

IBM

@server

iSeries

Védett socket réteg (SSL)

V5R3





@server

iSeries

Védett socket réteg (SSL)

V5R3

Megjegyzés

Mielőtt a jelen leírást és a vonatkozó terméket használná, feltétlenül olvassa el a “Megjegyzések” oldalszám: 19 helyen lévő tájékoztatót.

Ötödik kiadás (2005. augusztus)

Ez a kiadás az Operating System/400 (5722-SS1) V5R3M0 kiadására, illetve minden ezt követő változatra és módosításra vonatkozik mindaddig, amíg az újabb kiadások ezt másképp nem jelzik. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren illetve a CISC modelleken.

© Szerzői jog IBM Corporation 2002, 2005. Minden jog fenntartva

Tartalom

Védett socket réteg (SSL)	1
A V5R3 kiadás újdonságai.	1
A témakör nyomtatása	1
Példahelyzetek	2
Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével	2
Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével	5
Alapelvek	13
Az SSL története	13
Az SSL működése	13
Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok	13

Szerver hitelesítés	15
Kliens hitelesítés	15
SSL támogatás megteremtésének tervezése	15
Alkalmazások biztonságossá tétele SSL segítségével	16
SSL hibaelhárítás	16
Kapcsolódó információk	17

Megjegyzések.	19
Védjegyek	20
A kiadványok letöltésére és kinyomtatására vonatkozó feltételek	20

Védett socket réteg (SSL)

A Védett socket réteg (SSL) a nem védett hálózatok, például az Internet felett védett kommunikációt biztosító ipari szabvány biztonsági protokoll. Az SSL protokollról és az iSeries szerver alkalmazásairól további információkat az alábbi hivatkozások kiválasztásával kaphat:

- **A V5R3 kiadás újdonságai**
Itt található az SSL protokollal új vagy újonnan elérhetővé vált funkciók felsorolása.
- **SSL példahelyzetek**
Ez az új témakör néhány lehetséges példán keresztül mutatja be az SSL protokoll felhasználási lehetőségeit az iSeries szerveren.
- **SSL alapelvek**
Kiegészítő információk a Védett socket réteg (SSL) protokollok alapjairól.
- **SSL támogatás megteremtésének tervezése**
Ez a témakör adja meg az SSL bevezetésének előfeltételeit az iSeries szerveren, és ír le néhány hasznos tippet ezzel kapcsolatban.
- **Alkalmazások biztonságossá tétele SSL segítségével**
Itt található az iSeries szerver SSL segítségével biztonságossá tehető alkalmazásainak listája.
- **SSL hibaelhárítás**
Alapszintű útmutatásokat biztosít az SSL hibaelhárításhoz az iSeries szerveren.
- **SSL-hez kapcsolódó információk**
Hivatkozások a további információforrásokra.

A V5R3 kiadás újdonságai



A jelenlegi kiadásban a Védett socket réteg (SSL) kapcsán két új elem érdemel mindenképpen említést:

1. **Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével**
Ez az új példahelyzet írja körül, hogyan használható az SSL a távoli kliensek és egy helyi hálózat (LAN) központi rendszereként működő iSeries szerveren futó Kezelőközpont szerver közötti kapcsolat biztonságossá tételére.
2. **A GSKit API-k GSKit 6B változata**
A V5R3 kiadással kezdődően a GSKit alkalmazásprogram illesztők (API) a GSKit 6B változatán alapulnak. A korábbi kiadás alapját a 4D változat jelentette. A GSKit alkalmazásprogram illesztőkről itt talál további információkat.

A kiadás további újdonságairól és változásairól a Felhasználói feljegyzés  című cikkben olvashat.

Új vagy megváltozott információk elkülönítése

A technikai változások helyét az Információs központ az alábbiak szerint jelöli:

-  Kép jelöli az új vagy megváltozott információk kezdetének helyét.
-  Kép jelöli az új vagy megváltozott információk végét.

A témakör nyomtatása

A dokumentum PDF változata letölthető megjelenítési vagy nyomtatási céllal. Ehhez kattintson a Védett socket réteg (SSL) hivatkozásra (megközelítőleg 243 KB).

További információk


Megtekintheti vagy kinyomtathatja a témakörhöz kapcsolódó információkat is.

PDF fájlok mentése:

A PDF mentése a munkaállomásra megjelenítés vagy nyomtatás céljából:

1. A böngészőben kattintson a jobb egérgombbal a PDF hivatkozásra.
2. Válassza az előugró menü **Cél mentése másként...** menüpontját.
3. Válassza ki azt a könyvtárat, ahová a PDF fájlt menteni kívánja.
4. Kattintson a **Mentés** gombra.

Az Adobe Acrobat Reader letöltése

A PDF fájlok megjelenítéséhez és nyomtatásához szükség van az Adobe Acrobat Reader programra, amely letölthető az Adobe webhelyéről (www.adobe.com/products/acrobat/readstep.html). 

Példahelyzetek

Az alábbi példahelyzetek kialakítása úgy történt, hogy segítségükkel és ezek alapján maximálisan kihasználhassa az iSeries szerver SSL támogatása által biztosított előnyöket.

- **Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével**
Ez a példahelyzet azt írja le, hogyan használható az SSL egy távoli kliens és egy iSeries navigátor Kezelőközpont szerver futtatásával központi rendszerként működő iSeries szerver közötti kapcsolat biztonságossá tételére.
- **Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével**
Ez a példahelyzet azt írja le, hogyan oldható meg egy iSeries navigátor Kezelőközpont szerver futtatásával központi rendszerként működő iSeries szerver **összes** kapcsolatának biztonságossá tétele.
- **Példahelyzet: Biztonságos FTP**
Ez a példahelyzet írja le az SSL engedélyezését az FTP alkalmazásban.
- **Példahelyzet: Biztonságos Telnet**
Ez a példahelyzet írja le az SSL engedélyezését a Telnet alkalmazásban.
- **Példahelyzet: Az iSeries SSL teljesítményének növelése**
Ez a példahelyzet bemutatja, hogyan növelhető az SSL teljesítmény az iSeries szervereken kriptográfiai hardverek segítségével hívásával.
- **Példahelyzet: Magánkulcsok védelme kriptográfiai hardverrel**
Ez a példahelyzet mutatja be, hogyan alkalmazhatók a kriptográfiai hardverek az iSeries szerveren az SSL tranzakciókhoz használt magánkulcsok védelmére.

Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével



Alaphelyzet:

Egy vállalat helyi hálózatán (LAN) számos iSeries szerver található. A vállalati rendszeradminisztrátor az iSeries szerverek egyikét kijelölte a hálózat központi rendszerének (a továbbiakban A rendszer). Az adminisztrátor az A rendszeren futó Kezelőközpont szerverrel kezeli a LAN többi csomópontját.

Az adminisztrátor óvakodik az A rendszeren futó Kezelőközpont szerverre csatlakozástól a vállalat saját hálózatán kívülről. Mivel munkája sok utazással jár, jogos igényként merül fel benne egy biztonságos kapcsolat kialakítása a Kezelőközpont szerverrel, amíg úton van. Biztosítani szeretné, hogy a számítógépe és a Kezelőközpont szerver közötti kapcsolat biztonságos, amikor kívül van a vállalati irodán. Úgy dönt, hogy SSL kapcsolatot alakít ki a saját számítógépe és az A rendszer Kezelőközpont szervere között. Az SSL illetően engedélyezésével biztos lehet abban, hogy a Kezelőközpont szerverrel kialakított kapcsolata utazás közben is biztonságos.

Célok:

Az adminisztrátor biztonságossá szeretné tenni a számítógépe és a Kezelőközpont szerver közötti kapcsolatot. Az A rendszeren futó Kezelőközpont szerver és a helyi hálózat többi végpont rendszere között kialakított kapcsolatok nem igényelnek kiegészítő biztonságot. A többi alkalmazott a vállalati irodában dolgozik, így nekik szintén nincs szükségük biztonságos Kezelőközpont szerver kapcsolatra. Az adminisztrátor úgy tervezi beállítani a számítógépe és az A rendszeren futó Kezelőközpont szerver közötti kapcsolatot, hogy kliense szerver hitelesítést alkalmazzon. A hálózaton található többi számítógép és iSeries szerver Kezelőközpont kapcsolatát nem szükséges az SSL protokollal védeni.

