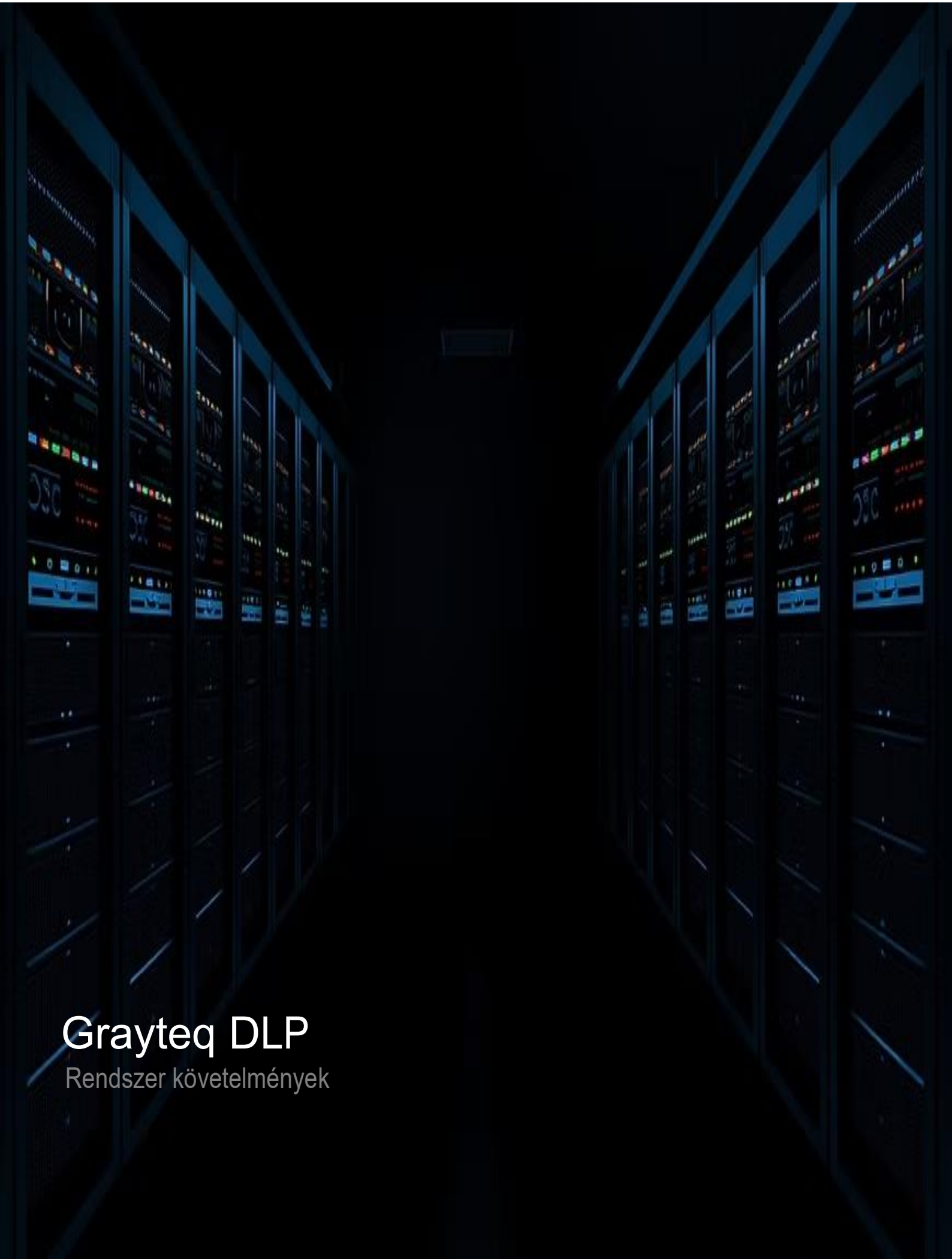


Grayteq DLP

Rendszer követelmények

Alapvetés

1. A Grayteq DLP rendszer egyaránt támogatja a 64-bites Windows desktop operációs rendszereket, Windows 11 Professionaltől, illetve a szerver operációs rendszereket Windows Server 2019-től felfelé.

