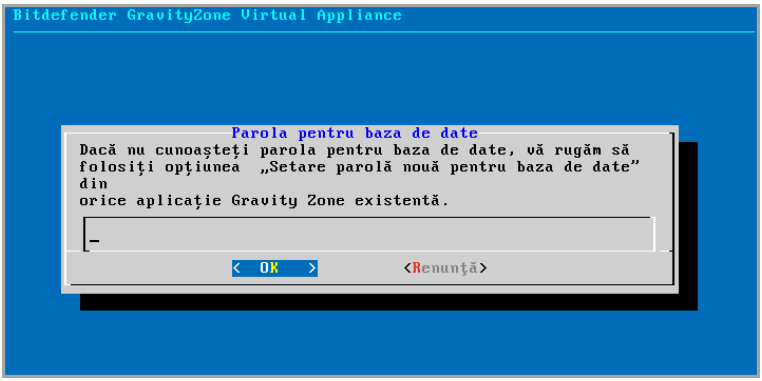
Notă
Asigurați-vă că setați o parolă pentru baza de date înainte de a accesa această opțiune. Dacă nu cunoașteți parola bazei de date, configurați o nouă parolă

accesând **Setări avansate > Setare parolă nouă pentru baza de date** din meniul principal.

4. Selectați **Configurare adresă Server bază de date**.
5. Introduceți adresa bazei de date folosind următoarea sintaxă:

   `<IP/Hostname>:<Port>`

   Specificarea portului este opțională. Portul implicit este 27017.
6. Introduceți parola primară pentru baza de date.



Interfață consolă aplicație: introduceți parola pentru baza de date

7. Selectați **OK** pentru a salva modificările.
8. Selectați **Afișare adresă Server bază de date** pentru a vă asigura că adresa a fost corect configurată.

Conectare la baza de date existentă (Cluster VPN Securizat)

Utilizați această opțiune dacă aveți nevoie să extindeți instalarea dvs. GravityZone cu mai multe aplicații și Cluster-ul VPN securizat este activat. Astfel, noua aplicație va împărți aceeași bază de date cu instalarea existentă într-un mediu securizat.

Pentru mai multe informații privind Cluster-ul VPN securizat, consultați „Activare Cluster VPN Securizat" (p. 116).

Cerințe preliminare

Înainte de a continua, asigurați-vă că dispuneți de următoarele:

- Adresa IP a Serverului de baze de date
- Parola pentru utilizatorul **bdadmin** de pe aplicație cu rolul de Server de baze de date

Conectare la Baza de date

Pentru conectarea aplicației la o bază de date GravityZone dintr-un Cluster VPN securizat:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Setări avansate**.
3. Selectați **Conectare la o bază de date existentă (Cluster VPN securizat)**.

   Veți fi informat cu privire la cerințe și alternative, în cazul în care acestea nu sunt întrunite.
4. Selectați **OK** pentru a lua la cunoștință și a continua.
5. Introduceți adresa IP a Serverului de baze de date din Cluster-ul VPN Securizat.
6. Introduceți parola pentru utilizatorul **bdadmin** de pe aplicație cu Serverul de baze de date.
7. Selectați **OK** pentru a salva modificările și a continua.

După finalizarea procesului veți primi un mesaj de confirmare. Noua aplicație devine membru al cluster-ului și va comunica cu celelalte aplicații într-un mod securizat. Toate aplicațiile vor folosi aceeași bază de date.

Verificare stare Cluster VPN Securizat

Această opțiune este disponibilă doar după ce ați activat Cluster-ul VPN securizat. Selectați această opțiune pentru a verifica dacă există aplicații în instalarea dvs, GravityZone care nu și-au securizat încă serviciile. Este posibil să fie necesar să investigați mai în detaliu pentru a vedea dacă aplicațiile sunt online și pot fi accesate.

Configurare limbă

Pentru a schimba limba pentru interfața de configurare a aplicației:

1. Selectați **Configurare limbă** din meniul principal.
2. Selectați limba dintre opțiunile disponibile:. Va apărea un mesaj de confirmare.

   Notă
   Este posibil să fie nevoie să derulați lista pentru a ajunge la limba dorită.

3. Selectați **OK** pentru a salva modificările.

5.2. Administrarea licenței

GravityZone este licențiat cu un singur cod pentru toate serviciile de securitate.

În afara serviciilor de securitate de bază, GravityZone oferă, de asemenea, caracteristici importante de protecție, precum add-on-urile. Fiecare add-on este licențiat cu o cheie separată și îl puteți utiliza numai împreună cu o licență de bază valabilă. Dacă licența principală nu este validă, veți putea vizualiza setările caracteristicilor, însă nu le veți putea folosi.

Puteți alege să testați GravityZone și să decideți dacă este soluția optimă pentru organizația dumneavoastră. Pentru activarea perioadei de evaluare, trebuie să introduceți în Control Center codul licenței de evaluare din e-mail-ul de înregistrare.

Notă
Control Center este pusă la dispoziție gratuit cu orice serviciu de securitate GravityZone.

Pentru a utiliza în continuare GravityZone după expirarea perioadei de evaluare, trebuie să achiziționați o cheie de licență și să o folosiți pentru înregistrarea produsului.

Pentru achiziționarea unei licențe, contactați un distribuitor Bitdefender sau contactați-ne prin e-mail la enterprisesales@bitdefender.com.

Cheile de licență GravityZone pot fi gestionate de pe pagina **Configurare > Licență** din Control Center. Când cheia de licență curentă este pe cale să expire, se va afișa un mesaj în consolă, prin care veți fi informat cu privire la necesitatea reînnoirii. Pentru a introduce o cheie de licență nouă sau a vizualiza detaliile licenței curente, mergeți la pagina **Configurare > Licență**.

5.2.1. Găsirea unui distribuitor

Distribuitorii noștri vă vor oferi asistență cu privire la toate informațiile necesare și vă vor ajuta să alegeți cea mai bună opțiune de licențiere.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți în pagina Localizare parteneri din site-ul Bitdefender.
2. Selectați țara dvs. de reședință pentru a vizualiza informațiile de contact ale partenerilor Bitdefender disponibili.
3. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa enterprisesales@bitdefender.com.

5.2.2. Introducerea cheilor de licență

Înregistrarea licenței GravityZone se poate efectua online sau offline (atunci când nu este disponibilă o conexiune la internet). În ambele cazuri, este necesar să furnizați o cheie de licență valabilă.

Pentru înregistrare offline, veți avea nevoie și de codul de înregistrare asociat cheii de licență.

Pentru a modifica cheia de licență curentă sau pentru a înregistra un add-on:

1. Autentificați-vă în Control Center folosind un cont de administrator organizație.
2. Mergeți la pagina **Configurare > Licență**.
3. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului.
4. Selectați tipul de înregistrare:
   - **online**. În acest caz, introduceți o cheie de licență validă în câmpul **Cheie de licență**. Cheia de licență va fi verificată și validată online.
   - **Offline**, atunci când nu este disponibilă o conexiune la internet. În acest caz, este necesar să furnizați o cheie de licență și codul de înregistrare asociat acesteia.

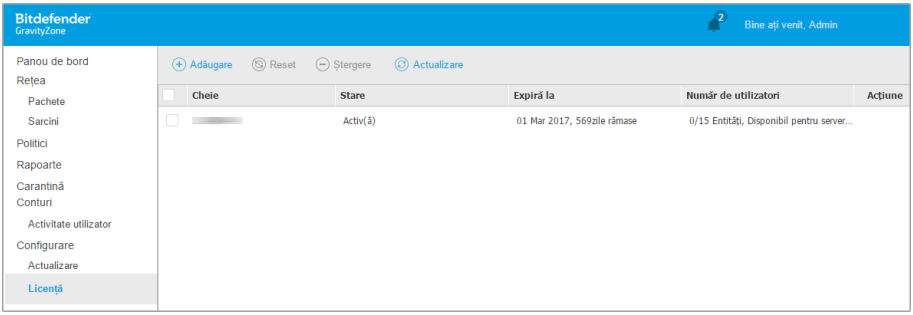
   Dacă o cheie de licență nu este valabilă, se afișează o eroare de validare ca mesaj deasupra câmpului **Cheie de licență**.
5. Faceți clic pe **Add**. Cheia de licență va fi adăugată în pagina **Licență**, unde puteți verifica detaliile acesteia.
6. Faceți clic pe **Salvare** pentru a aplica modificările. Control Center este repornită și este necesar să vă autentificați din nou pentru a vedea modificările.

Notă
Puteți utiliza add-on-urile cât timp dețineți o licență de bază compatibilă valabilă. În caz contrar, veți putea vizualiza caracteristicile, însă nu le veți putea folosi.

5.2.3. Verificare detalii licență curentă în curs

Pentru vizualizarea detaliilor unei licențe:

1. Autentificați-vă în Control Center folosind un cont de administrator organizație.
2. Mergeți la pagina **Configurare > Licență**.



Pagina Licență

3. În tabel puteți vizualiza detalii referitoare la cheile de licență existente.
   - Cheie de licență
   - Stare cheie licență
   - Data expirării și perioada rămasă din licență

     Important
     La expirarea licenței, modulele de protecție ale agenților instalați sunt dezactivate. Drept urmare, stațiile de lucru nu mai sunt protejate și nu puteți efectua nicio sarcină de scanare. Orice agent nou instalat va intra în perioada de evaluare.

   - Numărul de utilizatori ai licenței

5.2.4. Resetarea numărului de utilizări ale licenței

Puteți afla informații despre numărul de utilizatori ai licenței dvs. accesând pagina **Licență**, din coloana **Număr de utilizatori**.

Dacă aveți nevoie să actualizați informațiile referitoare la numărul de utilizatori ai licenței, selectați cheia de licență și dați clic pe butonul **Resetare** din partea de sus a tabelului.

5.2.5. Ștergerea cheilor de licență

Puteți opta pentru ștergerea cheilor de licență expirate pe pagina **Licență**.

Avertisment
Ștergerea unei chei de licență va elimina serviciul de securitate corespunzător din Control Center. Nu veți putea instala și administra protecția oferită de serviciul respectiv pe stațiile de lucru din rețeaua dumneavoastră. Cu toate acestea, stațiile de lucru rămân în continuare protejate cât timp cheia de licență este valabilă.
Dacă introduceți o nouă cheie de licență validă, care include serviciul șters anterior, se vor reactiva toate caracteristicile serviciului respectiv în Control Center.

Pentru a șterge o cheie de licență:

1. Autentificați-vă în Control Center folosind un cont de administrator organizație.
2. Mergeți la pagina **Configurare > Licență**.
3. Selectați cheia de licență pe care doriți să o eliminați și dați clic pe butonul **Ștergere** din partea de sus a tabelului.

5.3. Instalarea Endpoint Protection

În funcție de configurația stației și de mediul de rețea, puteți alege să instalați doar agenții de securitate sau să folosiți și un Security Server. În cel de-al doilea caz, va trebui să instalați mai întâi Security Server ș apoi agenții de securitate.

Vă recomandăm să folosiți Security Server în mediile virtuale, cum ar fi Nutanix, VMware sau Citrix Xen, sau dacă mașinile au resurse hardware limitate.

Important
Doar Bitdefender Endpoint Security Tools și Bitdefender Tools sunt compatibile pentru conectarea la un Security Server. Pentru mai multe informații, consultați capitolul „Arhitectura GravityZone” (p. 11).

5.3.1. Instalarea Security Server

Security Server este o mașină virtuală dedicată care anulează duplicatele și centralizează majoritatea funcțiilor contra programelor periculoase ale clienților antimalware, acționând ca și server de scanare.

Configurația Security Server este specifică mediului în care este instalată. Procedurile de instalare sunt descrise mai jos:

- Security Server pentru VMware NSX
- Security Server (Multi-platformă) sau pentru VMware vShield
- Security Server pentru Amazon EC2
- Security Server pentru Microsoft Azure

Instalarea Security Server pentru VMware NSX

În mediile VMware NSX, trebuie să configurați serviciul Bitdefender în fiecare cluster pe care doriți să îl protejați. Aplicația dedicată va configura automat toate gazdele din cluster. Toate mașinile virtuale de pe o gazdă sunt conectate automat prin Guest Introspection la instanța Security Server instalată pe gazda respectivă.

Security Server trebuie configurat exclusiv de pe vSphere Web Client.

Pentru a instala serviciul Bitdefender:

1. Conectați-vă la vSphere Web Client.
2. Mergeți la **Securitate & rețea > Instalare** și faceți clic pe secțiunea **Configurare servicii**.
3. Faceți clic pe butonul **Configurație nouă serviciu** (semnul plus). Se deschide fereastra de configurare.
4. Selectați **Guest Introspection** și faceți clic pe **Următorul**.
5. Selectați centrul de date și cluesterele pe care doriți să configurați serviciul și faceți clic pe **Următorul**.
6. Selectați rețeaua de stocare și administrare, faceți clic pe **Următorul** și apoi pe **Finalizare**.
7. Reluați pașii de la 3 la 6, selectând de această dată serviciul **Bitdefender**.

   Înainte de a continua cu instalarea, asigurați-vă că rețeaua selectată și GravityZone Control Center sunt conectate.

   După ce serviciul Bitdefender este instalat, acesta instalează automat Security Server pe toate gazdele ESXi din clusterele selectate.

Avertisment
Pentru ca serviciile să funcționeze corespunzător, este foarte important să le instalați în această ordine: mai întâi Guest Introspection și apoi Bitdefender și nu simultan.

Notă
Pentru informații suplimentare referitoare la adăugarea serviciilor partenere la NSX, consultați Baza de date VMware NSX.
Dacă selectați **Specificat pe gazdă** pentru stocare și administrarea rețelei, verificați dacă Agentul VM este configurat pe gazde atât pentru, Guest Introspection, cât și pentru serviciile Bitdefender.

Security Server are cerințe specifice care depind de numărul de mașini virtuale pe care trebuie să le protejeze. Pentru a ajusta configurația hardware a Security Server:

1. Conectați-vă la VMware vSphere Web Client.
2. Mergeți la **Gazde și clustere**.
3. Selectați clusterul pe care este configurat Security Server și apoi selectați **Obiecte asociate > Mașini virtuale**.
4. Opriți aplicația **Bitdefender**.
5. Faceți clic dreapta pe denumirea aplicației și apoi selectați **Modificare setări...** din meniul contextual.
6. În fereastra **Hardware virtual**, modificați valorile CPU și RAM în funcție de nevoile dvs. și apoi faceți clic pe **OK** pentru a salva modificările.
7. Reporniți aplicația.

Notă
Pentru a face upgrade de la VMWare vShield la NSX, consultați acest articol KB.

Instalarea Security Server Multi-Platformă sau pentru VMware vShield

1. Conectați-vă la platforma de virtualizare
2. Instalați Security Server pe gazde

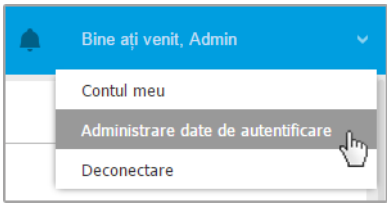
Conectarea la platforma de virtualizare

Pentru a accesa infrastructura de virtualizare integrată cu Control Center, trebuie să introduceți datele de autentificare pentru fiecare sistem de server virtual

disponibil. Control Center folosește datele dumneavoastră pentru a se conecta la infrastructura virtualizată, afișând doar resursele la care aveți acces (așa cum sunt acestea definite în vCenter Server).

Pentru a specifica datele de conectare la serverele de virtualizare:

1. Faceți clic pe numele de utilizator din colțul din dreapta sus al paginii și selectați **Administrare date de autentificare**.



Meniu Rețea > Pachete

2. Mergeți la secțiunea **Mediul virtualizat**.
3. Specificați datele de autentificare necesare.
   a. Selectați un server din meniul corespunzător.

      Notă
      Dacă meniul nu este disponibil, fie nu s-a configurat încă nicio integrare, fie toate datele au fost deja configurate.

   b. Introduceți numele de utilizator și parola și o descriere sugestivă.
   c. Faceți clic pe butonul ⊕ **Adăugare**. Noul set de date este afișat în tabel.

Notă
Dacă nu ați specificat datele de autentificare, când încercați să parcurgeți inventarul unui sistem vCenter Server vi se va solicita să le introduceți. După ce ați introdus datele, acestea sunt salvate în secțiunea Admnistrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

Instalarea Security Server pe gazde

Trebuie să instalați Security Server pe gazde, după cum urmează:

- În mediile VMware cu vShield Endpoint, trebuie să instalați aplicația dedicată pe fiecare gazdă care trebuie protejată. Toate mașinile virtuale de pe o gazdă sunt conectate automat prin vShield Endpoint la instanța Security Server instalată pe gazda respectivă.
- În mediile Citrix, este necesar să instalați Security Server pe fiecare gazdă pe care doriți să o protejați cu HVI, prin sarcina de instalare de la distanță.
- În mediile Nutanix Prism Element, este necesar să instalați un server de securitate pe fiecare sistem gazdă, prin intermediul sarcinii de instalare de la distanță.
- În toate celelalte medii, trebuie să instalați Security Server pe una sau mai multe gazde pentru a include numărul de mașini virtuale care trebuie protejate. Trebuie să aveți în vedere numărul de mașini virtuale protejate, resursele disponibile pentru Security Server pe gazde, precum și conectivitatea în rețea dintre Security Server și mașinile virtuale protejate. Agentul de securitate instalat pe mașinile virtuale se conectează la Security Server prin TCP/IP, folosind detalii configurate la instalare sau printr-o poliță.

În cazul în care Control Center este integrată cu vCenter Server, XenServer și Nutanix Prism Element, puteți configura automat Security Server pe sistemele gazdă din Control Center. Puteți, de asemenea, descărca pachetele Security Server pentru instalarea individuală de pe Control Center.

Notă
Pentru mediile VMware cu vShield Endpoint, puteți instala Security Server pe gazde exclusiv prin sarcinile de instalare.

Instalare locală

În toate mediile de virtualizare care nu sunt integrate cu Control Center, trebuie să instalați Security Server pe gazde manual, folosind un pachet de instalare. Pachetul Security Server poate fi descărcat de pe Control Center în mai multe formate diferite, compatibile cu principalele platforme de virtualizare.

Descărcarea Pachetelor de instalare Security Server

Pentru a descărca pachetele de instalare Security Server:

1. Mergeți la pagina **Rețea > Pachete**.
2. Selectați pachetul Security Server implicit:

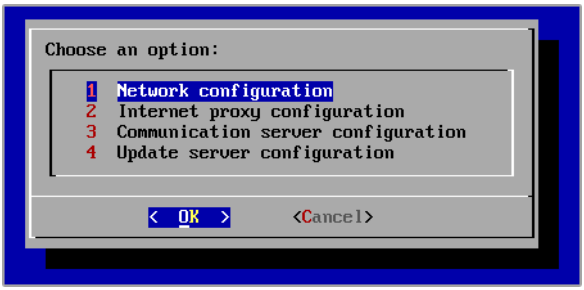
3. Faceți clic pe butonul **Descărcare** din partea de sus a tabelului și alegeți tipul de pachet din meniu.
4. Salvați pachetele selectate în locația dorită.

Executarea pachetelor de instalare Security Server

După ce aveți pachetul de instalare, configurați-l pe gazdă folosind instrumentul preferat de configurare a mașinii virtuale.

După configurare, setați Security Server după cum urmează:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere). Alternativ, vă puteți conecta la aplicație prin SSH.
2. Conectați-vă folosind datele implicite.
   - Nume de utilizator: `root`
   - Parolă: `sve`
3. Rulați comanda `sva-setup`. Veți accesa interfața de configurare a aplicației.



Interfața de configurare Security Server (meniu principal)

Pentru a naviga prin meniuri și opțiuni, folosiți tasta `Tab` tastele săgeți. Pentru a selecta o anumită opțiune, apăsați `Enter`.

4. Configurați setările rețelei.

   Security Server folosește protocolul TCP/IP pentru comunicarea cu componentele GravityZone. Puteți configura aplicația pentru a obține automat setările rețelei de la serverul DHCP sau puteți configura manual setările rețelei, în modul descris mai jos:

a. Din meniul principal, selectați **Configurare rețea**.

b. Selectați interfața de rețea.

c. Selectați modul de configurare IP:

- **DHCP**, dacă doriți ca Security Server să obțină automat setările de rețea de la serverul DHCP.
- **Static**, dacă un server DHCP este absent sau dacă s-a efectuat o rezervare IP pentru aplicație pe serverul DHCP. În acest caz, trebuie să configurați manual setările de rețea.

  i. Introduceți numele gazdei, adresa IP, masca de rețea, portalul și serverele DNS în câmpurile corespunzătoare.

  ii. Selectați **OK** pentru a salva modificările.

Notă
Dacă sunteți conectat la aplicație prin clientul SSH, modificarea setărilor de rețea va încheia imediat sesiunea.

5. Configurați setările proxy.

   Dacă în rețea se utilizează un server proxy, trebuie să furnizați detaliile acestuia, astfel încât Security Server să poată comunica cu GravityZone Control Center.

   Notă
   Sunt acceptate doar serverele proxy cu date de autentificare de bază.

   a. Din meniul principal, selectați **Configurare proxy internet**.

   b. Introduceți numele gazdei, numele de utilizator, parola și domeniul în câmpurile corespunzătoare.

   c. Selectați **OK** pentru a salva modificările.

6. Configurați adresa Serverului de comunicare.

   a. Din meniul principal, selectați **Configurare server comunicare**.

   b. Introduceți adresa serverului de comunicare, inclusiv numărul portului 8443, în formatul următor:

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

Alternativ, puteți folosi numele de gazdă al Serverului de comunicare în locul adresei IP.

c. Selectați **OK** pentru a salva modificările.

