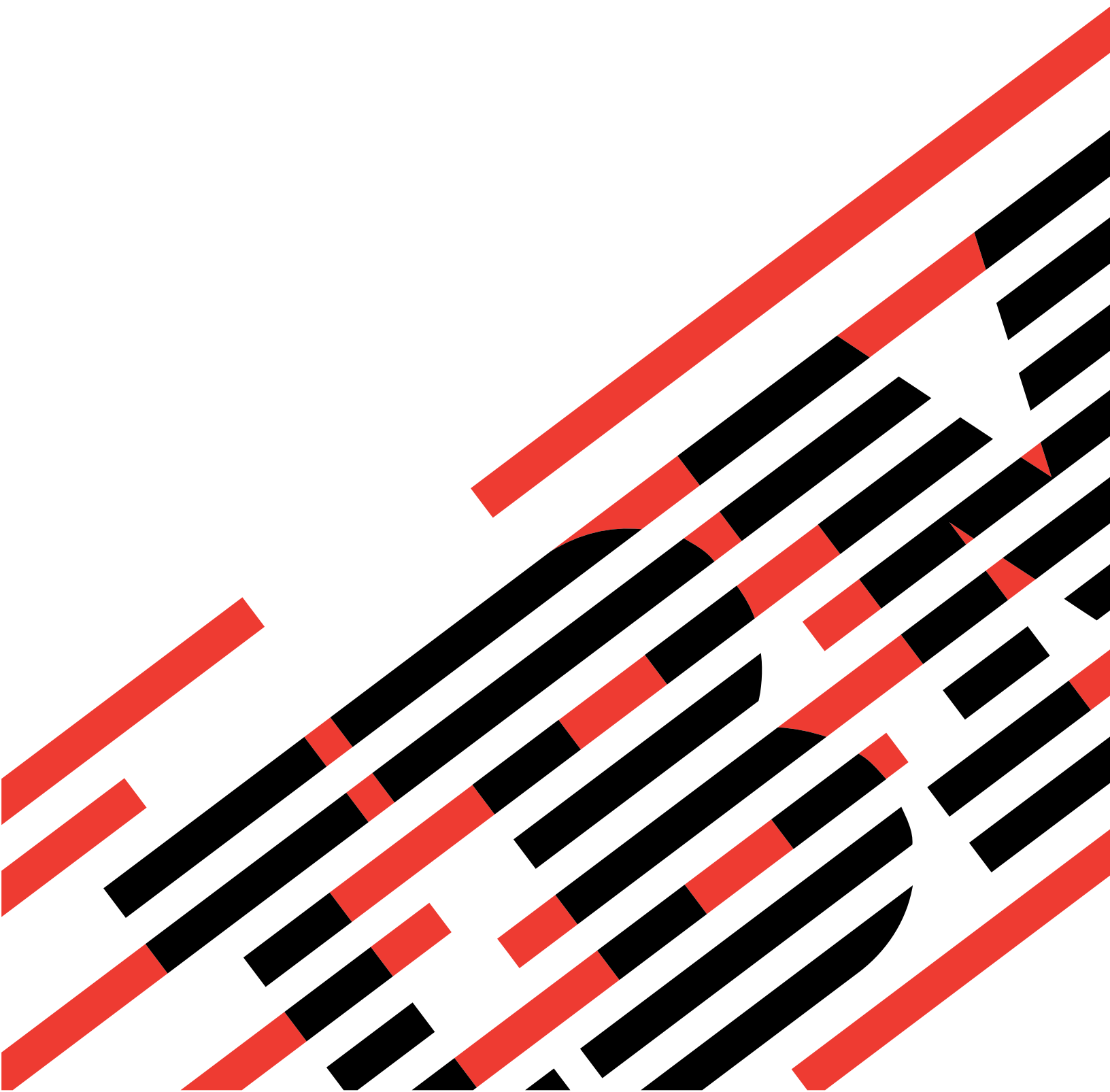




IBM Systems - iSeries  
Védett socket réteg (SSL)

*V5R4*







IBM Systems - iSeries  
Védett socket réteg (SSL)

*V5R4*

**Megjegyzés**

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

**Hatodik kiadás (2006. február)**

Ez a kiadás a V5R4M0 szintű i5/OS (termékszám: 5722–SS1) termékre, és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren illetve a CISC modelleken.

