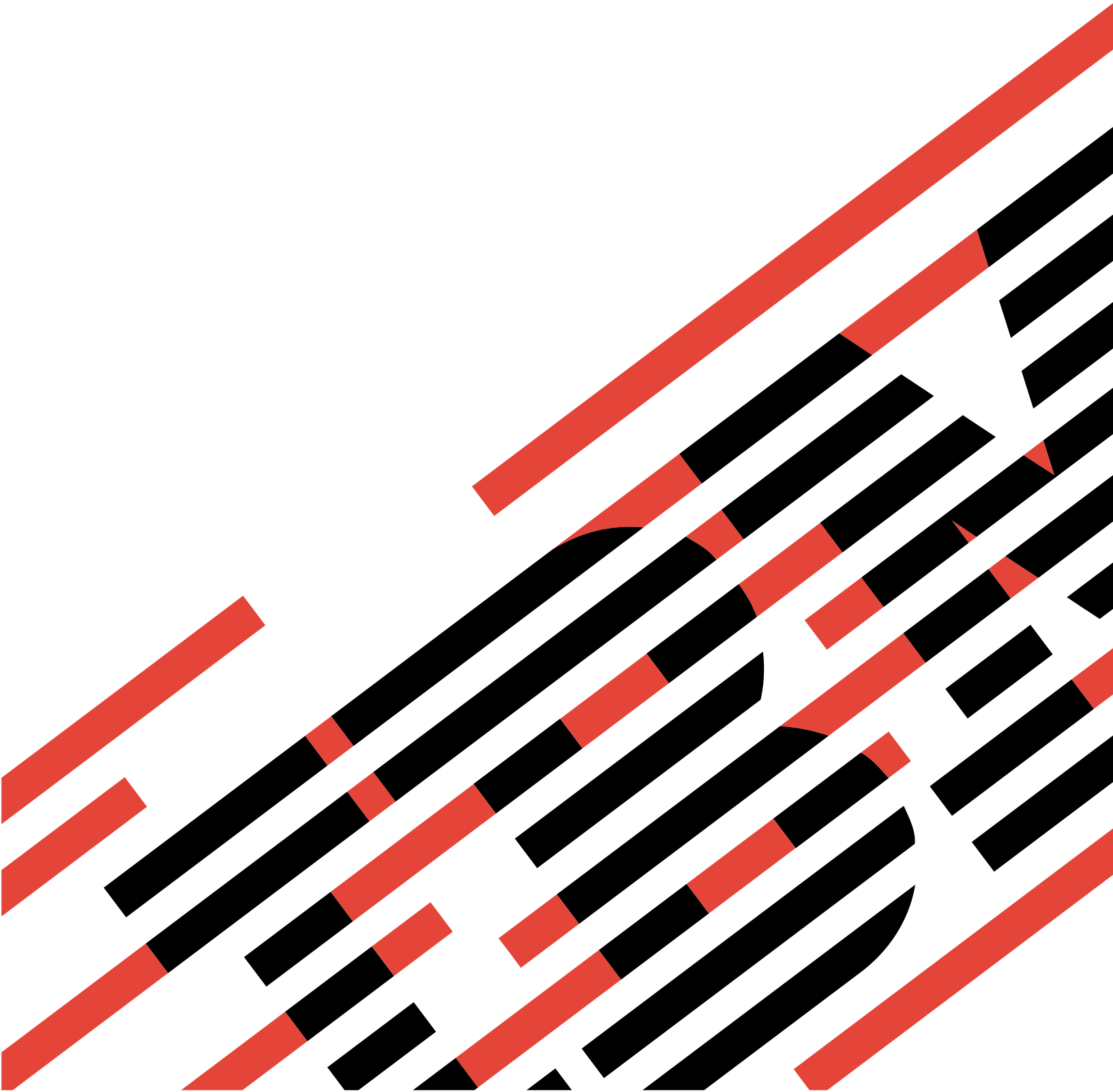
IBM

eserver

iSeries

Védett socket réteg (SSL)



IBM

@server

iSeries

Védett socket réteg (SSL)

© Szerzői jog IBM Corporation 2000, 2002. Minden jog fenntartva

Tartalom

© Szerzői jog IBM 2000, 2002

Rész 1. Védett socket réteg (SSL)

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

- **A V5R2 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**
  További információk, amelyekből ismereteket szerezhet a Védett socket réteget (SSL) felépítő technológiákról.
- **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.

© Szerzői jog IBM 2000, 2002

Fejezet 1. A V5R2 kiadás újdonságai

A V5R2M0 kiadásban rendelkezésre áll az iSeries 2058 kriptográfiai gyorsító tartozék. Ez a kriptográfiai hardvertartozék az iSeries szerver SSL teljesítményét hivatott növelni. További információkat a kriptográfiai hardver szakaszban talál róla.

Új Globális biztonsági eszközkészlet (GSKit) alkalmazásprogram illesztő (API)

Rendelkezésre áll egy új OS/400 Globális biztonsági eszközkészlet (GSKit) API, a gsk_secure_soc_startInit(). További információkat a Globális biztonságos eszközkészlet (GSKit) API-k témakörben talál.

A kiadás további újdonságairól és változásairól a Felhasználói feljegyzés

című cikkben olvashat.

Új vagy megváltozott információk elkülönítése

A technikai változásokon keresztülment helyeket az Információs központ az alábbiak szerint jelöli:

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

© Szerzői jog IBM 2000, 2002

Fejezet 2. A témakör nyomtatása

A dokumentum PDF változata letölthető megjelenítési vagy nyomtatási céllal. Ehhez válassza ki az Alkalmazások biztonságossá tétele SSL segítségével hivatkozást (megközelítőleg 215 KB vagy 34 oldal).

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 a könyvtárat, amelybe a PDF fájlt menteni kívánja.
4. Kattintson a **Mentés** gombra.

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)  .

© Szerzői jog IBM 2000, 2002

Fejezet 3. SSL példahelyzetek

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

- Példahelyzet: Biztonságos Kezelőközpont
- Példahelyzet: Biztonságos FTP
- Példahelyzet: Biztonságos Telnet
- Példahelyzet: Az iSeries SSL teljesítményének növelése
- Példahelyzet: Magánkulcsok védelme kriptográfiai hardverrel

SSL példahelyzet: Biztonságos Kezelőközpont

Helyzet

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 vállalat biztonsági szakértője, István az iSeries navigátorba épített Kezelőközpontot használja a központ iSeries szerverének (központi rendszer) eléréséhez. István a központi rendszer és a végpont rendszerek közötti összes kapcsolatot biztonságossá szeretné tenni.

Részletek

Az iSeries navigátor Kezelőközpont technológiájával István az összes végpont rendszert a központi rendszerről tudja kezelni. A Kezelőközpont SSL kapcsolatban használatával István a rendszerek kezelését **biztonságosan** tudja végezni. Ahhoz, hogy az SSL használható legyen a Kezelőközponttal, Istvánnak biztosítania kell az iSeries Access for Windows illetve az iSeries navigátor és a számítógépe közötti kapcsolatot.

A Kezelőközpont környezetben Istvánnak ehhez kétféle hitelesítési szint áll rendelkezésére:

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. A szerver hitelesítési szintnél magasabb biztonsági szintű megoldásnak tekinthető. 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.

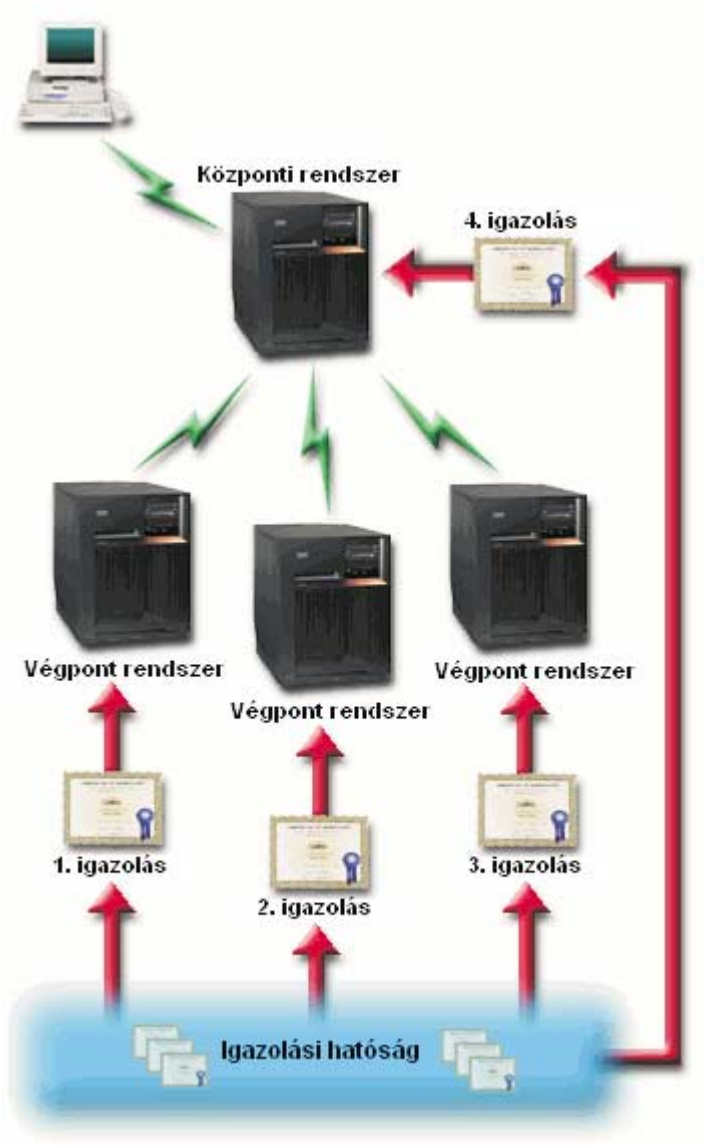
Más alkalmazásoktól eltérően a Kezelőközpont emellett ellenőrzési lista (más néven Megbízható csoport ellenőrzési lista) alapján is végezhet hitelesítést. Az ellenőrzési lista általában felhasználó

© Szerzői jog IBM 2000, 2002

azonosítási és hitelesítési információkat, például jelszavakat, személyi azonosítószámokat vagy digitális igazolásokat tartalmaz. A hitelesítési információk tárolás természetesen titkosított.

A legtöbb alkalmazás általában nem alkalmazza együtt a szerver és kliens hitelesítést. Ez azért van így, mert a szerver hitelesítésére szinte mindig 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 a központi rendszer a végpont rendszerekhez csatlakozik, akkor pedig kliens. 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

Az SSL támogatással rendelkező Kezelőközpont beállításához Istvánnak az alábbi adminisztrációs és konfigurációs feladatokat (lásd az ábrát: SSL által védett Kezelőközpont nagy kiterjedésű hálózaton (WAN)) kell elvégeznie:

1. A Kezelőközponttal használt iSeries szervernek teljesítenie kell az SSL előfeltételek szakaszban felvázolt SSL előfeltételeket.
2. A központi rendszernek és az összes végpont iSeries szervernek az OS/400 V5R2 kiadását kell futtatnia. A V5R1 kiadás használata esetén telepíteni kell az alábbi OS/400 (5722-SS1) javításokat:
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. Az iSeries navigátort futtató PC kliensnek az iSeries Access for Windows V5R2 változatával kell rendelkeznie. Ha a kliens a V5R1 változatot használja, akkor telepíteni kell az iSeries Access for Windows (5722-XE1) V5R1 kiadásának SI01907 jelű (vagy újabb) javítócsomagját. További információkat a V5R1 Információs központ: ″Kezelőközpont biztonságossá tétele″ című témakörében talál.
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 íratni 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, amely alapján az iSeries Access for Windows kliensek azonosíthatják azt.
   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. Ismételje 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.
   b. Töltse le az igazolási hatóságnak otthont adó rendszerről a hatóság igazolását.

Megjegyzés: Ha a használt igazolási hatóság gyökér igazolása nem található meg az iSeries Access for Windows kliensek kulcsadatbázisában, akkor ezt az SSL használatához hozzá kell adni az adatbázishoz.

Konfigurációs lépések

Mielőtt az SSL használható lenne a Kezelőközponthoz, telepíteni kell az előfeltétel programokat és be kell állítani a digitális igazolásokat az iSeries szerveren. A folytatás előtt nézze meg a példahelyzet Előfeltételek és feltételezések szakaszát. Az előfeltételek teljesülésekor a Kezelőközpont SSL támogatásának beállítása az alábbi eljárással történik.

Megjegyzés: Ha az SSL engedélyezett az iSeries navigátorban, akkor ezt le kell tiltani a Kezelőközpont SSL támogatásának engedélyezése előtt. Ha az SSL az iSeries navigátorhoz engedélyezett, de a Kezelőközponthoz nem, akkor a Kezelőközpontból kezdeményezett kapcsolatok meghiúsulnak a Kezelőközpont központi rendszerével.

Szerver hitelesítés (kötelező) esetén:

1. Központi rendszer beállítása szerver hitelesítésre
2. Végpont rendszerek beállítása szerver hitelesítésre

Kliens hitelesítés (nem kötelező) esetén:

Megjegyzés: A kliens hitelesítés konfigurálása nem végezhető el a szerver hitelesítés beállításának befejezésig.

1. Központi rendszer beállítása kliens hitelesítésre
2. Végpont rendszerek beállítása kliens hitelesítésre

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 hitelesítéssel kapcsolatos beállításokat a kliens hitelesítés beállításai előtt kell elvégezni.

1. Az iSeries navigátorban kattintson a jobb egérgombbal a **Kezelőközpont** kategóriára, majd válassza az előugró menü **Tulajdonságok** menüpontját.
2. Kattintson a **Biztonság** lapra, majd jelölje meg a **Védett socket réteg (SSL) használata** választógombot.
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.

Végpont rendszerek beállítása szerver hitelesítésre

A központi rendszer szerver hitelesítésének engedélyezése után az engedélyezést a végpont rendszereken is el kell végezni. A végpont rendszerek SSL használatának és szerver hitelesítésének beállításához tegye a következőket:

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 (SSL) használata beállítás értéke **Igen**.
   - Az SSL hitelesítési szint beállítás értéke **Szerver**.

   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. **Indítsa újra a központi rendszer Kezelőközpont szerverét:**
   a. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
   b. Bontsa ki a központi rendszert.
   c. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
   d. 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.
   e. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.
4. **Indítsa újra a Kezelőközpont szervert minden végpont rendszeren:**
   a. Bontsa ki az újraindításban érintett végpont rendszert.
   b. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
   c. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját.
   d. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.
   e. Ismételje meg az eljárást minden végpont rendszernél.
5. **Aktiválja az iSeries navigátor ügynök SSL támogatását:**
   a. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
   b. Kattintson a jobb egérgombbal a központi rendszerre, majd válassza az előugró menü **Tulajdonságok** menüpontját.
   c. Kattintson az **SSL** lapra, majd válassza ki a **Védett socket réteg (SSL) kapcsolat használata** beállítást.
   d. Lépjen ki az iSeries navigátorból, majd indítsa el újra.

A szerver hitelesítéssel kapcsolatos beállítások befejeződtek. Most már sor kerülhet a nem kötelező kliens hitelesítés beállítására:

- Központi rendszer beállítása kliens hitelesítésre
- Végpont rendszerek beállítása kliens hitelesítésre

A kliens hitelesítés a végpont rendszereket és a központi rendszert is ellenőrzi az igazolási hatóság és a megbízható csoport alapján.

Központi rendszer beállítása kliens hitelesítésre

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.

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.

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. Lásd a Management Central: A Smart Way to Manage AS/400 Systems

   című V4R4 vörös könyvet.

   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 (SSL) használata beállítás értéke **Igen**.
      - Az SSL hitelesítési szint beállítás értéke **Kliens és szerver**.

      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.
2. **Másolja át az ellenőrzési listát a végpont rendszerekre:**
   a. Az iSeries navigátorban bontsa ki a **Kezelőközpont → elemet**.
   b. Kattintson a jobb egérgombbal a **Csomag** elemre, majd válassza az előugró menü **Új meghatározás** menüpontját.
   c. 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/QUSRSYS.LIB/QYPSVLDL.VLDL elérési utat.

d. Kattintson a **Beállítások** lapra, majd jelölje ki a **Meglévő fájl felülírása az átküldött fájllal** választógombot.
e. Kattintson a **Továbbiak** gombra.
f. A **További beállítások** ablakban engedélyezze az objektum különbségeket a visszaállítás során.
g. Kattintson az **OK** gombra a meghatározások listájának frissítéséhez, vagyis az új csomag megjelenítéséhez.
h. Kattintson a jobb egérgombbal a csomagra, majd válassza az előugró menü **Küldés** menüpontját.
i. A **Küldés** párbeszédablakban adja hozzá a megbízható csoportot, távolítsa el az összes többit, majd kattintson az **OK** gombra. A Megbízható csoport az eljárás első lépésében meghatározott rendszercsoport.

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.

3. **Indítsa újra a központi rendszer Kezelőközpont szerverét:**
   a. Az iSeries navigátorban bontsa ki a **Kapcsolatok** nézetet.
   b. Bontsa ki a központi rendszert.
   c. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
   d. 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.
   e. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.
4. **Indítsa újra a Kezelőközpont szervert minden végpont rendszeren:**

   Megjegyzés: Ismételje meg az eljárást minden végpont rendszernél.
   a. Bontsa ki az újraindításban érintett végpont rendszert.
   b. Bontsa ki a **Hálózat → Szerverek** kategóriát, majd válassza ki a **TCP/IP** bejegyzést.
   c. Kattintson a jobb egérgombbal a **Kezelőközpont** elemre, majd válassza az előugró menü **Leállítás** menüpontját.
   d. A Kezelőközpont szerver leállása után kattintson az **Indítás** gombra az újraindításához.

Fejezet 4. SSL 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. Bár az SSL eredetileg a web böngésző és a szerver közötti kommunikációt volt hivatott biztosítani, a meghatározása más alkalmazások (például Telnet vagy FTP) is lehetővé teszi a felhasználását. 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. Általában a szerver hitelesítésére kerül sor, választhatóan azonban hitelesíthető a kliens is. A végpontoknak vagy az SSL kapcsolatot megvalósító alkalmazásoknak kioszthatói 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 kiadásban a CPU-nak az SSL kézfogásból adódó többletterhelése elkerülhető egy kriptográfiai hardver beépítésével.

© Szerzői jog IBM 2000, 2002

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 megvalósítás az SSL és TLS protokolloknak 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, amely tartalmaz bizonyos óvintézkedéseket az időzítési támogatások ellen, illetve az SHA1 kivonatkészítési 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

Az SSL 3.0 változatán alapuló Szállítási réteg biztonság (TLS) protokoll 1.0 változata a legújabb ipari szabvány SSL protokoll. A 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 biztonságosabbnak tekinthető az SSL 3.0 változatában használt Üzenet hitelesítési kódnál (MAC).
- **Bővített pszeudorandom függvény (PRF)**
  A kulcs adatok előállításához a TLS a Bővített pszeudorandom függvényt (PRF) használja. A TLS protokollban a PRF használata a HMAC algoritmussal együtt történik. A PRF két kivonatkészítés 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, és 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 (eredeti)
- IBM HTTP Server (Apache alapú)
- FTP szerver
- Telnet szerver
- Kezelőközpont végpont rendszer
- Címtár szolgáltatások (LDAP)

Fejezet 5. 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 V5R2M0 kiadásban az iSeries szerverhez az alábbi kriptográfiai hardvertartozékok állnak rendelkezésre:
  - 2058 kriptográfiai gyorsító (hardvertartozék kód: 4805)
  - 4758 kriptográfiai társprocesszor (hardvertartozék kód: 4801 vagy 4802)

  Kriptográfiai hardver telepítésekor telepíteni kell a 35. opciót is, a Cryptographic Service Provider terméket.

Ha az SSL-t bármilyen iSeries Access for Windows termékkel vagy az IBM Toolbox for Java összetevővel kívánja használni, akkor telepíteni kell az iSeries Client Encryption (128 bites, 5722-CE3) terméket is. A termékre az iSeries Access for Windows programnak van szüksége 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.

© Szerzői jog IBM 2000, 2002

Fejezet 6. Alkalmazások biztonságossá tétele SSL segítségével

Az SSL segítségével az alábbi iSeries szerver alkalmazások tehetők biztonságossá:

- IBM HTTP Server for iSeries (eredeti)
- IBM HTTP Server for iSeries (Apache alapú)
- FTP szerver
- Telnet szerver
- Osztott relációs adatbázis architektúra (DRDA) és Osztott adatkezelés (DDM) szerver
- Kezelőközpont
- Címtár szolgáltatások szerver (LDAP)
- Vállalati azonosság leképezés (EIM)
- iSeries Access for Windows alkalmazások, beleértve az iSeries navigátort
- Az iSeries Access for Windows alkalmazásprogram illesztőinek (API) felhasználásával írt alkalmazások
- A Developer Kit for Java segítségével fejlesztett programok, illetve az IBM Toolbox for Java terméket használó kliens 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.

© Szerzői jog IBM 2000, 2002

Fejezet 7. 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 az iSeries szerveren, akkor próbálkozzon meg a következőkkel:

- A szerver hibanaplójában 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 kereszthivatkozásai nélkül:
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.SSL

  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.

© Szerzői jog IBM 2000, 2002

Fejezet 8. 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.
- A Java védett socket réteg (JSSL) oldal rövid leírást biztosít a JSSL-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.

© Szerzői jog IBM 2000, 2002

Nyomtatva Dániában