Instalare de la distanță

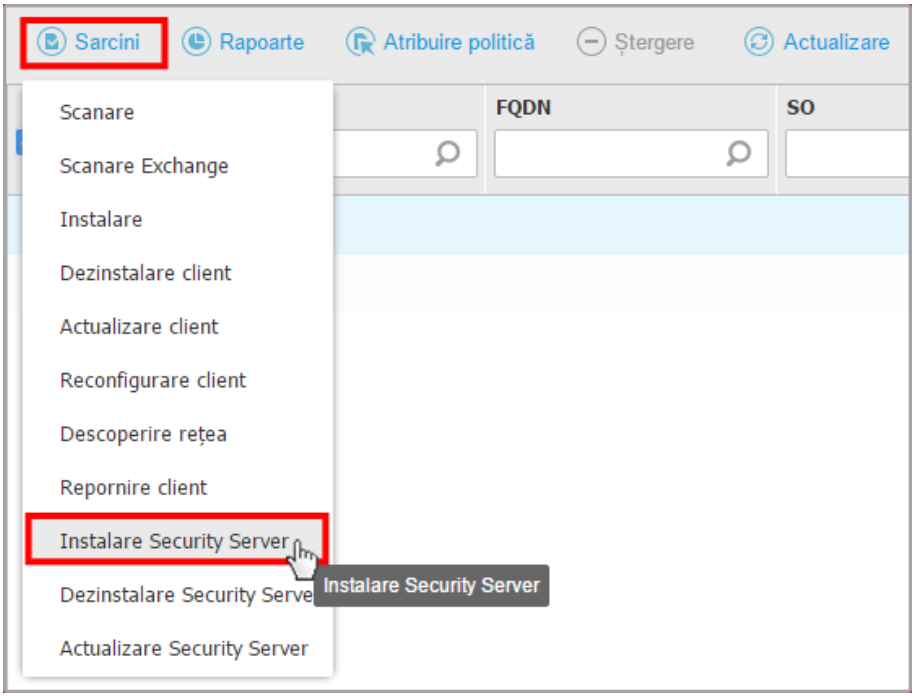
Control Center vă permite să instalați de la distanță Security Server pe gazde vizibile folosind sarcinile de instalare.

Pentru a instala Security Server de la distanță pe una sau mai multe gazde:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vizualizări.
3. Parcurgeți inventarul VMware, Citrix sau Nutanix și bifați casetele corespunzătoare sistemelor gazdă sau containerelor(Nutanix Prism, vCenter Server, XenServer sau centru de date) dorite. Pentru o selecție rapidă, puteți selecta direct containerul rădăcină (Inventarul Nutanix, VMware sau Citrix). Veți putea selecta gazdele individual din asistentul de instalare.

   Notă
   Nu puteți selecta gazde din diferite foldere.

4. Dați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare Security Server** din meniu. Se afișează fereastra **Instalare Security Server**.



Instalarea Security Server din meniul Sarcini

5. Selectați gazdele pe care doriți să instalați instanțele Security Server.
6. Alegeți setările de configurare pe care doriți să le folosiți.

> **Important**
> Folosirea unor setări comune la rularea mai multor instanțe Security Server simultan necesită ca gazdele să împărtășească același spațiu de stocare, să aibă adrese IP alocate de un server DHCP și să facă parte din aceeași rețea.

Atunci când alegeți să configurați fiecare Security Server în mod diferit, veți putea defini setările pe care le doriți pentru fiecare gazdă în pasul următor al asistentului. Pașii descriși în continuare se aplică în situația în care se folosește opțiunea **Configurați fiecare Security Server**.

7. Faceți clic pe **Înainte**.

8. Introduceți o denumire sugestivă pentru Security Server.
9. În cazul mediilor VMware, selectați containerul în care doriți să includeți Security Server din meniul **Configurare container**.
10. Selectați spațiul de stocare destinație.
11. Selectați tipul de administrare. Se recomandă să instalați aplicația folosind o administrare de disc standard.

    Important
    Dacă folosiți alocarea dinamică de resurse (la cerere) și nu mai există spațiu disponibil de stocare a datelor, Security Server va îngheța și, prin urmare, gazda va rămâne neprotejată.

12. Configurați memoria și alocarea resurselor CPU în funcție de procentul de consolidare MV de pe gazdă. Selectați **Scăzut**, **Mediu** sau **Ridicat** pentru a încărca setările recomandate pentru alocarea resurselor sau **Manual** pentru a configura manual alocarea resurselor.
13. Este necesar să setați o parolă de administrator pentru consola Security Server. Setarea unei parole administrative suprascrie parola principală implicită ("sve").
14. Setați fusul orar al aplicației.
15. Selectați tipul de configurare a rețelei pentru rețeaua Bitdefender. Adresa IP a Security Server nu trebuie să se modifice în timp, deoarece este utilizată de agenți Linux pentru comunicare.

    Dacă alegeți DHCP, asigurați-vă că ați configurat serverul DHCP pentru rezervarea adresei IP pentru aplicație.

    Dacă alegeți opțiunea statică, trebuie să introduceți adresa IP, masca de sub-rețea, portalul și informațiile DNS.
16. Selectați rețeaua vShield și introduceți datele vShield. Eticheta implicită pentru rețeaua vShield este `vmservice-vshield-pg`.
17. Faceți clic pe **Save**.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Notă
Pentru a face upgrade de la VMWare vShield la NSX, consultați acest articol KB.

Important
Instalarea Security Server pe Nutanix prin intermediul unei sarcini de la distanță poate eșua atunci când clusterul Prism Element este înregistrat în Prism Central sau din alte motive. În astfel de situații, se recomandă să efectuați o configurare manuală a Security Server. Pentru detalii suplimentare, consultați acest articol KB.

Instalarea Security Server pentru Amazon EC2

Puteți utiliza Security Server pentru a vă proteja instanțele Amazon EC2, după cum urmează:

- Configurați Security Server instalat pe rețeaua locală pentru comunicarea cu instanțele Amazon EC2. Astfel, veți putea să utilizați resursele locale, fizice sau virtuale, pentru a proteja și inventarul Amazon EC2.
- Instalați una sau mai multe instanțe Security Server în mediul Amazon EC2, după cum este necesar. În acest caz, urmați procedura descrisă în acest articol KB.

  Important
  - Pentru ca mașinile dvs. EC2 și instanțele Serverului de securitate instalate în inventarul Amazon EC2 să poată comunica, trebuie să configurați corect conexiunile Amazon VPC (Virtual Private Cloud) și Amazon VPN. Pentru informații suplimentare, consultați documentația Amazon VPC.
  - Vă recomandăm să instalați Security Server în aceeași regiune Amazon EC2 ca și instanțele pe care doriți să le protejați.

Modul implicit de scanare pentru instanțele EC2 este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați instanțele EC2 folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.

Instalarea Security Server pentru Microsoft Azure

Puteți utiliza Security Server pentru a vă proteja mașinile virtuale Microsoft Azure, după cum urmează:

- Configurați Security Server instalat pe rețeaua dumneavoastră locală pentru a comunica cu mașinile virtuale Microsoft Azure. Prin urmare, veți putea utiliza

resursele locale, fizice sau virtuale, pentru a proteja și inventarul Microsoft Azure.

- Instalați una sau mai multe instanțe Security Server în mediul dvs. Microsoft Azure, după cum este necesar. În acest caz, urmați procedura descrisă în acest articol KB.

  Important

  – Pentru o funcționare optimă a comunicării între mașinile dumneavoastră virtuale Microsoft Azure și instanțele Serverului de securitate instalate pe inventarul dumneavoastră Microsoft Azure, trebuie să configurați în mod corect rețeaua/sub-rețeaua dumneavoastră virtuală. Pentru mai multe detalii, consultați Documentația referitoare la rețeaua virtuală Microsoft Azure.

  – Vă recomandăm să instalați Security Server în aceeași zonă Microsoft Azure ca și cea în care se află mașinile virtuale pe care doriți să le protejați.

Modul implicit de scanare pentru mașinile virtuale Microsoft Azure este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați mașinile virtuale Microsoft Azure folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.

5.3.2. Instalarea agenților de securitate

Pentru a vă proteja stațiile de lucru fizice și virtuale, trebuie să instalați un agent de securitate pe fiecare dintre acestea. Pe lângă administrarea protecției protecției pe punctul de lucru local, agentul de securitate comunică și cu Control Center pentru primirea comenzilor administratorului și pentru transmiterea rezultatelor acțiunilor sale.

Pentru a afla mai multe despre agenții de securitate disponibili, consultați „Agenți de securitate” (p. 13).

Pe mașinile Windows și Linux, agentul de securitate poate avea două roluri și îl puteți instala după cum urmează:

1. Ca agent de scuritate simplu pentru stațiile de lucru.
2. Ca Releu, acționând ca și agent de securitate și ca șiserver de comunicare, proxy și de actualizare pentru alte stații de lucru din rețea.

Puteți instala agenții de securitate pe stații de lucru fizice și virtuale rulând pachetele de instalare local sau prin executarea sarcinilor de instalare de la distanță de pe Control Center.

Este foarte important să citiți cu atenție și să urmați instrucțiunile de pregătire a instalării.

În modul normal, agenții de securitate au o interfață de utilizator minimă. Permite utilizatorilor doar să verifice starea de protecție și să ruleze sarcini de securitate de bază (actualizări și scanări), fără a oferi acces la setări.

Dacă este activat de către administratorul de rețea prin intermediul pachetului de instalare și politicii de securitate, agentul de securitate poate rula și în modul Utilizator privilegiat pe stațiile de lucru Windows, permițând utilizatoului stației de lucru să vizualizeze și să modifice setările politicii. Cu toate acestea, administratorul Control Center poate controla în orice moment ce politici de securitate se aplică, având prioritate față de modul de Utilizator privilegiat.

În mod implicit, limba de afișare pentru interfața utilizatorului de pe stațiile de lucru Windows protejate este setată la momentul instalării, în funcție de limba contului dumneavoastră GravityZone.

Pe Mac, limba de afișare pentru interfața utilizatorului este setată la momentul instalării, în funcție de limba sistemului de operare al stației de lucru. În Linux, agentul de securitate nu are o interfață de utilizator localizată.

Pentru a instala interfața pentru utilizator în altă limbă pe anumite stații de lucru Windows, puteți crea un pachet de instalare și seta limba preferată în opțiunile de configurare ale acestuia. Această opțiune nu este disponibilă pentru stațiile de lucru Mac și Linux. Pentru mai multe informații cu privire la crearea pachetelor de instalare, consultați „Generarea pachetelor de instalare” (p. 138).

Pregătirea pentru instalare

Înainte de instalare, urmați pașii pregătitori de mai jos pentru a vă asigura că totul funcționează corect:

1. Asigurați-vă că toate stațiile de lucru țintă îndeplinesc cerințele minime de sistem. Pentru unele stații de lucru, se poate să fie necesară instalarea celui mai recent service pack disponibil sau eliberarea spațiului pe disc. Realizați o listă de stații de lucru care nu îndeplinesc cerințele necesare, pentru a le putea exclude din administrare.
2. Dezinstalați (nu doar dezactivați) orice program antimalware sau software de securitate Internet existent pe stațiile de lucru vizate. Rularea simultană a

agentului de securitate cu alte aplicații pe o stație de lucru poate afecta funcționarea acestora și poate cauza probleme majore de sistem.

Multe dintre programele de securitate incompatibile sunt detectate automat și eliminate în momentul instalării.

Pentru a afla mai multe și pentru a verifica lista programelor software de securitate detectate de Bitdefender Endpoint Security Tools pentru sistemele de operare Windows actuale, consultați acest articol din Baza de cunoștințe.

Important
Dacă doriți să instalați agentul de securitate pe un computer cu Bitdefender Antivirus for Mac 5.X, trebuie mai întâi să îl dezinstalați manual pe acesta din urmă. Pentru îndrumări, consultați acest articol KB.

3. Pentru instalare este necesară existența privilegiilor de administrare și a accesului la Internet. În cazul în care stațiile de lucru vizate se află într-un domeniu Active Directory, trebuie să utilizați datele de autentificare ale administratorului domeniului pentru o instalare la distanță. În caz contrar, verificați dacă aveți la îndemână datele de autentificare necesare pentru toate stațiile de lucru.
4. Stațiile de lucru trebuie să aibă conectivitate în rețea către aplicația GravityZone.
5. Se recomandă să folosiți o adresă IP statică pentru serverul releu. Dacă nu setați un IP static, folosiți numele de gazdă al mașinii.
6. La instalarea agentului prin intermediul unui releu Linux, trebuie respectate următoarele condiții suplimentare:
   - Endpoint-ul cu rol de Releu trebuie să aibă instalat pachetul Samba (`smbclient`) versiunea 4.1.0 sau mai recentă și să suporte comanda `net` binary/command, astfel încât să poată instala de la distanță agenți Windows.

     Notă
     De regulă, funcționalitatea `net` binary/command este livrată împreună cu pachetele samba-client și/sau samba-common. Pe anumite distribuții Linux (precum CentOS 7.4), comanda `net` se instalează numai în cazul instalării versiunii complete a suitei Samba (Common + Client + Server). Asigurați-vă că pe endpoint-ul cu rol de Releu este disponibilă comanda `net`.

   - Stațiile de lucru Windows trebuie să aibă activate funcțiile Partajare administrativă și Partajare rețea.

- Stațiile de lucru Linux și Mac vizate trebuie să aibă SSH activat.

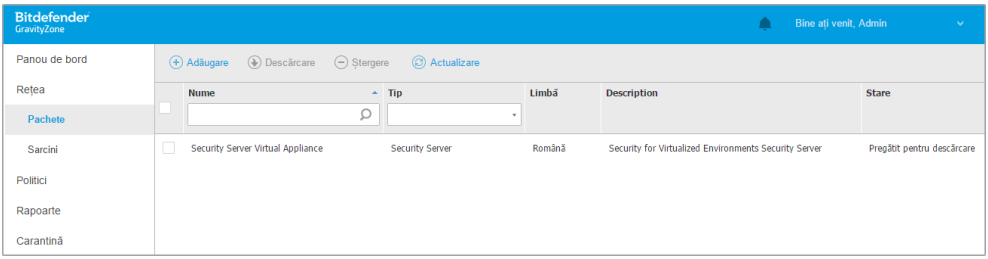
7. Începând cu macOS High Sierra (10.13), după instalarea manuală sau de la distanță a Endpoint Security for Mac, utilizatorilor li se solicită să aprobe extensiile kernel Bitdefender pe computerele lor. Este posibil ca anumite caracteristici Endpoint Security for Mac să nu funcționeze până când utilizatorii nu aprobă extensiile kernel Bitdefender. Pentru a elimina intervenția utilizatorului, puteți pre-aproba extensiile kernel ale Bitdefender prin adăugarea lor în lista de excepții utilizând un instrument de administrare a dispozitivelor mobile.
8. La instalarea agentului într-un inventar Amazon EC2, configurați grupele de securitate asociate cu instanțele pe care doriți să le protejați în **Tablou de comandă Amazon EC2 > Rețea & Securitate**, astfel:
   - Pentru instalarea de la distanță, permiteți accesul SSH* din instanța EC2.
   - Pentru instalarea locală, permiteți accesul SSH* și RDP (Remote Desktop Protocol) pentru calculatorul de pe care vă conectați.

   * Pentru instalarea de la distanță pe instanțele Linux trebuie să permiteți autentificarea SSH cu nume de utilizator și parolă.
9. Atunci când instalați agentul într-un inventar Microsoft Azure:
   - Mașina virtuală vizată trebuie să se afle în aceeași rețea virtuală ca și aplicația virtuală GravityZone.
   - Mașina virtuală vizată trebuie să se afle în aceeași rețea virtuală cu un Releu care comunică cu aplicația virtuală GravityZone atunci când acesta din urmă se află în altă rețea.

Instalare locală

O modalitate în care puteți instala agentul de securitate pe o stație de lucru este aceea de a rula local un pachet de instalare.

Puteți crea și gestiona pachetele de instalare în pagina **Rețea și pachete**.



Pagina pachete

După ce ați instalat primul client, acesta va fi utilizat pentru a detecta alte stații de lucru din aceeași rețea, pe baza mecanismului de Descoperire rețea. Pentru informații detaliate referitoare la descoperirea rețelei, consultați „Cum funcționează opțiunea de descoperire a rețelei” (p. 157).

Pentru a instala local agentul de securitate pe o stație de lucru, urmați acești pași:

1. Creați un pachet de instalare conform necesităților dumneavoastră.

   Notă
   Pasul nu este obligatoriu dacă un pachet de instalare a fost deja creat pentru rețeaua de sub contul dumneavoastră.

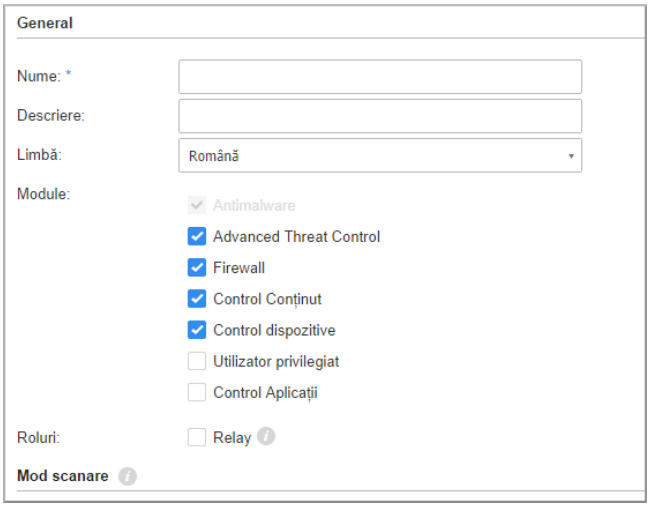
2. Descărcați pachetul de instalare pe stația de lucru țintă.

   Alternativ, puteți trimite link-urile de descărcare a pachetului de instalare prin e-mail mai multor utilizatori din rețeaua dumneavoastră.
3. Executați pachetul de instalare pe stația de lucru țintă.

Generarea pachetelor de instalare

Pentru a crea un pachet de instalare:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea > Pachete**.
3. Dați clic pe butonul ⊕ **Adăugare** situat în partea de sus a tabelului. Va apărea o fereastră de configurare.



Creare pachete - Opțiuni

4. Introduceți o denumire sugestivă și o descriere pentru pachetul de instalare pe care doriți să îl creați.
5. Din câmpul **Limbă**, selectați limba dorită pentru interfața clientului.

> **Notă**
> Această opțiune este disponibilă doar pentru sistemele de operare Windows.

6. Selectați modulele de protecție pe care doriți să le instalați.

> **Notă**
> Se vor instala doar modulele suportate pentru fiecare sistem de operare. Pentru mai multe informații, consultați capitolul „Agenți de securitate” (p. 13).

7. Selectați rolul stației de lucru țintă:
   - **Releu**, pentru a crea pachetul pentru o stație de lucru cu rol de Releu. Pentru mai multe informații, consultați capitolul „Relay” (p. 15)
   - **Server de cache pentru administrarea patch-urilor**, pentru a transforma releul într-un server intern pentru distribuirea patch-urilor software. Acest rol este

afișat atunci când este selectat rolul de releu. Pentru mai multe informații, consultați capitolul „Server de cache pentru patch-uri” (p. 15)

- **Protecție Exchange**, pentru instalarea modulelor de protecție pentru serverele Microsoft Exchange, inclusiv funcțiile antimalware, antispam, filtrare conținut și atașamente pentru traficul de e-mail Exchange și scanare antimalware la cerere a bazelor de date Exchange. Pentru mai multe informații, consultați capitolul „Instalarea Exchange Protection” (p. 169).

8. **Eliminare concurență**. Se recomandă să selectați această casetă pentru a elimina automat orice software de securitate necompatibil în timp ce agentul Bitdefender se instalează pe endpoint. Prin deselectarea acestei opțiuni, agentul Bitdefender se va instala alături de soluția de securitate existentă. Puteți elimina manual soluția de securitate instalată anterior mai târziu, cu propriul dvs. risc.

   Important
   Rularea simultană a agentului Bitdefender cu alte software-uri de securitate pe un endpoint le poate afecta funcționarea și poate cauza probleme majore în sistem.

9. **Mod scanare**. Alegeți tehnologia de scanare care se potrivește cel mai bine cu mediul de rețea și resursele stațiilor dvs. de lucru. Puteți defini modul de scanare selectând unul dintre următoarele tipuri:

   - **Automat**. În acest caz, agentul de securitate va detecta automat configurația stației de lucru și va adapta în mod corespunzător tehnologia de scanare:
     - Scanare centralizată în cloud public sau privat (cu Security Server) cu fallback pe Scanare hibrid (motoare light), pentru calculatoarele fizice cu performanțe hardware scăzute și pentru mașinile virtuale. Acest caz necesită ca cel puțin un Security Server să fie instalat în rețea.
     - Scanare locală (cu motoare full) pentru calculatoarele fizice cu performanță hardware ridicată.
     - Scanare locală pentru instanțele EC2 și mașinile virtuale Microsoft Azure.

     Notă
     Calculatoarele cu performanță scăzută sunt considerate a avea frecvența procesorului mai mică decât 1.5 GHz sau memorie RAM mai mică decât 1 GB.

- **Personalizat**. În acest caz, puteți configura modul de scanare alegând între mai multe tipuri de tehnologii de scanare pentru mașini fizice și virtuale:
  - Scanare centralizată în cloud public sau privat (cu Security Server), care poate avea fallback* pe Scanarea locală (cu motoare full) sau Scanarea hibridă (cu motoare light).
  - Scanare hibrid (cu motoare light)
  - Scanare locală (cu motoare full)

  Modul implicit de scanare pentru instanțele EC2 este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați instanțele EC2 folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.

  Modul implicit de scanare pentru mașinile virtuale Microsoft Azure este Scanarea locală (conținutul de securitate este stocat pe agentul de securitate instalat, iar scanarea se execută local pe sistemul respectiv). Dacă doriți să scanați mașinile virtuale Microsoft Azure folosind un Security Server, este necesar să configurați în mod corespunzător pachetul de instalare al agentului de securitate și politica aplicată.

  * Atunci când se folosește scanarea cu motoare duble, dacă primul motor este indisponibil, se va folosi motorul de rezervă (fallback). Consumul de resurse și gradul de utilizare a rețelei vor depinde de motoarele folosite.

  Pentru mai multe informații privind tehnologiile de scanare disponibile, consultați„Motoare de scanare” (p. 3)

10. **Configurați stația de lucru cu vShield atunci când este detectat un mediu VMware integrat cu vShield**. Această opțiune poate fi utilizată atunci când pachetul de instalare este instalat pe o mașină virtuală de pe un mediu VMware integrat cu vShield. În acest caz, stația de lucru VMware vShield va fi instalată pe mașina țintă în locul agentului de securitate Bitdefender.