Részletek:

Az alábbi táblázat mutatja be a felhasznált hitelesítési típusokat a PC kliens SSL támogatásának engedélyezésén és tiltásán alapulva:

1. táblázat: Kliens és Kezelőközpont szerver közötti SSL kapcsolat kialakításához szükséges elemek

SSL állapota az adminisztrátor számítógépén	Az A rendszer Kezelőközpont szerveréhez megadott hitelesítési szint	SSL kapcsolat
SSL kikapcsolva	Bármelyik	Nincs
SSL bekapcsolva	Bármelyik	Igen (szerver hitelesítés)

A **szerver hitelesítés** azt jelenti, hogy az adminisztrátor számítógépe hitelesíti a Kezelőközpont szerver igazolását. A Kezelőközpont szerverhez csatlakozáskor a számítógép SSL kliensként működik. A Kezelőközpont szerver SSL szervertként működik, így neki bizonyítani kell azonosságát. A Kezelőközpont szerver ezt egy olyan igazolási hatóságtól származó igazolás bemutatásával éri el, amelyben az adminisztrátor számítógépe megbízik.

Előfeltételek és feltételezések:

A számítógép és a Kezelőközpont szerver közötti kapcsolat biztonságossá tételéhez az alábbi adminisztrációs és beállítási lépések elvégzése szükséges:

- Az A rendszernek meg kell felelnie az SSL előfeltételeknek (lásd az SSL előfeltételek című témakört).
- Az A rendszerre az OS/400 V5R3 (vagy újabb) kiadása van telepítve. Ha az A rendszer az OS/400 V5R1 kiadását futtatja, akkor az alábbi OS/400 (5722-SS1) javítások (PTF) telepítése szükséges:
 - SI01375
 - SI01376
 - SI01377
 - SI01378
 - SI01838
- Az iSeries navigátor PC kliens az iSeries Access for Windows V5R3 vagy újabb változatát futtatja.
- Be kell állítani egy Igazolási hatóságot az iSeries szerverek számára.
- Létre kell hozni egy igazolási hatóság által aláírt igazolást az A rendszer számára.
- Az igazolási hatóság és a szerver igazolását el kell juttatni az A rendszerre, ott importálni kell azokat a kulcsadatbázisba.
- Az igazolást hozzá kell rendelni a Kezelőközpont szerver azonosításához.
 - Az A rendszeren Indítsa el az IBM Digitális igazolás kezelőt. Ezen a ponton kell beszerezni vagy létrehozni az igazolásokat, vagy beállítani az igazolások rendszerét. Az igazolási rendszer beállításáról további információkat a Digitális igazolás kezelő használata című cikkben talál.
 - Kattintson az **Igazolástároló kiválasztása** hivatkozásra.
 - Válassza ki a ***SYSTEM** igazolástárolót, majd kattintson a **Folytatás** gombra.
 - Adja meg a ***SYSTEM Igazolástároló jelszavát**, majd kattintson a **Folytatás** gombra. A menü újratöltése után bontsa ki az **Alkalmazások kezelése** kategóriát.
 - Kattintson az **Igazolás hozzárendelés frissítése** hivatkozásra.
 - Válassza ki a **Szerver** típust, majd kattintson a **Folytatás** gombra.

- g. Válassza ki a **Kezelőközpont szerver** bejegyzést, majd kattintson az **Igazolás hozzáférések frissítése** gombra. Itt rendelheti hozzá a Kezelőközpont szerverhez az igazolást, amely alapján az iSeries Access for Windows kliensek azonosíthatják azt.
 - h. Kattintson az **Új igazolás hozzáférése** elemre. A Digitális igazolás kezelő újratölti az **Igazolás hozzáférések frissítése** oldalt, és megjelenik egy megerősítést kérő üzenet.
 - i. Kattintson a **Kész** gombra.
8. Be kell állítani az iSeries navigátort:
- a. A szelektív telepítő segítségével telepítse az iSeries navigátor SSL összetevőjét a számítógépen.
 - b. Töltse le az igazolási hatóság igazolását a PC kliensre.

Konfigurációs lépések:

A PC kliens és az A rendszeren futó Kezelőközpont szerver kapcsolatának SSL védelméhez az alábbi lépéseket kell elvégezni:

1. lépés: SSL kikapcsolása az iSeries navigátor kliensben
2. lépés: A hitelesítési szint beállítása a Kezelőközpont szerveren
3. lépés: A Kezelőközpont szerver újraindítása az A rendszeren
4. lépés: SSL aktiválása az iSeries navigátor kliensben
5. Kihagyható lépés: SSL kikapcsolása az iSeries navigátor kliensben

A részletes beállítási lépések megtekintéséhez folytassa a Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével témakörnél.

Beállítás részletei: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével

Az alábbi szakasz feltételezi, hogy már végigolvasta a Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével című témakört. A példahelyzetben egy iSeries szerver van kijelölve egy vállalat helyi hálózatának központi rendszereként. Az adminisztrátor az A rendszernek nevezett központi rendszeren futó Kezelőközpont szerver segítségével kezeli a vállalati hálózat végpontjait. A most következő szakasz írja le egy külső kliens és a Kezelőközpont szerver kapcsolatának biztosításához szükséges lépéseket. A leírt példahelyzet megvalósításához kövesse a megadott lépéseket.

Mielőtt a Kezelőközpont szerveren engedélyezni lehetne az SSL támogatást, telepíteni kell az előfeltétel programokat és be kell állítani a digitális igazolásokat az iSeries szerveren. Mielőtt folytatná, nézze meg a példahelyzetre vonatkozó előfeltételeket és feltételezéseket. Az előfeltételek teljesülésekor a Kezelőközpont szerver SSL támogatásának beállítása az alábbi eljárással történik.

1. lépés: SSL kikapcsolása az iSeries navigátor kliensben

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Kattintson a jobb egérgombbal az A rendszerre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kattintson az **SSL** lapra, majd szüntesse meg a **Védett socket réteg (SSL) kapcsolat használata** beállítás kiválasztását.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

Az iSeries navigátorban eltűnik a lakat a Kezelőközpont tárolóból, így jelezve a nem biztonságos kapcsolatot. Ez jelzi, hogy a kliens és a vállalat központi rendszere közötti kapcsolat nem áll az SSL védelme alatt.

2. lépés: A hitelesítési szint beállítása a Kezelőközpont szerveren

1. Az iSeries navigátorban kattintson a jobb egérgombbal a **Kezelőközpont** nézetre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. Kattintson a **Biztonság** lapra, majd válassza ki a **Védett socket réteg (SSL) használata** beállítást.
3. Válassza ki a **Bármely** hitelesítési szintet. (A beállítás az iSeries Access for Windows V5R3 és újabb kiadásában választható.)

4. Kattintson az **OK** gombra az érték beállításához a központi rendszeren.

3. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Az **A rendszeren** bontsa ki a **Hálózat -> szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
3. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját. A központi rendszer nézet összeesik, és egy üzenet tudatja, hogy nem rendelkezik csatlakozással a szerverhez.
4. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

4. lépés: SSL bekapcsolása az iSeries navigátor kliensben

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Kattintson a jobb egérgombbal az **A rendszerre**, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kattintson az **SSL** lapra, majd válassza ki a **Védett socket réteg (SSL) kapcsolat használata** beállítást.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

Az iSeries navigátorban a Kezelőközpont szerver mellett megjelenik egy lakat, amely a biztonságos kapcsolatot jelzi. Ez jelzi, hogy a kliens és a vállalat központi rendszere közötti kapcsolat biztonságos.