Feltételek

2. A felkészüléshez szükséges a rendszerbe bevont munkaállomások listája és a rájuk telepített alkalmazások teljes listája, kompatibilitási vizsgálatokhoz.
3. Amennyiben a Grayteq DLP rendszer által védendő számítógépek száma meghaladja az 1000 darabot, az alábbiakban nevesített Grayteq Architecture Server (ARC) és Grayteq Reporting Server (REP) komponensek is használandók. 1000 védendő számítógép alatt csak a Grayteq Security Server (SEC) és a Grayteq Data Security Client komponensek szükségesek, Grayteq Reporting Server (REP) használata opcionális, de ajánlott.
4. A rendszer kialakításához, valamint a bevezetési időszak alatt létrehozandó dokumentációk elkészítéséhez, illetve a rendszer felügyeletéhez állandóan rendelkezésre álló VPN kapcsolatra van szükség, mely használata esetén esetlegesen RDP kapcsolatra is szükség lehet a Grayteq Architecture Server (ARC)-t, Grayteq Reporting Server (REP)-t és Grayteq Security Server (SEC)-eket futtató számítógépre.
5. A Grayteq rendszer jelentés-készítési funkcióinak (Reporting features) használatához (Report, Auto Report, File Audit, Media Audit) minimálisan szükséges feltételek:
   5.1. Grayteq Enterprise licensz vásárlása a Grayteq Security (SEC) és a Grayteq Reporting (REP) szerverekhez;

6. A Grayteq Server-ek futtatásához szükséges domain felhasználó jogai:
   6.1. Teljes elérési jog a system könyvtárakhoz és azok tartalmához a rendszerbe bevont munkaállomásokon (például a telepítendő számítógépeken a helyi Rendszergazdák csoportba felvéve a kijelölt domain felhasználót)
   6.2. Távoli Service indítási jogosultság a rendszerbe bevont munkaállomásokon
   6.3. Ugyanazon domainben kell lennie, mint a rendszerbe bevont munkaállomások.
7. Távoli telepítő alkalmazás, mely segítségével kiadhatóak az egyes telepítési csomagok a rendszerbe bevont számítógépekre. Ezen távoli telepítő (általában SCCM) kiváltható a Grayteq Architecture Server (ARC) / Grayteq Security Server (SEC) felületéről indított telepítéssel is, melyhez a szükséges jogosultságok lentebb olvashatóak.
8. Logon script-ek használhatósága, melyek a felhasználók bejelentkezésekor automatikusan beállítják a számítógépen futó Grayteq DLP Client kapcsolódási helyét. Ezen alkalmazás a Grayteq által készített kiegészítő-alkalmazás.
9. Távoli rendszer bevezetés, illetve támogatás során valamennyi Grayteq Server alkalmazást futtató számítógéphez a végfelhasználó által biztosított VPN elérés vagy bármely fizetett vagy ingyenes távoli elérést biztosító alkalmazás (javasoltan az ingyenes AnyDesk) segítségével távoli hozzáférés biztosítása szükséges, mely bejelentkezés session alapú és nem biztosít felügyelet nélküli bejelentkezési lehetőséget az adott számítógépre.
10. A Grayteq rendszer elemeinek háborítatlan működése biztosítása érdekében a használatban lévő Antivirus megoldásban szükséges a Grayteq szoftverek saját könyvtárainak engedélyezett/fehér listához történő hozzáadása szükséges. Ezen könyvtárlista a Grayteq Security Solutions gyártója által a bevezetés során kerül átadásra.
11. Amennyiben Symantec Endpoint Protection bármely verziója használatban van, a SEP felületén az alábbi beállítások szükségesek:
    11.1. A „General Exploit Mitigation” funkció kikapcsolt állapotban kell álljon.
    11.2. A "Enable early launch anti-malware" funkció kikapcsolt állapotban kell álljon.
12. Követelmények a kliensek Grayteq Security Orchestrator (SO) felületéről történő telepítéséhez:
    12.1. Admin share-ek megléte szükséges: IPC$, ADMIN$, valamint az operációs rendszert tartalmazó meghajtó adminisztrációs megosztása (általában: C$).

Bevezetési követelmények

13. A bevezetés első lépésének megvalósításához szükséges egy olyan, a bevezetés idejére rendelkezésre bocsátott, a szervezetben általánosan használt számítógépekkel megegyező, de legalább a Grayteq DLP Client Agent futtatásához minimálisan szükséges technikai paraméterekkel bíró asztali számítógép / laptop biztosítása, melyen a bevezetés során a bevezetést végző Grayteq szakember az egyes beállításokat és a rendszer kliens oldali általános működését ellenőrizheti.
14. Az előző pontban nevesített számítógépen a bevezetést végző Grayteq szakember számára az alábbi jogosultságok biztosítása szükséges:
    14.1. Domainbe felvett saját felhasználó, az általánosan a szervezetben használt felhasználói jogosultságok biztosításával. Több domain, illetve több Grayteq Security Server (SEC) használata esetén a domain fogalom ezen esetben azon domain-t jelenti, amelyben az adott Grayteq Security Server (SEC) található, melyhez az adott kliens számítógép csatlakozni kíván.
    14.2. Több Grayteq Security Servert (SEC) használó rendszer esetén a bevezetés során az egyes Grayteq alrendszerek (az egyes Grayteq Security Serverekhez (SEC) csatlakozó gépcsoportok) kialakítása során a Grayteq szakértő domain-es felhasználója valamennyi olyan domain-be felvételre kell kerüljön, amelyben Grayteq Security Server (SEC) is fel van véve.
    14.3. A bevezetés idejére helyi rendszergazdai jogosultág az adott számítógépre.
    14.4. A rendszer sikeres átadását követően – a bevezetést végző szakember írásos jelzése alapján – a helyi rendszergazdai jogai visszavonásra kerülhetnek, a szervezetben nem-helyi rendszergazdai jogosultságot birtokló felhasználókkal egyenértékű jogosultságok megtartása mellett.

Szerver oldali követelmények

15. A bevezetés második és harmadik lépésének megvalósításához (a rendszerbe bevont kliensek és szerverek mennyiségének teljessé tételéhez) úgy célszerű számolni, hogy az alábbiakban leírt Grayteq Architecture Server (ARC)-ból és Grayteq Reporting Server (REP)-ből 1-1 db, míg Grayteq Security Server (SEC)-ből nagyságrendileg minden 2000 db, a rendszerbe bevont kliens vagy szerver után 1 szerver állítandó rendszerbe. Ez egyrészről a rendszer menedzselhetőségét és átláthatóságát, a megfelelő elkülönülést, a szerverrel szemben támasztott technikai követelmények, valamint performanciális elvárások érdekében szükséges.
16. A Grayteq Architecture Server (ARC), Grayteq Reporting Server (REP) és Grayteq Security Server (SEC) virtuális környezetben (ESX, Oracle Virtual Box, VMware, Hyper-V, stb.) történő futtatása esetén a felhasznált virtuális futtató környezetnek (Host Server) különálló szervernek kell lennie, azon más szolgáltatást futtató Guest operációs rendszerek ne legyenek használatban a Grayteq Architecture Server (ARC), Grayteq Reporting Server (REP) és Grayteq Security Server (SEC)-t futtató Guest operációs rendszeren kívül.
17. Természetesen a leírt biztonsági szerver követelmények úgy fizikai, mint virtuális szerverre egyaránt érthetők és alkalmazhatók.
18. A Grayteq Architecture Server (ARC), Grayteq Reporting Server (REP), Grayteq Security Server (SEC) a beállításai alapján periodikusan automatikus életjel üzenetet küld emailben a beállított üzemeltetői email címekre, valamint a heartbeat@grayteq.com email címre.
19. A küldő email cím előre definiáltan a grayteq@cégesdomain. Ezen email címhez a bevezetés során szükséges Microsoft Exchange email fiókot létrehozni, valamint ezen fiók üzenet küldését a heartbeat@grayteq.com email címre engedélyezni. Ezen küldő email cím lehet de-perszonalizált.

Tűzfal oldali követelmények

20. Tűzfal használata esetén engedélyezni kell a „Microsoft File and Printer Sharing”-et.

21. KÖTELEZŐEN NYITANDÓ PORTOK:

21.1. Grayteq Server-Client log kommunikáció: **TCP/3999, mindkét irányba**

21.2. Grayteq Server-Client parancs kommunikáció: **TCP/15000, mindkét irányba**

21.3. Grayteq Server-Server kommunikáció: **TCP/3999 és TCP/39999, mindkét irányba**

21.4. Grayteq Server-Security Orchestrator kommunikáció: **TCP/37999, mindkét irányba**

21.5. Távoli telepítés Microsoft File Sharing protokollon keresztül: **UDP/139, TCP/135, UDP/445, a Grayteq Security Serverek (SEC) felől a Grayteq Security Client-eket futtató számítógépek irányába**

22. OPCIONÁLISAN NYITANDÓ PORTOK:

22.1. DNS name service requests to default DNS server port: **UDP/53**

22.2. Workgroups, Active Directory access: **UDP/445**

22.3. Microsoft SQL log átvitel SQL szerverbe: **TCP/1433**

22.4. PostgreSQL log átvitel SQL szerverbe: **TCP/1395**

22.5. Oracle log átvitel Oracle szerverbe: **TCP/4321**

22.6. SYSLOG log átvitel SYSLOG szerverbe: **UDP/514**

22.7. RDP protokoll engedélyezése a Grayteq Security Orchestrator-t futtató számítógépeken.

Hardver előfeltételek

Grayteq Security Orchestrator (SO)

Komponens	Minimum követelmény
Operációs rendszer	Windows 11 Pro vagy Enterprise Windows Server 2019-től felfelé valamennyi verzió
Hardver	Intel® Core™ i5-6200U vagy azzal egyenértékű CPU 8 GB RAM 20 GB szabad SSD Gigabit TCP/IP alapú hálózati kártya
Egyéb	Minimum .NET Framework 4.8 Internet kapcsolat a licencek aktiválásához

Grayteq Data Security Client

Komponens	Minimum követelmény
Operációs rendszer	Windows 11 Pro vagy Enterprise Windows Server 2019-től felfelé valamennyi verzió – (Grayteq DLP Server Client szükséges) **FONTOS: A Windows 10 operációs rendszer - a Microsoft End-of-Life policy-ével harmóniában - 2025. október 14-től a Grayteq rendszerek által hivatalosan nem támogatott, így bár a Grayteq komponensek működnek Windows 10 Pro, illetve Enterprise operációs rendszeren, esetleges védelmi funkcionális veszteségek tapasztalhatók lehetnek, melyek a további Grayteq verziókban (26.0.0 felett) Windows 10 futtató környezethez nem kerülnek javításra.**
Hardver	Intel® Core™ i5-6200U vagy azzal egyenértékű CPU

Komponens	Minimum követelmény
	12GB RAM – (16GB ajánlott) 20GB HDD (helyi naplózás esetére) Gigabit TCP/IP alapú hálózati kártya
Egyéb	Minimum .NET Framework 4.8

Grayteq Architecture Server (ARC), Grayteq Reporting Server (REP), Grayteq Security Server (SEC)

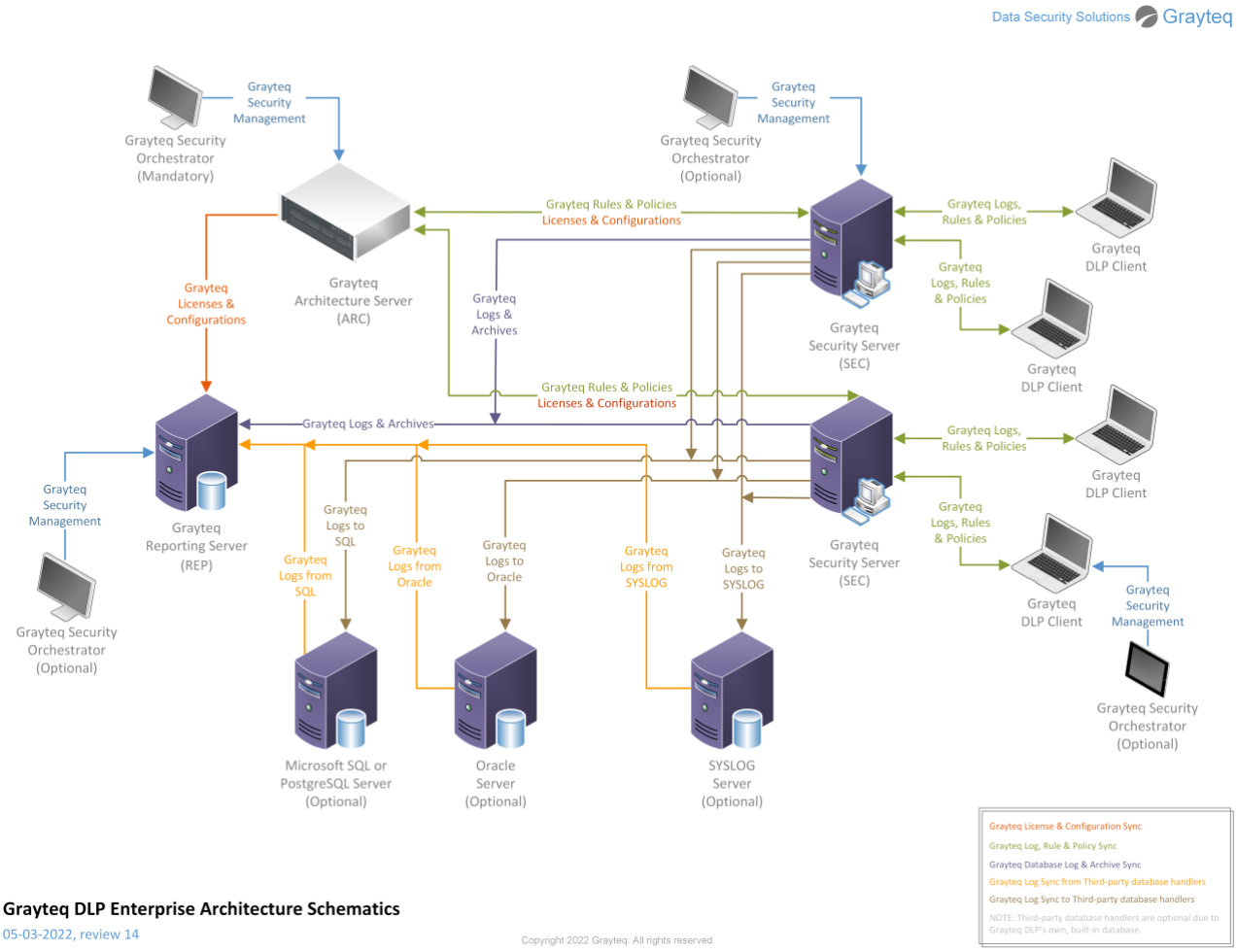
Komponens	Minimum követelmény
Operációs rendszer	Windows Server 2019-től felfelé valamennyi verzió
Hardver - Security Serverenként **<u>Fontos:</u> Az egy Security Serverre maximálisan csatlakoztatható kliens számítógépek száma: 2000db** **A 2000db-nál nagyobb mennyiségű kliens számítógépet használó rendszerek esetén több Security Server használata szükséges.**	500db csatlakoztatott kliens számítógépig: - Intel® Core™ Xeon CPU, 4 mag - 16GB RAM 500-1000db csatlakoztatott kliens számítógép között: - Intel® Core™ Xeon CPU, 8 mag - 24 GB RAM 1000-2000db csatlakoztatott kliens számítógép között: - Intel® Core™ Xeon CPU, 16 mag - 32 GB RAM 500 GB SSD (rendszer partíciótól elkülönítve) NTFS fájlrendszer Gigabit TCP/IP alapú hálózati kártya
Adatbázis	A Grayteq DLP saját adatbázist használ alap kiépítésben,

Komponens	Minimum követelmény
	mely átállítható 3rd-party adatbázis használatára. FONTOS: A Microsoft SQL redundáns tárolás miatt a naplóadatok tárolásához szükséges tárterület nagyságrendekkel növekszik. Pl. Míg a Grayteq DLP saját adatbázisában 2.5 millió logsor hozzávetőlegesen 350 MB tárterületet igényel, addig ugyanezen mennyiségű naplóadat MS SQL-ben történő tárolása nagyságrendileg 8 GB tárterületet igényel. **Támogatott adatbázisok:** Microsoft SQL Server 2019-től felfelé valamennyi verzió PostgreSQL Server (unicode és ANSI módban) Oracle 19 és felette
Egyéb	Statikus IP cím használata szükséges, melyhez a DNS beállításokban FQDN név létrehozása szükséges.

Adatbázis követelmények

24. A Grayteq DLP rendszer alap kiépítésben nem igényel semmilyen harmadik féltől származó adatbázist lévén saját, beépített adatbázissal rendelkezik. A saját adatbázisán kívül különböző, harmadik féltől származó adatbázisokat is támogat.
25. Támogatott adatbázisok:
    25.1. Microsoft SQL Server 2019-től valamennyi verzió
    25.2. PostgreSQL Server (unicode és ANSI módban)
    25.3. Oracle 19c és felette
26. Harmadik féltől származó adatbázis használata esetén, a Grayteq Reporting Server-be küldendő archív állományokból készítendő jelentések elkészítéséhez valamennyi, az adott Grayteq Reporting Server-hez csatlakozó Grayteq Security Server-nek azonos típusú külső adatbázist kell használnia. Ez lehet bármely, harmadik-féltől származó, a Grayteq DLP rendszer által támogatott verziójú adatbázis (Microsoft SQL, PostgreSQL, Oracle vagy SYSLOG).

Grayteq DLP Enterprise Architektúra



Grayteq DLP Enterprise Architecture Schematics

05-03-2022, review 14

Grayteq

Disztribútoraink és viszonteladóink elérhetőségeiért kérjük, lépjen kapcsolatba velünk!

Az Ön Grayteq partnere:

Kapcsolat:
info@grayteq.com

Támogatás:
support@grayteq.com