  Important
  Această opțiune este destinată instalărilor de la distanță, nu și celor locale. În cazul instalării locale în mediul VMware integrat cu vShield, aveți posibilitatea de a descărca pachetul Integrat cu vShield.

11. Atunci când personalizați motoarele de scanare folosind scanarea în cloud-ul public sau privat (Security Server), vi se solicită să selectați serverele Security Server instalate local pe care doriți să le utilizați și să configurați prioritatea acestora în secțiunea **Alocare Security Server**:

    a. Dați clic pe lista Security Server din capătul de tabel. Se afișează lista de Security Server detectate.

    b. Selectați o entitate.

    c. Dați clic pe butonul ⊕ **Adăugare** din capătul de coloană **Acțiuni**.

    Se adaugă Security Server în listă.

    d. Urmați aceiași pași pentru a adăuga mai multe servere de securitate, dacă sunt disponibile. În acest caz, le puteți configura prioritatea folosind săgețile ⌃ sus și ⌄ jos disponibile în partea dreaptă a fiecărei entități. Când primul Security Server nu este disponibil, va fi luat în considerare următorul și așa mai departe.

    e. Pentru a șterge o entitate din listă, dați clic pe butonul ⊗ **Ștergere** din partea de sus a tabelului.

    Puteți alege să criptați conexiunea la Security Server selectând opțiunea **Utilizare SSL**.

12. **Diverse**. Puteți configura următoarele opțiuni pentru mai multe tipuri de fișiere de pe stațiile de lucru țintă:

    - **Transmite imagine de memorie aferentă avariei**. Selectați această opțiune astfel încât fișierele de imagini de memorie să fie trimise la Laboratoarele Bitdefender pentru analiză în cazul în care agentul de securitate se blochează. Imaginile de memorie aferente avariilor vor ajuta inginerii noștri să își dea seama ce a cauzat problema și să prevină reapariția ei. Nu vor fi transmise informații cu caracter personal.

    - **Transmiterea fișierelor din carantină către Laboratoarele Bitdefender la fiecare (ore).** . În mod implicit, fișierele aflate în carantină sunt trimise automat la Laboratoarele Bitdefender din oră în oră. Puteți edita intervalul de timp când sunt trimise fișierele aflate în carantină. Fișierele mostră vor fi analizate de către cercetătorii Bitdefender în materie de malware. Dacă este confirmată prezența unui malware, va fi lansată o semnătură care să permită ștergerea acestuia.

- **Transmitere fișiere executabile suspecte către Bitdefender**. Selectați această opțiune astfel încât fișierele care par nesigure sau prezintă un comportament suspect să fie trimise către Laboratoarele Bitdefender pentru analiză.

13. Selectați **Scanare înainte de instalare** dacă doriți să vă asigurați că ați curățat mașinile înainte de a instala clientul pe acestea. Se va efectua o scanare rapidă în cloud pe mașinile vizate, înainte de pornirea instalării.
14. Bitdefender Endpoint Security Tools este instalat în directorul implicit de instalare. Selectați **Utilizare cale de instalare personalizată** dacă doriți să instalați agentul Bitdefender într-o altă locație. Dacă folderul specificat nu există, acesta va fi generat în timpul instalării.

    - Pentru Windows, calea implicită este `C:\Program Files\`. Pentru a instala Bitdefender Endpoint Security Tools într-o locație personalizată, utilizați convențiile Windows la introducerea căii. Spre exemplu, `D:\folder`.
    - Pentru Linux, Bitdefender Endpoint Security Tools este instalat implicit în directorul `/opt`. Pentru a instala agentul Bitdefender într-o locație personalizată, utilizați convențiile Linux la introducerea căii. Spre exemplu, `/folder`.

      Bitdefender Endpoint Security Tools nu este compatibil cu instalarea în următoarele căi personalizate:
      – Orice cale care nu începe cu slash (/). Singura excepție este locația Windows `%PROGRAMFILES%`, care este interpretată de agentul de securitate drept directorul implicit Linux `/opt`.
      – Orice cale din `/tmp` sau `/proc`.
      – Orice cale care conține următoarele caractere speciale: `$, !, *, ?, “, ‘, `, \, (,), [,], {, }`.
      – Specificatorul de sistem `systemd` (%).

      Pentru Linux, instalarea într-o cale personalizată necesită glibc 2.21 sau o versiune mai recentă.

> **Important**
> La utilizarea unei căi personalizate asigurați-vă că aveți pachetul corect de instalare pentru fiecare sistem de operare.

15. Dacă doriți, puteți seta o parolă pentru a împiedica utilizatorii să șteargă protecția. Selectați **Configurare parolă dezinstalare** și introduceți parola dorită în câmpurile corespunzătoare.
16. Dacă stațiile de lucru țintă sunt în Inventarul de rețea sub **Grupuri personalizate**, le puteți muta într-un anumit director imediat după finalizarea configurării agentului de securitate.

    Selectați **Utilizare folder personalizat** și alegeți un folder din tabelul corespunzător.
17. În secțiunea **Agent de instalare**, alegeți entitatea la care se vor conecta stațiile de lucru țintă pentru instalarea și actualizarea clientului:
    - **Aplicația GravityZone**, atunci când stațiile de lucru se conectează direct la aplicația GravityZone.

      În acest caz, puteți defini de asemenea:
      - Un server de comunicații personalizat introducând IP-ul sau numele de gazdă al acestuia, dacă este necesar.
      - Setări proxy, dacă stațiile de lucru țintă comunică cu aplicația GravityZone prin proxy. În acest caz, selectați **Utilizare proxy pentru comunicații** și introduceți setările de proxy necesare în câmpurile de mai jos.
    - **Releu Endpoint Security**, dacă doriți să conectați stațiile de lucru la un client de tip releu instalat în rețeaua dvs. Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați mașina de tip releu dorită. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.

      Important
      Portul 7074 trebuie să fie deschis pentru ca instalarea prin Bitdefender Endpoint Security Tools Relay să funcționeze.
18. Faceți clic pe **Save**.

Pachetul nou creat va fi adăugat în lista de pachete.

Notă
Setările configurate în cadrul unui pachet de instalare se vor aplica pe stațiile de lucru imediat după instalare. Imediat după aplicarea politicii de securitate la nivelul

clientului, setările configurate în cadrul politicii vor intra în vigoare, înlocuind anumite setări din pachetul de instalare (cum ar fi serverele de comunicații sau setările proxy).

Descărcați pachetele de instalare

Pentru a descărca pachetele de instalare ale agenților de securitate:

1. Înregistrați-vă în Control Center de pe stația de lucru pe care doriți să instalați protecția.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați pachetul de instalare pe care doriți să îl descărcați.
4. Faceți clic pe butonul **Descărcare** din partea de sus a tabelului și selectați tipul de instalare pe care doriți să o utilizați. Există două tipuri de fișiere de instalare:
   - **Aplicație de descărcare**. Aplicația de descărcare descarcă mai întâi setul complet de instalare de pe serverele cloud ale Bitdefender și apoi demarează instalarea. Este de dimensiuni reduse și poate fi rulată atât pe sistemele de 32, cât și pe cele de 64 de biți (ceea ce ușurează distribuția). Dezavantajul este că necesită o conexiune activă la Internet.
   - **Kit complet**. Kit-urile complete de instalare sunt mai mari și trebuie să ruleze pe un anumit tip de sistem de operare.

     Setul complet va fi utilizat pentru a instala protecția pe stațiile de lucru cu o conexiune slabă sau chiar inexistentă la internet. Descărcați acest fișier pe o stație de lucru conectată la Internet și apoi distribuiți-l pe alte stații de lucru folosind un mediu de stocare extern sau un director partajat în rețea.

     Notă
     Versiuni cu kit complet disponibile:
     - **Windows OS:** sisteme pe 32 de biți și pe 64 de biți
     - **Linux OS:** sisteme pe 32 de biți și pe 64 de biți
     - **macOS:** numai sisteme pe 64 de biți

     Asigurați-vă că folosiți versiunea corectă pentru stația de lucru pe care instalați.
5. Salvați fișierul pe stația de lucru.

Avertisment

- Executabilul de descărcare nu trebuie redenumit. În caz contrar, nu veți putea descărca fișierele de instalare de pe serverul Bitdefender.

6. În plus, dacă ați ales Aplicația de descărcare, puteți crea un pachet MSI pentru stațiile de lucru Windows. Pentru informații suplimentare, consultați acest articol KB.

Trimitere link-uri de descărcare pachete de instalare prin e-mail

Este posibil să trebuiască să informați rapid ceilalți utilizatori că pot descărca un pachet de instalare. În acest caz, urmați pașii de mai jos:

1. Mergeți la pagina **Rețea > Pachete**.
2. Selectați pachetul de instalare dorit.
3. Faceți clic pe butonul **Trimitere link-uri descărcare** din partea de sus a tabelului. Va apărea o fereastră de configurare.
4. Introduceți adresa de e-mail a fiecărui utilizator care urmează să primească link-ul de descărcare a pachetului de instalare. Apăsați `Enter` după fiecare adresă de e-mail.

   Asigurați-vă că fiecare adresă de e-mail introdusă este validă.
5. Dacă doriți să vizualizați link-urile de descărcare înainte de trimiterea acestora prin e-mail, faceți clic pe butonul **Link-uri de instalare**.
6. Faceți clic pe **Trimitere**. Un e-mail care conține link-ul de instalare este trimis fiecărei adrese de e-mail specificate.

Rularea pachetelor de instalare

Pentru ca instalarea să funcționeze, pachetul de instalare trebuie rulat folosind privilegii de administrator.

Pachetul se instalează diferit pe fiecare sistem de operare, după cum urmează:

- Pe sistemele de operare Windows și macOS:
  1. Pe stația de lucru țintă, descărcați fișierul de instalare de pe Control Center sau copiați-l dintr-o unitate de partajare a rețelei.
  2. Dacă descărcați setul complet, extrageți fișierele din arhivă.

3. Executați fișierul executabil.
4. Urmați instrucțiunile de pe ecran.

> **Notă**
> Pe macOS, după instalarea Endpoint Security for Mac, utilizatorilor li se va solicita să aprobe extensiile kernel ale Bitdefender pe computerele lor. Anumite caracteristici ale agentului de securitate nu vor funcționa decât în momentul în care utilizatorii aprobă extensiile kernel ale Bitdefender. Pentru detalii, consultați acest articol KB.

- Pe sistemele de operare Linux:
  1. Conectați-vă și autentificați-vă la Control Center.
  2. Descărcați sau copiați fișierul de instalare pe stația de lucru țintă.
  3. Dacă descărcați setul complet, extrageți fișierele din arhivă.
  4. Obțineți privilegiile de rădăcină executând comanda `sudo su`.
  5. Modificați permisiunile asupra fișierului de instalare pentru a-l putea executa:

     ```
     # chmod +x installer
     ```

  6. Rulați fișierul de instalare:

     ```
     # ./installer
     ```

  7. Pentru a verifica dacă agentul a fost instalat pe stația de lucru, executați următoarea comandă:

     ```
     $ service bd status
     ```

Duoă ce agentul de securitate a fost instalat, stația de lucru va apărea ca administrată în Control Center (pagina **Rețea**), în câteva minute.

Important
Dacă utilizați VMware Horizon View Persona Management, vă recomandăm să configurați Politica grupului activ de directoare pentru a exclude următoarele procese Bitdefender (fără calea completă):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Aceste excepții trebuie să fie aplicate atât timp cât agentul de securitate rulează la nivelul stației de lucru. Pentru detalii, consultați această pagină cu documentație VMware Horizon.

Instalare de la distanță

Control Center vă permite să instalați agentul de securitate pe stațiile de lucru din mediile de lucru integrate cu Control Center, cât și pe alte stații de lucru detectate în rețea, cu ajutorul sarcinilor de instalare. În mediile VMware, instalarea de la distanță se bazează pe VMware Tools, în timp ce în mediile Citrix XenServer și Nutanix Prism Element, se bazează pe partajările pentru administratori Windows și SSH.

Odată ce agentul de securitate este instalat pe o stație de lucru, este posibil să dureze câteva minute până când restul stațiilor de lucru din rețea devin vizibile în Control Center.

Bitdefender Endpoint Security Tools include un mecanism automat de descoperire a rețelei care permite detectarea stațiilor de lucru care nu sunt în Active Directory. Stațiile de lucru detectate sunt afișate ca fiind **neadministrate** pe pagina **Rețea**, modul de vizualizare **Calculatoare**, în **Grupuri personalizate**. Control Center șterge automat stațiile de lucru Active Directory din lista de stații de lucru detectate.

Pentru a permite descoperirea rețelei, trebuie să aveți Bitdefender Endpoint Security Tools instalat deja pe cel puțin o stație de lucru din rețea. Această stație de lucru va fi utilizată pentru a scana rețeaua și a instala Bitdefender Endpoint Security Tools pe stațiile de lucru neprotejate.

Pentru informații detaliate referitoare la descoperirea rețelei, consultați „Cum funcționează opțiunea de descoperire a rețelei” (p. 157).

Cerințe pentru instalarea de la distanță

Pentru ca instalarea de la distanță să funcționeze:

- Pe Windows:
  - Trebuie activată partajarea administrativă admin$. Configurați fiecare stație de lucru vizată pentru ca aceasta să nu utilizeze partajarea avansată de fișiere.
  - Configurați funcția Controlul contului utilizatorului (UAC - User Account Control) în funcție de sistemul de operare care rulează pe stațiile de lucru vizate. În cazul în care stațiile de lucru sunt într-un domeniu Active Directory, puteți utiliza o politică de grup pentru a configura funcția Controlul contului utilizatorului. Pentru detalii, consultați acest articol KB.
  - Dezactivați Firewall-ul Windows sau configurați-l pentru a permite traficul prin intermediul protocolului de Partajare fișiere și imprimante (File and Printer Sharing).

  Notă
  Implementarea la distanță funcționează doar pe sistemele de operare moderne, începând cu Windows 7 / Windows Server 2008 R2, pentru care Bitdefender acordă suport complet. Pentru mai multe informații, consultați capitolul „Sisteme de operare suportate” (p. 28).

- Pe Linux: trebuie activat SSH.
- Pe macOS: trebuie activate autentificarea de la distanță și partajarea fișierelor.

Rularea sarcinilor de instalare de la distanță

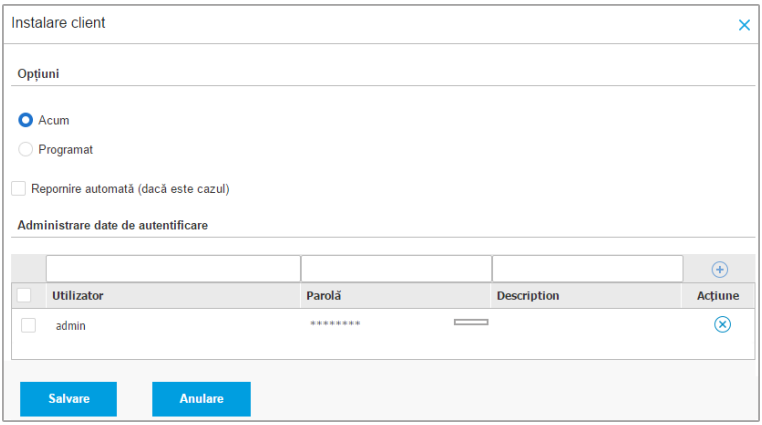
Pentru a rula o sarcină de instalare de la distanță:

1. Conectați-vă și autentificați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
4. Selectați grupul dorit din fereastra din stânga. Entitățile din grupul selectat sunt afișate în tabelul din fereastra din dreapta.

Notă
Opțional, puteți aplica filtre pentru a afișa exclusiv stațiile de lucru neadministrate. Dați clic pe meniul **Filtre** și selectați următoarele opțiuni: **Neadministrat** din fila **Securitate** și **Toate obiectele recursiv** din fila **Adâncime**.

5. Selectați entitățile (stațiile de lucru sau grupurile de stații de lucru) pe care doriți să instalați protecția.
6. Faceți clic pe butonul **Sarcini** din partea din dreapta sus a tabelului și selectați **Instalare**.

   Se afișează asistentul **Instalare client**.



Instalarea Bitdefender Endpoint Security Tools din meniul Sarcini

7. În secțiunea **Opțiuni**, configurați timpul de instalare:
   - **Acum**, pentru a lansa instalarea imediat.
   - **Programat**, pentru a configura intervalul de recurență al instalării. În acest caz, selectați intervalul de timp dorit (orar, zilnic sau săptămânal) și configurați-l conform necesităților dvs.

     Notă
     De exemplu, dacă sunt necesare anumite operațiuni pe mașina țintă înainte de a instala clientul (cum ar fi dezinstalarea altor aplicații și repornirea sistemului de operare), puteți programa sarcina de instalare să ruleze la fiecare

2 ore. Sarcina va începe pe fiecare mașină țintă la fiecare 2 ore până la finalizarea cu succes a instalării.

8. Dacă doriți ca stațiile de lucru țintă să fie repornite automat pentru finalizarea instalării, selectați **Repornire automată (dacă este necesar)**.
9. În secțiunea **Administrare date de autentificare**, specificați drepturile de administrare necesare pentru autentificarea de la distanță pe stațiile de lucru țintă. Puteți adăuga datele de autentificare introducând numele de utilizator și parola pentru fiecare sistem de operare țintă.

   Important
   Pentru stații de lucru cu sistem de operare Windows 8.1, este necesar să furnizați datele de autentificare ale contului de administrator încorporat sau ale unui cont de administrator de domeniu. Pentru mai multe informații, consultați acest articol KB.

   Pentru a adăuga datele SO necesare:

   a. Introduceți numele de utilizator și parola unui cont de administrator în câmpurile corespunzătoare din capul de tabel.

      În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

      Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

      - Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.comusername@domain.com` și `domain\userusername`).
      - Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

      Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont.

   b. Faceți clic pe butonul ⊕ **Adăugare**. Contul este adăugat la lista de date de autentificare.

Notă
Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți. Pentru a accesa funcția de Administrare date de autentificare, nu trebuie decât să dați clic pe numele dvs. de utilizator din colțul din dreapta sus al consolei.

Important
Dacă datele de autentificare furnizate nu sunt valabile, instalarea aplicației client va eșua pe stațiile de lucru respective. Asigurați-vă că actualizați datele de autentificare pentru sistemul de operare introduse în funcționalitatea de Administrare date de autentificare atunci când acestea se schimbă pe stațiile de lucru țintă.

10. Selectați casetele corespunzătoare conturilor pe care doriți să le folosiți.

Notă
Dacă nu ați selectat datele de autentificare, se va afișa un mesaj de avertizare. Acest pas este obligatoriu pentru instalarea de la distanță a agentului de securitate pe stațiile de lucru.

11. În secțiunea **Agent de instalare**, alegeți entitatea la care se vor conecta stațiile de lucru țintă pentru instalarea și actualizarea clientului:

- **Aplicația GravityZone**, atunci când stațiile de lucru se conectează direct la aplicația GravityZone.

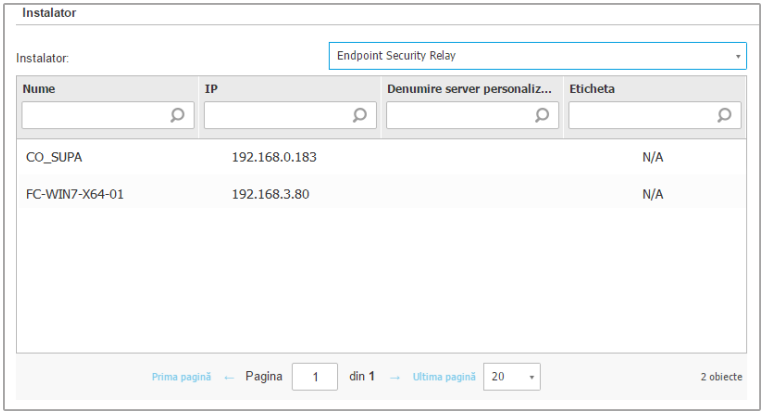
  În acest caz, puteți defini de asemenea:

  – Un server de comunicații personalizat introducând IP-ul sau numele de gazdă al acestuia, dacă este necesar.

  – Setări proxy, dacă stațiile de lucru țintă comunică cu aplicația GravityZone prin proxy. În acest caz, selectați **Utilizare proxy pentru comunicații** și introduceți setările de proxy necesare în câmpurile de mai jos.

- **Releu Endpoint Security**, dacă doriți să conectați stațiile de lucru la un client de tip releu instalat în rețeaua dvs. Toate mașinile cu rolul de releu detectate în rețeaua dvs. vor fi afișate în tabelul afișat mai jos. Selectați mașina de tip releu dorită. Stațiile de lucru conectate vor comunica cu Control Center exclusiv prin releul specificat.

Important
Portul 7074 trebuie să fie deschis pentru ca instalarea prin agentul releu să funcționeze.



12. Utilizați secțiunea **Ținte suplimentare** dacă doriți să instalați clientul pe anumite mașini din rețeaua dumneavoastră care nu sunt incluse în inventarul rețelei. Extindeți secțiunea și introduceți adresa IP sau numele de domeniu pentru mașinile respective în câmpul dedicat, separate printr-o virgulă. Puteți adăuga numărul necesar de adrese IP.
13. Trebuie să selectați un pachet de instalare pentru instalarea curentă. Dați clic pe lista **Utilizare pachet** și selectați pachetul de instalare dorit. Puteți găsi aici toate pachetele de instalare create anterior pentru contul dumneavoastră, precum și pachetul de instalare implicit disponibil în Control Center.
14. Dacă este necesar, puteți modifica o parte din setările pachetului de instalare făcând clic pe butonul **Personalizare** de lângă câmpul **Utilizare pachet**.

    Setările pachetului de instalare vor apărea mai jos și veți putea efectua modificările de care aveți nevoie. Pentru a afla mai multe despre modificarea pachetului de instalare, consultați „Generarea pachetelor de instalare” (p. 138).

    Dacă doriți să salvați modificările ca pachet nou, selectați opțiunea **Salvare ca pachete** situată în partea de jos a listei de setări a pachetului și introduceți o denumire pentru noul pachet de instalare.
15. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Important
Dacă utilizați VMware Horizon View Persona Management, vă recomandăm să configurați Politica grupului activ de directoare pentru a exclude următoarele procese Bitdefender (fără calea completă):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Aceste excepții trebuie să fie aplicate atât timp cât agentul de securitate rulează la nivelul stației de lucru. Pentru detalii, consultați această pagină cu documentație VMware Horizon.