© Szerzői jog IBM Corporation 2002, 2006. Minden jog fenntartva

---

# Tartalom

<b>Védett socket réteg (SSL)</b> . . . . .	<b>1</b>
A V5R4 kiadás újdonságai. . . . .	1
Nyomtatható PDF . . . . .	1
Példahelyzetek . . . . .	1
Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével . . . . .	2
Alaphelyzet: . . . . .	2
Célok: . . . . .	2
Részletek: . . . . .	2
Előfeltételek és feltételezések: . . . . .	3
Konfigurációs lépések . . . . .	3
Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével . . . . .	5
Alaphelyzet: . . . . .	5
Részletek: . . . . .	5
Előfeltételek és feltételezések: . . . . .	7
Konfigurációs lépések: . . . . .	8
Alapelvek . . . . .	13

Az SSL története . . . . .	13
Az SSL működése. . . . .	13
Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok . . . . .	14
Szerver hitelesítés . . . . .	15
Kliens hitelesítés . . . . .	15
Az SSL bevezetésének tervezése . . . . .	15
SSL előfeltételek . . . . .	16
Digitális igazolások . . . . .	16
Alkalmazások biztonságossá tétele SSL segítségével . . . . .	16
SSL hibaelhárítás . . . . .	17
A Védett socket réteg (SSL) protokollhoz kapcsolódó információk. . . . .	17

<b>Nyilatkozatok</b> . . . . .	<b>19</b>
Védjegyek . . . . .	21
Feltételek . . . . .	21



---

## Védett socket réteg (SSL)

Ez a témakör írja le az SSL használatát a szerveren.

A Védett socket réteg (SSL) a nem védett hálózatok, például az Internet felett védett kommunikációt biztosító ipari szabvány biztonsági protokoll.

---

## A V5R4 kiadás újdonságai



Ez a témakör írja le a kiadásnak a Védett socket réteg (SSL) funkciókat érintő újdonságait.

### Visszavont termék: IBM Cryptographic Access Provider product, 5722-AC3 (128 bit)

- | A 128 bites IBM Cryptographic Access Provider (5722-AC3) termékre már nincs szükség. Ez az i5/OS V5R4 kiadásának új fejlesztése. Minden V5R4 szintű rendszer alából biztosítja a korábban az 5722-AC3 termékben elérhető funkciókat.

## 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.

---

## Nyomtatható PDF

A témakör az itt leírtak PDF változatának megtekintését vagy nyomtatását ismerteti.

A dokumentum PDF változatának megtekintéséhez vagy letöltéséhez válassza ki a Védett socket réteg (SSL) hivatkozást.


## PDF fájlok mentése

A PDF mentése a munkaállomásra megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőjében (kattintás a jobb oldali egérgombbal a fenti hivatkozásra).
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a könyvtárat, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

## Adobe Acrobat Reader letöltése

A PDF állományok megtekintéséhez vagy nyomtatásához telepített Adobe Acrobat Reader programra van szükség.

Ingyenes példányát letöltheti az Adobe honlapjáról ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

---

## Példahelyzetek

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

A példahelyzetek elolvasásával néhány lehetséges példán keresztül ismerheti meg az SSL protokoll felhasználási lehetőségeit az iSeries szerveren.

### **Kapcsolódó tájékoztatás**

Példahelyzet: Biztonságos Telnet

Példahelyzet: Az iSeries SSL teljesítményének növelése

Példahelyzet: Magánkulcsok védelme kriptográfiai hardverrel

## **Példahelyzet: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével**

Ez a példahelyzet nyújt információkat a szerver és egy távoli kliens közötti kapcsolat SSL biztonságának használatáról.

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.

### **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 ilyen 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 bizonyítania 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:

1. Az A rendszernek meg kell felelnie az SSL előfeltételeknek.
2. Az A rendszeren az OS/400 V5R3 vagy újabb változatának, illetve i5/OS operációs rendszernek kell futnia.
3. Az iSeries navigátor PC kliens az iSeries Access for Windows V5R3 vagy újabb változatát futtatja.
4. Be kell állítani egy Igazolási hatóságot az iSeries szerverek számára.
5. Létre kell hozni egy igazolási hatóság által aláírt igazolást az A rendszer számára.
6. Az igazolási hatóság és a szerver igazolását el kell juttatni az A rendszerre, ott importálni kell azokat a kulcsadatbázisba.
7. Az igazolást hozzá kell rendelni a Kezelőközpont szerver azonosítójához, illetve az összes iSeries Access szerver alkalmazásazonosítójához. Az iSeries Access szerverek közé a TCP központi szerver, az adatbázis szerver, az adatsor szerver, a hálózati nyomtatási szerver, a távoli parancs szerver és a bejelentkezési szerver tartozik.
  - a. Az A rendszeren Indítsa el az IBM Digitális igazolás kezelőt. Ezen a ponton kell beszerezni vagy létrehozni az igazolásokat, vagy beállítani az igazolások rendszerét.
  - 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. Rendelje hozzá az igazolást minden iSeries Access szerverhez.
8. Töltse le az igazolási hatóság igazolását a PC kliensre.

Mielőtt a Kezelőközpont szerveren engedélyezni lehetne az SSL támogatást, telepíteni kell az SSL előfeltételeket, és be kell állítani a digitális igazolásokat az iSeries szerveren. Az előfeltételek teljesülésekor a Kezelőközpont szerver SSL támogatásának beállítása az alábbi eljárással történik.

### Kapcsolódó fogalmak

“SSL előfeltételek” oldalszám: 16

### Kapcsolódó tájékoztatás

A Digitális igazolás kezelő beállítása

A Digitális igazolás kezelő indítása

## Konfigurációs lépések

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

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

## Beállítás részletei: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével

Ez a témakör írja le a Kezelőközpont szerver kliens kapcsolatainak biztonságossá tételére vonatkozó további beállítási lépéseket.

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.

### Kapcsolódó fogalmak

“SSL előfeltételek” oldalszám: 16

### Kapcsolódó feladatok

“Előfeltételek és feltételezések:” oldalszám: 7

### Kapcsolódó tájékoztatás

Igazolások beállítása az első alkalommal

## 1. lépés: SSL kikapcsolása az iSeries navigátor kliensben:

Erre a lépésre csak akkor van szükség, ha már engedélyezte az SSL támogatást 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 kijelölését.
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 kiadásaiban 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** szerverre, 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 aktiválása 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. lépés: SSL aktiválása az iSeries navigátor kliensben” oldalszám: 4 helyen leírtakat. 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 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 kijelölését.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

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

Ez a példahelyzet írja le, hogyan használható az SSL egy iSeries szerver összes kapcsolatának biztonságossá tételére.

Ez a példahelyzet azt írja le, hogyan oldható meg egy iSeries navigátor Kezelőközpont szerver futtatásával központi rendszerként működő iSeries szerver összes kapcsolatának biztonságossá tétele.

### **Kapcsolódó fogalmak**

“Alkalmazások biztonságossá tétele SSL segítségével” oldalszám: 16

Ez a témakör sorolja fel az iSeries szerver SSL segítségével biztonságossá tehető alkalmazásainak listáját.

## **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 iSeries Access szerverei 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 navigátor programokat a számítógépen.

Ehhez kétféle hitelesítési szint közül lehet választani a Kezelőközpont szervernél:

### **Szerver hitelesítés**

Ez a szerver igazolásának hitelesítését biztosítja. Ilyenkor a kliens hitelesíti a szervert, akkor is, ha a kliens egy iSeries navigátor, és akkor is, ha a kliens a központi rendszer Kezelőközpont szervere. Amikor az iSeries navigátor csatlakozik a központi szerverre, akkor a PC az SSL kliens, és a központi rendszeren futó Kezelőközpont szerver az SSL szerver. A végpont rendszerekhez csatlakozó központi rendszer viszont SSL kliensként működik. Ilyenkor a végpont rendszer az SSL szerver. A szervernek igazolnia kell azonosságát a kliens felé egy olyan igazolás bemutatásával, amelyet a kliens által megbízhatónak tekintett igazolási hatóság bocsátott ki. Minden SSL szervernek rendelkeznie kell egy megbízható igazolási hatóság által kiadott igazolással.

## Kliens és szerver hitelesítés

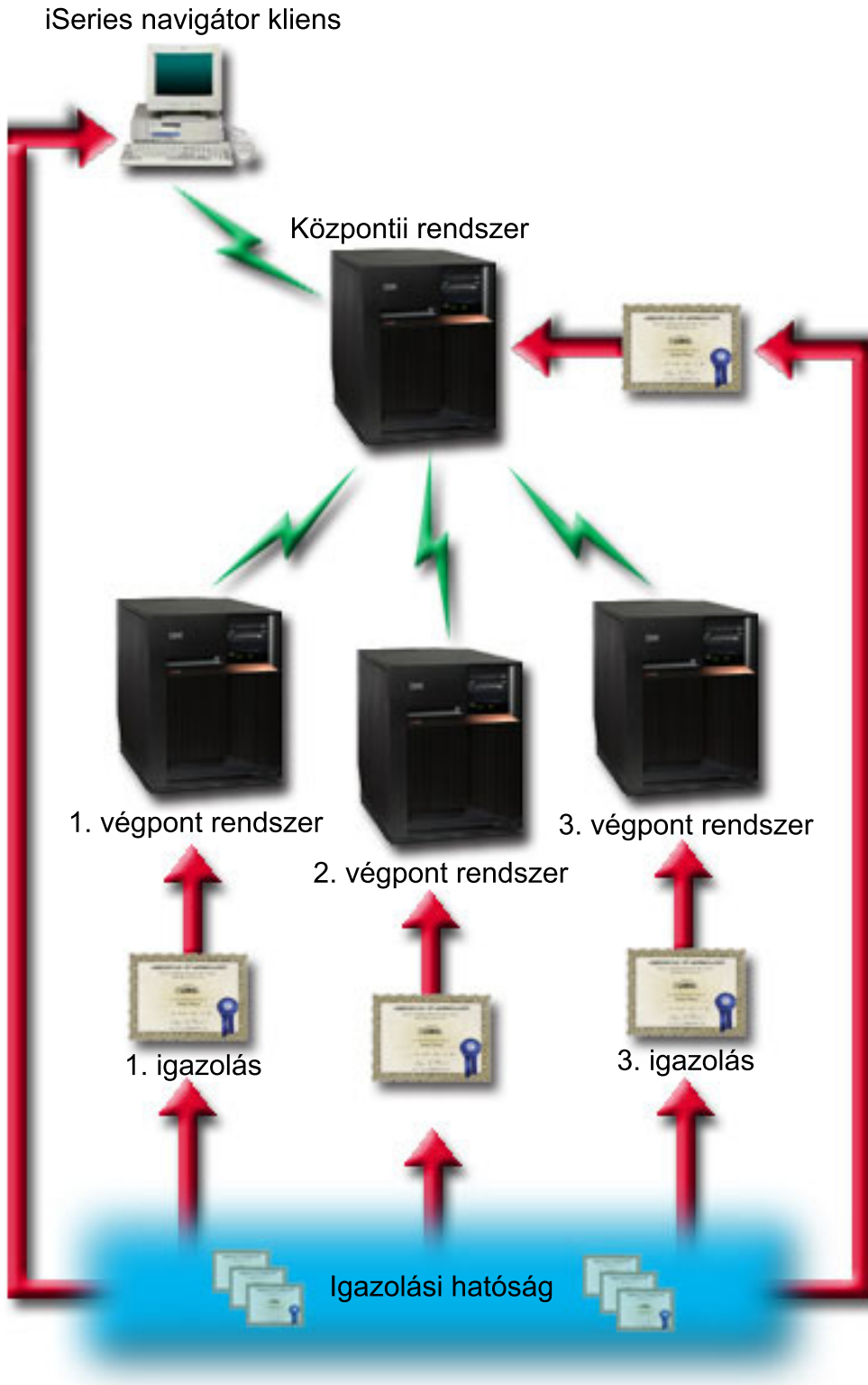
Ez a módszer a központi rendszer és a végpont rendszer igazolását is hitelesíti. Ez magasabb biztonsági szintet jelent a szerver hitelesítéshez képest. Más alkalmazások ezt kliens hitelesítésként emlegetik, amikor a kliensnek kell bemutatnia egy megbízható igazolást. Amikor a központi rendszer (SSL kliens)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

**Megjegyzés:** Egyidejű kliens és szerver hitelesítés csak két iSeries rendszer között szokott történni. A szerver nem végez kliens hitelesítést, ha a kliens egy PC.

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 a központi rendszerhez, akkor a központi rendszer működik szerverként. 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. Az igazolási hatóság igazolásának a központi rendszeren, a végpont rendszereken és a személyi számítógépeken is meg kell lennie.



## Előfeltételek és feltételezések:

A Kezelőközpont szerver összes kapcsolatának biztosításához az alábbi adminisztrációs és konfigurációs feladatokat kell elvégezni:

1. Az A rendszernek meg kell felelnie az SSL előfeltételeknek.
2. A központi rendszernek és az összes végpont iSeries szervernek az OS/400 V5R2 vagy újabb kiadását, vagy i5/OS operációs rendszert kell futtatnia. A V5R4 szintű i5/OS kliensek nem tudnak csatlakozni a V5R1 szintű OS/400 rendszerekhez.
3. Az iSeries navigátor PC kliens az iSeries Access for Windows V5R2 vagy újabb változatát futtatja.
4. Be kell állítani egy Igazolási hatóságot az iSeries szerverek számára.
5. Létre kell hozni egy igazolási hatóság által aláírt igazolást az A rendszer számára.
6. Az igazolási hatóság és a szerver igazolását el kell juttatni az A rendszerre, ott importálni kell azokat a kulcsadatbázisba.
7. Az igazolásokat hozzá kell rendelni a Kezelőközpont alkalmazásazonosítójához, illetve az összes iSeries Access szerver alkalmazásazonosítójához. Az iSeries Access szerverek közé a TCP központi szerver, az adatbázis szerver, az adatsor szerver, a hálózati nyomtatási szerver, a távoli parancs szerver és a bejelentkezési szerver tartozik.
  - a. Indítsa el az IBM Digitális igazolás kezelőt a Kezelőközpont szerveren. Ha igazolások beszerzésére vagy létrehozására, illetve az igazolási rendszer beállítására vagy módosítására van szükség, akkor erre ezen a ponton kell sort keríteni.
  - 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. Válassza ki az alkalmazáshoz hozzárendelni kívánt igazolást, majd kattintson az **Új igazolás hozzárendelése** gombra. A Digitális igazolás kezelő újratölti az **Igazolás hozzárendelés frissítése** oldalt, és megjelenik egy megerősítést kérő üzenet.
  - i. A **Mégse** gombra kattintva térjen vissza az alkalmazások listájához.
  - j. Ismétlje meg a fenti eljárást minden iSeries Access szerverre.
8. Töltse le az igazolási hatóság igazolását az iSeries navigátor PC kliensre.

#### **Kapcsolódó fogalmak**

“SSL előfeltételek” oldalszám: 16

#### **Kapcsolódó feladatok**

“Beállítás részletei: Kezelőközpont kliens kapcsolatának biztonságossá tétele az SSL segítségével” oldalszám: 4  
Ez a témakör írja le a Kezelőközpont szerver kliens kapcsolatainak biztonságossá tételére vonatkozó további beállítási lépéseket.

“Beállítás részletei: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével” oldalszám: 9

Ez a témakör írja le a Kezelőközpont szerver összes kapcsolatának biztonságossá tételére vonatkozó részleteket.

#### **Kapcsolódó tájékoztatás**

V5R1 információs központ, “Kezelőközpont biztonságossá tétele”

A Digitális igazolás kezelő használata

## **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 “Előfeltételek és feltételezések.” oldalszám: 7 szakaszt. 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. "1. lépés: Központi rendszer beállítása szerver hitelesítésre"
2. "2. lépés: Végpont rendszerek beállítása szerver hitelesítésre" oldalszám: 10
3. "3. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren" oldalszám: 10
4. "4. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren" oldalszám: 10
5. "5. lépés: SSL aktiválása az iSeries navigátor kliensben" oldalszám: 11
6. "6. lépés: Központi rendszer beállítása kliens hitelesítésre" oldalszám: 11
7. "7. lépés: Végpont rendszerek beállítása kliens hitelesítésre" oldalszám: 11
8. "8. lépés: Ellenőrzési lista másolása a végpont rendszerekre" oldalszám: 12
9. "9. lépés: A Kezelőközpont szerver újraindítása a központi rendszeren" oldalszám: 12
10. "10. lépés: A Kezelőközpont szerver újraindítása az összes végpont rendszeren" oldalszám: 12

#### **Kapcsolódó fogalmak**

"SSL előfeltételek" oldalszám: 16

#### **Kapcsolódó tájékoztatás**

Igazolások beállítása az első alkalommal

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

Ez a témakör írja le a Kezelőközpont szerver összes kapcsolatának biztonságossá tételére vonatkozó részleteket.

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. 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.

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.

#### **Kapcsolódó fogalmak**

"SSL előfeltételek" oldalszám: 16

#### **Kapcsolódó feladatok**

"Előfeltételek és feltételezések:" oldalszám: 7

#### **Kapcsolódó tájékoztatás**

Igazolások beállítása az első alkalommal

### **1. lépés: Központi rendszer beállítása szerver hitelesítésre:**

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** beállítását.
3. Válassza ki a **Szerver** hitelesítési szintet.
4. Kattintson az **OK** gombra az érték beállításához a központi rendszeren.

**Megjegyzés:** A Kezelőközpont szervert még **NE** indítsa újra, csak ha amikor az útmutatások ezt kifejezetten előírják. Ha ezen a ponton indítja újra a szervert, akkor nem fogja tudni elérni a végponti szervereket. A szerver újraindítása, vagyis az SSL aktiválása előtt további beállítási lépéseket is el kell még végezni. Ennek részeként át kell vinni az SSL konfigurációt a végpont rendszerekre az összehasonlítás és frissítés feladat segítségével.

## 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. Kattintson az OK gombra, és várja meg a feladat befejeződését.
  - c. Kattintson a jobb egérgombbal, majd válassza az előugró menü **Rendszercsoportok** → **Új rendszercsoport** menüpontját.
  - d. Határozzon meg egy új rendszercsoportot, amely az összes olyan végpont rendszert tartalmazza, amelyen engedélyezni kívánja az SSL-t. Nevezze el az új rendszercsoportot mondjuk "Megbízható rendszerek"-nek.
  - e. Az új "Megbízható rendszerek" 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. A **Kategória** mezőben válassza ki a **Kezelőközpont** bejegyzést.
  - i. Ellenőrizze, hogy az **SSL használata** beállítás értéke **Igen**-e, majd kattintson a **Frissítés** gombra az értéknek a "Megbízható rendszerek" csoportra terjesztéséhez.
  - j. Ellenőrizze, hogy az **SSL hitelesítési szint** beállítás értéke **Szerver**-e, majd kattintson a **Frissítés** gombra az értéknek a "Megbízható rendszerek" csoportra terjesztéséhez.

**Megjegyzés:** Ha az értékek nincsenek beállítva, akkor végezze el a 1. lépés: Központi rendszer beállítása szerver hitelesítésre helyen leírtakat.

- k. Kattintson az **OK** gombra. A folytatás előtt várja meg az **Összehasonlítás és frissítés** feladat feldolgozásának befejeződését.

## 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** szerverre, 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. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Bontsa ki az újraindításban érintett végpont rendszert.
3. Bontsa ki a **Hálózat** → **Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
4. Kattintson a jobb egérgombbal a **Kezelőközpont** szerverre, majd válassza az előugró menü **Leállítás** menüpontját.
5. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.
6. Ismételje meg az eljárást minden végpont rendszernél.

#### 5. lépés: SSL aktiválása 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** beállítását.
4. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

**Megjegyzés:** A lépések végrehajtásával a szerver hitelesítés a központi és a végpont rendszereken is be van állítva. Választható jelleggel a központi és végpont rendszerek kliens hitelesítésre is beállíthatók. A 6-10. lépéseket csak akkor kell elvégezni, ha a kliens hitelesítést is engedélyezni kívánja a központi és végpont rendszereken.

#### 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 szerver és kliens hitelesítéssel 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. Ha a szerver hitelesítés még nincs beállítva, akkor menjen vissza a megfelelő helyre, és végezze el a beállítást.

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** beállítását.
3. Válassza ki a **Kliens és szerver** hitelesítési szintet.
4. Kattintson az **OK** gombra az érték beállításához a központi rendszeren.

**Megjegyzés:** A Kezelőközpont szerveret még **NE** indítsa újra, csak ha amikor az útmutatások ezt kifejezetten előírják. Ha ezen a ponton indítja újra a szerveret, akkor nem fogja tudni elérni a végponti szervereket. A szerver újraindítása, vagyis az SSL aktiválása előtt további beállítási lépéseket is el kell még végezni. Ennek részeként át kell vinni az SSL konfigurációt a végpont rendszerekre az összehasonlítás és frissítés feladat segítségével.

#### 7. lépés: Végpont rendszerek beállítása kliens hitelesítésre:

Hasonlítsa össze és frissítse a végpont rendszerek rendszerváltozóit:

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. Kattintson az OK gombra, és várja meg a feladat befejeződését.
  - c. Az adatgyűjtés befejezése után kattintson a jobb egérgombbal a "Megbízható rendszerek" csoportra, majd válassza az előugró menü **Rendszerváltozók** → **Összehasonlítás és frissítés** menüpontját.

- d. Ellenőrizze, hogy a **Modellrendszer** mezőben a központi rendszer látható-e.
- e. A **Kategória** mezőben válassza ki a **Kezelőközpont** bejegyzést.
- f. Ellenőrizze, hogy az **SSL használata** beállítás értéke **Igen**-e, majd kattintson a **Frissítés** gombra az értéknek a "Megbízható rendszerek" csoportra terjesztéséhez.
- g. Ellenőrizze, hogy az **SSL hitelesítési szint** beállítás értéke **Kliens és szerver**-e, majd kattintson a **Frissítés** gombra az értéknek a "Megbízható rendszerek" csoportra terjesztéséhez.

**Megjegyzés:** Ha az értékek nincsenek beállítva, akkor végezze el az 6. lépés: Központi rendszer beállítása kliens hitelesítésre helyen leírtakat.

- h. Kattintson az **OK** gombra. A folytatás előtt várja meg az **Összehasonlítás és frissítés** feladat feldolgozásának befejeződését.

### 8. lépés: Ellenőrzési lista másolása a végpont rendszerekre:

A feladat feltételezi, hogy a központi rendszeren V5R3 vagy újabb operációs rendszer fut. A V5R3 előtti 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. V5R3 és újabb rendszereknél tegye a következőket:

1. Az iSeries navigátorban bontsa ki a **Kezelőközpont** → **Meghatározások** kategóriát.
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:
  - a. **Név:** Írja be a meghatározás nevét.
  - b. **Forrásrendszer:** Válassza ki a központi rendszer nevét.
  - c. **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 **Speciális beállítások** ablakban válassza az **Igen** értéket az Objektum különbségek engedélyezéséhez a visszaállításakor, és állítsa a **Célkiadás** mezőt a végpont rendszereken használt legkorábbi kiadásra.
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** párbeszédablak **Rendelkezésre álló rendszerek és csoportok** listájában bontsa ki a **Rendszercsoportok** → **Megbízható rendszerek** bejegyzést. Ez a "2. lépés: Végpont rendszerek beállítása szerver hitelesítésre" oldalszám: 10 helyen meghatározott csoport.

**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.

10. Ha a **Megbízható rendszerek** csoportjában vannak V5R3 előtti rendszerek, akkor ezeken a rendszereken saját kezűleg át kell helyeznie a QYPSVLDL.VLDL objektumot a QMGTC2.LIB könyvtárból a QUSRSYS.LIB könyvtárba. Ha a QYPSVLDL.VLDL már megtalálható a QUSRSYS.LIB könyvtárban, akkor törölje azt, és cserélje le a QMGTC2.LIB könyvtárból származó újabb változattal.

### 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** szerverre, 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 rendszerénél.

1. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
2. Bontsa ki az újraindításban érintett végpont rendszert.
3. Bontsa ki a **Hálózat** → **Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
4. Kattintson a jobb egérgombbal a **Kezelőközpont** szerverre, majd válassza az előugró menü **Leállítás** menüpontját.
5. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

---

## Alapelvek

Ez a témakör szolgál kiegészítő információkkal a Védett socket réteg (SSL) protokollok alapjairól.

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 adatsere bizalmasságát és integritását.

## 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.

### Kapcsolódó fogalmak

“Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok” oldalszám: 14

Ez a témakör írja le az i5/OS megvalósítás által támogatott SSL és TLS protokollváltozatokat.

## 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 V5R2 és újabb OS/400, illetve az i5/OS kiadásokban a CPU-nak az SSL kézfogásból adódó többletterhelése elkerülhető egy kriptográfiai hardver beépítésével.

### Kapcsolódó tájékoztatás

Digitális igazolásokkal kapcsolatos alapelvek

## Támogatott SSL és Szállítási réteg biztonság (TLS) protokollok

Ez a témakör írja le az i5/OS megvalósítás által támogatott SSL és TLS protokollváltozatokat.

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 i5/OS megvalósítás az SSL és TLS protokolloknak az alábbi változatait támogatja:

- TLS 1.0
- SSL 3.0 kompatibilitással rendelkező TLS 1.0

### Megjegyzés:

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 rejtjelkészleteket 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* című dokumentumban.

A TLS elsődleges célja az SSL még biztonságosabbá tétele, illetve a protokoll pontos és teljes meghatározása. A TLS az SSL 3.0 változathoz 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).
- **Kiterjesztett pszeudorandom függvény (PRF):** A PRF végzi a kulcsadatok előállítását. A TLS esetén a HMAC határozza meg a PRF-et. A PRF két kivonat készítés algoritmust használ oly módon, hogy ez garantálja a biztonságot. Az egyik algoritmus feltörése esetén az adatokat még mindig védi a második algoritmus.
- **A 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 változatótól eltérően a TLS megkísérli a felhasználandó igazolás típusának meghatározását.
- **Specifikus riasztási üzenetek:** A TLS több és kifejezőbb riasztást határoz meg a szekció végpontjai által észlelt problémák jelzésére. A TLS emellett dokumentálja bizonyos riasztások kiküldését.

#### **Kapcsolódó fogalmak**

“Az SSL története” oldalszám: 13

Az Internetes biztonsággal kapcsolatos egyre szélesebb körben megfogalmazódott problémákra reagálva a Védett socket réteg (SSL) protokollt a Netscape fejlesztette ki 1994-ben.

#### **Kapcsolódó tájékoztatás**

A TLS protokoll

## **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 (LDAP) szerver

---

## **Az SSL bevezetésének tervezése**

Ez a témakör tárgyalja az SSL bevezetésének előfeltételeit az iSeries szerveren, és ír le néhány hasznos tippet ezzel kapcsolatban.

#### **Kapcsolódó fogalmak**

“SSL hibaelhárítás” oldalszám: 17

Az alábbi nagyon alapszintű hibaelhárítási információk segítségével leszűkítheti az iSeries szerveren az SSL használatával kapcsolatban fellépő lehetséges problémák körét.

## SSL előfeltételek

- IBM Digitális igazolás kezelő (DCM), az i5/OS (5722-SS1) 34. termékopciója.
- 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.
- Az SSL kézfogási feldolgozás felgyorsítása érdekében célszerű lehet egy kriptográfiai hardver beszerzése is. Kriptográfiai hardver használata esetén telepíteni kell a 35. termékopciót is, a Cryptographic Service Provider szoftvert.

### **Kapcsolódó tájékoztatás**

Kriptográfiai hardver

## Digitális igazolások

A digitális igazolások kezelésére használható megoldás az IBM Digitális igazolás kezelője (DCM).

### **Kapcsolódó tájékoztatás**

Nyilvános és magán igazolások

A Digitális igazolás kezelő beállítása

---

## Alkalmazások biztonságossá tétele SSL segítségével

Ez a témakör sorolja fel az iSeries szerver SSL segítségével biztonságossá tehető alkalmazásainak listáját.

Az SSL segítségével az alábbi iSeries szerver alkalmazások tehetők biztonságossá:

- Vállalati azonosság leképezés (EIM)
- FTP szerver
- HTTP szerver (Apache alapú)
- iSeries Access for Windows
- Címtár (LDAP) szerver
- 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.

### **Kapcsolódó fogalmak**

“Példahelyzet: A Kezelőközpont szerver összes kapcsolatának biztonságossá tétele az SSL segítségével” oldalszám: 5

Ez a példahelyzet írja le, hogyan használható az SSL egy iSeries szerver összes kapcsolatának biztonságossá tételére.

### **Kapcsolódó tájékoztatás**

Vállalati azonosság leképezés

FTP szerver biztonságossá tétele SSL segítségével

HTTP szerver



Védett socket réteg (SSL) adminisztráció (iSeries Access for Windows témakör)

Telnet példahelyzet: Biztonságos Telnet

Védett Socket API

---

## 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, csak egyszerű irányvonalakat nyújt a legáltalánosabb problémák megoldásához.

Ellenőrizze, hogy teljesülnek-e a következők:

- Az iSeries szerver megfelel az SSL előfeltételeknek.
- 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. 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 keresztshivatkozásai 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.

### Kapcsolódó fogalmak

“Az SSL bevezetésének tervezése” oldalszám: 15

Ez a témakör tárgyalja az SSL bevezetésének előfeltételeit az iSeries szerveren, és ír le néhány hasznos tippet ezzel kapcsolatban.

### Kapcsolódó tájékoztatás


Szerviz és támogatás

Védett Socket API hibakód üzenetek

---

## A Védett socket réteg (SSL) protokollhoz kapcsolódó információk



### Webhelyek

- RFC 2246: "The TLS Protocol Version 1.0"  (<ftp://ftp.isi.edu/in-notes/rfc2246.txt>)

Ez a hely nyújt részletes leírást a TLS protokollról.

- RFC2818: "HTTP Over TLS"  (<ftp://ftp.isi.edu/in-notes/rfc2818.txt>)

Ez a hely írja le a TLS használatát az Interneten folyó HTTP kapcsolatok biztonságossá tételére.

- A The SSL Protocol Version 3.0 című dokumentum  (<http://home.netscape.com/eng/ssl3/ssl-toc.html>)  
Ez a hely magyarázza el részletekbe menően az SSL 3.0 változatát.
- Az SSL Encryption explained című dokumentum  (<http://www.digicert.com/ssl>)  
Ez a hely nyújt áttekintést az SSL titkosításról, különös tekintettel az igazolásokra.

## Egyéb információk

- Az SSL és a Java védett socket kiterjesztése
- IBM Toolbox for Java

## PDF fájlok mentése

A PDF mentése a munkaállomásra megjelenítés vagy nyomtatás céljából:

1. Kattintson a jobb egérgombbal a PDF fájlra a böngészőjében (kattintás a jobb oldali egérgombbal a fenti hivatkozásra).
2. Kattintson a PDF helyi mentésére szolgáló opcióra.
3. Válassza ki azt a könyvtárat, ahová menteni kívánja a PDF fájlt.
4. Kattintson a **Mentés** gombra.

## Adobe Acrobat Reader letöltése

A PDF állományok megtekintéséhez vagy nyomtatásához telepített Adobe Acrobat Reader programra van szükség.

Ingyenes példányát letöltheti az Adobe honlapjáról ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .



---

## Nyilatkozatok

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.

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

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba saját 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 106-0032, 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 "JELENLEGI FORMÁJÁBAN", 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 YBWA

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.

A dokumentumban tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat az IBM az IBM Vásárlói megállapodás, az IBM Nemzetközi programlicenc szerződés, az IBM Gépi kódra vonatkozó licencszerződés vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban található 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 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 információkat az IBM a termékek szállítóitól, az általuk közzétett bejelentésekből, illetve egyéb nyilvánosan elérhető forrásokból szerezte be. 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.

A közzétett árak az IBM által javasolt aktuális kiskereskedelmi árak, amelyek előzetes bejelentés nélkül bármikor változhatnak. Az egyes forgalmazók árai eltérhetnek ezektől.

A leírtak csak tervezési célokat szolgálnak. Az információk a tárgyalt termékek elérhetővé válása előtt megváltozhatnak.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

Szerzői jogi licenc:

A kiadvány forrásnyelvi alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, marketing célból, illetve olyan alkalmazási programok terjesztése céljából, amelyek megfelelnek azon operációs rendszer alkalmazásprogram illesztőjének, ahol a példaprogramot írta. Ezek a példák nem kerültek minden körülmények között tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, szervizelhetőségüket, de még a programok funkcióit sem.

Jelen példaprogramok minden másolatának, leszármazottjának vagy kódrészletének tartalmaznia kell a következő szerzői jogi megjegyzést:

© (cégnév) (évszám). A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak. © Copyright IBM Corp. (évszám vagy évszámok). Minden jog fenntartva.

Ha az információkat elektronikus formában tekinti meg, akkor elképzelhető, hogy a fotók és a színes ábrák nem jelennek meg.

---

## Védjegyek

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

DRDA  
i5/OS  
IBM  
iSeries  
OS/400

Az Intel, az Intel Inside (logók), az MMX, és a Pentium az Intel Corporation védjegyei 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.

A Java, valamint minden Java alapú kifejezés a Sun Microsystems, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

A Linux Linus Torvalds védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX a The Open Group bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

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

---

## Feltételek

A kiadványok használata az alábbi feltételek és kikötések alapján lehetséges.

**Személyes használat:** A kiadványok másolhatók személyes, nem kereskedelmi célú használatra, de valamennyi tulajdonosi feljegyzést meg kell tartani. Az IBM kifejezett engedélye nélkül nem szabad a kiadványokat vagy azok részeit terjeszteni, megjeleníteni, illetve belőlük származó munkát készíteni.

**Kereskedelmi használat:** A kiadványok másolhatók, terjeszthetők és megjeleníthetők, de kizárólag a vállalaton belül, és csak az összes tulajdonosi feljegyzés megtartásával. Az IBM kifejezett hozzájárulása nélkül nem készíthetők olyan munkák, amelyek a kiadványokból származnak, továbbá nem másolhatók, nem terjeszthetők és nem jeleníthetők meg, még részben sem, a vállalaton kívül.

A jelen engedélyben foglalt, kifejezetten megadott hozzájáruláson túlmenően a kiadványokra, illetve a bennük található információkra, adatokra, szoftvekre vagy egyéb 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, A SZABÁLYOSSÁGRA ÉS AZ ADOTT CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁKAT IS.







Nyomtatva Dániában