Megjegyzés: Az eljárás csak egy PC és a Kezelőközpont szerver közötti kapcsolatot biztosítja. A Kezelőközpont szerverhez csatlakozó más kliensek kapcsolatai, illetve a végpont rendszerek és a Kezelőközpont szerver között kialakított kapcsolatok nem lesznek biztonságosak. További kliensek biztonságossá tételéhez győződjön meg róla, hogy megfelelnek az előfeltételeknek, majd ismétlje meg a 4. lépést. A Kezelőközpont szerver további kapcsolatainak biztonságossá tételével kapcsolatban olvassa el a Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével című témakört.

Kihagyható lépés: SSL kikapcsolása az iSeries navigátor kliensben

Ha az adminisztrátor a vállalati irodából fog dolgozni, vagyis nem kívánja a számítógépének teljesítményét csökkentő SSL biztonságot, akkor könnyen kikapcsolhatja azt az alábbi lépésekkel:

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kattintson az **SSL** lapra, majd szüntesse meg a **Védett socket réteg (SSL) kapcsolat használata** beállítás kiválasztását.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

Az iSeries navigátorban eltűnik a lakat a Kezelőközpont szerverről, így jelezve a nem biztonságos kapcsolatot. Ez jelzi, hogy a PC kliens és a Kezelőközpont szerver közötti kapcsolat nem áll az SSL védelme alatt.

További SSL példahelyzetekre mutató hivatkozásokat a Példahelyzetek című témakörben talál.

Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével

Alaphelyzet:

Egy vállalat befejezte egy több iSeries szerverből (végpont rendszerek) álló nagy kiterjedésű hálózat (WAN) kialakítását. A szerverek központi kezelése a vállalat központjában található központi iSeries szerverről történik. A példahelyzet a vállalat biztonsági szakértőjéről szól, aki a Védett socket réteg (SSL) használatával biztosítani kívánja a Kezelőközpont szerver és a vállalati hálózat végpont rendszerei és kliensei közötti összes kapcsolatot.

Részletek:

A Kezelőközpont szerver összes kapcsolatán engedélyezhető az SSL **biztonság**. Ahhoz, hogy az SSL használható legyen a Kezelőközponttal, biztosítani kell a központi rendszer elérésére használt iSeries Access for Windows illetve iSeries navigátor programokat a számítógépen.

Ehhez kétféle hitelesítési szint közül lehet választani:

Szerver hitelesítés

Ez a végpont rendszer igazolásának hitelesítését biztosítja. A központi rendszer SSL kliensként működik a végpont rendszerhez csatlakozáskor. A végpont rendszer SSL szerverként tevékenykedik, amihez igazolnia kell az azonosságát a központi rendszer által megbízhatónak tekintett igazolási hatóság által kibocsátott igazolás bemutatásával. Minden végpont rendszernek rendelkeznie kell egy megbízható igazolási hatóság által kiadott igazolással.

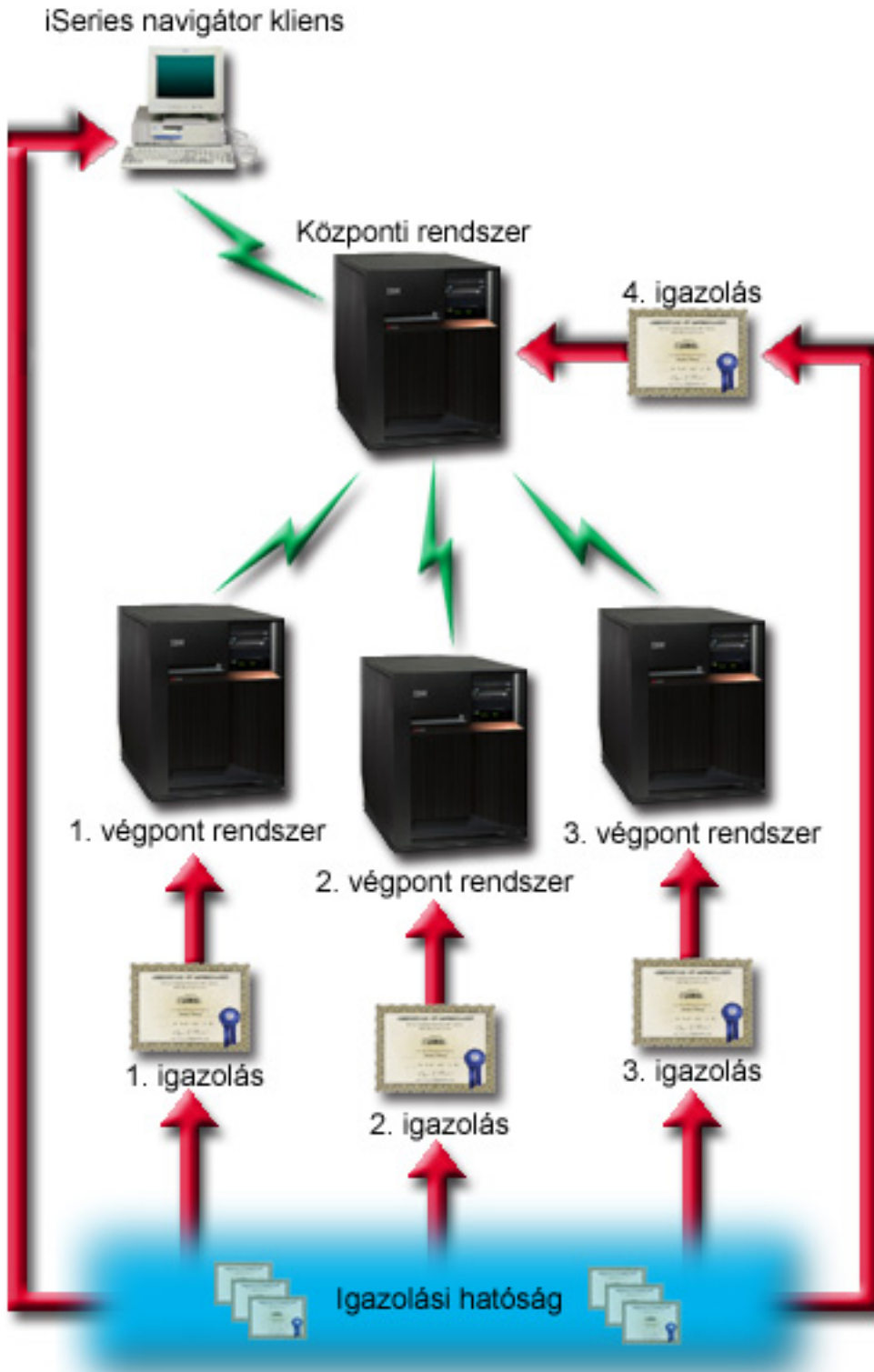
Kliens és szerver hitelesítés

Ez a módszer a központi rendszer és a végpont rendszer igazolását is hitelesíti. Ez magasabb biztonsági szintet jelent a szerver hitelesítéshez képest. Más alkalmazások ezt kliens hitelesítésként emlegetik, amikor a kliensnek kell bemutatnia egy megbízható igazolást. Amikor a központi rendszer (SSL kliens) kapcsolatot kezdeményez egy végpont rendszerrel (SSL szerver), akkor a központi rendszer és a végpont rendszer is hitelesíti a másik fél igazolását.

Más alkalmazásoktól eltérően a Kezelőközpont emellett ellenőrzési lista (más néven Megbízható csoport ellenőrzési lista) alapján is végezhet hitelesítést. Az ellenőrzési lista általában felhasználó azonosítási és hitelesítési információkat, például jelszavakat, személyi azonosítószámokat vagy digitális igazolásokat tartalmaz. A hitelesítési információk tárolás természetesen titkosított.

A legtöbb alkalmazás általában nem hangsúlyozza a szerver és kliens hitelesítés együttes alkalmazásának szükségességét, mivel a szerver hitelesítésre majdnem minden esetben sor kerül az SSL szekció kialakítása során. Az alkalmazások többsége kliens hitelesítéshez szükséges konfigurációs beállításokkal rendelkezik. A Kezelőközpont a kliens hitelesítés helyett a "szerver és kliens" hitelesítés kifejezés használatával a központi szervernek a hálózatban betöltött kettős szerepére utal. Amikor egy személyi számítógép csatlakozik az SSL támogatással rendelkező központi rendszerhez, akkor ez utóbbi szerverként működik. Amikor azonban a központi rendszer a végpont rendszerekhez csatlakozik, akkor már kliensként működik. A központi rendszer szerver és kliens működését az alábbi ábra szemlélteti.

Megjegyzés: Az illusztráción látható Igazolási hatóság igazolását tárolni kell a központi rendszer és minden végpont rendszer kulcsadatbázisában.



Előfeltételek és feltételezések:

A Kezelőközpont szerver összes kapcsolatának biztosításához az alábbi adminisztrációs és konfigurációs feladatokat (lásd az ábrát: SSL által védett Kezelőközpont nagy kiterjedésű hálózaton (WAN)) kell elvégezni:

1. A központi rendszernek meg kell felelnie az SSL előfeltételeknek (lásd az SSL előfeltételek című témakört).
2. A központi rendszernek és az összes végpont iSeries szervernek az OS/400 V5R2 vagy újabb kiadását kell futtatnia. Ha a központi rendszer és a végpontok az OS/400 V5R1 kiadását futtatják, akkor az alábbi OS/400 (5722-SS1) javítások (PTF) telepítése szükséges:
 - a. SI01375
 - b. SI01376
 - c. SI01377
 - d. SI01378
 - e. SI01838
3. Az iSeries navigátor PC kliens az iSeries Access for Windows V5R2 vagy újabb változatát futtatja. Ha a kliens a V5R1 változatot használja, akkor telepíteni kell az iSeries Access for Windows (5722-XE1) V5R1 kiadásának SI01907 jelű (vagy újabb) javítócsomagját.
4. Be kell állítani egy Igazolási hatóságot az iSeries szerverek számára.
5. Az SSL kapcsolattal rendelkező Kezelőközponttal kezelt valamennyi iSeries szerverhez létre kell hozni egy igazolást, amit alá kell írni az igazolási hatósággal.
6. Az igazolási hatóság igazolását, valamint a megfelelő igazolást el kell juttatni minden iSeries szerverre, ahol importálni kell azokat a kulcsadatbázisba.
7. Az igazolásokat hozzá kell rendelni a Kezelőközpont alkalmazásazonosítójához, illetve az iSeries navigátor által használt valamennyi végpont szerver alkalmazásazonosítójához:
 - a. Indítsa el az IBM Digitális igazolás kezelőt a központi szerveren. Ha az igazolások még nincsenek létrehozva vagy nem kerültek beszerzésre, illetve ha az igazolási rendszer beállításra szorul, akkor erre most kell sort keríteni. Az igazolási rendszer beállításával kapcsolatban nézze meg a Digitális igazolás kezelő használata témakört.
 - b. Kattintson az **Igazolástároló kiválasztása** hivatkozásra.
 - c. Válassza ki a ***SYSTEM igazolástárolót**, majd kattintson a **Folytatás** gombra.
 - d. Adja meg a ***SYSTEM Igazolástároló jelszavát**, majd kattintson a **Folytatás** gombra. A menü újratöltése után bontsa ki az **Alkalmazások kezelése** kategóriát.
 - e. Kattintson az **Igazolás hozzárendelés frissítése** hivatkozásra.
 - f. Válassza ki a **Szerver** típust, majd kattintson a **Folytatás** gombra.
 - g. Válassza ki a **Kezelőközpont szerver** bejegyzést, majd kattintson az **Igazolás hozzárendelés frissítése** gombra. Itt rendelheti hozzá a Kezelőközpont szerverhez az igazolást.
 - h. Kattintson az **Új igazolás hozzárendelése** elemre. A Digitális igazolás kezelő újratölti az **Igazolás hozzárendelés frissítése** oldalt, és megjelenik egy megerősítést kérő üzenet.
 - i. Kattintson a **Kész** gombra.
 - j. Ismétlje meg az eljárást az iSeries navigátor által használt valamennyi végpont szerveren.
8. Be kell állítani az iSeries navigátort:
 - a. A szelektív telepítő segítségével telepítse az iSeries navigátor SSL összetevőjét a számítógépen.
 - b. Töltse le az igazolási hatóság igazolását a PC kliensre.

Konfigurációs lépések:

Mielőtt a Kezelőközpont szerveren engedélyezni lehetne az SSL támogatást, telepíteni kell az előfeltétel programokat és be kell állítani a digitális igazolásokat a központi rendszeren. Mielőtt folytatná, nézze meg a példahelyzetre vonatkozó előfeltételeket és feltételezéseket. Az előfeltételek teljesülése esetén a Kezelőközpont szerver összes kapcsolatának biztosítása az alábbi eljárással történik:

Megjegyzés: Ha az SSL engedélyezett az iSeries navigátorban, akkor ezt először le kell tiltani a Kezelőközpont szerver SSL támogatásának engedélyezéséhez. Ha az SSL engedélyezett az iSeries navigátorban, de a Kezelőközpont szerveren nem, akkor az iSeries navigátornak a központi rendszerre való csatlakozási kísérletei megghiúsulnak.

- 1. lépés: Központi rendszer beállítása szerver hitelesítésre
- 2. lépés: Végpont rendszerek beállítása szerver hitelesítésre
- 3. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren
- 4. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren
- 5. lépés: SSL aktiválása az iSeries navigátor kliensben
- 6. lépés: Központi rendszer beállítása kliens hitelesítésre
- 7. lépés: Végpont rendszerek beállítása kliens hitelesítésre
- 8. lépés: Ellenőrzési lista másolása a végpont rendszerekre
- 9. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren
- 10. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren

A részletes beállítási lépések megtekintéséhez nézze meg a Beállítás részletei: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével című témakört.

Beállítás részletei: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével

Az alábbi szakasz feltételezi, hogy már végigolvasta a Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével című témakört. A most következő szakasz írja le a Kezelőközpont szerver összes kapcsolatának biztonságossá tételéhez szükséges lépéseket. A leírt példahelyzet megvalósításához kövesse a megadott lépéseket.

Mielőtt a Kezelőközpont szerveren engedélyezni lehetne az SSL támogatást, telepíteni kell az előfeltétel programokat és be kell állítani a digitális igazolásokat az iSeries szerveren. Mielőtt folytatná, nézze meg a példahelyzetre vonatkozó előfeltételeket és feltételezéseket. Az előfeltételek teljesülése esetén a Kezelőközpont szerver összes kapcsolatának biztosítása az alábbi eljárással történik.

Megjegyzés: Ha az SSL engedélyezett az iSeries navigátorban, akkor ezt először le kell tiltani a Kezelőközpont szerver SSL támogatásának engedélyezéséhez. Ha az SSL engedélyezett az iSeries navigátorban, de a Kezelőközpont szerveren nem, akkor az iSeries navigátornak a központi rendszerre való csatlakozási kísérletei meghiúsulnak.

1. lépés: Központi rendszer beállítása szerver hitelesítésre

Az SSL lehetővé teszi a központi rendszer és a végpont rendszerek, illetve az iSeries navigátor kliens és a központi rendszer közötti adatforgalom titkosítását. Az SSL szállítási, igazolás hitelesítési és adattitkosítási szolgáltatásokat biztosít. SSL kapcsolat csak olyan végpontok között építhető ki, amelyek mindegyike támogatja az SSL használatát. A szerver hitelesítés beállítását a kliens hitelesítés beállítása előtt el kell végezni.

1. Az iSeries navigátorban kattintson a jobb egérgombbal a **Kezelőközpont** nézetre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. Kattintson a **Biztonság** lapra, majd válassza ki a **Védett socket réteg (SSL) használata** beállítást.
3. Válassza ki a **Szerver** hitelesítési szintet.
4. Kattintson az **OK** gombra az érték beállításához a központi rendszeren.

Megjegyzés: A Kezelőközpont szervert **NE** indítsa újra, amíg a végpont rendszereken nem állította be a szerver hitelesítést.

5. Állítsa be a végpont rendszereket szerver hitelesítésre.

2. lépés: Végpont rendszerek beállítása szerver hitelesítésre

A központi rendszer szerver hitelesítésének beállítása után a végpont rendszereket is be kell állítani a szerver hitelesítésre. Ez a következő feladatokból áll:

1. Bontsa ki a **Kezelőközpont** nézetet.
2. Hasonlítsa össze és frissítse a végpont rendszerek rendszerváltozóit:

- a. A **Végpont rendszerek** mappában kattintson a jobb egérgombbal a központi rendszerre, majd válassza az előugró menü **Tároló → Adatgyűjtés** menüpontját.
- b. Az Adatgyűjtés párbeszédablakban válassza ki a **Rendszerváltozók** adatgyűjtését a központi rendszer rendszerváltozóira vonatkozó értékek összegyűjtéséhez. A többi beállítás kiválasztását szüntesse meg.
- c. Kattintson a jobb egérgombbal a **Rendszercsoportok** mappára, majd válassza az előugró menü **Új rendszercsoport** menüpontját.
- d. Határozzon meg egy új rendszercsoportot, amely az összes olyan végpont rendszert tartalmazza, amelyen engedélyezni kívánja az SSL-t.
- e. Az új csoport megjelenítéséhez bontsa ki a rendszercsoportok listáját.
- f. Az adatgyűjtés befejezése után kattintson a jobb egérgombbal a rendszercsoportra, majd válassza az előugró menü **Rendszerváltozók → Összehasonlítás és frissítés** menüpontját.
- g. Ellenőrizze, hogy a **Modellrendszer** mezőben a központi rendszer látható-e.
- h. Jelölje ki a **Kezelőközpont** kategóriát, és ellenőrizze a következő értékeket a mellettük található jelölőnégyzet kiválasztásával:
 - A **Védett socket réteg használata** beállításnál válassza az **Igen** értéket.
 - Válassza ki a **Szerver SSL** hitelesítési szintet.

A központi rendszer ezen értékeinek beállítása a Központi rendszer beállítása szerver hitelesítésre eljárásban történt meg.
- i. Kattintson az **OK** gombra az értékek beállításához a rendszercsoport végpont rendszerein.
- j. A Kezelőközpont szerver újraindításával várja meg az **Összehasonlítás és frissítés** folyamat befejeződését. Ez néhány percig tarthat.

3. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Bontsa ki a központi rendszert.
3. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
4. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját. A központi rendszer nézet összeesik, és egy üzenet tudatja, hogy nem rendelkezik csatlakozással a szerverhez.
5. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

4. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren

1. Bontsa ki az újraindításban érintett végpont rendszert.
2. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
3. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját.
4. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.
5. Ismétlje meg az eljárást minden végpont rendszerénél.

5. lépés: SSL bekapcsolása az iSeries navigátor kliensben

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Kattintson a jobb egérgombbal a központi rendszerre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
3. Kattintson az **SSL** lapra, majd válassza ki a **Védett socket réteg (SSL) kapcsolat használata** beállítást.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

6. lépés: Központi rendszer beállítása kliens hitelesítésre

A szerver hitelesítéssel kapcsolatos beállítások befejeződtek. Most már sor kerülhet a nem kötelező kliens hitelesítés beállítására. A kliens hitelesítés a végpont rendszereket és a központi rendszert is ellenőrzi az igazolási hatóság és a megbízható csoport alapján. Amikor a központi rendszer (SSL kliens) SSL kapcsolatot próbál létesíteni egy végpont

rendszerrel (SSL szerver), akkor a központi rendszer és a végpont rendszer is hitelesíti a másik fél igazolását. Ezt a folyamatot más néven igazolási hatóság és megbízható csoport hitelesítésnek is nevezzük.

Megjegyzés: A kliens hitelesítés beállítása nem kezdhető meg addig, amíg a szerver hitelesítés nincs beállítva.

1. Az iSeries navigátorban kattintson a jobb egérgombbal a **Kezelőközpont** nézetre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. Kattintson a **Biztonság** lapra, majd válassza ki a **Védett socket réteg (SSL) használata** beállítást.
3. Válassza ki a **Kliens és szerver** hitelesítési szintet.
4. Kattintson az **OK** gombra az érték beállításához a központi rendszeren.

Megjegyzés: A Kezelőközpont szervert **NE** indítsa újra, amíg az összes végpont rendszeren be nem állította a kliens és szerver hitelesítést.

5. Állítsa be a végpont rendszereket kliens hitelesítésre.

7. lépés: Végpont rendszerek beállítása kliens hitelesítésre

1. Hasonlítsa össze és frissítse a végpont rendszerek rendszerváltozóit:

Megjegyzés: Ez a feladat nem működik az OS/400 V4R5 kiadását futtató iSeries végpont szervereken.

- a. A **Végpont rendszerek** mappában kattintson a jobb egérgombbal a központi rendszerre, majd válassza az előugró menü **Tároló → Adatgyűjtés** menüpontját.
- b. Az Adatgyűjtés párbeszédablakban válassza ki a **Rendszerváltozók** adatgyűjtését a központi rendszer rendszerváltozóira vonatkozó értékek összegyűjtéséhez. A többi beállítás kiválasztását szüntesse meg.
- c. Kattintson a jobb egérgombbal a **Rendszercsoportok** mappára, majd válassza az előugró menü **Új rendszercsoport** menüpontját.
- d. Határozzon meg egy új rendszercsoportot, amely az összes olyan végpont rendszert tartalmazza, amelyen engedélyezni kívánja az SSL-t.
- e. Az új csoport megjelenítéséhez bontsa ki a rendszercsoportok listáját.
- f. Az adatgyűjtés befejezése után kattintson a jobb egérgombbal a rendszercsoportra, majd válassza az előugró menü **Rendszerváltozók → Összehasonlítás és frissítés** menüpontját.
- g. Ellenőrizze, hogy a **Modellrendszer** mezőben a **Központi rendszer** látható-e.
- h. Jelölje ki a **Kezelőközpont** kategóriát, és ellenőrizze a következőket:
 - A **Védett socket réteg használata** beállításnál válassza az **Igen** értéket.
 - Válassza ki a **Kliens és szerver** SSL hitelesítési szintet.

A központi rendszer ezen értékeinek beállítása a Központi rendszer beállítása kliens hitelesítésre eljárásban történt meg. Jelölje be az értékek melletti **Frissítés** jelölőnégyzetet.

- i. Kattintson az **OK** gombra az értékek beállításához a rendszercsoport végpont rendszerein.

8. lépés: Ellenőrzési lista másolása a végpont rendszerekre

1. Az alábbi lépések feltételezik, hogy a központi rendszer V5R3 vagy újabb szintű: Az iSeries navigátorban bontsa ki a **Kezelőközpont → Meghatározások** elemet.
2. Kattintson a jobb egérgombbal a **Csomag** elemre, majd válassza az előugró menü **Új meghatározás** menüpontját.
3. Az **Új meghatározás** ablakban állítsa be az alábbi értékeket:
 - **Név:** Írja be a meghatározás nevét.
 - **Forrásrendszer:** Válassza ki a központi rendszer nevét.
 - **Kijelölt fájlok és mappák:** Kattintson a mezőre, majd írja be a /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL elérési utat.
4. Kattintson a **Beállítások** lapra, majd jelölje ki a **Meglévő fájl felülírása az átküldött fájljal** választógombot.
5. Kattintson a **Továbbiak** gombra.
6. A **További beállítások** ablakban engedélyezze az objektum különbségeket a visszaállítás során.

7. Kattintson az **OK** gombra a meghatározások listájának frissítéséhez, vagyis az új csomag megjelenítéséhez.
8. Kattintson a jobb egérgombbal a csomagra, majd válassza az előugró menü **Küldés** menüpontját.
9. A **Küldés** párbeszédablakban bontsa ki a **Rendszercsoportok -> Megbízható csoport** elemet, amely a **Rendelkezésre álló rendszerek és csoportok** listájában található. Egyedileg vegye fel a V5R3 vagy újabb rendszereket a **Kiválasztott rendszerek és csoportok** listájába. Távolítsa el a többi rendszert a **Kiválasztott rendszerek és csoportok** listájából, majd kattintson az **OK** gombra. A Megbízható csoport a 7. lépés: Végpont rendszerek beállítása kliens hitelesítéshez című témakör 1.c. részében megadott rendzercsoport.

Megjegyzés: A **Küldési** feladat a központi rendszernél mindig meghiúsul, mivel minden esetben ez a forrásrendszer. A végpont rendszereken a **Küldési** feladatnak sikeresen le kell futnia.

A V5R3 előtti iSeries rendszereknél QYPSVLDL.VLDL helye a QUSRSYS.LIB könyvtárban volt, és nem a QMGTC2.LIB könyvtárban. Éppen ezért, ha V5R3 előtti rendszerei vannak, el kell küldenie az érvényesítési listát hozzájuk, és a QUSRSYS.LIB könyvtárban kell elhelyezni QMGTC2.LIB helyett. Ehhez tegye a következőt:

- a. Kattintson a jobb egérgombbal a fentiekben létrehozott csomag meghatározásra, és válassza ki az **Új másik alapján** elemet.
- b. Hozzon létre meghatározást egy új névvel, hogy megkülönböztethető legyen az első meghatározástól.
- c. A meghatározás **Általános** fülén, a **Cél elérési útvonal** oszlopban kattintson a /QSYS.LIB/QMGTC2.LIB/QYPSVLDL.VLDL útvonalra. Ez lehetővé teszi a szerkesztését. Módosítson QMGTC2 könyvtárról QUSRSYS könyvtárra.

Megjegyzés: Figyeljen oda, a **Cél elérési útvonalat** szerkessze, és ne a **Forrás elérési útvonalat**.

- d. Kattintson az **OK** gombra az új csomag meghatározás mentéséhez.
- e. Kattintson a jobb egérgombbal az új csomag meghatározásra, majd válassza a **Küldés** menüpontot.
- f. A **Küldés** párbeszédablakban bontsa ki a **Rendszercsoportok -> Megbízható csoport** elemet, amely a **Rendelkezésre álló rendszerek és csoportok** listájában található. Egyedileg vegye fel a V5R3 előtti rendszereket a **Kiválasztott rendszerek és csoportok** listájába. Távolítsa el a többi rendszert a **Kiválasztott rendszerek és csoportok** listájából, majd kattintson az **OK** gombra. A **Megbízható csoport** a 7. lépés: Végpont rendszerek beállítása kliens hitelesítéshez című témakör 1.c. részében megadott rendzercsoport.

9. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Bontsa ki a központi rendszert.
3. Bontsa ki a **Hálózat** —> **Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
4. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját. A központi rendszer nézet összeesik, és egy üzenet tudatja, hogy nem rendelkezik csatlakozással a szerverhez.
5. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

10. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren

Megjegyzés: Ismételje meg az eljárást minden végpont rendszernél.

1. Bontsa ki az újraindításban érintett végpont rendszert.
2. Bontsa ki a **Hálózat** —> **Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
3. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját.
4. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

További SSL példahelyzetekre mutató hivatkozásokat a PélDAHelyzetek című témakörben talál.

Alapelvek

Az SSL protokoll felhasználásával lehetővé válik a védett kapcsolatok kialakítása a kliensek és szerver alkalmazások között, továbbá lehetőség van a kapcsolati végpontok hitelesítésére is. Az SSL emellett biztosítja a kliens és a szerver alkalmazás közötti adatcsere bizalmasságát és integritását.

Az SSL és az iSeries szerver közötti viszony mélyebb megértéséhez érdemes átolvasni az SSL protokollal kapcsolatos fogalmi információkat.

- Az SSL története
- Az SSL működése
- Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok
- Szerver hitelesítés
- Kliens hitelesítés

Az SSL története

Az Internetes biztonsággal kapcsolatos egyre szélesebb körben megfogalmazódott problémákra reagálva a Védett socket réteg (SSL) protokollt a Netscape fejlesztette ki 1994-ben. Az SSL eredetileg a web böngészők és szerverek közötti kapcsolatok biztosítását célozta meg. A kialakítása ettől függetlenül olyan volt, hogy más alkalmazások (például Telnet vagy FTP) is használhatták. Az SSL és a Szállítási réteg biztonság (TLS) protokollokkal kapcsolatban további információkat a Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok című témakörben talál.

Az SSL működése

Az SSL valójában két protokollból áll. Az egyik a megvalósítási, a másik a kézfogási protokoll. A megvalósítási protokoll irányítja az adatfolyamot az SSL szekció két végpontja között.

A kézfogási protokoll hitelesíti az SSL szekció végpontját (vagy végpontjait), és alakít ki egy egyedi szimmetrikus kulcsot az SSL szekció adatforgalmának titkosítására és visszafejtésére használt kulcsok előállításához. Az SSL a szekció végpontjainak hitelesítését aszimmetrikus kriptográfiai módszerekkel, illetve digitális igazolásokkal és egy SSL kézfogással végzi el. Az SSL általában a szerver hitelesítésére szolgál. Választhatóan a kliensek hitelesítésére is alkalmas. A végpontoknak vagy az SSL kapcsolatot megvalósító alkalmazásoknak kiosztható egy igazolási hatóság által kibocsátott digitális igazolás.

A digitális igazolások egy megbízható igazolási hatóság által aláírt nyilvános kulcsból és néhány azonosító információból állnak. Minden nyilvános kulcshoz tartozik egy magánkulcs is. A magánkulcs tárolása az igazolástól elkülönül. Mind a szerver, mind a kliens hitelesítésnél annak ellenőrzése történik meg, hogy a hitelesített fél hozzáfér-e a digitális igazolásához tartozó magánkulcshoz.

Az SSL kézfogás a nyilvános- és magánkulcsokkal kapcsolatos kriptográfiai műveletek miatt teljesítményigényes tevékenység. A végpontok közötti kezdeti SSL szekció kialakítása után a végpontokra vagy alkalmazásokra vonatkozó SSL szekcióinformációk a későbbi SSL szekciók kialakításának felgyorsítása érdekében egy biztonságos memóriában ideiglenesen tárolhatók. Az SSL szekciók folytatása esetén a végpontok a nyilvános- és magánkulcsok felhasználása nélkül egy rövidített kézfogással győződnek meg arról, hogy a másik fél hozzáfér az egyedi szekcióinformációkhoz. Ha mindkét végpont bebizonyítja, hogy hozzáfér az említett egyedi információkhoz, akkor az SSL kialakítja az új szimmetrikus kulcsokat, és az SSL szekció "folytatódik". A TLS 1.0 és az SSL 3.0 változatánál az ideiglenes tárolt információk legfeljebb 24 órán keresztül maradnak a biztonságos memóriában. A V5R2M0 és újabb kiadásokban a CPU-nak az SSL kézfogásból adódó többletterhelése elkerülhető egy kriptográfiai hardver beépítésével.

Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok

Az SSL protokollnak többféle változatát is meghatározták. A legújabb változat, a Szállítási réteg biztonság (TLS) az IETF munkája, amely az SSL 3.0 változatán alapszik. Az OS/400 megvalósítja az SSL és TLS protokollok az alábbi változatait támogatja:

- TLS 1.0
- SSL 3.0 kompatibilitással rendelkező TLS 1.0

Megjegyzések:


1. Az SSL 3.0 kompatibilitással rendelkező TLS 1.0 azt jelenti, hogy lehetőség szerint TLS 1.0 kapcsolat egyeztetésére kerül sor. Amennyiben ez nem lehetséges, úgy az SSL 3.0 változata kerül felhasználásra. Ha SSL 3.0 kapcsolat sem egyeztethető, akkor az SSL kézfogás meghiúsul.
 2. A TLS 1.0 változata SSL 3.0 és 2.0 kompatibilitással is támogatott. Ez a protokoll **ALL** beállításával érhető el, és azt eredményezi, hogy a TLS sikertelen egyeztetése esetén a rendszer kísérletet tesz az SSL 3.0 egyeztetésére. Ha az SSL 3.0 változatának egyeztetése meghiúsul, akkor kísérlet történik az SSL 2.0 változatának használatára. Ha SSL 2.0 kapcsolat sem egyeztethető, akkor az SSL kézfogás meghiúsul.
- SSL 3.0
 - SSL 2.0
 - SSL 3.0 változat 2.0 kompatibilitással

Az SSL 3.0 és az SSL 2.0 összehasonlítása

Az SSL 3.0 változata a 2.0 változathoz képest egy teljesen eltérő protokoll. A két protokoll közötti lényegesebb különbségek:

- Az SSL 3.0 változatának kézfogási menete eltér az SSL 2.0 változatában alkalmazottól.
- Az SSL 3.0 változata az RSA Data Security, Inc. BSAFE 3.0 megvalósítását tartalmazza. A BSAFE 3.0 tartalmaz bizonyos óvintézkedéseket az időzíti támogatások ellen, és az SHA1 kivonatkezelési algoritmust használja. Az SHA1 algoritmus biztonságosabbnak tekinthető, mint az MD5. Az SHA1 használatával az SSL 3.0 változata további rejtjelkezeléseket is biztosít, amelyek az MD5 helyett szintén az SHA1 algoritmust alkalmazzák.
- Az SSL protokoll 3.0 változata csökkenti az SSL kézfogás során lehetséges közbeálló ember (MITM) támadások esélyét. Az SSL 2.0 változatában bármennyire is valószínűtlen, elképzelhető volt, hogy egy MITM támadás elérje a rejtjelmeghatározás gyengítését. A rejtjel gyengítése pedig megkönnyíti a jogosulatlan személyeknek az SSL szekciókulcs feltörését.

A TLS 1.0 és az SSL 3.0 összehasonlítása

A legújabb ipari szabvány SSL protokoll az SSL 3.0 változatán alapuló Szállítási réteg biztonság (TLS) protokoll 1.0 változata. Meghatározásait az IETF fektette le az RFC 2246 "The TLS Protocol" dokumentumban. 

A TLS elsődleges célja az SSL még biztonságosabbá tétele, illetve a protokoll pontos és teljes meghatározása. A TLS az SSL 3.0 változatához képest az alábbi bővítéseket nyújtja:

- Még biztonságosabb MAC algoritmus
- Finomabban szabályozható riasztások
- A "homályos" területek pontosabb definíciója

Minden SSL használatra képes iSeries szerver alkalmazás automatikusan megkísérli a TLS használatát, kivéve, ha a beállítások kifejezetten csak az SSL 3.0 vagy 2.0 használatát írják elő.

A TLS az alábbi biztonsági továbbfejlesztéseket nyújtja:

- **Üzenet hitelesítési kulcs kivonatolás**
A TLS az Üzenet hitelesítési kulcs kivonatolási kódot (HMAC) használja, amely biztosítja, hogy a nyílt hálózatokon, például az Interneten forgalmazott adatok nem változtathatók meg a szállítás során. Az SSL 3.0 változata is biztosít kulcs alapján végzett üzenet hitelesítést, de a HMAC biztonságosabb az SSL 3.0 változatában használt Üzenet hitelesítési kódnál (MAC).
- **Bővített pszeudorandom függvény (PRF)**
A kulcs adatok előállítását a Bővített pszeudorandom függvénnyel (PRF) történik. A TLS esetén a HMAC határozza meg a PRF-et. A PRF két kivonatkezelési algoritmust használ oly módon, hogy ez garantálja a biztonságot. Az egyik algoritmus feltörése esetén az adatokat még mindig védi a második algoritmus.
- **Befejeződött üzenet tökéletesített ellenőrzése**
A TLS 1.0 és az SSL 3.0 is elküld egy Befejeződött üzenetet mindkét végpontnak, amelyek ellenőrzik, hogy a cserélt

üzenetek nem változtak-e meg. A TLS viszont a Befejeződött üzenetet a PRF és HMAC értékek alapján származtatja, amelyről már kijelentettük, hogy biztonságosabbak az SSL 3.0 megoldásainál.

- **Konzisztens igazoláskezelés**
Az SSL 3.0 változatától eltérően a TLS megkísérli a felhasználandó igazolás típusának meghatározását.
- **Egyedi riasztási üzenetek**
A TLS több és kifejezőbb riasztást határoz meg a szekció végpontjai által észlelt problémák jelzésére. A TLS emellett dokumentálja bizonyos riasztások kiküldését.

Szerver hitelesítés

A szerver hitelesítéssel a kliens meggyőződhet arról, hogy a szerver igazolása érvényes, és olyan igazolási hatóság írta alá, amelyben a kliens megbízik. Az SSL aszimmetrikus kriptográfiai módszerekkel és a kézfogási protokoll segítségével előállít egy szimmetrikus kulcsot, amely csak az adott SSL szekcióban kerül felhasználásra. Ezen kulcs alapján jön létre egy kulcskészlet, amely az SSL szekció adatforgalmának titkosítását és visszafejtését elvégzi. Ennek megfelelően az SSL kézfogás végére a kommunikációs összeköttetés mindkét végpontja hitelesítésre kerül. Emellett létrejön egy egyedi kulcs az adatok titkosításához és visszafejtéséhez. A kézfogás befejezése után az alkalmazásszintű adatok titkosított formában haladnak át az SSL szekcióban.

Kliens hitelesítés

Több alkalmazás is lehetőséget nyújt kliens hitelesítésre. A kliens hitelesítéssel a szerver meggyőződhet arról, hogy a kliens igazolása érvényes, és olyan igazolási hatóság írta alá, amelyben a szerver megbízik. A kliens hitelesítést az alábbi iSeries szerver alkalmazások támogatják:

- IBM HTTP Server (Apache alapú)
- FTP szerver
- Telnet szerver
- Kezelőközpont végpont rendszer
- Címtár szolgáltatások (LDAP)

SSL támogatás megteremtésének tervezése

Az iSeries szerver SSL támogatásának bevezetésekor érdemes átgondolni a következőket:

- SSL előfeltételek
- A beszerzendő digitális igazolások típusa és beszerzési forrása

SSL előfeltételek:

- IBM Digitális igazolás kezelő (DCM), az OS/400 (5722-SS1) 34. opciója.
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- Ha a HTTP szerveren használni kívánja a Digitális igazolás kezelőt, akkor telepíteni kell az IBM Java fejlesztőkészletet (5722-JV1). Ellenkező esetben a HTTP adminisztrációs szerver nem indul el.
- IBM Cryptographic Access Provider (128 bites, 5722-AC3). A termék bitszáma a kriptográfiai műveletekben használt szimmetrikus kulcsokban alkalmazható titkos rész maximális méretére utal. A szimmetrikus kulcsok méretére több országban is export- és importkorlátozások vonatkoznak. A nagyobb bitméret biztonságosabb kapcsolatot eredményez.
- Az SSL kézfogási feldolgozás felgyorsítása érdekében célszerű lehet egy kriptográfiai hardver beszerzése is. A rendelkezésre álló lehetőségekről a kriptográfiai hardver című témakörben tájékozódhat. Kriptográfiai hardver (4758 vagy 4764 típusú IBM Cryptographic Coprocessor) telepítésekor telepíteni kell a 35. opciót is, a Cryptographic Service Provider terméket.

Ha az SSL protokollt az iSeries Access for Windows összetevőivel kívánja használni, akkor telepíteni kell az iSeries Client Encryption (5722-CE3) terméket is. Ezt az iSeries Access for Windows követeli meg a biztonságos kapcsolat kialakításához.

Megjegyzés: A Personal Communications termékkel szállított PC5250 emulátor használatához a Client Encryption termék telepítése nem szükséges. A Personal Communications saját, beépített titkosítási kóddal rendelkezik.

Digitális igazolások

A nyilvános és saját digitális igazolások közötti különbségeket, illetve ezek beszerzési lehetőségeit részletesen a Nyilvános igazolások használata és saját igazolások kibocsátása című témakörben találja.

A digitális igazolások kezelésére használható iSeries megoldás az IBM Digitális igazolás kezelője (DCM). A Digitális igazolás kezelőről további részleteket az Információs központ A Digitális igazolás kezelő használata című témakörében olvashat.

Alkalmazások biztonságossá tétele SSL segítségével

Az SSL segítségével az alábbi iSeries szerver alkalmazások tehetőek biztonságossá:

- Vállalati azonosság leképezés (EIM)
- FTP szerver
- HTTP szerver (Apache alapú)
- iSeries Access for Windows
- Címtár szolgáltatások (LDAP)
- Osztott relációs adatbázis architektúra (DRDA) és Osztott adatkezelés (DDM) szerver
- Kezelőközpont szerver
- Telnet szerver
- Websphere Express alkalmazáskiszolgáló
- Az iSeries Access for Windows API készlet felhasználásával írt alkalmazások
- Az iSeries szerveren támogatott SSL alkalmazásprogram illesztők (API) felhasználásával írt alkalmazások. A támogatott API-k a Globális biztonsági eszközkészlet (GSKit) és az iSeries saját SSL_ alkalmazásprogram illesztői. A GSKit és az SSL_ alkalmazásprogram illesztőkről további információkat a Védett socket API-k című témakörben talál.

SSL hibaelhárítás

Az alábbi nagyon alapszintű hibaelhárítási információk segítségével leszűkítheti az iSeries szerveren az SSL használatával kapcsolatban fellépő lehetséges problémák körét. Fontos megjegyezni, hogy ez távol áll egy teljes hibaelhárítási útmutatótól.

Ellenőrizze, hogy teljesülnek-e a következők:

- Az iSeries szerver megfelel az SSL előfeltételeknek (lásd az SSL előfeltételek című témakört).
- Ha az iSeries navigátor Kezelőközpontját V5R1 rendszeren használja, akkor telepítve vannak az alábbi javítások:
 - si01375
 - si01376
 - si01377
 - si01378
 - si01838
- Az igazolási hatóság és az igazolások érvényesek, és nem jártak le.

Ha a fentieket ellenőrizte a rendszeren, és még mindig SSL problémákat tapasztal, akkor próbálkozzon meg a következőkkel:

- A szerver munkanaplójában található SSL hibakód kikereshető egy hibatáblázatból, amely több információt nyújt a hibáról. A védett socket hibakód üzenetekkel kapcsolatos információkat a Védett socket API hibakód üzenetek című témakörben találja. Ez a táblázat például a -93 hibakódot az SSL_ERROR_SSL_NOT_AVAILABLE konstansra képezi le.

- A negatív visszatérési kódok SSL_ API használatára utalnak.
- A pozitív visszatérési kódokat a GSKit API használatakor kaphat. A programozók a `gsk_strerror()` vagy `SSL_Strerror()` segítségével szerezhetnek egy rövid leírást a hibás visszatérési kódról. Bizonyos alkalmazások ez alapján részletesebb hibaüzenetet írnak a munkanaplóba.

Ha részletesebb információkra van szükség, akkor a táblázatban megadott üzenetazonosító megjeleníthető az iSeries szerveren a hiba lehetséges okának és elhárításának feltüntetésével. A hibakódokkal kapcsolatban elképzelhető, hogy további dokumentációt biztosít a hibát visszaadó védett socket API is.

- A következő két header fájl a táblázattal megegyező SSL visszatérési kódokat tartalmazza az üzenetazonosítók keresztthivatkozásai nélkül:
 - QSYSINC/H.GSKSSL
 -



QSYSINC/H.QSOSSL

Ne feledje, hogy bár a rendszer SSL visszatérési kódjai konstansok a két fájlban, minden egyes visszatérési kódhoz egynél több egyedi hiba is társítható.

További iSeries hibaelhárítási információkért tekintse meg a Hibaelhárítás és szerviz című témakört.



Kapcsolódó információk

Az SSL protokollal kapcsolatban további ismereteket az alábbi forrásokból szerezhet:

IBM források

- Az SSL és Java védett socket kiterjesztés (JSSE) témakör rövid leírást biztosít a JSSE-ről és annak használatáról.
- Az IBM Toolbox for Java témakörben megtalálja a rendelkezésre álló Java osztályok felsorolását és használatuk rövid leírását.

RFC leírások

- Az RFC 2246: "The TLS Protocol Version 1.0"  magyarázza el a TLS protokoll részleteit.
- Az RFC2818: "HTTP Over TLS"  írja le a TLS használatát az Interneten folyó HTTP kapcsolatok biztonságossá tételére.

Egyéb források

- A The SSL Protocol Version 3.0 dokumentum  magyarázza el részletekbe menően az SSL 3.0 változatát.

Megjegyzések

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Elképzelhető, hogy a dokumentumban szereplő termékeket, szolgáltatásokat vagy lehetőségeket az IBM más országokban nem forgalmazza. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviselők szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett, vagy bejegyzés alatt álló szabadalmi lehetnek. Ezen dokumentum nem ad semmiféle jogos licenct ezen szabadalmakhoz. A licenckérelmeket írásban a következő címre küldheti:

IBM
Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatban az országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

IBM
World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT "ÖNMAGÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem IBM webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti ezen webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

Az IBM a könyvben tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat IBM Vásárlói megállapodás, IBM nemzetközi programlicenc szerződés, vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban megadott teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információk a termékek szállítóitól, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint az egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóhoz.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célokat jelentenek.

Védjegyek

A következő kifejezések az International Business Machines Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

DRDA
IBM
iSeries
Operating System/400
OS/400

A Lotus, a Freelance és a WordPro az International Business Machines Corporation és a Lotus Development Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, a Windows, a Windows NT és a Windows logó a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

Más cégek, termékek és szolgáltatások nevei mások védjegyei vagy szolgáltatás védjegyei lehetnek.

A kiadványok letöltésére és kinyomtatására vonatkozó feltételek

A letöltésre kiválasztott kiadványok használatára vonatkozó engedélyt az alábbi feltételek és kikötések elfogadásának jelzése adja meg.

Személyes használat: A Kiadványok reprodukálhatók személyes, nem kereskedelmi célú használatra, valamennyi tulajdonosi feljegyzés megtartásával. Az IBM kifejezett engedélye nélkül nem szabad a Kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.

Kereskedelmi használat: A Kiadványok reprodukálhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett engedélyének hiányában nem készíthetők Kiadványokból származó munkák, nem reprodukálhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.

A jelen engedélyben foglalt, kifejezetten megadott engedélyeken túlmenően a Kiadványokra, illetve a bennük található információkra, adatokra, szoftverre vagy bármilyen szellemi tulajdonra semmilyen más kifejezett vagy vélelmezett engedély nem vonatkozik.

Az IBM fenntartja magának a jogot, hogy jelen engedélyeket saját belátása szerint bármikor visszavonja, ha úgy ítéli meg, hogy a Kiadványokat az IBM érdekeit sértő módon használják fel, vagy a fenti útmutatásokat nem megfelelően követik.

Jelen információk kizárólag valamennyi vonatkozó törvény és előírás betartásával tölthetők le, exportálhatók és reexportálhatók, beleértve az Egyesült Államok exportra vonatkozó törvényeit és előírásait is. Az IBM A KIADVÁNYOK TARTALMÁRA VONATKOZÓAN SEMMIFÉLE GARANCIÁT NEM NYÚJT. A KIADVÁNYOK "ÖNMAGUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA VÁLLALÁSA NÉLKÜL KERÜLNEK KÖZREADÁSRA, IDEÉRTVE, DE NEM KIZÁRÓLAG A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.

Valamennyi anyag szerzői jogának birtokosa az IBM Corporation.

A webhelyen található kiadványok letöltésével vagy nyomtatásával jelzi, hogy elfogadja jelen feltételeket és kikötéseket.



Nyomtatva Dániában