Pregătirea sistemelor Linux pentru scanarea la accesare

Bitdefender Endpoint Security Tools pentru Linux include funcția de scanare la accesare, care funcționează cu anumite distribuții Linux și versiuni de kernel. Pentru mai multe informații, consultați cerințele de sistem.

În continuare veți afla cum să compilați manual modulul DazukoFS.

Compilarea manuală a modulului DazukoFS

Urmați pașii de mai jos pentru a compila DazukoFS pentru versiunea de kernel a sistemului și apoi încărcați modulul:

1. Descărcați headerele de kernel corespunzătoare.
   - Pe sistemele **Ubuntu**, executați comanda următoare:

     ```
     $ sudo apt-get install linux-headers-`uname -r`
     ```

   - Pe sistemele **RHEL/CentOS**, executați comanda următoare:

```
$ sudo yum install kernel-devel kernel-headers-`uname -r`
```

2. Pe sistemele **Ubuntu**, aveți nevoie de `build-essential`:

```
$ sudo apt-get install build-essential
```

3. Copiați și extrageți codul sursă DazukoFS în directorul preferat:

```
# 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. Compilați modulul:

```
# make
```

5. Instalați și încărcați modulul:

```
# make dazukofs_install
```

Cerințele pentru utilizarea scanării la accesare cu DazukoFS

Pentru ca DazukoFS și scanarea la accesare să funcționeze bine împreună, trebuie să se îndeplinească o serie de condiții. Vă rugăm să verificați dacă oricare dintre afirmațiile de mai jos se aplică sistemului dumneavoastră Linux și să urmați instrucțiunile pentru a evita eventualele probleme.

- Politica SELinux trebuie să fie dezactivată sau setată pe nivelul **permisiv**. Pentru a verifica și ajusta setările politicii SELinux, editați fișierul `/etc/selinux/config`.

- Bitdefender Endpoint Security Tools este compatibil exclusiv cu versiunea DazukoFS inclusă în pachetul de instalare. Dacă DazukoFS este deja instalat pe sistem, îndepărtați-l înainte de a instala Bitdefender Endpoint Security Tools.
- DazukoFS suportă doar anumite versiuni kernel. Dacă pachetul DazukoFS furnizat împreună cu Bitdefender Endpoint Security Tools nu este compatibil cu versiunea kernel a sistemului, încărcarea modulului nu va reuși. În acest caz puteți fie actualiza kernelul conform versiunii suportate sau puteți recompila modulul DazukoFS pentru versiunea dvs. de kernel. Puteți găsi pachetul DazukoFS în directorul de instalare Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`
- Atunci când partajați fișiere folosind servere dedicate precum NFS, UNFSv3 sau Samba, trebuie să porniți serviciile în următoarea ordine:
  1. Activați scanarea la accesare prin intermediul politicii din Control Center.

     Pentru informații suplimentare, consultați Ghidul administratorului GravityZone.
  2. Porniți serviciul de partajare în rețea.

     Pentru NFS:

     ```
     # service nfs start
     ```

     Pentru UNFSv3:

     ```
     # service unfs3 start
     ```

     Pentru Samba:

     ```
     # service smbd start
     ```

Important
Pentru serviciul NFS, DazukoFS este compatibil doar cu serverul de utilizatori NFS User Server.

Cum funcționează opțiunea de descoperire a rețelei

În afara integrării cu Active Directory, GravityZone include și un mecanism automat de descoperire a rețelei, dedicat detectării calculatoarelor din grupul de lucru.

GravityZone se bazează pe serviciul **Microsoft Computer Browser** și pe instrumentul **NBTscan** pentru descoperirea rețelei.

Serviciul Computer Browser este o tehnologie de rețelistică utilizată de calculatoarele care rulează Windows pentru menținerea unei liste actualizate de domenii, grupuri de lucru și a calculatoarelor incluse în acestea și pentru furnizarea acestor liste către calculatoarele client, la cerere. Calculatoarele detectate în rețea de serviciul Computer Browser pot fi vizualizate prin rularea comenzii **net view** într-o fereastră de introducere a comenzii.

Comanda net view

Instrumentul NBTscan scanează rețelele calculatoarelor folosind NetBIOS. Acesta interoghează fiecare stație de lucru din rețea și extrage informații precum adresa IP, numele calculatorului NetBIOS și adresa MAC.

Pentru a permite descoperirea automată a rețelei, trebuie să aveți Bitdefender Endpoint Security Tools Relay instalat deja pe cel puțin o stație de lucru din rețea. Acest calculator va fi utilizat pentru scanarea rețelei.

Important

Control Center nu utilizează informații privind rețeaua din Active Directory sau din funcția harta rețelei. Harta rețelei se bazează pe o altă tehnologie de descoperire a rețelei: protocolul Link Layer Topology Discovery (LLTD).

Control Center nu este implicată activ în funcționarea serviciului Computer Browser. Bitdefender Endpoint Security Tools interoghează doar serviciul Computer Browser pentru a obține lista de stații de lucru și servere vizibile la momentul respectiv în rețea (cunoscută sub numele de lista de navigare) și apoi o trimite către Control

Center. Control Center procesează lista de parcurgere și include noile calculatoare detectate în lista **Calculatoare neadministrate**. Calculatoarele detectate anterior nu sunt șterse după o nouă interogare de descoperire a rețelei; prin urmare, trebuie să excludeți și să ștergeți manual & calculatoarele care nu mai sunt în rețea.

Interogarea inițială aferentă listei de parcurgere este efectuată de primul Bitdefender Endpoint Security Tools instalat în rețea.

- Dacă releul este instalat pe un calculator aparținând unui grup de lucru, numai calculatoarele din acest grup vor fi vizibile în Control Center.
- Dacă releul este instalat pe un calculator de domeniu, numai calculatoarele din domeniul respectiv vor fi vizibile în Control Center. Calculatoarele din alte domenii pot fi detectate dacă există o relație de încredere cu domeniul pe care este instalat releul.

Interogările ulterioare pentru descoperirea rețelei sunt efectuate regulat, în fiecare oră. Pentru fiecare nouă interogare, Control Center împarte spațiul calculatoarelor administrate în zonele de vizibilitate și apoi identifică un releu în fiecare zonă, pentru executarea sarcinii. O zonă de vizibilitate este un grup de calculatoare care se detectează reciproc. În general, o zonă de vizibilitate este definită de un grup de lucru sau domeniu, însă aceasta depinde de topologia și configurația rețelei. În anumite cazuri, o zonă de vizibilitate poate include mai multe domenii și grupuri de lucru.

Dacă un releu selectat nu efectuează interogarea, Control Center așteaptă până la următoarea interogare programată, fără a alege un alt releu pentru a relua încercarea.

Pentru vizibilitate completă a rețelei, releul trebuie instalat pe cel puțin un calculator din fiecare grup de lucru sau domeniu din rețeaua dumneavoastră. Ideal, Bitdefender Endpoint Security Tools trebuie instalat pe cel puțin un calculator din fiecare sub-rețea.

Mai multe despre serviciul Microsoft Computer Browser

Pe scurt despre serviciul Computer Browser:

- Operează independent de Active Directory.
- Rulează exclusiv pe rețelele IPv4 și operează independent în limitele unui grup LAN (grup de lucru sau domeniu). O listă de parcurgere este realizată și menținută pentru fiecare grup LAN.

- În mod tipic, utilizează pentru comunicarea între noduri transmisiile prin servere și nevalidate.
- Utilizează NetBIOS prin TCP/IP (NetBT).
- Necesită o rezoluție de nume NetBIOS. Se recomandă existența unei infrastructuri Windows Internet Name Service (WINS) care să ruleze în rețea.
- Nu este activată implicit pe Windows Server 2008 și 2008 R2.

Pentru informații detaliate privind serviciul Computer Browser, accesați Computer Browser Service Technical Reference de pe Microsoft Technet.

Cerințe pentru aplicația de descoperire a rețelei

Pentru descoperirea cu succes a tuturor calculatoarelor (servere și stații de lucru) care vor fi administrate de pe Control Center, sunt necesare următoarele:

- Calculatoarele trebuie să fie asociate într-un grup de lucru sau domeniu și conectate printr-o rețea locală IPv4. Serviciul Computer Browser nu funcționează pe rețelele IPv6.
- Mai multe calculatoare din fiecare grup LAN (grup de lucru sau domeniu) rebuie să ruleze serviciul Computer Browser. Controlerele principale ale domeniului trebuie să ruleze de asemenea serviciul.
- NetBIOS prin TCP/IP (NetBT) trebuie să fie activată pe calculatoare. Firewall-ul local trebuie să permită traficul NetBT.
- Dacă se utilizează un releu Linux pentru a descoperi alte stații de lucru Linux sau Mac, este necesar fie să instalați Samba pe stațiile de lucru țintă, fie să le uniți în Active Directory și să folosiți DHCP. În acest fel, NetBIOS va fi configurat automat pe acestea.
- Partajarea fișierelor trebuie să fie activată pe toate calculatoarele. Firewall-ul local trebuie să permită partajarea fișierelor.
- O infrastructură Windows Internet Name Service (WINS) trebuie să fie configurată și să funcționeze corespunzător.
- Funcția de descoperire a rețelei trebuie activată (**Control Panel >; Network and Sharing Center >; Change Advanced Sharing Settings**).

  Pentru activarea acestei funcții, trebuie inițiate următoarele servicii:
  - DNS Client
  - Function Discovery Resource Publication

  - SSDP Discovery
  - UPnP Device Host
- În medii cu mai multe domenii, se recomandă configurarea unor relații de încredere între domenii, pentru a permite calculatoarelor să acceseze listele de parcurgere din alte domenii.

Calculatoarele de pe care Bitdefender Endpoint Security Tools interoghează serviciul Computer Browser trebuie să poată identifica numele NetBIOS.

Notă
Mecanismul de descoperire a rețelei funcționează pentru toate sistemele de operare acceptate, inclusiv versiunile de Windows Embedded, cu condiția să fie îndeplinite cerințele.

5.4. Instalarea EDR

Acest modul este livrat implicit cu setul de instalare Bitdefender Endpoint Security Tools și necesită activarea Senzorului de incidente la prima introducere a cheii de licență.

Înaintea instalării, asigurați-vă că endpoint-urile vizate îndeplinesc cerințele minime. Cerințele minime pentru incidente corespund cerințelor agentului de securitate.

Pentru a vă proteja stațiile de lucru cu EDR, puteți selecta una dintre cele două opțiuni:

- Instalați agenții de securitate împreună cu Senzorul EDR atunci când introduceți cheia de licență. Consultați secțiunea Activarea licenței.
- Utilizați sarcina **Reconfigurare**.

Important
The Incidents Sensor no longer provides support for Internet Explorer.

Pentru informații suplimentare, consultați Ghidul administratorului GravityZone.

5.5. Instalarea Sandbox Analyzer On-Premises

Pentru a vă asigura că instalarea se efectuează fără probleme, parcurgeți pașii următori:

1. Pregătirea pentru instalare
2. Instalarea Aplicației virtuale Sandbox Analyzer

3. Instalare aplicație virtuală de securitate pentru rețea

5.5.1. Pregătirea pentru instalare

Înainte de a instala Sandbox Analyzer On-Premises, asigurați-vă că:

- Hypervisor-ul VMWare ESXi este instalat și configurat. Pentru detalii, consultați documentația Instalare și configurare vSphere, secțiunea 2: „Instalarea și configurarea hypervysor-ului ESXi".
- Aplicația virtuală Bitdefender GravityZone este instalată și configurată.

Notă
În ceea ce privește hypervisor-ul VMWare ESXi, asigurați-vă că:

- Versiunea ESXi este 6.5 sau mai recentă.
- Versiunea spațiului de stocare a datelor VMFS este 5.
- SSH este activat în **Politică pornire** cu configurația **Pornire și oprire odată cu gazda**.
- Serviciul NTP este activ și configurat.

Cheia de licență Sandbox Analyzer On-Premises determină numărul maxim de detonări simultane. Deoarece fiecare detonare necesită o instanță de mașină virtuală în curs, numărul de detonări simultane se reflectă în numărul de mașini virtuale create. Pentru detalii despre adăugarea de chei de licență în GravityZone Control Center, consultați „Introducerea cheilor de licență" (p. 121).

5.5.2. Instalarea Aplicației virtuale Sandbox Analyzer

Pentru instalarea Aplicației virtuale Sandbox Analyzer:

1. Autentificați-vă în GravityZone Control Center.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați caseta **Sandbox Analyzer** din tabel.
4. Selectați butonul **Descărcare** din partea de stânga sus a paginii. Selectați opțiunea **Security Appliance (componentă individuală ESXi)**.
5. Utilizați instrumentul dvs. pentru administrarea platformei de virtualizare (spre exemplu, vSphere Client) pentru importarea fișierului descărcat OVA în mediul dvs. virtual.

Notă
La instalarea fișierului OVA, configurați rețelele după cum urmează:

- **Rețea Bitdefender** - aceasta este rețeaua în care se găsesc alte componente Bitdefender (interfață `eth0`). Sandbox Analyzer și aplicația GravityZone trebuie să fie în aceeași rețea și trebuie să comunice prin `eth0`.
- **Rețea privată de detonare** - Sandbox Analyzer utilizează această rețea pentru comunicare internă (interfață `eth1`). Această rețea trebuie să fie izolată de alte segmente ale rețelei.
- **Rețea acces internet** - Sandbox Analyzer utilizează această rețea pentru a obține cele mai recente actualizări (interfață `eth1`). Interfața `eth2` nu trebuie să aibă același IP sau aceeași rețea ca și `eth0`.

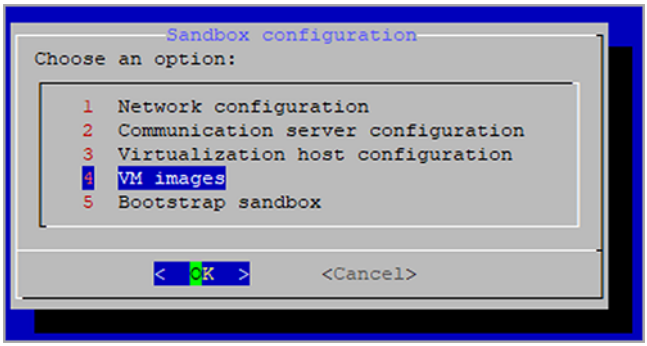
6. Porniți aplicația.
7. Din instrumentul dvs. pentru administrarea platformei de virtualizare, accesați interfața consolei Aplicației virtuale Sandbox Analyzer.
8. La solicitarea datelor de autentificare, utilizați `root` pentru numele de utilizator și `sve` pentru parolă.
9. Accesați meniul de configurare prin executarea următoarei comenzi:

```
/opt/bitdefender/bin/sandbox-setup
```

10. În meniul **Configurare Sandbox** efectuați următoarele setări:
    a. **Configurare rețea**. Selectați această opțiune pentru configurarea cardului NIC de administrare. Sandbox Analyzer va utiliza această interfață de rețea pentru comunicarea cu GravityZone.

       Adresa IP poate fi specificată manual sau automat prin DHCP.

       Notă
       Dacă aplicația GravityZone este într-o altă rețea față de `eth0`, trebuie să adăugați o rută statică în **Configurare rețea > Rețea BitDefender > Rute** pentru ca Sandbox Analyzer să funcționeze corespunzător.



Consola aplicației Sandbox Analyzer

b. **Configurare proxy internet**. Pentru ca instalarea să aibă succes, Sandbox Analyzer necesită conexiunea la internet. În acest caz, puteți configura Sandbox Analyzer să utilizeze un server proxy, specificând aceste detalii:

   - **Gazdă** - IP sau FQDN a serverului proxy. Utilizați următoarea sintaxă: `http://<IP/Hostname>:<Port>`.
   - **Utilizator și parolă** - este necesar să introduceți parola de două ori.
   - **Domeniu** - domeniul Active Directory domain, dacă este cazul.

c. **Configurarea serverului de comunicare**. Specificați fie adresa IP, fie gazda aplicației care rulează cu rolul de Server de comunicare.

   Utilizați următoarea sintaxă: `http://<IP/Hostname>:<Port>`. Portul implicit este `8443`.

   Notă
   Imediat după specificarea adresei IP sau numelui gazdei și salvarea configurației, instanța Sandbox Analyzer va deveni vizibilă în GravityZone Control Center, în pagina **Sandbox Analyzer >; Infrastructură**.

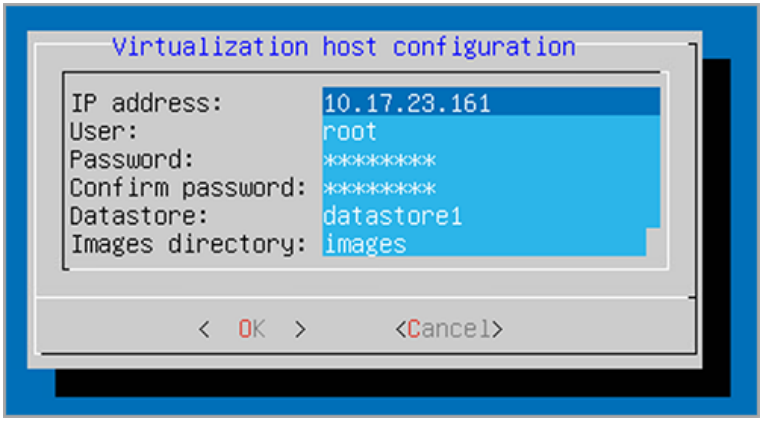
d. **Configurarea gazdei virtuale**. Sandbox Analyzer utilizează serverul ESXi pentru a dispune infrastructura de analiză malware. Prin utilizarea **Configurarea gazdei virtuale**, conectați aplicația Sandbox Analyzer la gazda ESXi prin furnizarea următoarelor informații:

   - Adresa IP a serverului ESXi.

- Date de autentificare root pentru accesarea gazdei ESXi.
- Spațiu de stocare a datelor dedicat pentru Sandbox Analyzer.

  Introduceți numele spațiului de stocare a datelor așa cum este afișat de ESXi.
- Numele directorului utilizat de spațiul de stocare a datelor pentru stocarea imaginilor mașinii virtuale.

  Dacă acest director nu există, este necesar să îl creați în spațiul de stocare a datelor înainte de a salva configurația Sandbox Analyzer.



Consolă aplicație Sandbox Analyzer

e. **Imagini de mașină virtuală**. Pentru construirea mașinilor virtuale de detonare pentru Sandbox Analyzer, este necesar să copiați fișierele VMDK care conțin imaginile dorite în fișierul **Imagini** specificat în meniul **Configurarea gazdei virtuale**. Pentru fiecare imagine, puteți efectua următoarele setări în meniul **Imagini de mașină virtuală**:

   i. În meniul **Configurare imagini**, specificați numele imaginii (așa cum va fi afișat în GravityZone Control Center) și sistemul de operare.

   Notă
   Directorul care conține imagini de mașină virtuală este scanat periodic și intrările noi sunt raportate către GravityZone. Aceste intrări sunt vizibile

în Control Center, în pagina **Sandbox Analyzer >; Infrastructură >; Administrare imagini**.

În anumite cazuri, când utilizați Sandbox Analyzer, este posibil să întâmpinați probleme cu mașinile virtuale de detonare. Pentru rezolvarea acestor probleme, este necesar să dezactivați opțiunea anti-amprentă. Pentru detalii, consultați „Tehnici anti-amprentă” (p. 165).

ii. În meniul **Gazde DMZ**, puteți introduce pe lista albă numele gazdelor care sunt necesare serviciilor terțe și componentelor integrate în mașinile virtuale pentru comunicarea cu Sandbox Manager. Pentru detalii consultați „Gazde DMZ” (p. 166)

iii. În meniul **Ștergere**, puteți șterge imaginile de mașină virtuală de care nu mai aveți nevoie.

f. **Bootstrap sandbox**. După ce ați adăugat detaliile privind configurația Sandbox Analyzer, continuați instalarea selectând această opțiune. Starea instalării va fi afișată în GravityZone Control Center, în pagina **Sandbox Analyzer >; Infrastructură**.

Tehnici anti-amprentă

În mod implicit, în timpul procesului de construire a imaginilor, Sandbox Analyzer va activa diferite tehnici anti-amprentă. Unele tipuri de malware sunt capabile să determine dacă rulează sau nu într-un mediu sandbox și, dacă da, nu-și vor activa comportamentele periculoase.

Scopul tehnicilor anti-amprentă este simularea mai multor condiții cu copul de a imita un mediu real. Din cauza unei combinații virtuale eliminate de software instalat și configurație de mediu, o combinație care nu poate fi prevăzută sau controlată, este posibil ca anumite tehnici să nu fie compatibile cu software-ul instalat în modelul de tip „golden image”. Puteți recunoaște astfel de situații rare prin următoarele semne:

- Erori apărute în timpul procesului de construire a imaginilor.
- Erori apărute la încercările de a executa software în interiorul imaginilor.
- Mesaje de eroare afișate la detonarea mostrelor.
- Software-ul licențiat nu mai funcționează din cauza cheilor de licență nevalide.

O soluție rapidă pentru astfel de situații rare este reconstruirea imaginii cu tehnicile anti-amprentă dezactivate. Pentru a face acest lucru, urmați pașii de mai jos:

1. Autentificați-vă în GravityZone Control Center și ștergeți imaginea.

2. Autentificați-vă în aplicația Sandbox Analyzer și lansați consola aplicației Sandbox Analyzer prin executarea următoarei comenzi:

```
/opt/bitdefender/bin/sandbox-setup
```

3. Mergeți la **Imagini de mașină virtuală >; Configurare imagini**.
4. Selectați imaginea care cauzează probleme.
5. Mergeți la opțiunea **Anti-amprentă**.
6. Deselectați caseta corespondentă pentru dezactivarea tehnicilor anti-amprentă.

Gazde DMZ

În timpul procesului de construire a imaginilor, va fi creată o infrastructură virtuală pentru facilitarea comunicării dintre Sandbox Manager și mașinile virtuale. Din perspectiva rețelei, acest lucru se traduce într-un mediu izolat de rețea care va conține toată comunicarea posibilă care ar putea fi creată de o mostră detonată.

Meniul serverelor DMZ permite includerea pe lista albă a numelor gazdelor care sunt necesare serviciilor terțe și componentelor integrate în mașinile virtuale pentru comunicarea cu, pentru o funcționare optimă.

Un exemplu pentru această situație ar fi serverele de licențiere KMS utilizate de licențierea Windows, dacă se aplică o licență pentru mai multe dispozitive (Volume license) pe mașinile virtuale furnizate.

5.5.3. Instalare aplicație virtuală de securitate pentru rețea

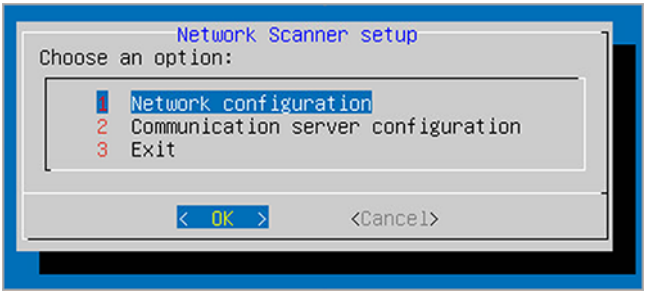
Această secțiune informează despre modul în care se instalează Aplicația virtuală de securitate pentru rețea, o componentă Sandbox Analyzer care monitorizează traficul din rețea și trimite mostre suspecte pentru analiză comportamentală.

Pentru instalarea aplicației virtuale de securitate pentru rețea:

1. Autentificați-vă în GravityZone Control Center.
2. Mergeți la pagina **Rețea > Pachete**.
3. Selectați caseta **Aplicație virtuală de securitate pentru rețea** din tabel.
4. Selectați butonul **Descărcare** din partea de stânga sus a paginii și apoi selectați opțiunea **(VMware OVA)**.

5. Utilizați instrumentul dvs. pentru administrarea platformei de virtualizare (spre exemplu, vSphere Client) pentru importarea fișierului descărcat OVA în mediul dvs. virtual.
6. În asistentul de instalare, selectați cardul NIC (network interface card) utilizat pentru comunicarea cu GravityZone și cardul NIC utilizat pentru monitorizarea traficului.
7. Porniți aplicația.
8. Din instrumentul dvs. pentru administrarea platformei de virtualizare, accesați interfața consolei GravityZone SVE SVA Aplicație virtuală de securitate pentru rețea.
9. La solicitarea datelor de autentificare, utilizați `root` pentru numele de utilizator și `sve` pentru parolă.
10. Accesați meniul de configurare prin executarea următoarei comenzi:

```
/opt/bitdefender/bin/nsva-setup
```



Consola aplicației de securitate pentru rețea

11. Accesați opțiunea **Configurarea serverului de comunicare** din meniu.
12. Specificați adresa IP sau numele gazdei și portul unui Server de comunicare GravityZone.

    Utilizați următoarea sintaxă: `http://<IP/Hostname>:<Port>`. Portul implicit este `8443`.
13. Salvați configurația.

Configurarea Senzorului de rețea pentru detonarea fișierelor pcap

Senzorul de rețea poate extrage conținut din fișierele extrase din rețea (pcap) și îl poate trimite automat pentru a fi detonat către instanța Sandbox Analyzer.

Pentru detonarea conținutului din fișierele pcap:

1. Autentificați-vă în Aplicația virtuală de securitate pentru rețea.
2. La solicitarea datelor de autentificare, utilizați `root` pentru numele de utilizator și `sve` pentru parolă.
3. Executați următoarea comandă:

   ```
   /opt/bitdefender/bin/scan-pcap <local pcap path>
   ```

   În comanda de sus, `<local pcap path>` reprezintă locația în care este încărcat fișierul pcap în Aplicația virtuală de securitate pentru rețea.

Pentru mai multe detalii despre utilizarea senzorului de rețea, consultați capitolul **Politici >; Sandbox Analyzer** din Ghidul administratorului GravityZone.

5.6. Instalarea Full Disk Encryption

GravityZone Full Disk Encryption este livrat ca serviciu ce necesită activare pe bază de cheie de licență. Pentru a face acest lucru, trebuie să accesați **Configurare > Licență** și să introduceți cheia de licență.

Pentru informații detaliate cu privire la cheile de licență, consultați „Administrarea licenței” (p. 120).

Agenții de securitate Bitdefender suportă modulul Full Disk Encryption începând cu versiunea 6.2.22.916 pe Windows și 4.0.0173876 pe Mac. Pentru a vă asigura că agenții sunt pe deplin compatibili cu acest modul, aveți la dispoziție două opțiuni:

- Instalați agenții de securitate cu modulul de Criptare inclus.
- Utilizați sarcina **Reconfigurare**.

Pentru informații detaliate despre utilizarea modulului Full Disk Encryption în rețeaua dvs., consultați capitolul **Politici de securitate > Criptare** din Ghidul administratorului GravityZone.

5.7. Instalarea Exchange Protection

Security for Exchange se integrează automat cu serverele Exchange, în funcție de rolul serverului. Pentru fiecare rol sunt instalate doar caracteristicile compatibile, după cum este descris în continuare:

Funcționalități	Microsoft Exchange 2019/2016/2013		Microsoft Exchange 2010/2007		
	Edge	Mailbox	Edge	Hub	Mailbox
Nivel Transport					
Filtrare antimalware	x	x	x	x	
Filtrare Antispam	x	x	x	x	
Filtrare pe bază de conținut	x	x	x	x	
Filtrare atașamente	x	x	x	x	
Exchange Store					
Scanare antimalware la cerere		x			x

5.7.1. Pregătirea pentru instalare

Înainte de a instala Security for Exchange, asigurați-vă că toate cerințele sunt îndeplinite, în caz contrar este posibil ca Bitdefender Endpoint Security Tools să se instaleze fără modulul de Protecție Exchange.

Pentru ca modulul de Protecție Exchange să funcționeze fără probleme și să prevină apariția conflictelor și rezultatele nedorite, dezinstalați agenții antimalware și de filtrare e-mail.

Bitdefender Endpoint Security Tools detectează automat și dezinstalează majoritatea produselor antimalware, dezactivând agentul antimalware integrat în Exchange Server de la versiunea 2013. Pentru detalii privind lista de software-uri detectate, consultați acest articol KB.

Puteți reactiva manual agentul antimalware Exchange integrat în orice moment, însă nu este recomandat să faceți acest lucru.

5.7.2. Instalarea protecției pe serverele Exchange

Pentru a proteja serverele Exchange, este necesar să instalați Bitdefender Endpoint Security Tools cu rol de Protecție Exchange pe fiecare dintre acestea.

Aveți mai multe opțiuni pentru configurarea Bitdefender Endpoint Security Tools pe serverele Exchange:

- Instalare locală, prin descărcarea și executare pachetului de instalare de pe server.
- Instalare de la distanță, prin executarea unei sarcini de **Instalare**.
- De la distanță, prin executarea sarcinii **Reconfigurare client**, dacă Bitdefender Endpoint Security Tools asigură deja protecția sistemului de fișiere de pe server.

Pentru a vedea pașii de instalare detaliați, consultați „Instalarea agenților de securitate” (p. 134).

5.8. Instalarea HVI

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Pentru a putea folosi HVI pe mașini virtuale de pe gazdele Xen, este necesar să urmați acești pași:

1. Faceți clic pe cerințele de instalare
2. Instalarea Security Server
3. Instalați pachetul suplimentar HVI

Cerințe preliminare

- XenServer este integrat cu GravityZone.
- XenCenter este instalat pe mașina dumneavoastră.

Instalarea Security Server

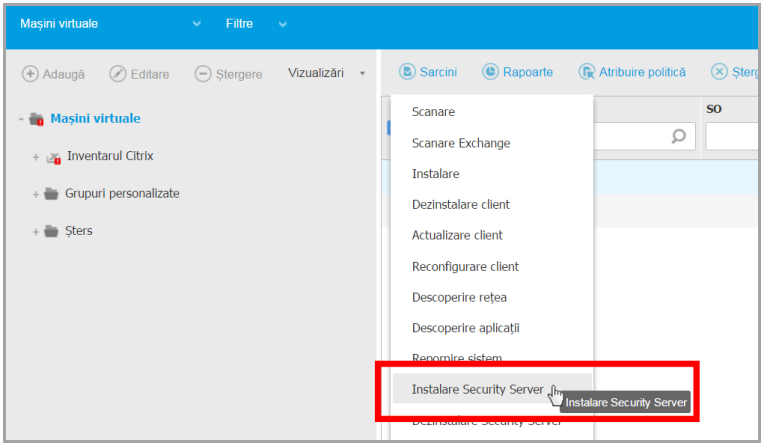
Pentru a instala Security Server pe una sau mai multe gazde:

1. Mergeți la pagina **Rețea**.

2. Selectați **Mașini virtuale** din selectorul de vizualizări.
3. Parcurgeți inventarul Citrix și bifați casetele corespunzătoare gazdelor vizate. Pentru o selecție rapidă, puteți selecta direct containerul rădăcină (Inventarul Citrix). Veți putea selecta gazdele individual din asistentul de instalare.

> **Notă**
> Nu puteți selecta gazde din diferite foldere.

4. Dați clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Instalare Security Server** din meniu. Se afișează fereastra **Instalare Security Server**.



Instalarea Security Server

5. Selectați gazdele pe care doriți să instalați instanțele Security Server.
6. Alegeți setările de configurare pe care doriți să le folosiți.

> **Important**
> Folosirea unor setări comune la rularea mai multor instanțe Security Server simultan necesită ca gazdele să împărtășească același spațiu de stocare, să aibă adrese IP alocate de un server DHCP și să facă parte din aceeași rețea.

Atunci când alegeți să configurați fiecare Security Server în mod diferit, veți putea defini setările pe care le doriți pentru fiecare gazdă în pasul următor al

asistentului. Pașii descriși în continuare se aplică în situația în care se folosește opțiunea **Configurați fiecare Security Server**.

7. Faceți clic pe **Înainte**.

   Notă
   În funcție de selecția efectuată anterior, este posibil ca unele opțiuni descrise aici să nu se aplice în situația dumneavoastră.

8. Introduceți o denumire sugestivă pentru Security Server.
9. Selectați containerul în care doriți să includeți Security Server din meniul **Container**.
10. Selectați spațiul de stocare destinație.
11. Selectați tipul de administrare. Se recomandă să instalați aplicația folosind o administrare de disc standard.

    Important
    Dacă folosiți alocarea dinamică de resurse (la cerere) și nu mai există spațiu disponibil de stocare a datelor, Security Server va îngheța și, prin urmare, gazda va rămâne neprotejată.

12. Configurați memoria și alocarea resurselor CPU în funcție de procentul de consolidare MV de pe gazdă. Selectați **Scăzut**, **Mediu** sau **Ridicat** pentru a încărca setările recomandate pentru alocarea resurselor sau **Manual** pentru a configura manual alocarea resurselor.
13. Setați fusul orar al aplicației.
14. Setați o parolă de administrator pentru consola Security Server. Setarea unei parole administrative suprascrie parola principală implicită ("sve").
15. Selectați tipul de configurare a rețelei pentru rețeaua Bitdefender. Adresa IP a Security Server nu trebuie să se modifice în timp, deoarece este utilizată de agenți Linux pentru comunicare.

    Dacă alegeți DHCP, asigurați-vă că ați configurat serverul DHCP pentru rezervarea adresei IP pentru aplicație.

    Dacă alegeți opțiunea statică, trebuie să introduceți adresa IP, masca de sub-rețea, portalul și informațiile DNS.

16. Faceți clic pe **Save**.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Instalarea pachetului suplimentar HVI

1. Mergeți la pagina **Configurare > Actualizare**.
2. Selectați pachetul suplimentar HVI din lista de **Componente** și faceți clic pe butonul **Download** din partea de sus a tabelului.
3. Mergeți la pagina **Rețea** și selectați **Mașini virtuale** din selectorul de vizualizări.
4. Selectați **Server** din meniul **Vizualizări** din secțiunea din stânga.
5. Selectați una sau mai multe gazde Xen din inventarul rețelei. Puteți vizualiza cu ușurință gazdele disponibile selectând opțiunea **Tip > Gazde** din meniul **Filtre**.
6. Faceți clic pe butonul **Sarcini** din secțiunea din dreapta și selectați **Instalare pachet suplimentar HVI**. Se va deschide fereastra de instalare.
7. Programați sarcina de instalare pentru când doriți să fie executată. Puteți opta pentru executarea sarcinii imediat după salvare sau la un anumit moment. În cazul în care instalarea nu poate fi realizată la momentul specificat, sarcina se repetă automat conform setărilor de recurență. De exemplu, dacă selectați mai multe gazde și una dintre acestea nu este disponibilă atunci când pachetul este programat pentru instalare, sarcina se va executa din nou la momentul specificat.
8. Gazda trebuie să fie repornită pentru aplicarea modificărilor și finalizarea instalării. Dacă doriți să reporniți gazda fără supraveghere, selectați **Repornire automată gazdă**.
9. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

5.9. Instalarea Protecției spațiului de stocare

Security for Storage este un serviciu Bitdefender conceput pentru protejarea dispozitivelor de stocare atașate la rețea (NAS) și a soluțiilor de partajare a fișierelor conforme cu ICAP (Internet Content Adaptation Protocol). Pentru a vedea sistemele acceptate de partajare a fișierelor, accesați „Protecție spațiu de stocare” (p. 56).

Pentru a folosi Security for Storage împreună cu soluția dvs. GravityZone:

1. Instalați și configurați cel puțin două Security Server în mediul dumneavoastră, care să funcționeze ca servere ICAP. Severele de securitate Security Server ale

Bitdefender analizează fișierele, trimit rezultatele către sistemele de stocare și iau măsurile necesare, dacă este cazul. În caz de supraîncărcare, primul Security Server redirecționează surplusul de date către cel de-al doilea.

Notă
Pentru a vă conforma celor mai bune practici, instalați serverele de securitate Security Server dedicate protecției spațiului de stocare, separat de serverele de securitate Security Server folosite pentru alte roluri, cum ar fi scanarea antimalware.

Pentru detalii despre procedura de instalare a Security Server, consultați secțiunea **Instalarea Security Server** din acest ghid.

2. Configurați modulul **Protecție spațiu de stocare** din setările politicii GravityZone.

   Pentru detalii, consultați capitolul **Politici de securitate > Politici computer și mașini virtuale > Protecție spațiu de stocare** din Ghidul administratorului GravityZone.

Pentru detalii despre configurarea și administrarea serverelor ICAP pe un anumit dispozitiv NAS sau sistem de partajare a fișierelor, consultați documentația pentru platforma respectivă.

5.10. Instalarea protecției pentru dispozitive mobile

Security for Mobile este o soluție de administrare pentru dispozitive mobile dedicat dispozitivelor iPhone, iPad și Android. Pentru o listă completă de versiuni de sisteme de operare compatibile, verificați cerințele de sistem.

Pentru a gestiona Security for Mobile din Control Center, trebuie să adăugați dispozitive mobile în Active Directory sau utilizatori personalizați, apoi să instalați aplicația GravityZone Mobile Client pe dispozitive. După ce ați configurat serviciul, puteți executa sarcini administrative pe dispozitive mobile.

Înainte de a începe, asigurați-vă că ați configurat o adresă publică (externă) pentru Serverul de comunicații.

Pentru a instala Security for Mobile:

1. Dacă nu aveți integrarea cu Active Directory, trebuie să creați utilizatorii pentru proprietarii de dispozitive mobile.
2. Adăugați dispozitive utilizatorilor.
3. Instalați GravityZone Mobile Client pe dispozitive și activați-l.

5.10.1. Configurați Adresa externă pentru Serverul de comunicații

În configurația implicită GravityZone, dispozitivele mobile pot fi administrate numai dacă sunt direct conectate la rețeaua companiei (prin Wi-Fi sau VPN). Acest lucru se întâmplă deoarece la înregistrarea dispozitivelor mobile, acestea sunt configurate pentru a se conecta la adresa locală a aplicației Serverului de comunicații.

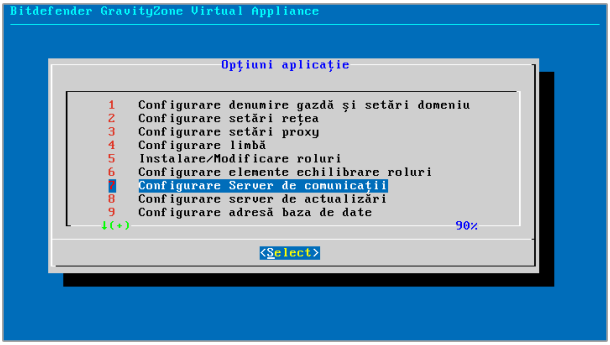
Pentru a putea administra dispozitivele prin Internet, indiferent de locația acestora, trebuie să configurați Serverul de comunicații cu o adresă ce poate fi accesată public.

Pentru a putea administra dispozitivele mobile atunci când nu sunt conectate la rețeaua companiei, sunt disponibile următoarele opțiuni:

- Configurați redirecționarea portului pe gateway-ul companiei pentru aplicația care îndeplinește rolul de Server de comunicații.
- Adăugați un adaptor de rețea suplimentar care îndeplinește rolul de Server de comunicații și alocați-i o adresă IP publică.

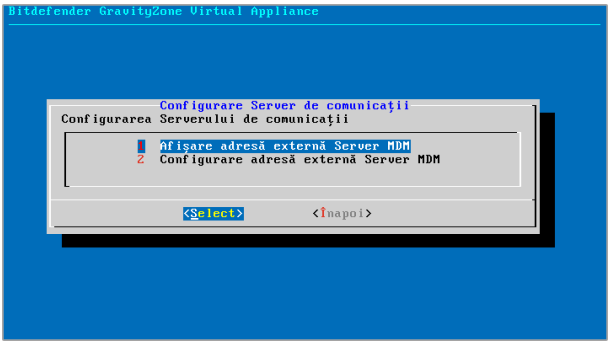
În ambele cazuri, trebuie să configurați Serverul de comunicații cu adresa externă care va fi utilizată pentru administrarea dispozitivului mobil:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).
2. Din meniul principal, selectați **Configurare Server comunicații**.



Fereastra Opțiuni aplicație

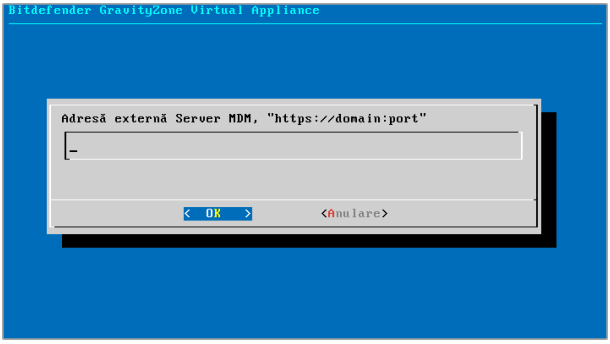
3. Selectați **Configurare adresă externă Server MDM**.



Fereastra Configurare Server de comunicații

4. Introduceți adresa externă.

   Utilizați următoarea sintaxă: `https://<IP/Domain>:<Port>`.



Fereastra de introducere a adresei externe a serverului MDM

   - Dacă utilizați opțiunea de redirecționare a portului, trebuie să introduceți adresa IP publică sau numele de domeniu și portul deschis pe portal.
   - Dacă folosiți o adresă publică pentru Serverul de comunicații, trebuie să introduceți adresa IP publică sau numele de domeniu și portul Serverului de comunicații. Portul implicit este 8443.

5. Selectați **OK** pentru a salva modificările.

5.10.2. Crearea și organizarea utilizatorilor personalizați

În situații care nu includ Active Directory, trebuie să creați mai întâi utilizatori personalizați, pentru a avea o modalitate de identificare a deținătorilor de dispozitive mobile. Utilizatorii de dispozitive mobile specificați nu sunt asociați în niciun mod cu Active Directory sau orice alți utilizatori definiți în Control Center.

Crearea utilizatorilor personalizați

Pentru crearea unui utilizator personalizat:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vizualizări.
3. În fereastra din stânga, selectați **Grupuri personalizate**.
4. Faceți clic pe pictograma **Adăugare utilizator** din bara de instrumente de acțiune. Va apărea o fereastră de configurare.
5. Specificați detaliile de utilizator necesare:
   - Un nume de utilizator sugestiv (de exemplu, numele complet al utilizatorului)
   - Adresa e-mail a utilizatorului

   Important
   - Asigurați-vă că introduceți o adresa e-mail valabilă. Utilizatorul va primi instrucțiuni de instalare prin e-mail, în momentul în care adăugați un dispozitiv.
   - Fiecare adresă e-mail poate fi asociată exclusiv unui utilizator.

6. Faceți clic pe **OK**.

Organizarea utilizatorilor personalizați

Pentru a organiza utilizatorii personalizați:

1. Creați grupuri personalizate.
   a. Selectați **Grupuri personalizate** din fereastra din stânga și dați clic pe pictograma **Adăugare** din bara de instrumente pentru acțiuni (deasupra ferestrei).
   b. Introduceți o denumire sugestivă pentru grup și faceți clic pe **OK**. Noul grup este afișat în **Grupuri personalizate**.
2. Mutați utilizatorii personalizați în grupurile personalizate corespunzătoare.

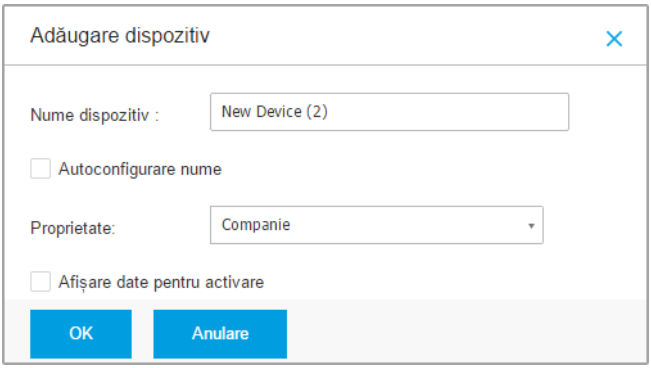
a. Selectați utilizatorii în fereastra din dreapta.

b. Trageți și inserați selecția deasupra grupului ales din fereastra din stânga.

5.10.3. Adăugarea de dispozitive utilizatorilor

Pentru a adăuga un dispozitiv unui utilizator:

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vizualizări.
3. Căutați utilizatorul din folderele din Active Directory sau din Grupurile personalizate.
4. Dați clic pe pictograma ⊕ **Adăugare dispozitiv** din partea de sus a tabelului de rețea. Va apărea o fereastră de configurare.



Adăugarea unui dispozitiv mobil la un utilizator

5. Introduceți o denumire sugestivă pentru dispozitiv.
6. Utilizați opțiunea **Configurare automată nume** dacă doriți ca numele dispozitivului să fie generat automat. Atunci când este adăugat, acest dispozitiv are o denumire generică. După ce dispozitivul a fost activat, acesta este redenumit automat cu informațiile corespunzătoare referitoare la producător și model.
7. Selectați tipul de proprietar al dispozitivului (de serviciu sau personal).
8. Selectați opțiunea **Afișare date de activare** după ce faceți clic pe butonul **OK** dacă urmează să instalați GravityZone Mobile Client pe dispozitivul utilizatorului.

9. Faceți clic pe **OK**. Utilizatorului i se transmite imediat un e-mail cu instrucțiunile de instalare și detaliile de activare care trebuie configurate pe dispozitiv. Detaliile de activare includ token-ul de activare și adresa serverului de comunicații (și codul QR corespunzător).

Notă

- Puteți vizualiza detaliile de activare ale unui dispozitiv în orice moment, făcând clic pe denumirea acestuia în Control Center.
- Puteți adăuga și dispozitive mobile unei selecții de utilizatori și grupuri. În acest caz, fereastra de configurare va permite exclusiv definirea proprietarului dispozitivului. Dispozitivele mobile create prin selecție multiplă vor fi identificate printr-o denumire generică implicită. Imediat după înregistrarea unui dispozitiv, denumirea acestuia se va modifica imediat, incluzând etichetele corespunzătoare care includ informații privind producătorul și modelul.

5.10.4. Instalați GravityZone Mobile Client pe dispozitive

Aplicația GravityZone Mobile Client este distribuită exclusiv prin Apple App Store și Google Play.

Pentru a instala GravityZone Mobile Client pe un dispozitiv:

1. Căutați aplicația pe app store-ul oficial.
   - Link Google Play
   - Link App Store Apple
2. Descărcați și instalați aplicația pe dispozitiv.
3. Demarați aplicația și efectuați configurațiile necesare:
   a. Pe dispozitivele Android, apăsați **Activare** pentru activarea GravityZone Mobile Client în calitate de administrator de dispozitiv. Citiți cu atenție informațiile furnizate.

Notă

- Sarcina de blocare pentru dispozitivele Android (7.0 sau mai recent) va pune în aplicare setul de parole din consola dumneavoastră GravityZone numai dacă pe dispozitiv nu este configurată o protecție la blocare. În caz contrar, pentru protejarea dispozitivului se vor utiliza opțiunile existente de blocare a ecranului, precum model, PIN, parolă, amprentă sau blocare inteligentă.

- Sarcina de deblocare nu mai este disponibilă pentru dispozitivele Android (7.0 sau mai recent).
- Din cauza unor limitări de ordin tehnic, sarcinile de Blocare și Ștergere nu sunt disponibile pe Android 11.

b. Introduceți token-ul de activare și adresa serverului de comunicații sau, alternativ, scanați codul QR primit prin e-mail.

c. Selectați **Sigur** când vi se solicită să acceptați certificatul serverului de comunicații. În acest fel, GravityZone Mobile Client validează serverul de comunicații și va accepta mesaje doar de la acesta, prevenind astfel atacurile de tip „man-in-the-middle".

d. Apăsați **Activare**.

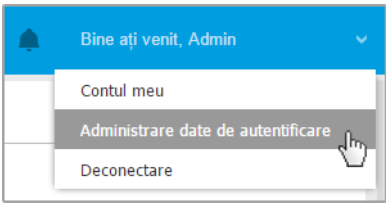
e. Pe dispozitivele iOS, vi se solicită să instalați profilul MDM. Dacă dispozitivul este protejat prin parolă, vi se va solicita să o introduceți. De asemenea, este necesar să permiteți accesul GravityZone la setările dispozitivului dumneavoastră. În caz contrar, procesul de instalare va reveni la pasul anterior. Urmați instrucțiunile de pe ecran pentru finalizarea instalării profilului.

Notă
Utilizatorii trebuie să permită accesarea locației pe dispozitive în fundal, nu doar atunci când utilizează aplicația, astfel încât caracteristica de Localizare să funcționeze corespunzător.

5.11. Manager Credențiale

Funcția Administrare date de autentificare vă ajută să definiți drepturile necesare pentru accesarea inventarelor vCenter Server existente, precum și să vă autentificați de la distanță pe diferite sisteme de operare din rețea.

Pentru a deschide fereastra Administrare date de autentificare, faceți clic pe numele de utilizator din colțul din dreapta sus al paginii și selectați **Administrare date de autentificare**.



Meniul Administrare date de autentificare

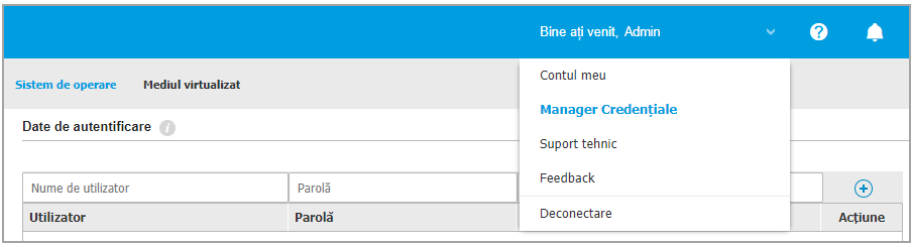
Fereastra **Administrare date de autentificare** include două secțiuni:

- Sistem de operare
- Mediul virtualizat

5.11.1. Sistem de operare

Din secțiunea **Sistem de operare**, puteți administra drepturile necesare pentru autentificarea de la distanță la executarea sarcinilor de instalare transmise calculatoarelor și mașinilor virtuale din rețea.

Pentru a adăuga un set de date de autentificare:



Manager Credențiale

1. Introduceți numele de utilizator și parola unui cont de administrator pentru fiecare sistem de operare țintă, în câmpurile corespunzătoare din partea de sus a capului de tabel. Opțional, puteți adăuga o descriere care vă va ajuta să identificați cu mai multă ușurință fiecare cont. În cazul în care calculatoarele sunt într-un domeniu, este suficient să introduceți datele de autentificare ale administratorului de domeniu.

   Folosiți convențiile Windows la introducerea denumirii contului de utilizator:

- Pentru mașinile Active Directory folosiți următoarele sintaxe: `username@domain.com` și `domain\username`. Pentru a vă asigura că datele de autentificare introduse vor funcționa, adăugați-le în ambele forme (`user@domain.comusername@domain.com` și `domain\userusername`).
- Pentru mașinile din grupul de lucru, e suficient să introduceți numai numele de utilizator, fără numele grupului de lucru.

2. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Noul set de date de autentificare este adăugat la tabel.

> **Notă**
> Dacă nu ați specificat datele de autentificare, vi se va solicita să le introduceți atunci când executați sarcinile de instalare. Datele specificate sunt salvate automat în secțiunea Administrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

5.11.2. Mediul virtualizat

Din fereastra Mediul virtual puteți administra drepturile de autentificare pentru sistemele de server virtualizat disponibile.

Pentru a accesa infrastructura virtualizată integrată cu Control Center, trebuie să introduceți datele de utilizator pentru fiecare sistem de server virtualizat. Control Center folosește datele dumneavoastră pentru a se conecta la infrastructura virtualizată, afișând doar resursele la care aveți acces (așa cum sunt acestea definite în serverul virtual).

Pentru a specifica datele de autentificare necesare pentru conectarea la un server virtual:

1. Selectați serverul din meniul corespunzător.

> **Notă**
> Dacă meniul nu este disponibil, fie nu s-a configurat încă nicio integrare, fie toate datele au fost deja configurate.

2. Introduceți numele de utilizator și parola și o descriere sugestivă.
3. Faceți clic pe butonul ⊕ **Adăugare**. Noul set de date de autentificare este adăugat la tabel.

Notă

Dacă nu configurați datele de autentificare în fereastra Administrare date de autentificare, va trebui să le introduceți când încercați să parcurgeți inventarul oricărui sistem de server virtual. După ce ați introdus datele, acestea sunt salvate în secțiunea Admnistrare date de autentificare, astfel încât nu trebuie să le reintroduceți.

Important

Ori ce câte ori modificați parola de utilizator pentru serverul virtual, nu uitați să o și actualizați în fereastra Administrare date de autentificare.

5.11.3. Ștergerea datelor din fereastra Administrare Date de Autentificare

Pentru a șterge datele de autentificare care nu mai sunt valabile din fereastra Administrare date de autentificare:

1. Îndreptați cursorul către rândul din tabel care include datele pe care doriți să le ștergeți.
2. Faceți clic pe butonul ⊗ **Ștergere** din dreapta rândului corespunzător din tabel. Contul selectat va fi șters.

6. ACTUALIZARE GRAVITYZONE

Bitdefender publică pe internet toate actualizările de produse și conținut de securitate prin intermediul serverelor Bitdefender. Toate actualizările sunt criptate și semnate digital astfel încât să nu poată fi modificate.

GravityZone include un rol de Server de actualizări, menit să servească drept punct centralizat de distribuire a actualizările pentru configurația GravityZone. Serverul de actualizări verifică și descarcă toate actualizările GravityZone disponibile din serverele de actualizare ale Bitdefender pe Internet, punându-le la dispoziție în rețeaua locală. Componentele GravityZone pot fi configurate pentru actualizarea automată de la un server de actualizări local, în locul Internetului.

Atunci când este disponibilă o nouă actualizare, aplicația GravityZone, agentul de securitate sau Security Server verifică autenticitatea semnăturii digitale a actualizării și integritatea conținutului pachetului. În continuare, fiecare fișier de actualizare este analizat și se verifică dacă versiunea sa corespunde celei instalate. Fișierele mai noi sunt descărcate local și codul lor hash MD5 este verificat pentru a se asigura că acestea nu sunt modificate.

Dacă în orice moment nu se validează o verificare, procesul de actualizare se oprește, generând o eroare. În caz contrar, actualizarea este considerată validă și gata de instalare.

Pentru a actualiza aplicațiile GravityZone instalate în mediul dumneavoastră și pachetele de instalare ale componentelor GravityZone, autentificați-vă folosind un cont de administrator de organizație și mergeți la pagina **Configurare > Actualizare**.

6.1. Actualizarea aplicațiilor GravityZone

Prin intermediul actualizărilor aplicației GravityZone, Bitdefender introduce noi caracteristici și îmbunătățiri ale caracteristicilor existente. Acestea sunt vizibile în Control Center.

Înainte de a efectua o actualizare, vă recomandăm să verificați următoarele:

- Starea de actualizare
- Orice mesaj de informare sau avertizare care ar putea apărea.
- Jurnalul de modificări

Pentru a verifica starea de actualizare:

1. Accesați pagina **Configurare > Actualizare > Roluri GravityZone**.

2. În secțiunea **Stare actuală**, citiți mesajul care indică starea generală a configurării. Dacă GravityZone necesită o actualizare, butonul **Actualizare** devine disponibil.
3. În secțiunea **Infrastructură**, verificați detaliile pentru fiecare rol GravityZone instalat în rețeaua dumneavoastră. Deoarece rolurile se actualizează independent, pentru fiecare rol puteți vedea: numele aplicației care îl găzduiește, adresa IP, versiunea actuală, cea mai recentă versiune disponibilă și starea actualizării.

Pentru a verifica jurnalul modificărilor:

1. Accesați pagina **Configurare > Actualizare > Roluri GravityZone**.
2. Accesați linkul **Vizualizare jurnal modificări**. Va apărea o fereastră pop-up cu lista tuturor versiunilor și a modificărilor incluse.

   Note privind fiecare nouă versiune de produs sunt de asemenea publicate pe Bitdefender Support Center.

Există două modalități prin care puteți actualiza GravityZone:

- Manual
- Automat

6.1.1. Actualizare manuală

Alegeți această metodă dacă doriți să aveți control deplin asupra momentului în care să se desfășoare actualizarea.

Pentru a actualiza manual GravityZone:

1. Accesați pagina **Configurare > Actualizare > Roluri GravityZone**.
2. Apăsați pe butonul **Actualizare** (dacă este disponibil).

   Actualizarea poate dura câteva minute. Așteptați finalizarea procesului.
3. Ștergeți datele din memoria cache a browser-ului.

În timpul actualizării, Control Center deconectează toți utilizatorii și îi informează cu privire la actualizarea în curs. Veți putea vizualiza progresul detaliat al procesului de actualizare.

După finalizarea actualizării, Control Center afișează pagina de autentificare.

6.1.2. Actualizarea Auto

Permițând instalarea automată a actualizărilor, vă asigurați că GravityZone este întotdeauna actualizat cu cele mai recente caracteristici și patch-uri de securitate.

Pentru GravityZone sunt disponibile două tipuri de actualizări automate:

- Actualizări produs
- Actualizările de software produs de terți

Actualizări produs

Aceste actualizări introduc noi caracteristici în GravityZone și rezolvă problemele generate de aceste caracteristici.

Deoarece actualizările pot perturba activitatea utilizatorilor GravityZone, acestea sunt proiectate să ruleze pe baza unui program. Puteți programa actualizarea astfel încât să se efectueze la ore convenabile pentru dumneavoastră. În mod implicit, actualizările automate ale produselor sunt dezactivate.

Pentru a activa și programa actualizarea produsului.

1. Accesați pagina **Configurare > Actualizare > Roluri GravityZone**.
2. Bifați opțiunea **Activează actualizările automate ale produsului GravityZone**.
3. Configurați **Recurența** pe **Zilnic**, **Săptamânal** (selectați una sau mai multe zile ale săptămânii) sau **Lunar**.
4. Definiți un **Interval**. Puteți programa o oră pentru începerea procesului de actualizare dacă este disponibilă o actualizare nouă.

GravityZone afișează în mod implicit un mesaj de avertizare pentru toți utilizatorii Control Center cu 30 de minute înainte de începerea actualizării automate. Pentru a dezactiva avertizarea, debifați caseta **Activare notificare de indisponibilitate cu 30 de minute înainte de actualizare**.

Actualizările de software produs de terți

Aplicația virtuală GravityZone integrează o serie de produse software furnizate de alți producători. Scopul acestui tip de actualizare este de a instala patch-urile pentru un astfel de software cât mai curând posibil, diminuând eventualele riscurile de securitate.

Aceste actualizări se execută în mod silențios, fără a întrerupe utilizarea Control Center.

Această opțiune este activată în mod implicit. Pentru a dezactiva această opțiune:

1. Accesați pagina **Configurare > Actualizare > Roluri GravityZone**.
2. Debifați caseta **Activează actualizările automate de securitate pentru componentele GravityZone produse de terți**.

   Patch-urile pentru software-ul produs de terți vor deveni disponibile odată cu actualizarea produsului GravityZone.

6.2. Configurarea serverului de actualizări

În mod implicit, Serverul de actualizări descarcă actualizările de pe Internet, în fiecare oră. Se recomandă să nu modificați setările implicite ale Serverului de actualizări.

Pentru a verifica și configura setările Serverului de actualizări:

1. Mergeți la pagina **Actualizare** din Control Center și faceți clic pe fila **Componente**.
2. Faceți clic pe butonul **Setări** din partea de sus a secțiunii din stânga pentru a afișa fereastra **Setări server de actualizare**.
3. În pagina **Configurare server de actualizare**, puteți verifica și configura setările principale.
   - **Adresă pachete.** Adresa de unde se descarcă pachetele.
   - **Adresă de actualizare.** Serverul de actualizare este configurat pentru `verificarea și descărcarea actualizărilor de la upgrade.bitdefender.com:80`. Aceasta este o adresă generică înlocuită automat cu adresa celui mai apropiat server din regiunea dvs. pe care sunt stocate actualizările Bitdefender.
   - **Port.** La configurarea diferitelor componente GravityZone care vor fi actualizate de pe Serverul de actualizări, trebuie să furnizați acest port. Portul implicit este 7074.
   - **IP.** Adresa IP a serverului de actualizare.
   - **Perioadă actualizare (ore).** Dacă doriți să modificați intervalul de actualizare, introduceți o altă valoare în câmpul editabil. Valoarea implicită este 1.
4. Puteți configura serverul de actualizare astfel încât acesta să descarce Security Server și kiturile pentru stațiile de lucru.

5. Serverul de actualizare poate acționa ca gateway pentru datele transmise de produsele client ale Bitdefender instalate în rețea pe serverele Bitdefender. Aceste date pot include rapoarte anonime referitoare la activitatea virușilor, rapoarte privind defectarea produselor și datele utilizate pentru înregistrarea online. Activarea rolurilor de gateway este utilă pentru controlul traficului și în rețele fără acces la Internet.

   Notă
   Puteți dezactiva modulele din produs care trimit date statistice sau rapoarte de avarie la Bitdefender Labs oricând doriți. Puteți utiliza politici pentru a controla la distanță aceste opțiuni pe calculatoarele și mașinile virtuale administrate de Control Center.

6. Faceți clic pe **Save**.

6.3. Descărcarea actualizărilor de produs

Puteți vizualiza informațiile referitoare la pachetele de componente GravityZone existente, în fila **Componente**. Datele disponibile includ versiunea curentă, versiunea actualizată (dacă exist) și starea operațiunilor de actualizare inițiate.

Pentru a actualiza o componentă GravityZone:

1. Mergeți la pagina **Actualizare** din Control Center și faceți clic pe fila **Componente**.
2. Faceți clic pe componenta pe care doriți să o actualizați din lista de **Produse**. Toate versiunile disponibile sunt afișate în tabelul **Pachete**. Bifați caseta corespunzătoare versiunii pe care doriți să o descărcați.

   Notă
   Pachetele noi vor avea starea **Nedescărcat**. Odată ce este lansată o nouă versiune de către Bitdefender, cea mai veche versiune nedescărcată va fi eliminată din tabel.

3. Faceți clic pe **Acțiuni** din partea de sus a tabelului și selectați **Publicare**. Versiunea selectată va fi descărcată și starea se va schimba în mod corespunzător. Reîmprospătați conținutul tabelului făcând clic pe butonul **Reîmprospătare** și verificați starea corespunzătoare.

Important
Aplicația GravityZone nu include pachetele Security Server în mod implciit. Trebuie să descărcați manual pachetele Security Server necesare pentru mediul dumneavoastră.

6.4. Actualizări produse offline

În mod implicit, GravityZone utilizează un sistem de actualizare conectat la internet. Pentru rețele izolate, Bitdefender oferă o alternativă, punând la dispoziție actualizări ale conținutului de securitate și componente și offline.

6.4.1. Cerințe preliminare

Pentru a utiliza actualizări offline, aveți nevoie de:

- O instanță GravityZone instalată într-o rețea cu acces la Internet („instanță online"). Instanța online trebuie să aibă:
  - Acces direct la Internet
  - Acces la porturile 80 și 443. Pentru mai multe detalii cu privire la porturile utilizate de GravityZone, consultați acest articol din Baza de cunoștințe .
  - Doar rolurile Bază de date și Server de actualizare instalate
- Una sau mai multe instanțe GravityZone instalate într-o rețea fără acces la Internet („instanțe offline")
- Ambele instanțe GravityZone trebuie să aibă aceeași versiune de aplicație

6.4.2. Configurare instanță online GravityZone

Pe parcursul acestei faze, veți instala o instanță GravityZone într-o rețea cu acces la Internet, apoi o veți configura pentru a funcționa ca un server de actualizare offline.

1. Instalați GravityZone pe o mașină cu conexiune la Internet.
2. Instalați doar rolurile Bază de date și Server de actualizare.
3. Accesați terminalul TTY al mașinii în mediul dumneavoastră virtual (sau conectați-vă la acesta prin intermediul SSH).
4. Autentificați-vă cu ajutorul numelui de utilizator `bdadmin` și al parolei pe care ați stabilit-o.

5. Rulați comanda sudo su pentru a obține privilegii **root**.
6. Executați următoarele comenzi pentru a instala pachetul offline `gzou-mirror`:

```
# apt update # gzcli update # apt install gzou-mirror
```

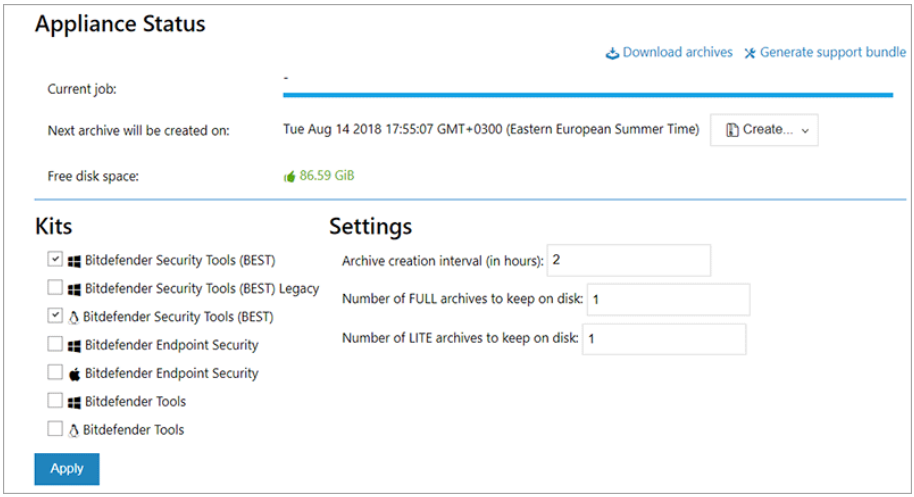
`gzou-mirror` are următoare roluri:

- Configurați Serverul de actualizare pentru a genera în mod automat arhive de actualizare offline.
- Stabiliți un serviciu web pentru instanța online, asigurând opțiuni de configurare și descărcare pentru arhivele de actualizare offline.

6.4.3. Configurarea și descărcarea fișierelor de actualizare inițiale

Pe parcursul acestei etape, veți configura setările arhivei de actualizare prin intermediul serviciului web instalat pe instanța online, apoi veți crea fișierele de arhivare necesare pentru configura instanța offline. Apoi, va trebui să descărcați fișierele de actualizare și să le plasați pe un dispozitiv media portabil (stick USB).

1. Accesați serviciul web prin intermediul unui URL cu formatul următor: `https://Online-Instance-Update-Server-IP-or-Hostname`, cu numele de utilizator `bdadmin` și parola pe care ați stabilit-o.



Instanța online – Serviciu Web

2. Configurați arhiva de actualizare offline după cum urmează:
   - Din secțiunea **Kituri**: selectați kiturile agentului de pe stația de lucru pe care doriți să le includeți în arhiva de actualizare offline.
   - Din **Setări**, editați preferințele dumneavoastră referitoare la arhiva de actualizare.

     O sarcină CRON instalată pe instanța online va verifica o dată pe minut dacă există noi fișiere de actualizare disponibile și dacă spațiul liber de pe disc este mai mare de 10 GB. La fiecare perioadă stabilită de opțiunea **Interval de creare a arhivei (în ore)**, sarcina CRON va crea următoarele fișiere:

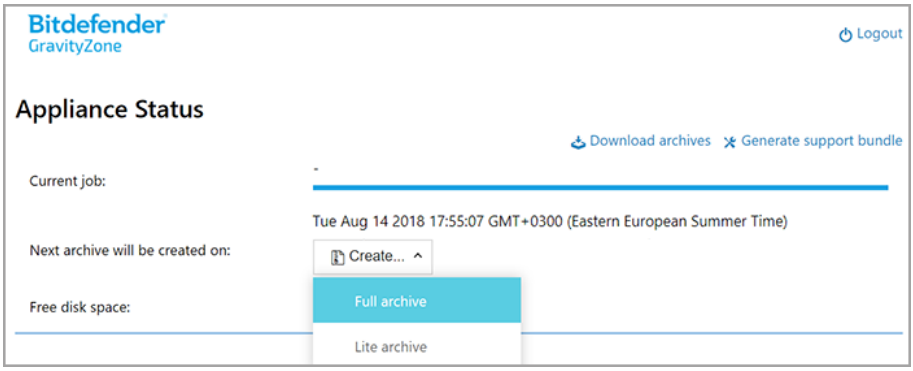
     – **Arhiva completă (produs + conținut de securitate)**, atunci când sunt disponibile noi fișiere de actualizare

     – **Arhiva în formă redusă** (doar conținutul de securitate), atunci când nu există fișiere noi de actualizare

     Arhivele vor fi create în următoarea locație:

     `https://Online-Instance-Update-Server-IP-or-Hostname/snapshots`

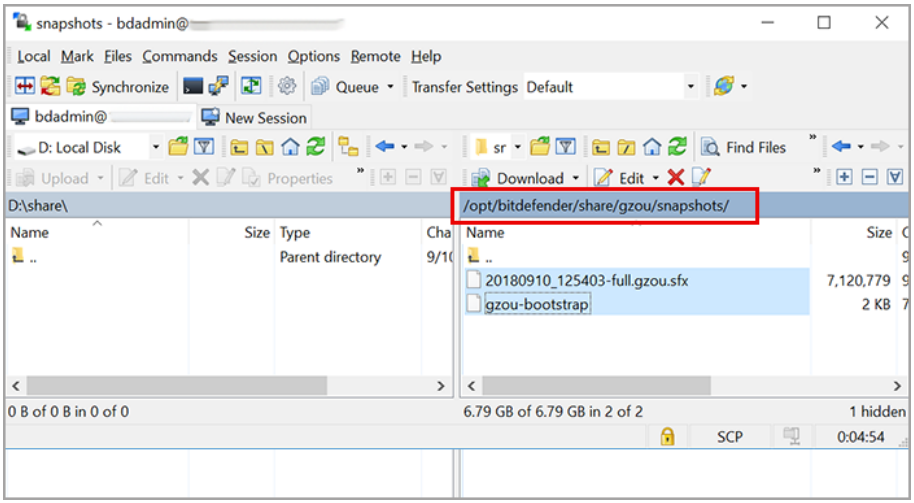
3. Selectați **Creare > Arhivă completă** pentru a crea prima arhivă completă. Așteptați până în momentul în care este creată arhiva



Instanța online – Serviciu Web: Crearea arhivei

4. Descărcați arhiva de actualizare completă și fișierul `gzou-bootstrap` din instanța online. Aveți la îndemână mai multe opțiuni:
   - Prin intermediul serviciului web: selectați **Descărcare arhive** pentru a accesa pagina care include linkurile către fișierele de actualizare. Selectați arhiva completă de actualizare și accesați linkurile către fișierul `gzou-bootstrap` pentru a le descărca pe stația dumneavoastră de lucru.
   - Utilizați clientul SCP/SCTP preferat (WinSCP, spre exemplu) pentru a stabili o sesiune SCP cu instanța online și transferați fișierele menționate mai sus în orice locație din rețeaua dumneavoastră online. Calea implicită pe instanța online este:

     `/opt/bitdefender/share/gzou/snapshots`



Transferarea fișierelor de actualizare utilizând SCP

- Prin intermediul partajării SAMBA. Utilizați o partajare SAMBA disponibilă doar în citire pentru a recupera arhivele de actualizare offline din următoarea locație:

  `\\Online-Instance-Update-Server-IP-or-Hostname\gzou-snapshots`

  Notă
  Datele de autentificare pentru a accesa partajarea SAMBA, dacă este cazul, sunt aceleași cu datele de autentificare pentru instanța online (numele de utilizator și parola `bdadmin`).

6.4.4. Configurare instanță offline GravityZone

Pe parcursul acestei etape, veți implementa și veți configura instanța offline pentru a primi actualizări prin intermediul arhivelor generate de instanța online. Cu excepția situațiilor în care se specifică în alt fel, toate comenzile trebuie rulate ca **root**.

1. Instalați GravityZone pe o mașină dintr-un mediu izolat.
2. Instalați doar rolurile Bază de date și Server de actualizare.

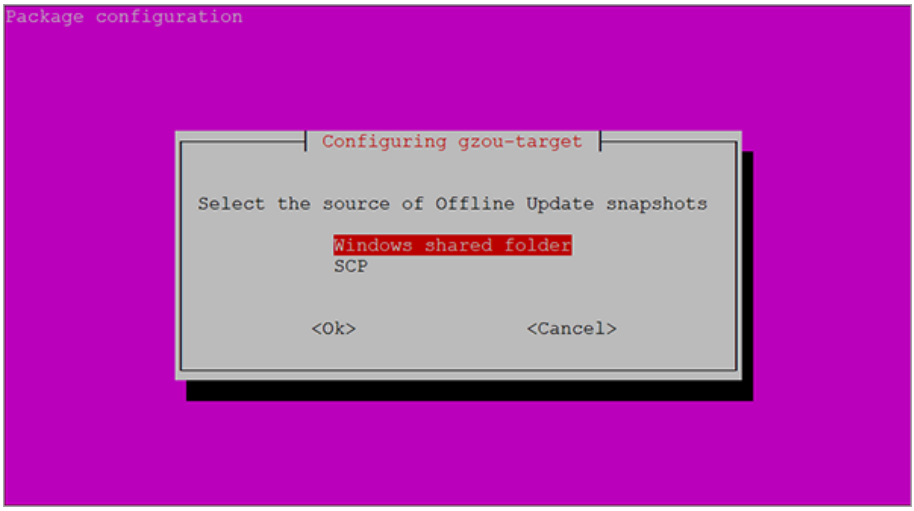
3. Transferați arhiva cu actualizări și fișierul `gzou-bootstrap` descărcat din instanța online în `/directorul home/bdadmin` al instanței offline utilizând un dispozitiv media portabil (stick USB).

   Important
   Pentru ca actualizarea offline să funcționeze, asigurați-vă că:
   - Arhiva de actualizare și `gzou-bootstrap` se află în același director.
   - Arhiva de actualizare este o **arhivă completă**.

4. Executați fișierul `gzou-bootstrap`, după cum urmează:
   a. Accesați terminalul TTY al mașinii în mediul dumneavoastră virtual (sau conectați-vă la acesta prin intermediul SSH).
   b. Transformați `gzou-bootstrap` într-un executabil:

      ```
      #
      chmod +x gzou-bootstrap
      ```

   c. Rulați: `./gzou-bootstrap`
5. Alegeți metoda de transfer al arhivelor de actualizare către instanța offline:
   - Selectați **directorul partajat Windows** (partajare Samba). În acest caz, va trebui să specificați calea către o locație partajată Windows din rețeaua izolată, la care instanța offline se va conecta în mod automat pentru a recupera arhivele de actualizare. Introduceți datele de autentificare necesare pentru a accesa locația specificată.
   - Selectați SCP dacă veți transfera manual fișierele în directorul `/opt/bitdefender/share/gzou/snapshots/` al instanței offline prin intermediul SCP.



Instanța offline GravityZone – Configurarea modului de transfer al fișierelor de actualizare

Notă
În cazul în care doriți să modificați metoda de transfer ulterior:

a. Accesați terminalul TTY al instanței offline în mediul dumneavoastră virtual (sau conectați-vă la acesta prin intermediul SSH).
b. Autentificați-vă cu ajutorul numelui de utilizator `bdadmin` și al parolei pe care ați stabilit-o.
c. Rulați comanda `sudo su` pentru a obține privilegii root.
d. Executați comanda:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Va apărea dialogul de configurare, în care puteți efectua modificările dorite.

6. Treceți la linia de comandă a consolei offline GravityZone și instalați celelalte roluri.
7. Accesați consola offline din browserul dumneavoastră web și introduceți cheie dumneavoastră de licență (în mod offline).

6.4.5. Utilizarea actualizărilor offline

După ce ați setat instanțele GravityZone, urmați etapele de mai jos pentru a actualiza instalarea offline:

1. Descărcați cea mai recentă arhivă de actualizare offline din instanța online în locația partajată preferată din rețea. Pentru mai multe detalii, vă rugăm consultați „Configurarea și descărcarea fișierelor de actualizare inițiale” (p. 190).
2. Utilizați un stick USB pentru a transfera arhiva de actualizare în partajarea Samba configurată din rețeaua izolată. Pentru mai multe detalii, vă rugăm consultați „Configurare instanță offline GravityZone” (p. 193).

   Fișierele vor fi trase în mod automat în următorul director al instanței offline:

   `/opt/bitdefender/share/gzou/snapshots/`

6.4.6. Utilizarea consolei web

Accesați consola web introducând numele gazdei/IP-ul aplicației în browserul web. Puteți edita opțiunile disponibile:

- Control Center
- Setări generale

Control Center

Stare aplicație afișează detaliile cu privire la ultimul job efectuat (tipul de arhivă, data și ora) și următorul job programat.

Aveți posibilitatea de a:

- **Crearea arhivei de conținut de securitate**
- **Crea arhiva completă**

În secțiunea **Arhive create**, puteți descărca arhivele de conținut de securitate și arhivele complete.

Selectați arhiva (arhivele) din lista disponibilă și faceți clic pe butonul **Descărcare**.

Puteți, de asemenea, vizualiza spațiul disponibil pe discul aplicației.

Setări generale

Puteți defini un program de descărcare pentru kiturile GravityZone.

1. Faceți clic pe butonul **Editare setări**.
2. Selectați unul sau mai multe kituri din lista **Kituri disponibile**.
3. În secțiunea **Programare**, puteți defini un interval pentru crearea arhivelor, precum și numărul de arhive ce urmează a fi păstrate pe unitatea de disc.
4. Faceți clic pe butonul **Aplicare** pentru a salva modificările.

7. DEZINSTALAREA PROTECȚIEI

Puteți dezinstala și reinstala componentele GravityZone în situații cum ar fi cea în cre trebuie să folosiți un cod de licență pentru o altă stație, pentru a remedia erori sau pentru a trece la versiuni superioare.

Pentru a dezinstala corect protecția Bitdefender de pe stațiile de lucru din rețeaua dumneavoastră, urmați instrucțiunile descrise în acest capitol.

- Dezinstalarea Endpoint Protection
- Dezinstalarea HVI
- Dezinstalarea Exchange Protection
- Dezinstalarea protecției pentru dispozitive mobile
- Dezinstalarea Sandbox Analyzer On-Premises
- Dezinstalarea rolurilor de server GravityZone

7.1. Dezinstalarea Endpoint Protection

Pentru a șterge în siguranță protecția Bitdefender, trebuie să dezinstalați mai întâi agenții de securitate și apoi Security Server, dacă este necesar. Dacă doriți să dezinstalați doar Security Server, conectați mai întâi agenții acestuia la un alt Security Server.

- Dezinstalarea agenților de securitate
- Dezinstalarea Security Server

7.1.1. Dezinstalarea agenților de securitate

La dezinstalarea agenților de securitate, aveți două opțiuni:

- De la distanță în Control Center
- Manual pe stația țintă

Avertisment
Agenții de securitate și serverele de securitate joacă un rol esențial în protejarea stațiilor de lucru contra oricăror tipuri de amenințări, iar dezinstalarea lor poate periclita întreaga rețea.

Dezinstalarea de la distanță

Pentru a dezinstala protecția Bitdefender de pe orice terminal administrat de la distanță:

1. Mergți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Toate calculatoarele din containerul selectat sunt afișate în tabelul din fereastra din dreapta.
4. Selectați stațiile de lucru de pe care doriți să dezinstalați agentul de securitate Bitdefender.
5. Faceți clic pe **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare client**. Este afișată o fereastră de configurare.
6. În fereastra de sarcini **Dezinstalare agent** puteți selecta dacă doriți să păstrați fișierele trecute în carantină pe stația de lucru sau să le ștergeți.

   Pentru mediile VMware integrate cu vShield, trebuie să selectați datele de autentificare necesare pentru fiecare mașină. În caz contrar, instalarea va eșua. Selectați **Utilizare date de autentificare pentru integrarea cu vShield**, apoi adăugați datele de autentificare corespunzătoare din tabelul Administrare date de autentificare afișat mai jos.
7. Faceți clic pe **Salvare** pentru a genera sarcina. Se va afișa un mesaj de confirmare.

Puteți vizualiza și administra sarcina în **Rețea > Sarcini**.

Dacă doriți să reinstalați agenții de securitate, consultați „Instalarea Endpoint Protection” (p. 123).

Dezinstalare locală

Pentru a dezinstala manual agentul de securitate Bitdefender de pe o stație Windows:

1. În funcție de sistemul de operare:
   - Pentru Windows 7, megeți la **Start > Control Panel > Uninstall a program** din categoria **Programs**.
   - Pentru Windows 8, mergeți la **Settings > Control Panel > Uninstall a program** din categoria **Program**.

- Pentru Windows 8.1, faceți clic dreapta pe butonul **Start**, apoi selectați **Control Panel > Programs & features**.
- Pentru Windows 10, mergeți la **Start > Settings > System > Apps & features**.

2. Selectați agentul Bitdefender din lista programelor.
3. Faceți clic pe **Dezinstalare**.
4. Introduceți parola Bitdefender, dacă este activată în politica de securitate. În timpul instalării, puteți vizualiza progresul sarcinii.

Pentru a dezinstala manual agentul de securitate Bitdefender de pe o mașină Linux:

1. Deschideți terminalul.
2. Obțineți acces la rădăcină folosind comenzilee `su` sau `sudo su`.
3. Navigați folosind comanda `cd` către calea următoare: `/opt/BitDefender/bin`
4. Rulați scriptul:

```
# ./remove-sve-client
```

5. Introduceți parola Bitdefender pentru a continua, dacă este activată în politica de securitate.

Pentru a dezinstala manual agentul Bitdefender de pe un Mac:

1. Mergeți la **Căutare > Aplicații**.
2. Deschideți directorul Bitdefender.
3. Faceți dublu clic pe **Dezinstalare Mac Bitdefender**.
4. În fereastra de confirmare, faceți clic pe **Verificare** și **Dezinstalare** pentru a continua.

Dacă doriți să reinstalați agenții de securitate, consultați „Instalarea Endpoint Protection” (p. 123).

7.1.2. Dezinstalarea Security Server

Puteți dezinstala Security Server în același mod în care a fost instalat, fie din Control Center, fie din interfața pe bază de meniu a aplicației virtuale GravityZone.

Pentru a dezinstala Security Server din Control Center:

1. Mergeți la pagina **Rețea**.
2. Selectați **Mașini virtuale** din selectorul de vizualizări.
3. Selectați centrul de date sau folderul care conține gazda pe care este instalat Security Server. Stațiile de lucru sunt afișate în partea dreaptă a ecranului.
4. Selectați caseta de bifare corespunzătoare gazdei pe care este instalat Security Server.
5. În meniul **Sarcini**, selectați **Dezinstalare Security Server**.
6. Introduceți datele de autentificare vShield (dacă este cazul) și faceți clic pe **Da** pentru generarea sarcinii.

Puteți vizualiza și administra sarcina în **Rețea > Sarcini**.

Dacă Security Server este instalat pe aceeași aplicație virtuală ca și celelelate roluri GravityZone, îl puteți șterge folosind interfața cu linii de comandă a aplicației. Urmați acești pași:

1. Accesați consola aplicației din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere).

   Utilizați tastele săgeți și tasta `Tab` pentru a naviga prin meniuri și opțiuni. Apăsați `Enter` pentru a selecta o anumită opțiune.
2. În meniul **Opțiuni aplicații**, mergeți la **Setări avansate**.
3. Selectați **Dezinstalare Server securitate**. Se va afișa o fereastră de confirmare.
4. Apăsați tasta `Y` sau `Enter` selectând opțiunea **Da** pentru a continua. Așteptați până când instalarea este finalizată.

7.2. Dezinstalarea HVI

Pentru a șterge HVI de pe o gazdă, este suficient să dezinstalați Pachetul suplimentar HVI. Puteți utiliza Security Server și ca server de scanare, cu condiția să aveți o cheie de licență valabilă pentru Security for Virtualized Environments.

Dacă doriți să ștergeți complet Bitdefender, este necesar să dezinstalați atât Pachetul suplimentar HVI, cât și Security Server.

Notă
Modulul HVI poate fi disponibil pentru soluția dumneavoastră GravityZone cu o cheie separată de licență.

Dezinstalarea Pachetului suplimentar HVI

Aveți două opțiuni pentru dezinstalarea Pachetului suplimentar:

- De la distanță, din Control Center, prin executarea unei sarcini de dezinstalare.
- De la distanță, din XenCenter, prin executarea câtorva comenzi pe gazda țintă.

Pentru a înlătura dezinstala HVI folosind Control Center:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Rețea** și selectați **Mașini virtuale** din selectorul de vizualizări.
3. Selectați **Server** din meniul **Vizualizări** din secțiunea din stânga.
4. Selectați una sau mai multe gazde Xen din inventarul rețelei. Puteți vizualiza cu ușurință gazdele disponibile selectând opțiunea **Tip > Gazde** din meniul **Filtre**.
5. Faceți clic pe butonul **Sarcini** din secțiunea din dreapta și selectați **Dezinstalare pachet suplimentar HVI**. Se deschide fereastra de configurare.
6. Programați momentul eliminării pachetului. Puteți opta pentru executarea sarcinii imediat după salvare sau la un anumit moment. În cazul în care dezinstalarea nu poate fi realizată la momentul specificat, sarcina se repetă automat conform setărilor de recurență. De exemplu, dacă selectați mai multe gazde și una dintre acestea nu este disponibilă atunci când pachetul este programat pentru dezinstalare, sarcina se va executa din nou la momentul specificat.
7. Gazda trebuie să fie repornită pentru finalizarea dezinstalării. Dacă doriți să reporniți gazda fără supraveghere, selectați **Repornire automată gazdă (dacă este necesar)**.
8. Faceți clic pe **Save**. Va apărea un mesaj de confirmare.

   Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

Pentru a dezinstala pachetul HVI folosind XenCenter:

1. Autentificați-vă în XenCenter.
2. Deschideți consola gazdei Xen.
3. Introduceți parola pentru gazda XenServer.
4. Executați următoarele comenzi:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-r
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # serviciux
```

Dezinstalarea Security Server

Pentru a dezinstala Security Server de pe una sau mai multe gazde:

1. Conectați-vă la Control Center.
2. Mergeți la pagina **Rețea**.
3. Selectați **Mașini virtuale** din selectorul de vizualizări.
4. Parcurgeți inventarul Citrix și bifați casetele corespunzătoare gazdelor vizate. Pentru o selectare rapidă, puteți filtra inventarul rețelei pentru a vizualiza numai Security Server.
5. Faceți clic pe butonul **Sarcini** din partea de sus a tabelului și selectați **Dezinstalare Security Server** din meniu. Va apărea un mesaj de confirmare. Faceți clic pe **Da** pentru a continua.

Puteți vizualiza și administra sarcina pe pagina **Rețea > Sarcini**.

7.3. Dezinstalarea Exchange Protection

Puteți șterge Protecția Exchange de pe orice Server Microsoft Exchange cu Bitdefender Endpoint Security Tools cu acest rol instalat. Puteți efectua dezinstalarea din Control Center.

1. Mergeți la pagina **Rețea**.
2. Selectați **Calculatoare și Mașini virtuale** din selectorul de vederi.
3. Selectați containerul dorit din fereastra din stânga. Entitățile vor fi afișate în tabelul din partea dreaptă a ecranului.
4. Selectați stația de lucru de pe care doriți să dezinstalați Protecția Exchange.
5. Faceți clic pe **Reconfigurare client** din meniul **Sarcini** din partea superioară a tabelului. Este afișată o fereastră de configurare.
6. În secțiunea **General**, debifați caseta **Exchange Protection**.

Avertisment
În fereastra de configurare, asigurați-vă că ați selectat toate celelalte roluri active pe stația de lucru. În caz contrar, acestea vor fi dezinstalate.

7. Faceți clic pe **Salvare** pentru a genera sarcina.

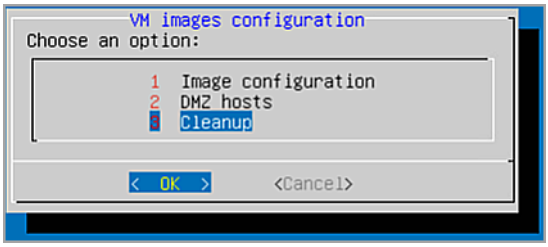
Puteți vizualiza și administra sarcina în **Rețea > Sarcini**.

Dacă doriți să reinstalați Protecția Exchange, consultați „Instalarea Exchange Protection” (p. 169).

7.4. Dezinstalarea Sandbox Analyzer On-Premises

Pentru dezinstalarea Sandbox Analyzer On-Premises:

1. Ștergeți imaginile de mașină virtuală din consola aplicației Sandbox Analyzer.
   a. Autentificați-vă în interfața aplicației Sandbox Analyzer.
      Utilizați tastele săgeți și tasta Tab pentru a naviga prin meniuri și opțiuni.
      Apăsați Enter pentru a selecta o anumită opțiune.
   b. În meniul **Configurare Sandbox**, selectați opțiunea **Imagini de mașină virtuală**.
   c. În meniul **Configurare imagini de mașină virtuală**, selectați opțiunea **Ștergere**.



Consola aplicației Sandbox Analyzer - Configurare Sandbox - Ștergere

   d. Confirmați că doriți să ștergeți imaginile de mașină virtuală instalate.
      Așteptați finalizarea acestei acțiuni. În timpul acestei acțiuni, datele asociate imaginilor de mașină virtuală vor fi și ele șterse.
2. Ștergeți Aplicația virtuală Sandbox Analyzer:
   a. Opriți aplicația virtuală Sandbox Analyzer:

b. Ștergeți aplicația din inventarul ESXi.

7.5. Dezinstalarea protecției pentru dispozitive mobile

Dacă ștergeți protecția Bitdefender de pe un dispozitiv mobil, va trebui să o ștergeți atât din Control Center, cât și de pe dispozitiv.

Atunci când ștergeți un dispozitiv din Control Center:

- Clientul mobil GravityZone nu este conectat, dar nu este șters din aparat.
- Toate jurnalele referitoare la dispozitivul șters sunt încă disponibile.
- Informațiile personale și aplicațiile dvs. nu sunt afectate.
- Pentru dispozitivele iOS, profilul MDM este șters. Dacă dispozitivul nu este conectat la internet, profilul MDM rămâne instalat până când devine disponibilă o nouă conexiune.

Avertisment

- Dispozitivele mobile șterse nu pot fi recuperate.
- Asigurați-vă că dispozitivul țintă nu este blocat înainte de a-l șterge. Dacă ștergeți din greșeală un dispozitiv blocat, este necesar să resetați dispozitivul la setările din fabrică pentru a-l debloca.

1. Mergeți la pagina **Rețea**.
2. Selectați **Dispozitive mobile** din selectorul de vizualizări.
3. Faceți clic pe **Filter** din partea de sus a ferestrei de rețea și selectați **Dispozitive** din categoria **Vizualizare**. Faceți clic pe **Save**.
4. Selectați containerul dorit din fereastra din stânga. Toate dispozitivele sunt afișate în tabelul din dreapta ferestrei.
5. Bifați caseta de selecție a dispozitivului de pe care doriți să ștergeți protecția.
6. Faceți clic pe opțiunea ⊖ **Șterge** din partea de sus a tabelului.

Apoi, trebuie să dezinstalați software-ul de pe aparat.

Pentru a dezinstala protecția Bitdefender de pe un dispozitiv Android:

1. Mergeți la **Securitate > Administratori dispozitive**.
2. Debifați caseta GravityZone. Va apărea o fereastră de confirmare.

3. Apăsați pe **Dezactivare**. Se va afișa un mesaj de avertizare prin care veți fi informat că funcțiile antifurt nu vor mai funcționa și veți pierde accesul la rețelele și datele corporative.
4. Dezinstalați Clientul mobil GravityZone la fel ca în cazul oricărei alte aplicații.

Pentru a dezinstala protecția Bitdefender de pe un dispozitiv iOS:

1. Mergeți la pictograma Client mobil Bitdefender GravityZone și apăsați-o timp de câteva secunde.
2. Apăsați pe cercul atașat după afișarea acestuia. Aplicația va fi ștearsă.

Dacă doriți să reinstalați protecția mobilă, consultați„Instalarea protecției pentru dispozitive mobile” (p. 174)

7.6. Dezinstalarea Rolurilor aplicației virtuale GravityZone

Puteți dezinstala rolurile aplicației virtuale GravityZone din interfața pe bază de meniu. Rețeaua va fi în continuare protejată, chiar dacă ștergeți una dintre ele. Cu toate acestea, aveți nevoie de cel puțin o instant a fiecărui rol pentru ca GravityZone să funcționeze corespunzător.

Într-un scenario cu o singură aplicație cu toate rolurile GravityZone, dacă ștergeți un rol, stațiile de lucru vor fi în continuare protejate, chiar dacă o parte dintre funcțiile aplicației nu vor mai fi disponibile în funcție de fiecare rol.

Într-un scenariu cu mai multe aplicații GravityZone, puteți dezinstala în siguranță unul dintre roluri atât timp cât o altă instanță a aceluiași rol este disponibilă. În mod implicit, mai multe instanțe ale rolurilor Serverului de comunicații și Consolei web pot fi instalate pe mai multe aplicații și conectate cu rolurile printr-o aplicație de echilibrare a rolurilor. Drept urmare, dacă dezinstalați o instanță a unui rol, funcția acestuia va fi preluată de unul dintre celelalte roluri.

Dacă este necesar, puteți dezinstala Serverul de comunicații de pe o aplicație alocân această funcție unei alte instanțe a acestui rol. Pentru o migrație lină, urmați pașii de mai jos:

1. În Control Center, mergeți la pagina **Politici**.
2. Selectați o politică existentă sau faceți clic pe **Adăugare** pentru a crea una nouă.
3. În secțiunea **General**, mergeți la **Comunicare**.

4. În tabelul **Alocare Comunicare Endpoint**, faceți clic pe câmpul **Nume**. Este afișată lista de servere de comunicații detectate.
5. Selectați serverul de comunicații la care doriți să se conecteze stațiile de lucru.
6. Faceți clic pe butonul ⊕ **Adăugare** din dreapta tabelului. Dacă aveți mai multe servere de comunicații în listă, le puteți configura prioritatea folosind săgețile în sus și în jos din dreapta fiecărei entități.
7. Faceți clic pe **Salvează** pentru a crea politica. Stațiile de lucru vor comunica cu Control Center prin intermediul serverului de comunicație specificat.
8. Pe interfața cu linii de comandă GravityZone, dezinstalați vechiul rol al Serverului de comunicații.

Avertisment
Dacă dezinstalați Serverul de comunicații fără a fi configurat mai întâi politica, se va pierde definitiv comunicarea și va trebui să reinstalați agenții de securitate.

Pentru a dezinstala rolurile aplicației virtuale GravityZone:

1. Accesați interfața consolei din instrumentul de administrare a virtualizării (de exemplu, Clientul vSphere). Utilizați tastele săgeți și tasta Tab pentru a naviga prin meniuri și opțiuni. Apăsați `Enter` pentru a selecta o anumită opțiune.
2. Selectați **Setări avansate**.
3. Selectați **Instalare/dezinstalare roluri**.
4. Mergeți la **Adăugare sau ștergere roluri**.
5. Folosind bara de `spaţiu`, deselectați orice rol dorit și apăsați `Enter`. Se va afișa o fereastră de confirmare a ștergerii rolului.
6. Apăsați `Enter` pentru a continua și așteptați finalizarea dezinstalării.

Dacă doriți să reinstalați un rol, consultați „Instalare/dezinstalare roluri” (p. 110).

8. OBȚINERE AJUTOR

Bitdefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic. Dacă vă confruntați cu o problemă sau dacă aveți orice întrebare cu privire la produsul Bitdefender dvs., mergeți la Centrul de asistență online. Acesta oferă mai multe resurse pe care le puteți folosi pentru a găsi rapid o soluție sau un răspuns. Sau, dacă preferați, puteți contacta echipa de Servicii clienți a Bitdefender. Reprezentanții noștri pentru suport tehnic vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

Notă
Puteți afla informații despre serviciile de suport oferite și politica noastră de suport la Centrul de asistență.

8.1. Centrul de asistență Bitdefender

Centrul de asistență Bitdefender este locul unde veți găsi tot ajutorul de care aveți nevoie pentru produsul dumneavoastră Bitdefender.

Puteți utiliza mai multe resurse pentru a găsi rapid o soluție sau un răspuns:

- Articolele din Knowledge Base
- Forum asistență Bitdefender
- Documentație de produs

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania Bitdefender.

Articolele din Knowledge Base

Bitdefender Knowledge Base este o bază online de informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea virușilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Knowledge Base este deschisă pentru public și putând fi efectuate căutări în mod liber. Prin intermediul informațiilor extinse pe care le conține, putem oferi clienților Bitdefender cunoștințele tehnice și înțelegerea de care au nevoie. Toate solicitările valide pentru informații sau rapoartele de eroare care vin din

partea clienților Bitdefender ajung la Baza de date Bitdefender sub formă de rapoarte de remediere a erorilor, notițe de evitare a erorilor, articole informaționale pentru a completa fișierele de ajutor ale produsului.

Bitdefender Knowledge Base pentru produsele business este disponibilă oricând la adresa http://www.bitdefender.ro/support/business.html.

Forum asistență Bitdefender

Forumul de suport al Bitdefender le oferă utilizatorilor Bitdefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții. Puteți posta orice probleme sau întrebări legate de produsul dumneavoastră Bitdefender.

Tehnicienii pentru suport tehnic ai Bitdefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator Bitdefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al Bitdefender este disponibil la https://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română. Faceți clic pe link-ul **Protecție Bussiness** pentru a accesa secțiunea dedicată produselor business.

Documentație de produs

Documentația de produs este sursa cea mai completă de informații despre produs.

Cea mai ușoară metodă de a accesa documentația este din pagina **Ajutor și asistență** din Control Center. Efectuați clic pe numele de utilizator din colțul din dreapta sus al consolei, selectați **Ajutor & Asistență** și apoi accesați linkul ghidului care vă interesează. Ghidul se va deschide într-un nou tab în browser.

8.2. Solicitarea de asistență profesională

Puteți solicita asistență prin intermediul Centrului nostru de asistență online. Completați formularul de contact și transmiteți-l.

8.3. Utilizarea Modulului de Suport Tehnic

Modulul de Suport Tehnic GravityZone este conceput pentru a ajuta utilizatorii și pentru a sprijini tehnicienii în obținerea cu ușurință a informațiilor necesare pentru rezolvarea problemelor. Rulați Modulului de Suport Tehnic pe calculatoarele afectate

și trimiteți arhiva rezultată cu informațiile de depanare la reprezentantul de asistență alBitdefender .

8.3.1. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Windows

Se execută Modulul de Suport Tehnic

Pentru a genera jurnalul pe calculatorul afectat, utilizați una din metodele de mai jos:

- Linia de comandă

  Pentru orice probleme cu BEST, instalat pe computer.

- Problemă la instalare

  Pentru situațiile în care BEST nu este instalat pe computer și instalarea eșuează.

Metode liniei de comandă

Utilizând linia de comandă, puteți colecta jurnalele direct de la computerul afectat. Această metodă este utilă în situațiile în care nu aveți acces la GravityZone Control Center sau în care computerul nu comunică cu consola.

1. Deschideți Command Prompt cu privilegii de administrator.
2. Mergeți la folderul de instalare al produsului. Calea implicită este:

   `C:\Program Files\Bitdefender\Endpoint Security`
3. Colectați și salvați jurnalele prin executarea acestei comenzi:

   ```
   Product.Support.Tool.exe collect
   ```

   Jurnalele sunt salvate implicit în `C:\Windows\Temp`.

   Opțional, în cazul în care doriți să salvați jurnalul instrumentului de suport într-o altă locație, utilizați calea opțională:

   ```
   Product.Support.Tool.exe collect [path="<path-to-file>"]
   ```

   Exemplu:

```
Product.Support.Tool.exe collect path="D:\Test"
```

În timpul executării comenzii, veți observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei care conține jurnalele și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support accesați `C:\Windows\Temp` sau locația personalizată și căutați fișierul de arhivă denumit `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

Problemă la instalare

1. Pentru a descărca Instrumentul de suport BEST, faceți clic aici.
2. Rulați fișierul executabil ca administrator. Va apărea o fereastră.
3. Alegeți o locație în care să salvați arhiva jurnalelor.

   Pe măsură ce jurnalele sunt colectate, vei observa o bară de progres pe ecran. Atunci când procesul s-a încheiat, este afișată denumirea arhivei și locația acesteia.

Pentru trimiterea jurnalelor către Bitdefender Enterprise Support, accesați locația selectată și căutați fișierul de arhivă `ST_[computername]_[currentdate]`. Atașați arhiva la tichetul de asistență pentru remedierea problemelor.

8.3.2. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Linux

Pentru sistemele de operare Linux, Modulul de Suport Tehnic este integrat cu agentul de securitate Bitdefender.

Pentru a colecta informațiile de sistem Linux folosind Modulul de Suport Tehnic, executați următoarea comandă:

```
# /opt/BitDefender/bin/bdconfigure
```

folosind următoarele opțiuni disponibile:

- `--help` pentru afișarea tuturor comenzilor aferente Modulului de Suport Tehnic

- `enablelogs` pentru activarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)
- `disablelogs` pentru dezactivarea jurnalelor modulului produs și de comunicare (toate serviciile vor fi repornite automat)
- `deliverall` pentru a crea:
  - O arhivă cu jurnalele produsului și ale modulului de comunicare, transmisă către directorul `/tmp` în următorul format: `bitdefender_machineName_timeStamp.tar.gz`.

  După ce arhiva a fost creată:

  1. Veți fi întrebat dacă doriți să dezactivați jurnalele. Dacă este necesar, serviciile sunt repornite automat.
  2. Veți fi întrebat dacă doriți să ștergeți jurnalele.
- `deliverall -default` transmite aceleași informații ca și opțiunea anterioară, însă se iau acțiuni implicite asupra jurnalelor, fără ca utilizatorul să fie întrebat (jurnalele sunt dezactivate și șterse).

De asemenea, puteți executa comanda `/bdconfigure` direct din pachetul BEST (kitul complet sau aplicația de descărcare) fără ca produsul să fie instalat.

Pentru a raporta o problemă GravityZone care vă afectează sistemele Linux, urmați pașii de mai jos, folosind opțiunile descrise anterior:

1. Activați jurnalele pentru produs și modulul de comunicare.
2. Încercați să reproduceți problema.
3. Dezactivați jurnalele.
4. Creați arhiva jurnalelor.
5. Deschideți un bilet de asistență prin e-mail folosind formularul disponibil pe pagina de **Suport tehnic** din Control Center, cu o descriere a problemei și jurnalele atașate.

Modulul de Suport Tehnic pentru Linux furnizează următoarele informații:

- Directoarele `etc`, `var/log`, `/var/crash` (dacă este disponibil) și `var/epag` din `/opt/BitDefender`, cu jurnalele și setările Bitdefender

- Fișierul `/var/log/BitDefender/bdinstall.log`, care conține informații referitoare la instalare
- Fișierul `network.txt`, care conține informații privind setările de rețea/ conectivitatea mașinii
- Fișierul `product.txt`, care include conținutul tuturor fișierelor `update.txt` din `/opt/BitDefender/var/lib/scan` și o listă recursivă completă a tuturor fișierelor din `/opt/BitDefender`
- Fișierul `system.txt`, care conține informații generale despre sistem (versiune distribuție și kernel, memorie RAM disponibilă și spațiul liber pe hard-disk)
- Fișierul `users.txt`, care conține informații referitoare la utilizator
- Alte informații privind produsul asociat sistemului, cum ar fi conexiunile externe ale proceselor și utilizarea CPU
- Jurnale de sistem

8.3.3. Utilizarea Modulului de Suport Tehnic pe sistemele de operare Mac

La trimiterea unei solicitări către echipa de suport tehnic a Bitdefender, este necesar să furnizați următoarele:

- O descriere detaliată a problemei întâmpinate.
- O captură de ecran (dacă este cazul) care să includă exact mesajul de eroare afișat.
- Jurnalul Modulului de Suport Tehnic.

Pentru a colecta informații despre sistemul Mac folosind Modulul de Suport Tehnic:

1. Descărcați arhiva ZIP conținând Modulul de Suport Tehnic.
2. Extrageți fișierul **BDProfiler.tool** din arhivă.
3. Deschideți o fereastră Terminal.
4. Navigați la locația fișierului **BDProfiler.tool**.

   De exemplu:

```
cd /Users/Bitdefender/Desktop;
```

5. Adăugați drepturi de executare pentru fișierul:

```
chmod +x BDProfiler.tool;
```

6. Executați modulul.

   De exemplu:

```
/Users/Bitdefender/Desktop/BDProfiler.tool;
```

7. Apăsați D și introduceți parola atunci când vi se solicită să furnizați parola de administrator.

   Așteptați câteva minute până când modulul finalizează generarea jurnalului. Veți găsi fișierul de arhivă rezultat (**Bitdefenderprofile_output.zip**) pe desktop.

8.4. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 18 ani Bitdefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

8.4.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Centrul de asistență:http://www.bitdefender.ro/support/business.html
Documentație: gravityzone-docs@bitdefender.com
Distribuitori locali:http://www.bitdefender.ro/partners
Programe de Parteneriat: partners@bitdefender.com
Relații Media: pr@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Website: http://www.bitdefender.com

8.4.2. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.ro/partners.
2. Mergeți la **Localizare partener**.
3. Datele de contact ale distribuitorilor locali Bitdefender ar trebui să se afișeze automat. În caz contrar, selectați țara de reședință pentru a accesa aceste informații.
4. În cazul în care nu găsiți un distribuitor Bitdefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa enterprisesales@bitdefender.com.

8.4.3. Filialele Bitdefender

Reprezentanțele Bitdefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Statele Unite ale Americii

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
United States
Telefon (vânzări&suport tehnic): 1-954-776-6262
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrul de asistență: http://www.bitdefender.com/support/business.html

Franța

Bitdefender
49, Rue de la Vanne
92120 Montrouge
Fax: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
E-mail: b2b@bitdefender.fr

Site-ul web: http://www.bitdefender.fr
Centrul de asistență: http://www.bitdefender.fr/support/business.html

Spania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Fax: (+34) 93 217 91 28
Telefon (birou&vânzări): (+34) 93 218 96 15
Telefon (suport tehnic): (+34) 93 502 69 10
Vânzări: comercial@bitdefender.es
Site-ul web: http://www.bitdefender.es
Centrul de asistență: http://www.bitdefender.es/support/business.html

Germania

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (birou&vânzări): +49 (0) 2304 94 51 60
Telefon (suport tehnic): +49 (0) 2304 99 93 004
Vânzări: firmenkunden@bitdefender.de
Site-ul web: http://www.bitdefender.de
Centrul de asistență: http://www.bitdefender.de/support/business.html

Marea Britanie și Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (vânzări&suport tehnic): (+44) 203 695 3415
E-mail: info@bitdefender.co.uk
Vânzări: sales@bitdefender.co.uk
Site-ul web: http://www.bitdefender.co.uk
Centrul de asistență: http://www.bitdefender.co.uk/support/business.html

România

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Fax: +40 21 2641799
Telefon (vânzări&suport tehnic): +40 21 2063470
Vânzări: sales@bitdefender.ro
Site-ul web: http://www.bitdefender.ro
Centrul de asistență: http://www.bitdefender.ro/support/business.html

Emiratele Arabe Unite

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (vânzări&suport tehnic): 00971-4-4588935 / 00971-4-4589186
Fax: 00971-4-44565047
Vânzări: sales@bitdefender.com
Web: http://www.bitdefender.com
Centrul de asistență: http://www.bitdefender.com/support/business.html

A. Anexe

A.1. Tipuri de fișiere acceptate

Motoarele de scanare antimalware incluse în soluțiile de securitate Bitdefender pot scana toate tipurile de fișiere care ar putea conține amenințări. Lista de mai jos cuprinde cele mai des întâlnite tipuri de fișiere care sunt analizate.

{*; 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. Obiecte Sandbox Analyzer

A.2.1. Tipuri și extensii de fișiere acceptate pentru trimitere manuală

Următoarele extensii de fișiere sunt acceptate și pot fi detonate manual în Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, fișiere MZ/PE (executabile), PDF, PEF (executabile), PIF (executabile), RTF, SCR, URL (binar), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer poate detecta tipurile de fișiere menționate mai sus și dacă sunt incluse în arhive de următoarele tipuri: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, Arhivă comprimată LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolum), ZOO, XZ.

A.2.2. Tipurile de fișiere acceptate de modulul de filtrare preliminară a conținutului la trimiterea automată

Filtrarea preliminară a conținutului va stabili un anumit tip de fișier prin intermediul unei combinații care include conținutul și extensia obiectului. Acest lucru înseamnă că un fișier executabil cu extensia `.tmp` va fi recunoscut ca fiind o aplicație și, dacă este depistat ca fiind suspect, va fi trimis către Sandbox Analyzer.

- Aplicații - fișiere care au formatul PE32, inclusiv, dar fără a se limita la următoarele extensii: exe, dll, com.
- Documente - fișiere cu format de document, inclusiv, dar fără a se limita la următoarele extensii: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm, dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf.

- Script-uri: `ps`, `wsf`, `ws`, `php`, `py`, `js`, `vb`, `vbs`, `pyc`, `pyo`, `wsc`, `wsh`, `psc1`, `jse`, `vbe`.
- Arhive: `zip`, `jar`, `7z`, `bz`, `bz2`, `tgz` , `msi`, `rar`, `rev`, `z`, `arj`, `iso`, `lha`, `lhz`, `uu`, `uue`, `xxe`, `lzma`, `ace`, `r00`.
- E-mail-uri (memorate în sistemul de fișiere): `eml`, `tnef`.

A.2.3. Excluderi implicite la trimiterea automată

`asc`, `avi`, `bmp`, `gif`, `jpeg`, `jpg`, `mkv`, `mp4`, `pgp`, `png`, `txt`.

A.2.4. Aplicații recomandate pentru mașinile virtuale de detonare

Sandbox Analyzer On-Premises solicită ca anumite aplicații să fie instalate pe mașinile virtuale de detonare, astfel încât acestea să deschidă mostrele trimise.

Aplicații	Tipuri de fișiere
Suita Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Windows implicit	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 WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml

A.3. Kerneluri compatibile cu senzorul de incidente

Senzorul de incidente este compatibil cu următoarele kerneluri: