

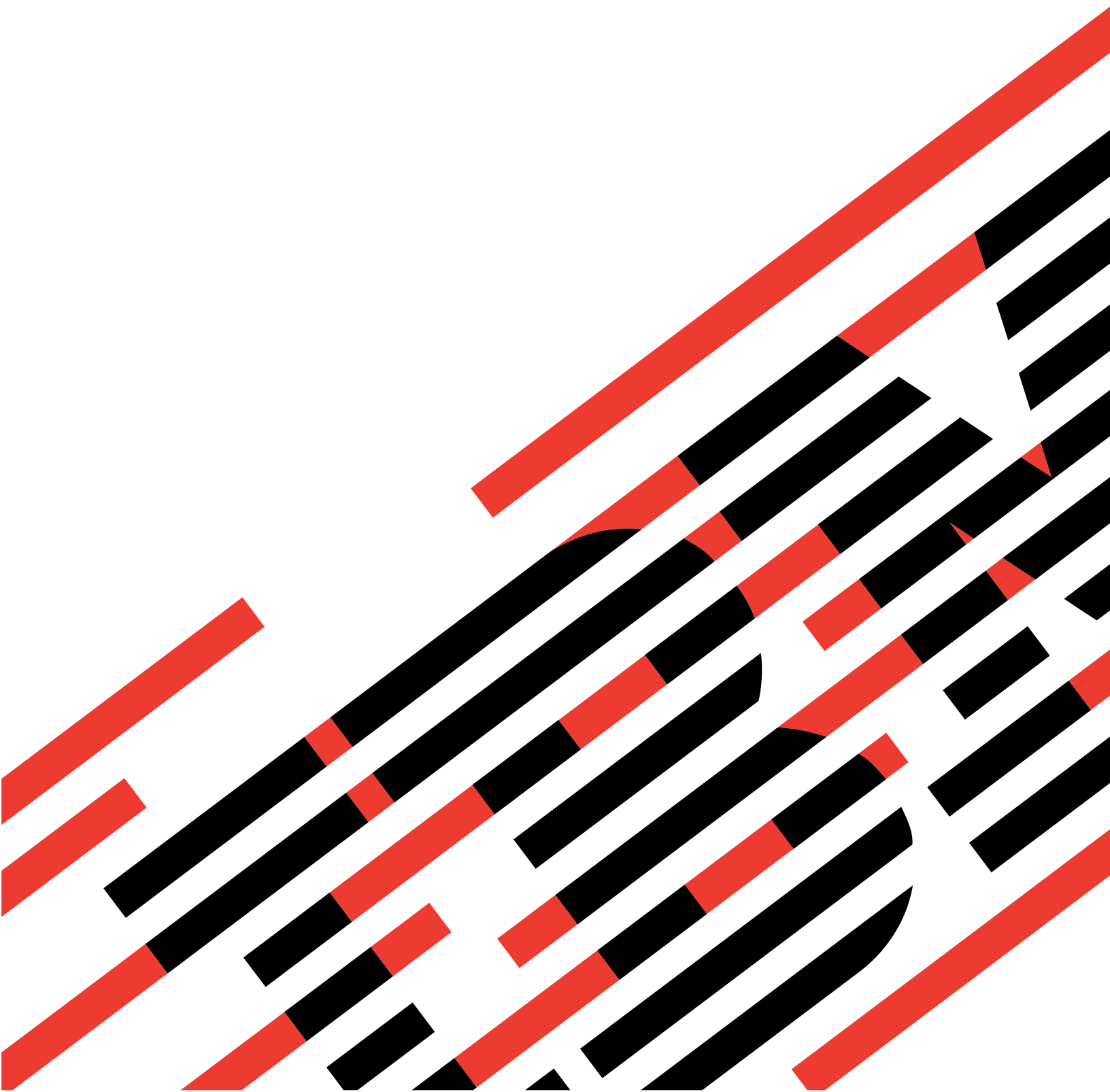
IBM

@server

iSeries

Telnet

Versiunea 5 Ediția 3





@server

iSeries

Telnet

Versiunea 5 Ediția 3

Notă

Înainte de a folosi aceste informații și produsul la care se referă, aveți grijă să citiți “Observații”, la pagina 95.

Ediția a șasea (august 2005)

Această ediție este valabilă pentru IBM Operating System/400 (număr de produs 5722-SS1) Versiunea 5, Ediția 3, Modificarea 0 și pentru toate edițiile și modificările următoare, până când se specifică altceva în noile ediții. Această versiune nu rulează pe toate modelele RISC și nici pe modelele CISC.

© Copyright International Business Machines Corporation 1998, 2005. Toate drepturile rezervate.

Cuprins

Telnet.	1	INIT0100: Formatul informației de descriere a dispozitivelor	43
Tipăriți acest subiect	2	INIT0100: Formatul informației de descriere a conexiunii	44
Scenarii Telnet	2	Program de ieșire pentru terminare dispozitiv	46
Scenariu Telnet: Configurarea serverului Telnet	2	Exemple de programe de ieșire Telnet	46
Scenariu Telnet: Sesiuni Telnet în cascadă	4	Gestionarea clientului Telnet.	47
Scenarii de procesare a cererilor sistem	5	Controlul funcțiilor server Telnet de pe client.	48
Folosirea unui job de grup	7	Sesiunile client Telnet 5250	49
Scenariu Telnet: Securizarea Telnet cu SSL.	9	Pornirea unei sesiuni client Telnet 5250	49
Detalii de configurare	11	Sesiunile client Telnet 3270	51
Planificarea serverului Telnet	15	Pornirea unei sesiuni client Telnet 3270	51
Descrierile de dispozitiv virtual	15	Considerații 3270 tot-ecranul	52
Securitate Telnet	16	Folosirea unei stații de afișare	53
Împiedicarea accesului Telnet	16	Maparea tastaturii 3270 pentru serverele Telnet	54
Controlul accesului Telnet	17	Sesiunile client Telnet VTxxx	56
Configurarea serverului Telnet	20	Pornirea unei sesiuni client Telnet VTxxx	56
Pornirea serverului Telnet	20	Considerații VTxxx tot-ecranul	58
Setarea numărului de dispozitive virtuale	21	Opțiuni de emulare VTxxx	61
Configurarea automată a dispozitivelor virtuale	21	Valorile tastelor VTxxx	62
Crearea propriilor dumneavoastră dispozitive virtuale	22	Suportul pentru limba națională VTxxx	67
Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare	23	Modul național VTxxx	67
Setarea parametrului păstrare-în-viață al sesiunii	24	Tastatura numerică	69
Asocierea de dispozitive la subsisteme	24	Editarea keypad	71
Activarea subsistemului QSYSWRK	25	Valorile tastelor VTxxx prin funcția 5250	72
Crearea profilurilor de utilizator.	25	Moduri de operare ale stațiilor de lucru VT220	76
Tipurile de emulare suportate de iSeries ^(TM)	25	Tastele funcționale din linia de sus la VT220	76
Configurarea serverului Telnet pentru modul 5250 tot-ecranul	26	Cuvinte Cheie Caractere de Control la VT100 și VT220	77
Configurarea serverului Telnet pentru modul eran plin 3270	26	Stabilirea unei sesiuni Telnet în cascadă	78
Tipurile de terminal 3270 suportate	28	Trecerea între sesiunile Telnet în cascadă	78
Configurarea serverului Telnet pentru modul VTxxx tot-ecranul	28	Terminarea unei sesiuni client Telnet	79
Securizarea Telnet cu SSL	31	Depanarea problemelor Telnet	80
Configurarea SSL pe serverul Telnet	31	Determinarea problemelor cu Telnet	80
Înlăturarea restricțiilor de port	31	Ping către serverul dumneavoastră gazdă	83
Asignarea unui certificat serverului Telnet.	32	Depanarea tipurilor de emulare	83
Activarea autentificării de client pentru serverul Telnet (pas opțional)	33	Depanarea serverului Telnet SSL	85
Activare SSL pe serverul Telnet.	35	Verificarea stării sistemului	85
Inițializare și dialog de confirmare (handshake) SSL	35	Verificarea existenței unui ascultător SSL activ	86
Gestionarea serverului Telnet	36	Verificarea istoricului jobului Telnet	86
Configurarea sesiunilor de imprimare Telnet	36	Coduri de retur SSL	87
Necesitățile pentru sesiunile de imprimantă Telnet	37	Ieșiri ale programului serviciu TRCTCPAPP	89
Terminarea sesiunii server	38	Materialele necesare pentru raportarea problemelor Telnet	92
Terminare joburi Device Manager	38	Informații de diagnoză generate automat	93
Utilizarea programelor punct de ieșire Telnet	38	Informații înrudite despre Telnet	93
Program de ieșire inițializare dispozitiv	40		
Formatul punctului de ieșire Telnet INIT0100: Grup de parametri necesari	41		
INIT0100: Formatul informației de descriere a utilizatorului	42		
		Anexa. Observații	95
		Mărci comerciale	96
		Termeni și condiții pentru descărcarea și tipărirea informațiilor	97
		Informații de declinare a responsabilității pentru cod	97

Telnet

Telnet este un protocol care vă permite să vă conectați la un calculator la distanță și să îl folosiți ca și cum ați fi direct conectat la el în cadrul rețelei locale. Mașina (de obicei un PC) sau sistemul în fața căruia vă aflați fizic este clientul Telnet. Serverul Telnet este calculatorul de la distanță la care este atașat clientul. TCP/IP iSeries^(TM) suportă atât clientul, cât și serverul Telnet.

Una dintre cele mai importante funcții din Telnet este abilitatea de a negocia transmisia de fluxuri de date între client și server. Acest tip de negociere permite atât clientului, cât și serverului să inițieze o cerere sau să onoreze o cerere.

Sunt disponibile câteva tipuri diferite de emulări pentru negocierea acestor cereri și convertirea lor într-o ieșire. Pentru Telnet iSeries, tipul preferat este emularea 5250. Telnet iSeries suportă de asemenea tipul de stații de lucru 3270 și VTxxx, precum și modurile de suport pentru imprimantă RFC 2877 (TN5250E). În continuare este prezentată o introducere în Telnet, care vă furnizează informații ajutătoare pentru administrarea Telnet pe serverul dumneavoastră iSeries.

Notă: Citiți Declinarea responsabilității pentru exemplul de cod pentru informații juridice importante.

Tipăriți acest subiect

Dacă doriți să citiți aceste informații de pe hârtie, puteți tipări întregul subiect ca fișier PDF.

Scenarii Telnet

Acest subiect furnizează exemple de utilizare Telnet pentru a introduce conceptele de bază și operațiile de configurare.

Planul pentru serverul Telnet

Acest subiect explică cum să determinați numărul dispozitivelor virtuale pentru a fi asociate cu stațiile de lucru care sunt conectate la sistemul dumneavoastră. Furnizează de asemenea proceduri de securitate pentru controlul sau împiedicarea accesului la Telnet.

Configurarea serverului Telnet

Acest subiect explică cum se configurează serverul Telnet pentru suportul mai multor tipuri de emulatoare.

Gestionarea serverului Telnet

Acest subiect descrie cum să lucrați cu serverul dumneavoastră Telnet și să folosiți programele de ieșire pentru a controla accesul utilizatorilor.

Gestionarea clientului Telnet

Acest subiect vă furnizează pași pentru a porni o sesiune client Telnet folosind tipuri diferite de emulări. Această secțiune explică cum să stabiliți o sesiune Telnet cascadată.

Depanarea problemelor Telnet

Găsirea de indicii și instrucțiuni pentru depanarea serverului Telnet, tipuri de emulări și SSL.

Informații înrudite

Găsiți legături către alte informații despre Telnet.

Tipăriți acest subiect

Pentru a vizualiza sau pentru a descărca versiunea PDF, selectați Telnet (aproximativ 728 KB).

Salvarea fișierelor PDF

Pentru a salva un PDF pe stația dumneavoastră de lucru în scopul vizualizării sau tipăririi

1. Faceți clic dreapta pe PDF în browser-ul dumneavoastră (faceți clic dreapta pe legătura de mai sus).
2. Faceți clic pe **Save Target As...**
3. Navigați în directorul în care doriți să salvați fișierul PDF.
4. Faceți clic pe **Save**.

Descărcarea programului Adobe Acrobat Reader

Dacă aveți nevoie de Adobe Acrobat Reader pentru a vizualiza sau tipări aceste PDF-uri, puteți descărca o copie de la situl web Adobe (www.adobe.com/products/acrobat/readstep.html)



Scenarii Telnet



Următoarele scenarii Telnet furnizează exemple pentru a vă ajuta să înțelegeți cum să configurați și să folosiți Telnet.

Configurarea serverului Telnet

În acest scenariu, un administrator configurează un server Telnet.

Sesiuni Telnet în cascadă

Acest scenariu demonstrează abilitatea de porni sesiuni Telnet în timp ce sunteți încă într-o sesiune Telnet. O dată conectat, puteți trece între sisteme folosind valorile SysReq (cerere sistem). **Securizarea Telnet cu SSL**

Puteți utiliza SSL pentru a proteja Telnet pe iSeries^(TM). Acest scenariu furnizează un exemplu de configurare pas cu pas.



Scenariu Telnet: Configurarea serverului Telnet



Situație și obiective

Ken Harrison este administratorul unui nou server iSeries^(TM) pentru Culver Pharmaceuticals. El trebuie să configureze serverul Telnet pentru a îndeplini următoarele specificații:

- Permitearea a până la 100 de dispozitive virtuale pentru a fi create automat.
- Afișarea întotdeauna a ecranului de semnare.
- Restricționarea utilizatorilor privilegiați la anumite dispozitive.
- Limitarea fiecărui utilizator la o sesiune de dispozitiv.

Cerințe preliminare și supoziții

Listati cerințele dumneavoastră sau supozițiile despre echipamentul utilizatorilor, starea curentă sau locația într-un proces mai mare care trebuie să fie îndeplinit pentru folosirea acestui scenariu.

- Culver Pharmaceuticals folosește un server iSeries la Versiunea 5 Ediția 2.
- TCP/IP-ul este configurat.
- Ken are autorizare IOSYSCFG.

Detalii de configurare

1. Pornirea unui server Telnet

- Expandati **serverul dumneavoastră iSeries** → **Rețea** → **Servere** → **TCP/IP**.
- În panoul din dreapta, localizați **Telnet** în coloana Nume server.
- Confirmați că apare **Pornit** în coloana Stare.
- Dacă serverul nu rulează, faceți clic dreapta pe **Telnet** și selectați **Pornire**.

2. Setarea numărului de dispozitive virtuale

- În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, → **Configurare și service** → **Valori sistem**.
- În panoul din dreapta, faceți clic dreapta pe **Dispozitive** și selectați **Proprietăți**.
- În pagina **Valori sistem dispozitive**, activați **Dispozitive Pass-through și TELNET** și setați **Numărul maxim de dispozitive** la 100.

3. Configurarea proprietăților serverului Telnet

- În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, → **Rețea** → **Servere** → **TCP/IP**.
- În panoul din dreapta, faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.

Faceți clic pe această fișă...	Și...
Semnare în sistem	Selectați: <ul style="list-style-type: none"> • Restricționare utilizatori privilegiați la anumite dispozitive. • Limitarea fiecărui utilizator la o sesiune de dispozitiv.
Semnare la distanță	Specificați numărul încercărilor de semnare permise și acțiunea care să fie luată dacă se atinge numărul maxim de încercări.
La distanță	Selectați opțiunea Afișarea întotdeauna a semnării pentru Folosire Telnet pentru semnarea de la distanță .
Timeout	Specificați acțiunea care să fie luată când joburile ajung la timeout. Puteți specifica de asemenea cât timp să acordați unei operații înainte ca jobul să intre în timeout. Puteți specifica informații atât pentru joburile inactive, cât și pentru cele deconectate.

Notă:

Aceste setări se aplică tuturor dispozitivelor inactive și joburilor pe serverul dumneavoastră iSeries, nu doar pentru Telnet.

4. Asocierea dispozitivelor la subsisteme

- La interfața în mod text, introduceți:
ADDWSE SBS(D(QINTER) WRKSTNTYPE(*ALL)

5. Activarea subsistemului QSYSWRK

Verificarea stării subsistemului QSYSWRK:

- În interfața caracter a serverului iSeries, introduceți **WRKSBS** (Work with active subsystems - Gestionare subsisteme active).
- Verificați că sunt afișate următoarele sisteme:
 - QSYSWRK

- QINTER
- QSPL

Dacă subsistemul QSYSWRK nu este activ, efectuați următorii pași:

- În interfața caracter a serverului iSeries, introduceți STRSBS (Start subsystem - Pornire subsistem).
- Introduceți QSYSWRK pentru descrierea de subsistem și QSYS pentru bibliotecă, apoi apăsați pe **Enter**.
- Repețiți pentru Nume subsistem **QINTER** cu Biblioteca **QSYS** și pentru Nume subsistem **QSPL** și Biblioteca **QSYS**.

6. Crearea profilurilor de utilizator Telnet

- Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries**.
- Faceți clic dreapta pe **Utilizatori și grupuri** și selectați **Utilizator nou**.
- Introduceți numele utilizatorului, descrierea și parola.
- Pentru a specifica descrierea unui job, faceți clic pe **Joburi** și introduceți descrierea jobului.
- Faceți clic pe **OK**.

7. Verificați dacă funcționează Telnet-ul

Ken pornește o sesiune de emulare 5250 și se conectează la serverul Telnet.

Subiecte înrudite

Pentru mai multe informații despre această procedură, faceți referire la:

Configurarea serverului Telnet
Tipurile de emulare suportate de iSeries



Scenariu Telnet: Sesiuni Telnet în cascadă

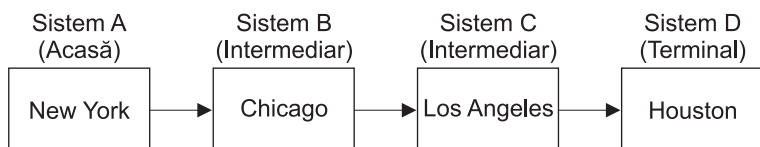


În acest scenariu, utilizatorul stabilește sesiuni Telnet cu mai multe servere. Aceasta este cunoscută ca **sesiuni Telnet în cascadă**. Folosind această metodă, acesta va putea să:

- Stabilească o sesiune Telnet între biroul de acasă și Chicago.
- Se conecteze la servere Telnet suplimentare fără a termina sesiunea inițială.
- Comute între sesiuni pentru a se întoarce la un job pe sistemul din New York.

Situație și obiective

Janice Lowe este director de marketing la Culver Pharmaceuticals. Ea se conectează de la biroul din New York și accesează sistemul principal din Chicago folosind Telnet. O dată ce Janice a stabilit o sesiune client cu serverul Telnet din Chicago, ea realizează că are nevoie să lucreze cu unele fișiere de la biroul din Los Angeles. Janice folosește clientul Telnet din Chicago pentru a se conecta la serverul Telnet din Los Angeles. În timp ce este conectată la Los Angeles, ea decide să stabilească o sesiune cu Houston.



RZAIW513-1

Această imagine înfățișează conexiunile pe care le face Janice. Serverul iSeries^(TM) pe care l-a pornit din New York se numește sistem principal. De aici, ea se conectează la sistemul intermediar B din Chicago, apoi se conectează la sistemul intermediar C din Los Angeles, care se conectează la sistemul terminal D din Houston.

Detalii

Acest scenariu face următoarele supoziții:

- Serverul Telnet rulează pe toate sistemele.
- Janice are o semnătură pe toate sistemele.
- Toate sistemele sunt servere iSeries pe care rulează V4R5 sau o versiune mai nouă.

Janice efectuează următorii pași pentru a se conecta la sistemele Telnet:

1. De la sistemul din New York, introduce STRTCPTLN CHICAGO.
2. Pe sistemul din Chicago, introduce STRTCPTLN LA.
3. Pe sistemul din Los Angeles, introduce STRTCPTLN HOUSTON.

O dată ce ea s-a conectat la sistemul din Houston, ea dorește să efectueze o operație pe sistemul (de bază) din New York.

1. Apasă tasta **SysReq (Cerere sistem)**.
2. Selectează opțiunea 14 (Transfer la sistemul de bază). Aceasta o întoarce la jobul alternativ de pe sistemul din New York.

O dată ce a terminat lucrul pe sistemul din New York, ea se poate întoarce pe sistemul din Houston astfel:

1. Apasă tasta **SysReq (Cerere sistem)**.
2. Selectează opțiunea 15 (Transfer la sistemul terminal). Această operație o mută de pe orice sistem intermediar sau de bază pe sistemul terminal.

Pentru a închide toate sesiunile, ea folosește comanda SIGNOFF. Aceasta închide sesiunea curentă și o întoarce la ecranul de semnare al sistemului de bază.

Subiecte înrudite

Pentru detalii suplimentare despre sesiunile Telnet în cascadă și exemple de sesiuni în cascadă mult mai complexe, faceți referire la următoarele subiecte:

- Procesarea cererii sistem conține scenarii pentru alte sisteme în cascadă.
- Folosirea unui job de grup descrie folosirea joburilor alternative și a joburilor de grup pentru a lucra cu mai multe sisteme.
- Stabilirea unei sesiuni în cascadă furnizează informații suplimentare despre stabilirea sesiunilor în cascadă.
- Mutarea între sesiuni Telnet în cascadă conține valorile SysReq (cerere sistem) pentru lucrul cu mai multe sesiuni.

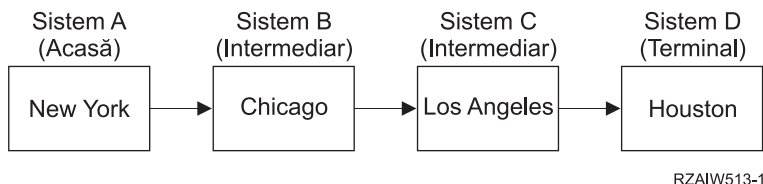


Scenarii de procesare a cererilor sistem

Următoarele scenarii explică cum lucrează procesarea cererilor sistem cu tipuri multiple de sisteme.

Scenariul 1

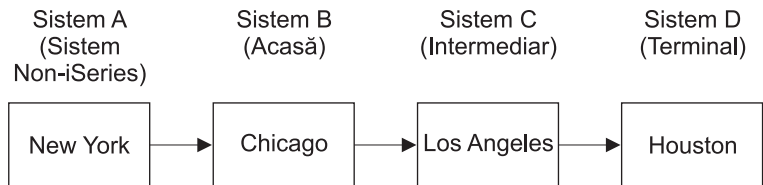
Toate serverele sunt servere iSeries^(TM). Procesarea cererii sistem lucrează normal.



RZAIW513-1

Scenariul 2

Sistemul din New York este un server non-iSeries care folosește 3270 sau VTxxx Telnet.

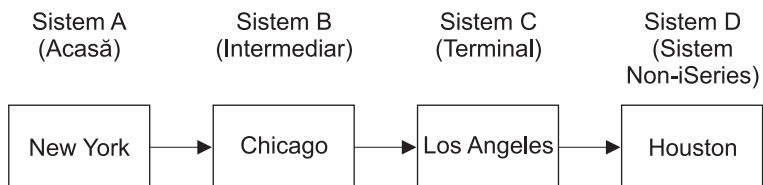


RZAIW516-1

Procesarea cererii sistem lucrează ca primul scenariu cu excepția considerării Chicago ca sistem gazdă. Toate cererile sistem trimise sistemului gazdă se procesează pe sistemul Chicago.

Scenariul 3

Sistemul din Houston este un server non-iSeries care folosește 3270 sau VTxxx Telnet.

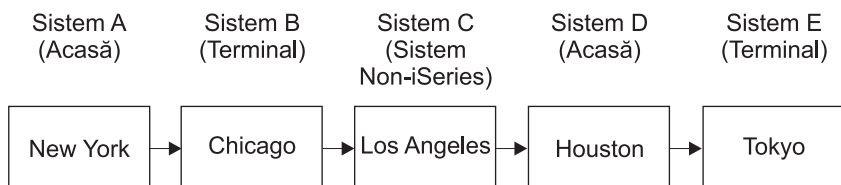


RZAIW517-1

Procesarea cererii sistem lucrează ca primul scenariu cu excepția considerării Los Angeles ca sistem terminal pentru toată procesarea cererii sistem. Dacă apăsați tasta SysReq (Cerere sistem) și apoi apăsați tasta Enter, va fi afișat meniul Cerere sistem pentru Los Angeles.

Scenariul 4

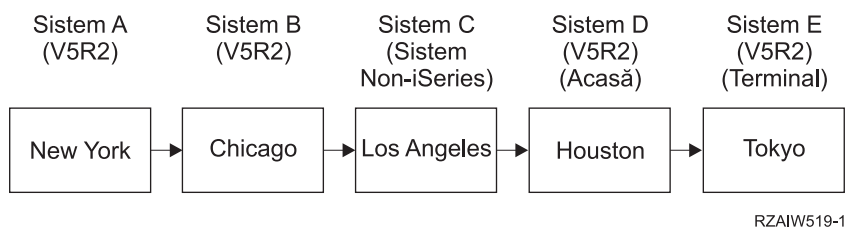
Sistemul Los Angeles este un server non-iSeries care folosește 3270 sau VTxxx Telnet.



RZAIW518-1

Procesarea cererii sistem lucrează ca primul scenariu cu excepția considerării Chicago ca sistem terminal pentru procesarea cererii sistem. Dacă apăsați tasta SysReq (Cerere sistem) și apoi apăsați tasta Enter, va fi afișat meniul Cerere sistem pentru Chicago Angeles.

Dacă vreți să trimiteți o cerere sistem sistemului din Tokio, puteți mapa o tastă funcțională de pe sistemul de la Houston la tasta SysReq (Cerere sistem). Dacă mapați această funcție, atunci sistemul Tokio este sistemul terminal, iar sistemul Houston este sistemul gazdă.



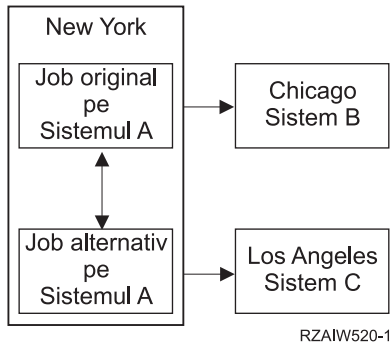
Ca exemplu al acestei funcții de mapare pentru un server Telnet iSeries 3270, maparea implicită de tastatură identifică tasta SysReq (Cerere sistem) ca o tastă 3270 PF11. Pentru un client Telnet iSeries 3270, tasta F11 este mapată tastei 3270 PF11. Dacă sistemul Los Angeles este un sistem care folosește flux de date 3270, apoi apăsând F11 se mapează pe tasta SysReq (cerere sistem) de pe sistemul de la Houston. Cererea sistem este transmisă sistemului de la Tokyo și este afișat meniul Cerere sistem pentru sistemul Tokyo.

Notă:

Această funcție de mapare este complexă în special dacă folosiți flux de date VTxxx și mapați între blocuri de date și date caracter.

Folosirea unui job de grup

Puteți folosi Telnet și jobul alternativ pentru a vă conecta la diferite sisteme de la sistemul dumneavoastră de acasă. Considerați următorul exemplu:



Telnet stabilește o conexiune de la New York la Chicago. Vreți, de asemenea, să mergeți la sistemul din Los Angeles și să rămâneți conectați la sistemul din Chicago. Puteți porni un job alternativ pe sistemul din New York folosind opțiunea 11 din Cerere sistem. Folosiți comanda Telnet pentru a stabili o sesiune cu sistemul din Los Angeles. Puteți ajunge la alt sistem (Houston, de exemplu) pornind o altă sesiune Telnet de pe sistemul din Chicago sau de pe cel din Los Angeles.

O alternativă la folosirea jobului alternativ este folosirea unui job de grup. Un job de grup este unul din cele până la 16 joburi interactive care sunt asociate într-un grup cu același dispozitiv stație de lucru și același utilizator. Pentru a seta un job de grup, faceți următoarele:

1. Modificați jobul curent într-un job de grup utilizând comanda CHGGRPA (Change Group Attributes - Modificare attribute grup).
CHGGRPA GRPJOB(home)
2. Porniți un job de grup pentru sistemul din Chicago folosind comanda TFRGRPJOB (Transfer to Group Job - Transfer la jobul de grup).
TFRGRPJOB GRPJOB(CHICAGO) INLGRPPGM(QCMD)

3. Stabiliți o sesiune Telnet cu sistemul din Chicago.
Telnet CHICAGO
4. Întoarceți-vă în sistemul de acasă apăsând tasta ATTN. Apăsarea tastei ATTN vă arată meniul Send Telnet Control Functions (Trimitere funcții de control Telnet).
5. În interfața bazată pe caracter pentru meniul Trimitere funcții de control Telnet, introduceți:
TFRGRPJOB GRPJOB(home)
Aceasta vă întoarce la jobul dumneavoastră original.

Puteți porni la fel alte joburi de grup și sesiuni Telnet.

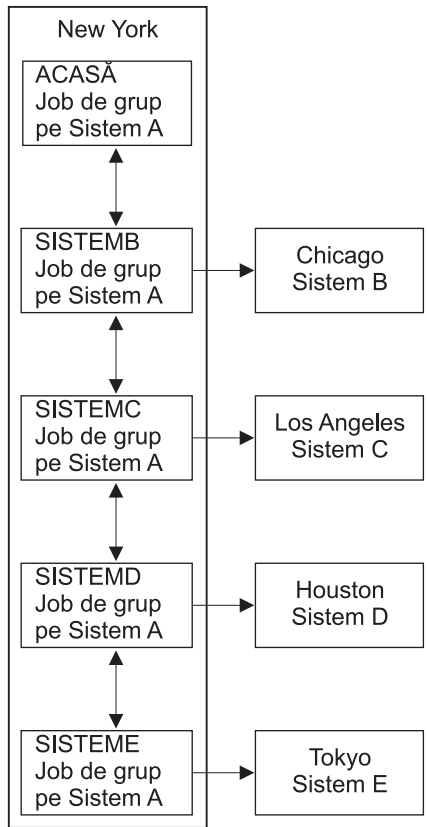
Puteți folosi comanda TFRGRPJOB GRPJOB(*SELECT) pentru a selecta care job de grup îl doriți. De exemplu, dacă joburile de grup cu numele CHICAGO, LOSANGELES, HOUSTON și TOKYO pornesc, comanda TFRGRPJOB GRPJOB(*SELECT) arată următorul ecran:

```

+-----+
|                                     Transfer la jobul de grup                                     |
|                                                                                               Sistem: SYS198                               |
| Job de grup activ. . . : HOME                                                                |
| Text . . . . . :                                     |
| Opțiune tip, apăsați Enter.                                                                |
|   1=Transfer la jobul de grup                                                                |
| -----Joburi de grup suspendate-----                                                    |
| Opț Job grup   Text                                                                           |
| -           TOKYO                                                                            |
| -           HOUSTON                                                                           |
| -           LOSANGELES                                                                       |
| -           CHICAGO                                                                           |
| Sfârșit      F3=Ieșire F5=Reîmprospătare F6=Pornire nou job de grup F12=Anulare           |
+-----+

```

Puteți folosi Telnet pentru a stabili o sesiune cu fiecare sistem de la jobul corepunzător. În continuare este un exemplu de scenariu job de grup:



RZAIW521-1

Descriere: Scenariu job de grup

Când vreți să terminați jobul de grup, folosiți comanda ENDGRPJOB.

Pentru a trece la alt job de grup în timpul unei sesiuni Telnet:

1. Apăsați tasta ATTN.
2. Introduceți TFRGRPJOB în interfața în mod text.

Scenariu Telnet: Securizarea Telnet cu SSL



Acest scenariu descrie cum să securizați Telnet cu SSL.

Situație

Bob este în cursul creării unei afaceri de brokeraj. El s-a retras din poziția lui de broker la o firmă comercială importantă și dorește să continue să ofere servicii de brokerage unui număr mic de clienți de la el de acasă. El își rulează afacerile pe un mic server iSeries^(TM), pe care i-ar plăcea să-l folosească pentru a furniza cont de acces pentru clienții lui prin sesiuni Telnet 5250. Bob lucrează pentru moment la o modalitate de a permite clienților lui acces continuu la conturile lor, astfel încât ei să poată să-și gestioneze acțiunile. Bob dorește ca clienții lui să folosească sesiuni Telnet 5250 pentru a-și accesa conturile, dar este îngrijorat pentru securitatea serverului, cât și pentru sesiunile clienților lui. După studierea opțiunilor de securitate Telnet ale serverului iSeries, Bob decide să folosească SSL pentru a asigura secretul datelor în sesiunile Telnet 5250 între serverul lui iSeries și clienții lui.

Obiective

În acest scenariu, Bob dorește să securizeze sesiunile Telnet 5250 ale clienților lui la conturile lor de pe serverul iSeries. Bob dorește să activeze SSL pentru a proteja integritatea datelor client pe măsură ce acestea sunt transmise prin Internet. El vrea de asemenea să activeze certificate pentru autentificarea clientului pentru a asigura că serverul lui verifică faptul că numai clienții lui accesează conturile lor. O dată ce Bob a configurat serverul Telnet pentru SSL și a activat autentificarea server și client, el poate spune această nouă opțiune de acces la conturi clienților lui, asigurându-i pe aceștia că sesiunile de acces la conturi vor fi în siguranță. O dată ce Bob a îndeplinit următoarele obiective, el poate spune această nouă opțiune de acces la conturi clienților lui, asigurându-i pe aceștia că sesiunile lor Telnet 5250 vor fi în siguranță:

- Securizarea serverului Telnet cu SSL
- Activarea serverului Telnet pentru autentificare clientului
- Obținerea unui certificat privat de la CA (Local Certificate Authority - Autoritatea de certificare locală) și asocierea acestuia serverului Telnet.

Detalii

Afacerea de brokeraj a lui Bob condusă de acasă

- Rularea serverului iSeries OS/400^(R) Versiunea 5 Ediția 2 (V5R2) și furnizarea contului de acces acționarului prin sesiuni Telnet 5250.
- Aplicația serverului OS/400^(R) Telnet este pornită pe serverul iSeries.
- Serverul Telnet inițializează SSL și verifică informația certificat în ID-ul aplicației QIBM_QTV_TELNET_SERVER.
- Dacă configurarea certificatului Telnet este corectă, serverul Telnet începe să asculte pe portul SSL conexiunile client.
- Un client inițiază o cerere pentru accesul la serverul Telnet.
- Serverul Telnet răspunde prin furnizarea certificatelor sale clientului.
- Software-ul client validează certificatul ca o sursă acceptabilă, de încredere în comunicarea cu serverul.
- Serverul Telnet cere un certificat de la software-ul client.
- Software-ul client prezintă un certificat serverului Telnet.
- Serverul Telnet validează certificatul și recunoaște dreptul clientului de a stabili o sesiune 5250 cu serverul.
- Serverul Telnet stabilește o sesiune 5250 cu clientul.

Cerințe preliminare și supoziții

Bob trebuie să se asigure că a îndeplinit următoarele cerințe ale acestui scenariu:

- Server iSeries pe care rulează OS/400 Versiunea 5 Ediția 2 (V5E2)
- TCP/IP-ul este configurat.
- Bob are autorizare IOSYSCFG.
- Serverul Telnet este configurat.
- Bob a tratat situațiile din Planificarea activării SSL.
- Bob a creat o Autoritate de certificare locală pe serverul lui iSeries.

Pașii operației

Sunt două seturi de operații pe care Bob trebuie să le efectueze pentru a implementa acest scenariu: Un set de operații îi permit să seteze serverul lui iSeries pentru a folosi SSL și să ceară certificate pentru autentificarea utilizatorului. Celălalt set de operații permite utilizatorilor pe clienții Telnet să participe în sesiuni SSL cu serverul Telnet al lui Bob și să obțină certificate pentru autentificarea utilizatorului.

Bob realizează următorii pași pentru a completa acest scenariu:

Pași operațiilor pe serverul Telnet

Pentru a implementa acest scenariu, Bob trebuie să realizeze aceste operații pe serverul lui iSeries:

1. Înlăturarea restricțiilor de port (page 11)
2. Crearea și operarea Autorității de certificare locală (page 11)
3. Configurarea serverului Telnet pentru a cere certificate pentru autentificarea clientului (page 12)
4. Activarea și pornirea SSL pe serverul Telnet (page 13)

Pașii operației de configurare client

Pentru a implementa acest scenariu, fiecare utilizator care va accesa serverul Telnet pe serverul iSeries al lui Bob trebuie să realizeze aceste operații:

5. Activarea SSL pe clientul Telnet (page 13)
6. Activarea clientului Telnet pentru a prezenta certificat pentru autentificare (page 14)

Aceste operații realizează ambele autentificări client și SSL prin certificate, rezultând în accesul securizat SSL la informațiile contului pentru clienții lui Bob care folosesc sesiuni Telnet 5250.



Detalii de configurare

Urmați următorii pași de operație pentru Securizarea Telnet cu SSL.

Pasul 1: Înlăturați restricțiile de port

Înainte de V5E1, restricțiile de port au fost utilizate deoarece suportul SSL (Secure Sockets Layer) nu a fost disponibil pentru Telnet. Acum puteți specifica dacă să pornească SSL, non-SSL sau ambele. Prin urmare, nu mai este nevoie de restricțiile de port. Dacă ați definit restricții de port în edițiile anterioare, va trebui să înlăturați restricțiile de port pentru a putea folosi parametrul SSL.

Pentru a determina dacă aveți restricții de port Telnet și să le înlăturați pentru a putea configura serverul Telnet pentru a folosi SSL, urmați acești pași:

1. Pentru a vizualiza orice restricții curente de port, porniți Navigator iSeries^(TM) și expandați serverul dumneavoastră de rețea **iSeries** —> .
2. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Proprietăți**.
3. Faceți clic pe fișa **Restricții port** pentru a vedea o listă a setărilor restricțiilor de port.
4. Selectați restricția de port pe care doriți să o înlăturați.
5. Faceți clic pe **Înlăturare**.
6. Faceți clic pe **OK**

Implicit setarea este să se pornească sesiunile SSL pe portul 992 și sesiunile non-SSL pe portul 23. Serverul Telnet folosește intrarea tabelă de serviciu pentru Telnet pentru a obține portul non-SSL și Telnet-SSL pentru a obține portul SSL.

Pasul 2: Creare și operare Autoritate de certificare locală

Pentru a folosi Managerul de certificare digitală (Digital Certificate Manager - DCM) pentru a crea și opera o CA locală pe serverul iSeries, urmați acești pași:

1. Porniți DCM.
2. În cadrul de navigare al DCM, selectați **Crearea unei Autorități de certificare (CA)** pentru a se afișa o serie de formulare. Aceste formulare vă ghidează prin procesul de creare a unei CA locale și de completare a altor operații necesare pentru a începe folosirea certificatelor digitale pentru SSL, semnarea obiectelor, verificarea semnăturii.

3. Completați toate formularele care sunt afișate. Este un formular pentru fiecare din operațiile pe care este nevoie să le realizați pentru a putea crea și opera o CA locală pe serverul iSeries. Completarea acestor formulare vă permite să:
- Alegeți cum să memorați cheia privată pentru certificatul CA local. Acest pas este inclus doar dacă aveți un Coprocesor IBM^(R) 4758-023 PCI Cryptographic instalat pe sistemul dumneavoastră iSeries. Dacă sistemul dumneavoastră nu are un coprocesor criptografic, DCM memorează automat certificatul și cheia lui primară în depozitul de certificate CA local.
 - Furnizează identificarea informațiilor pentru CA local.
 - Instalați certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră. Aceasta permite software-ului să recunoască CA local și să valideze certificatele emise de CA.
 - Alege politica de date pentru CA-ul dumneavoastră local.
 - Folosiți noul CA local pentru a lansa un certificat client sau server pe care aplicațiile îl pot folosi pentru conexiunile SSL. Dacă aveți un Coprocesor Criptografic IBM^(R) 4758-023 PCI instalat pe serverul iSeries, acest pas vă permite să selectați modul de stocare a cheii private pentru certificatul serverului sau a clientului. Dacă sistemul nu are un coprocesor, DCM va plasa automat certificatul și cheia privată în depozitul de certificate *SYSTEM. DCM creează depozitul de certificate *SYSTEM ca parte a acestei operații.
 - Selectați aplicațiile care pot folosi certificatul client sau server pentru conexiuni SSL. Notă: Fți siguri că ați selectat application ID pentru serverul OS/400^(R) Telnet (QIBM_QTV_TELNET_SERVER).
 - Folosiți noul CA local pentru a lansa un certificat de semnare obiect pe care aplicațiile îl pot folosi pentru a însemna digital obiectele. Aceasta creează depozitul de certificate *OBJECTSIGNING, pe care îl folosiți pentru a gestiona certificatele de semnare obiect. Notă: Deși acest scenariu nu folosește certificatele de semnare obiect, asigurați-vă că ați completat acest pas. Dacă anulați în acest punct, operația se termină și trebuie să realizați operații separate pentru a termina configurarea certificatului dumneavoastră SSL.
 - Selectați aplicațiile care doriți să folosească CA-ul local. Notă: Asigurați-vă că selectați ID-ul aplicației pentru Serverul Telnet OS/400 (QIBM_QTV_TELNET_SERVER).

O dată ce ați completat aceste formulare pentru această operație ghidată, puteți configura Serverul Telnet pentru a cere autentificarea clientului.

Pasul 3: Configurarea serverului Telnet pentru a cere certificatelor autentificarea clientului

Pentru a activa acest suport, administratorul de sistem va indica cum se lucrează cu suportul SSL. Folosiți fișa General din Proprietăți Telnet din Navigator iSeries pentru a indica dacă suportul pentru SSL, non-SSL sau pentru ambele va porni la pornirea serverului Telnet. Implicit, suporturile SSL și non-SSL pornesc întotdeauna.

Administratorul de sistem are posibilitatea de a indica dacă sistemul cere autentificare client SSL pentru toate sesiunile Telnet. Când SSL este activ și sistemul cere autentificarea clientului, prezența unui certificat client valid înseamnă că clientul este de încredere.

Pentru a configura serverul Telnet pentru a cere certificatelor autentificarea clientului, urmați acești pași:

1. Porniți DCM.
2. Faceți clic pe **Selectare memorie certificat**.
3. Selectați *SYSTEM ca memorie certificat pentru a fi deschisă și apăsați pe **Continuare**.
4. Introduceți parola corespunzătoare pentru depozitul de certificate *SYSTEM și faceți clic pe **Continuare**.
5. Când meniul navigabil din stânga se reîncarcă, selectați **Gestiune aplicații** pentru a afișa o listă de operații.
6. Selectați operația **Actualizare definiție aplicație** pentru a afișa o serie de formulare.
7. Selectați aplicație **Server** și faceți clic pe **Continuare** pentru a afișa o listă de aplicații server.
8. Din lista de aplicații, selectați **Server Telnet TCP/IP OS/400**.
9. Faceți clic pe **Actualizare definiție aplicație**.
10. În tabelul care este afișat, selectați **Da** pentru a cere autentificarea clientului.

11. Faceți clic pe **Aplicare**. Pagina **Actualizare definiție aplicație** este afișată cu un mesaj pentru a confirma modificările dumneavoastră.
12. Faceți clic pe **Terminare**.

Acum că ați configurat serverul Telnet pentru a cere certificatelor autentificarea clientului, puteți activa și porni SSL pentru serverul Telnet.

Pasul 4: Activare și pornire SSL pe serverul Telnet

Pentru a activa SSL pe serverul Telnet, urmați acești pași:

1. Deschideți Navigator iSeries.
2. Expandați **Serverul meu iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
3. Faceți clic dreapta pe **Telnet**.
4. Selectați **Proprietăți**.
5. Selectați fișa **General**.
6. Alegeți una din aceste opțiuni pentru suportul SSL:
 - **Numai securizat**
Selectați aceasta pentru a permite numai sesiunile SSL cu serverul Telnet.
 - **Numai non-securizat**
Selectați aceasta pentru a interzice sesiunile securizate cu serverul Telnet. Încercările de semnare la un port SSL nu se vor conecta.
 - **Atât securizat, cât și non-securizat**
Permite ambele sesiuni securizate și non-securizate cu serverul Telnet.

Pentru a porni serverul Telnet folosind Navigator iSeries, urmați acești pași:

1. Expandați **serverul dumneavoastră iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
2. În panoul din dreapta, localizați **Telnet** în coloana Nume server.
3. Confirmați că apare **Pornit** în coloana Stare.
4. Dacă serverul nu rulează, faceți clic dreapta pe **Telnet** și selectați **Pornire**.

Pasul 5: Activare SSL pe clientul Telnet

Pentru a participa într-o sesiune SSL, clientul Telnet trebuie să fie capabil să recunoască și să accepte certificatul pe care îl prezintă serverul Telnet pentru a stabili sesiunea SSL. Pentru a autentifica certificatul serverului, clientul Telnet trebuie să aibă o copie a certificatului Autoritate de certificare (Certificate Authority - CA) în baza de date chei iSeries. Când serverul Telnet folosește un certificat din CA-ul local, clientul Telnet trebuie să obțină o copie a certificatului CA local și să îl instaleze în baza de date chei iSeries.

Pentru a adăuga un certificat CA local dintr-un iSeries astfel încât clientul Telnet să poată participa în sesiunile SSL cu serverele Telnet care folosesc un certificat din CA-ul local, urmați acești pași:

1. Deschideți Navigator iSeries.
2. Faceți clic dreapta pe numele sistemului dumneavoastră.
3. Selectați **Proprietăți**.
4. Selectați fișa **Secure Sockets**.

Notă:

Această fișă nu va apărea decât dacă ați efectuat o instalare selectivă a Clientului de criptare iSeries (128-biți), 5722-CE3.

5. Faceți clic pe **Descărcare**. Aceasta va descărca automat certificatul Autoritate de certificare iSeries în baza de date chei a certificatului.

6. Vi se va cere parola dumneavoastră pentru baza de date chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, **ca400**. Este afișat un mesaj de confirmare. Apăsați **OK**.

Butonul de descărcare actualizează automat baza de date chei PC IBM^(R) Toolbox pentru Java^(TM).

Pasul 6: Activare client Telnet pentru a prezenta certificat pentru autentificare

Ați configurat SSL pentru serverul Telnet, ați specificat că serverul trebuie să folosească certificatele emise de CA-ul local și ați specificat să se ceară cerificate pentru autentificarea clientului. Acum, utilizatorii trebuie să prezinte un certificat client valid și de încredere serverului Telnet pentru fiecare încercare de semnare.

Clienții trebuie să folosească CA local pentru a obține un certificat pentru autentificare la serverul Telnet și trebuie să importe acel certificat la baza de date IBM^(R) Key Management înainte ca clientul să se autentifice.

Mai întâi, clienții trebuie să folosească DCM pentru a obține un certificat utilizator urmând acești pași:

1. Porniți DCM.
2. În cadrul de navigare din stânga, selectați **Creare certificat** pentru a afișa o listă de operații.
3. Din lista de operații, selectați **Certificat utilizator** și faceți clic pe **Continuare**.
4. Completați formularul **Certificat utilizator**. Doar acele câmpuri marcate prin "Necesar" trebuiesc completate. Selectați **Continuare**.
5. În funcție de browser-ul pe care îl utilizați, vi se va cere să generați un certificat care va fi încărcat în browser-ul dumneavoastră. Urmăriți instrucțiunile furnizate de browser.
6. Când pagina **Creare certificat utilizator** se reîncarcă, faceți clic pe **Instalare certificat**. Aceasta va instala certificatul în browser.
7. Exportați certificatul pe PC-ul dumneavoastră. Trebuie să memorați certificatul într-un fișier protejat prin parolă.

Notă:

Se cer Microsoft^(R) Internet Explorer 5 sau Netscape 4.5 pentru utilizarea funcțiilor de exportare și importare.

După care, trebuie să importați certificatul în baza de date IBM^(R) Key Management pentru ca clientul Telnet să-l poată folosi pentru autentificare prin parcurgerea pașilor următori:

Trebuie să adăugați Autoritatea de certificare care a creat certificatul client în baza de date de chei a PC-ului, altfel importarea certificatului client nu va funcționa.

1. Faceți clic **Start** → **Programs** → **IBM^(R) iSeries^(TM) Access pentru Windows^(R)** → **Proprietăți iSeries Access pentru Windows**.
2. Selectați fișa **Secure Sockets**.
3. Faceți clic pe **IBM Key Management**.
4. Vi se va cere parola dumneavoastră pentru baza de date chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, **ca400**. Este afișat un mesaj de confirmare. Apăsați **OK**.
5. Din meniul derulant, selectați **Certificate personale**.
6. Faceți clic pe **Importare**.
7. În ecranul **Importare cheie**, introduceți numele fișierului și calea pentru certificat. Apăsați **OK**.
8. Introduceți parola pentru fișierul protejat. Aceasta este aceeași parolă pe care ați specificat-o când ați creat un certificat utilizator în DCM. Apăsați **OK**. Când certificatul a fost adăugat cu succes la certificatele dumneavoastră personale în IBM Key Management, puteți folosi emulatorul PC5250 sau orice altă aplicație Telnet.

Cu acești pași completați, serverul Telnet poate stabili o sesiune SSL cu clientul Telnet și serverul poate autentifica utilizatorul resurselor pe baza certificatului pe care îl prezintă clientul.

Planificarea serverului Telnet

Înainte de a configura serverul dumneavoastră Telnet, sunt câteva chestiuni de securitate și operaționale de care trebuie să Țineți seama. Trebuie să știți câte dispozitive virtuale vreți ca Telnet să creeze automat sau dacă vreți să vă creați propriile dispozitive virtuale. Numărul de dispozitive virtuale configurate automat afectează numărul de încercări de semnare permise. Un număr crescut de încercări de semnare crește șansele ca un utilizator neautorizat să capete accesul la serverul dumneavoastră. Puteți de asemenea dori să luați în considerare alte măsuri de securitate, cum ar fi ca serverul Telnet să detecteze conexiunile pierdute.

Descrierile de dispozitiv virtual

Citiți mai multe despre configurarea și numirea descrierilor de dispozitiv virtual.

Securitate Telnet

Acest subiect furnizează proceduri pentru securizarea Telnet pe serverul dumneavoastră.

Descrierile de dispozitiv virtual



Telnet folosește descrierile dispozitiv virtual pentru a păstra informațiile stației de lucru client pentru a deschide sesiuni Telnet. Un **dispozitiv virtual** este o descriere de dispozitiv utilizată pentru formarea unei conexiuni între un utilizator și o stație de lucru atașată fizic la un sistem aflat la distanță. Dispozitivele virtuale furnizează informații despre dispozitivul dumneavoastră fizic (ecran sau imprimantă) programelor de pe server. Serverul caută protocolul client/server de atașat pentru a specifica un dispozitiv virtual. Dacă serverul nu poate găsi dispozitivul virtual specificat, el caută un dispozitiv virtual desemnat într-un program de ieșire înregistrat. Dacă serverul nu poate găsi un dispozitiv virtual, el încearcă să potrivească o descriere de dispozitiv virtual cu un dispozitiv de un tip și model similare cu ale dispozitivului de pe sistemul local.

Convențiile de nume pentru dispozitivele și controlerile virtuale

Serverul Telnet utilizează convențiile următoare pentru denumirea controlerelor și dispozitivelor create automat conform standardelor OS/400^(R):

- Pentru controlerul virtual, serverul folosește numele QPACTL *nn*
- Pentru dispozitivele virtuale, serverul folosește numele QPADEV *xxxx*
- Pentru dispozitivele virtuale numite, serverul dă controlerelor virtuale numele QVIRCD *nnnn*

Notă:

- În conformitate cu regulile de denumire OS/400, controlerul virtual trebuie numit QPACTL *nn*, unde *nn* reprezintă numărul zecimal 01 sau mai mare.
- Dispozitivul virtual are numele QPADEV *xxxx*, unde *xxxx* este un caracter alfanumeric de la 0001 la *zzzzz*, excluzând vocalele.
- Trebuie să acordați profilului utilizator QTCP autorizarea la dispozitivele virtuale create de utilizator.
- Convențiile de denumire pot fi modificate pentru dispozitivele virtuale create automat folosind opțiunea *REGFAC din QAUTOVRT. Vedeți despre QAUTOVRT în subiectul Valori sistem pentru informații suplimentare.

Numai dispozitivele virtuale care sunt atașate la QPACTL *nn* contează ca număr pentru valoarea lui QAUTOVRT (QAUTOVRT= Valori sistem dispozitive - Număr maxim de dispozitive). Numărul de încercări de semnare permise crește o dată cu dispozitivele virtuale configurate automat. Numărul total de încercări de semnare este egal cu numărul de încercări de semnare la sistem permise, înmulțit cu numărul dispozitivelor virtuale care pot fi create. Valorile sistem de semnare definesc numărul încercărilor de semnare permise.

Serverul Telnet reutilizează dispozitivele virtuale care au fost create automat prin selectarea dispozitivelor virtuale de același tip și model. Când nu mai există corespondențe de tipuri și modele de dispozitiv, dar mai există dispozitive virtuale disponibile, atunci tipul și modelul dispozitivului vor fi modificate, astfel încât să corespundă dispozitivului client și modelului negociat. Acest lucru este adevărat atât pentru dispozitivele virtuale create automat (QPADEV xxx), cât și pentru dispozitivele virtuale numite.

Dacă alegeți să creați manual propriile dispozitive, ar trebui să stabiliți convențiile de numire ce vă vor permite să administrați ușor configurația dumneavoastră. Puteți selecta orice nume de dispozitive și de controlere, cu condiția ca numele să se conformeze regulilor de numire a obiectelor OS/400.

Pentru proceduri pentru crearea dispozitivelor virtuale, consultați Setarea numărului de dispozitive virtuale.



Securitate Telnet

Când invocați Telnet peste o conexiune TCP, trebuie să luați în considerare măsurile de protecție care să prevină sau să permită utilizatorului accesul la serverul iSeries^(TM) prin Telnet. De exemplu, trebuie să stabiliți limite și să controlați numărul de încercări de semnare de către utilizatori, precum și numărul de dispozitive la care se poate conecta un utilizator.

Pentru informații despre procedura de control al accesului utilizatorilor la Telnet, consultați aceste subiecte:

Împiedicarea accesului Telnet

Dacă nu plănuieți să folosiți serverul Telnet, utilizați pașii furnizați aici pentru a-l dezactiva. Aceasta va asigura că nu va fi folosit fără cunoștința dumneavoastră.

Controlul accesului Telnet

Acest subiect furnizează indicii pentru protejarea de probleme a serverului dumneavoastră Telnet.

Împiedicarea accesului Telnet



Dacă nu vreți ca oricine altcineva să utilizeze Telnet pentru accesarea serverului dumneavoastră iSeries^(TM), ar trebui să preveniți rularea serverului Telnet. Pentru a împiedica accesul Telnet la serverul dumneavoastră iSeries, efectuați operațiile de mai jos.

Prevenirea pornirii automate a Telnet

Pentru a împiedica joburile server Telnet să fie pornite automat când porniți TCP/IP, urmați acești pași:

1. În Navigator iSeries, expandați **serverul dumneavoastră iSeries** → **Rețea** → **Servere** → **TCP/IP**.
2. Faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.
3. Deselectați **Pornire la pornirea TCP/IP**.

Împiedicarea accesului la porturile Telnet

Pentru a împiedica pornirea Telnet și pentru a împiedica pe cineva să asocieze o aplicație utilizator, cum ar fi o aplicație socket, cu portul pe care iSeries îl folosește în mod normal pentru Telnet, efectuați următoarele:

1. În Navigator iSeries, expandați **serverul dumneavoastră iSeries** → **Rețea** → **Servere** → **TCP/IP**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Proprietăți**.
3. În fereastra **Proprietăți configurare TCP/IP**, faceți clic pe fișa **Restricții port**.
4. În pagina **Restricții port**, faceți clic pe **Adăugare**.
5. În pagina **Adăugare restricții port**, specificați următoarele:

- **Nume utilizator:** Specificați un nume de profil utilizator care este protejat în iSeries-ul dumneavoastră. (Un profil utilizator protejat este un profil utilizator care nu deține programe care adoptă autorizare și nu are o parolă care este cunoscută de ceilalți utilizatori.) Prin restricționarea portului la un anumit utilizator, excludeți automat toți ceilalți utilizatori.
- **Portul de pornire:** 23 (Pentru TELNET non-SSL) sau 992 (pentru TELNET SSL)
- **Portul de terminare:** 23 (pentru TELNET non-SSL) sau 992 (pentru TELNET SSL)
- **Protocol:** TCP

Notă:

Aceste numere de port sunt specificate în Gestionare intrări tabelă service (WRKSRVTBLE) la .telnet...și .telnet-ssl. Ele pot fi mapate la alte porturi decât 23 și 992. Repetați acest proces pentru fiecare port pe care doriți să-l restricționați. Internet Assigned Numbers Authority (IANA) furnizează informații despre asocierile de numere de port obișnuite.



6. Faceți clic pe **OK** pentru adăugarea restricției.
7. În pagina **Restricții port**, faceți clic pe **Adăugare** și repetați procedura pentru protocolul UDP.
8. Faceți clic pe **OK** pentru a salva restricțiile dumneavoastră de port și pentru a închide fereastra **Proprietăți Configurare TCP/IP**.
9. Restricția de port are efect data următoare când porniți TCP/IP. Dacă TCP/IP este activ când setați restricțiile de port, trebuie să opriți TCP/IP și să-l porniți din nou.



Controlul accesului Telnet



Următoarele sunt sugestii și considerente de securitate când doriți ca sistemul dumneavoastră să poată fi accesat de clienți Telnet:

Autentificare client

Serverul Telnet suportă autentificarea clientului în plus față de autentificarea server SSL care este suportată curent. Când este activat, serverul dumneavoastră Telnet iSeries^(TM) va autentifica atât certificatul serverului, cât și pe cel al clientului atunci când clienții Telnet se conectează la portul Telnet SSL. Clienții Telnet care nu trimit un certificat client valid la încercarea de conectare la portul SSL Telnet vor eșua la stabilirea unei sesiuni de imprimare sau afișare. Pentru V4R5, o descriere despre cum să porniți Autentificarea client SSL se găsește în PTF Cover Letter 5769-SS1-PTF SF61427. Începând cu V5E1, autentificarea client SSL poate fi activată sau dezactivată folosind DCM (Digital Certificate Manager).

Protejarea parolelor

Parolele Telnet nu sunt codate când sunt trimise între clientul tradițional și server. În funcție de metodele dumneavoastră de conexiune, sistemul dumneavoastră poate fi vulnerabil la parolele furate prin ascultarea liniei. Parolele Telnet sunt codate dacă sunt folosite negocierile TN5250E pentru a schimba o parolă codată. Într-un astfel de caz, panoul de semnare poate fi ocolit și nici o parolă nu este trimisă în text în clar prin rețea. Cu TN5250E este codată doar parola, SSL necesită codificarea întregului trafic.

Notă:

Monitorizarea unei linii folosind echipamente electronice este referită des ca **sniffing**.

Totuși, dacă folosiți serverul Telnet SSL și un client Telnet cu SSL activat, atunci toate tranzacțiile, inclusiv parolele, sunt codate și protejate. Portul SSL Telnet este definit în intrarea WRKSRVTBLE sub .Telnet-ssl. Limitarea numărului de încercări de semnare: Deși valoarea sistem QMAXSIGN se aplică la Telnet, veți reduce eficacitatea acestei valori

sistem dacă setați sistemul dumneavoastră pentru a configura automat dispozitivele virtuale. Când valoarea sistem QAUTOVRT are o valoare mai mare decât 0, utilizatorul Telnet fără succes se poate reconecta și atașa la un dispozitiv virtual nou creat. Aceasta poate continua până când se produce una din situațiile următoare:

- Toate dispozitivele virtuale sunt dezactivate și sistemul a depășit limita pentru crearea de noi dispozitive virtuale.
- Toate profilurile utilizator sunt dezactivate.
- Hacker-ul reușește să se semneze pe sistemul dumneavoastră.

Configurarea automată a dispozitivelor virtuale mărește numărul încercărilor Telnet care sunt disponibile.

Notă:

Pentru a ușura controlul dispozitivelor virtuale, veți dori să setați valoarea sistem QAUTOVRT la o valoare care este mai mare decât 0 pentru o perioadă scurtă de timp. Fie folosiți Telnet pentru a forța sistemul să creeze dispozitive, fie așteptați până când alți utilizatori au făcut ca sistemul să producă suficiente dispozitive virtuale. Setați apoi valoarea sistem QAUTOVRT la 0.

Îmbunătățirile Telnet furnizează o opțiune pentru limitarea numărului de încercări pe care un hacker le poate face pentru a intra în sistemul dumneavoastră. Puteți crea un program de ieșire pe care sistemul îl apelează ori de câte ori un client încearcă să pornească o sesiune Telnet. Programul de ieșire primește adresa IP a solicitantului. Dacă programul dumneavoastră vede o serie de cereri de la aceeași adresă IP într-o perioadă mică de timp, programul dumneavoastră poate lua anumite decizii, cum ar fi refuzarea cererilor viitoare de la această adresă și trimiterea unui mesaj în coada de mesaje QSYSOPR. "Privire generală asupra capacităților programului de ieșire Telnet" furnizează o prezentare a posibilităților programului de ieșire Telnet.

Notă:

Alternativ, puteți folosi programul dumneavoastră de ieșire Telnet pentru a furniza înregistrarea în istoric. Mai degrabă decât să aveți programul dumneavoastră care să ia deciziile despre eventualele încercări de pătrundere, puteți folosi posibilitatea de înregistrare în istoric pentru a monitoriza încercările de pornire de sesiuni Telnet.

Terminarea sesiunilor inactive

Sesiunile Telnet sunt incluse în procesarea sistemului pentru QINACTITV. Valoarea sistem QINACTMSGQ definește acțiunea pentru sesiunile Telnet interactive care sunt inactive când intervalul de timp de așteptare job inactiv expiră. Dacă QINACTMSGQ specifică faptul că jobul trebuie deconectat, sesiunea trebuie să suporte funcția de deconectare job. Altfel, jobul se va termina mai degrabă decât să fie deconectat. Sesiunile Telnet care continuă să folosească descrieri de dispozitiv care sunt numite QPADEVxxxx nu vor permite utilizatorilor să se deconecteze de la acele joburi. Deconectarea de la aceste joburi nu este permisă deoarece descrierea de dispozitiv la care un utilizator este reconectat nu poate fi precizată. Deconectarea unui job necesită aceeași descriere dispozitiv pentru utilizator când jobul este reconectat. Pentru informații suplimentare, faceți referire la Setarea parametrului de menținere în viață a unei sesiuni.

Limitarea încercărilor de semnare

Numărul permis de încercări de deschidere de sesiune Telnet se mărește dacă dețineți dispozitive virtuale configurate automat. Valorile sistem ale dispozitivelor din Navigator iSeries definesc numărul dispozitivelor virtuale pe care Telnet le poate crea.

Folosiți valorile sistem de semnare pentru a defini numărul încercărilor de semnare la sistem permise. Pentru instrucțiuni despre setarea acestei valori în Navigator iSeries, faceți referire la Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare..

Restricționarea profilurilor de utilizator puternice

Puteți folosi valoarea de sistem QLMTSECOFR pentru a restricționa utilizatorii cu autorizare specială *ALLOBJ sau *SERVICE. Utilizatorul sau QSECOFR trebuie să fie autorizat explicit la un dispozitiv pentru a semna. Astfel, puteți împiedica pe oricine cu autorizare specială *ALLOBJ să utilizeze Telnet pentru a accesa sistemul dumneavoastră,

asigurându-vă că QSECOFR nu are autorizare la nici un dispozitiv virtual. Decât să împiedicați toți utilizatorii Telnet care au autorizarea specială *ALLOBJ, puteți mai degrabă împiedica utilizatorii Telnet cu autorizări speciale după locație. Cu punctul de ieșire inițiere Telnet, puteți crea un program de ieșire care asociază o anumită descriere de dispozitiv iSeries la o cerere de sesiune pe baza adresei IP a solicitantului.

Controlarea funcției după locație

Veți putea dori să controlați ce funcții să permiteți sau ce meniu vede utilizatorul pe baza locației unde a fost inițiată cererea Telnet. API-ul (application programming interface - interfață de programare aplicație) QDCRDEVD vă furnizează acces la adresa IP a solicitantului. În continuare urmează câteva sugestii pentru utilizarea acestui suport:

- Puteți folosi API-ul într-un program inițial pentru toți utilizatorii (dacă activitatea Telnet este semnificativă în mediul dumneavoastră).
- Ați putea seta meniul pentru utilizator sau chiar comutarea la un anumit profil utilizator pe baza adresei IP a utilizatorului care solicită semnarea.
- Puteți folosi programul de ieșire Telnet pentru a lua decizii pe baza adresei IP a solicitantului. Aceasta elimină necesitatea definirii unui program inițial în fiecare profil utilizator. Puteți, de exemplu, seta meniul inițial pentru utilizator, seta programul inițial pentru utilizator sau specifica sub ce profil utilizator va rula sesiunea Telnet.

În plus, cu accesul la adresa IP a utilizatorului, puteți furniza tipărire dinamică la o imprimantă asociată cu adresa IP a utilizatorului. API-ul QDCRDEVD va întoarce de asemenea adresele IP pentru imprimante, ca și în cazul terminalelor de afișare. Selectați formatul DEVD1100 pentru imprimante și DEVD0600 pentru terminalele de afișare.

Controlul semnării automate

Telnet suportă posibilitatea pentru un utilizator iSeries Access pentru Windows^(R) de a ocoli ecranul de semnare prin trimiterea unui nume de utilizator de profil și a unei parole cu cererea de sesiune Telnet. Sistemul folosește setarea pentru valoarea sistem QRMTSIGN (Remote sign-on - Semnare la distanță) pentru a determina cum să trateze cererile pentru semnare automată. Tabelul de mai jos afișează opțiunile. Aceste opțiuni se aplică numai când cererea Telnet include un ID utilizator și o parolă.

Opțiune	Modul de lucru QRMTSIGN cu Telnet
*REJECT	Sesiunile Telnet care solicită semnare automată nu sunt permise
*VERIFY	Dacă profilul utilizator și parola sunt valide, sesiunea Telnet pornește. ¹
*SAMEPRF	Dacă profilul utilizator și parola sunt valide, sesiunea Telnet pornește. ¹
*FRCSIGNON	Sistemul ignoră profilul utilizator și parola. Utilizatorul vede ecranul de Semnare.

¹- Un program de ieșire înregistrat Telnet poate să omită setările QRMTSIGN prin alegerea dacă să permită sau nu semnarea automată unui solicitant (probabil bazată pe o adresă IP).

Această validare apare înainte ca programul de ieșire Telnet să ruleze. Programul de ieșire primește o indicație dacă validarea a fost cu succes sau fără. Programul de ieșire poate încă permite sau refuza sesiunea, în ciuda indicației. Indicația are una din următoarele valori:

- Valoare = 0, Parola/formula de acces client (sau tichetul Kerberos) nu a fost validată sau nu a fost recepționat nimic.
- Valoare = 1, Parola/formula de acces client în text în clar a fost validată
- Valoare = 2, Parola/formula de acces client codată (sau tichetul Kerberos) a fost validată

Permiterea semnării anonime

Puteți folosi programele de ieșire Telnet pentru a furniza Telnet.anonymous sau .guest pe sistemul dumneavoastră. Cu programul dumneavoastră de ieșire puteți detecta adresa IP a solicitantului. Dacă adresa IP provine din afara organizației dumneavoastră, puteți asocia sesiunea Telnet unui profil utilizator care are autorizare limitată și un anumit meniu. Puteți ocoli ecranul de Semnare astfel încât vizitatorul nu are oportunitatea să folosească un alt, mult mai puternic profil utilizator. Cu această opțiune, utilizatorul nu are nevoie să furnizeze un ID utilizator și parolă.

Prezentarea capacităților programului de ieșire Telnet

Puteți înregistra programele de ieșire scrise de utilizator care rulează în ambele cazuri când o sesiune Telnet pornește și când se termină. În continuare sunt exemple despre ce puteți face când porniți programul de ieșire:

- Puteți folosi certificatul Client SSL pentru a asocia un profil utilizator certificatului și pentru a asocia acel profil utilizator sesiunii Telnet, ocolind ecranul de Semnare.
- Puteți folosi adresa IP (locală) a serverului pe serverele multiple iSeries pentru a ruta conexiunile la subsisteme diferite pe baza interfeței de rețea (adresă IP).
- Permiteți sau refuza sesiunea, pe baza oricărui criteriu cunoscut, cum ar fi adresa IP a utilizatorului, momentul din zi și profilul utilizator solicitat, tipul dispozitivului (cum ar fi o imprimantă) și așa mai departe.
- Asociați o anumită descriere dispozitiv iSeries pentru sesiune. Aceasta permite rutarea jobului interactiv către orice subsistem setat pentru a primi aceste dispozitive.
- Asociați anumite valori Limbă națională pentru sesiune, cum ar fi tastatura și setul de caractere.
- Asocierea unui anumit profil utilizator pentru sesiune.
- Înregistrați automat solicitantul (fără afișarea ecranului de Semnare).
- Setări înregistrarea în istoricul de auditare pentru sesiune.

Pentru mai multe exemple și informații de programare, faceți referire la următoarele subiecte:

Folosirea programelor punct de ieșire Telnet
Atelier tehnic: Programe de ieșire Telnet



Configurarea serverului Telnet

Una dintre cele mai importante funcții din Telnet este abilitatea de a negocia opțiunile între client și server. Acest tip de negociere deschisă permite atât clientului, cât și serverului să inițieze o cerere sau să onoreze o cerere. Mai multe tipuri de emulare diferite vă sunt disponibile pentru negocierea cererilor și convertirea lor la ieșire. Serverul iSeries^(TM) suportă stații de lucru tip 3270 și stații de lucru tip VTxxx, dar tipul preferat este emularea 5250.

Pentru a vă configura serverul Telnet pentru un alt tip de emulări suportate, completați următorii pași:

1. Pornire server Telnet
2. Setări numărului de dispozitive virtuale
3. Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare
4. Setarea parametrului păstrare-în-viață al sesiunii
5. Asocierea dispozitivelor la subsisteme
6. Activarea subsistemului QSYSWRK
7. Crearea profilurilor de utilizator
8. Selectați și configurați tipul dumneavoastră de emulare

O dată ce ați configurat Telnet, veți dori să realizați securizarea Telnet cu SSL (Secure Sockets Layer).

Pornirea serverului Telnet

Serverul Telnet activ deține una sau mai multe instanțe ale fiecăruia dintre aceste joburi ce rulează pe subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

Pentru a porni serverul Telnet utilizând Navigator iSeries^(TM), urmăriți acești pași:

1. Expandați **serverul dumneavoastră iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
2. În panoul din dreapta, localizați **Telnet** în coloana Nume server.

3. Confirmați că apare **Pornit** în coloana Stare.
4. Dacă serverul nu rulează, faceți clic dreapta pe **Telnet** și selectați **Pornire**.

Pentru informații despre deconectare, consultați Terminarea sesiunii dumneavoastră server Telnet.

Ce să faceți în continuare:

Dacă configurați serverul Telnet pentru prima dată, continuați la Setarea numărului de dispozitive virtuale.

Setarea numărului de dispozitive virtuale



Acest subiect furnizează instrucțiuni pentru setarea numărului de dispozitive virtuale configurate automat pentru serverul Telnet și limitarea numărului de încercări de semnare permise. Pentru informații suplimentare despre dispozitivele virtuale și convențiile de nume Telnet, faceți referire la Descrierile de dispozitiv virtual.

Puteți activa serverul Telnet să configureze automat un număr setat de dispozitive virtuale și controlere folosind Valorile sistem pentru dispozitive QAUTOVRT. Puteți specifica numărul de dispozitive care sunt pornite automat și numărul maxim de dispozitive care sunt configurate automat de serverul iSeries^(TM). Serverul iSeries configurează sau creează un dispozitiv o dată, după necesități, până la o limită specificată.

1. În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, —> **Configurare și service** —> **Valori sistem**.
2. În panoul din dreapta, faceți clic dreapta pe **Dispozitive** și selectați **Proprietăți**.
3. În pagina **Valori sistem dispozitive**, activați **Dispozitive Pass-through și TELNET** și selectați o opțiune pentru configurarea automată a dispozitivelor virtuale. Opțiunile sunt:
 - **Fără număr maxim de dispozitive** - Permite un număr nelimitat de dispozitive
 - **Număr maxim de dispozitive (1-32500)** - Specifică o valoare cuprinsă între 1 și 32500 pentru numărul maxim de dispozitive care pot fi configurate automat.
 - **Rulați programul de ieșire înregistrat** - Apelați programul înregistrat pentru punctul de ieșire QIBM_QPA_DEVSEL (Virtual Device Selection - Selecție dispozitiv virtual) când un dispozitiv virtual trebuie să fie selectat sau creat automat.

Pentru informații suplimentare despre dispozitivele virtuale, faceți referire la următoarele subiecte:

Configurarea automată a dispozitivelor virtuale

Puteți configura serverul dumneavoastră Telnet pentru a crea automat dispozitive virtuale după necesități până la un număr maxim setat

Crearea propriilor dumneavoastră dispozitive virtuale

Puteți crea manual dispozitive virtuale, cu nume personalizate sau nume generate automat.

Pentru informații suplimentare și exemple, consultați Studio tehnic: Programe de ieșire Telnet



Ce să faceți în continuare:

Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea numărului de semnări



Configurarea automată a dispozitivelor virtuale

Puteți activa serverul Telnet pentru configurarea automată a dispozitivului dumneavoastră virtual și a controlerelor utilizând Valorile de sistem pentru dispozitive QAUTOVRT din Navigator iSeries^(TM). Puteți specifica numărul

dispozitivelor care sunt pornite automat și puteți specifica numărul maxim de dispozitive pe care serverul iSeries le configurează automat. Serverul iSeries configurează sau creează un dispozitiv o dată, după necesități, până la o limită specificată.

Serverul Telnet nu elimină dispozitivele virtuale când se configurează automat dispozitive virtuale cu Telnet și nici după închiderea sesiunii. Dispozitivele nu sunt șterse chiar dacă numărul de dispozitive atașate controlerelor virtuale depășește limita maximă. Dacă dispozitivele există deja pe controlerul virtual, ele pot fi folosite de către serverul Telnet. Serverul Telnet va schimba atributele unui dispozitiv existent pentru a se potrivi cererii clientului dacă dispozitivul virtual este cerut după nume.

Dacă nu ați permis niciodată configurarea automată a dispozitivelor virtuale pe serverul dumneavoastră, valoarea Numărul maxim de dispozitive este 0. O încercare de conexiune Telnet va eșua când numărul dispozitivelor în folosință va depăși valoarea Numărului maxim de dispozitive. Un dispozitiv în folosință are starea ACTIVE sau SIGNON DISPLAY. Dacă încercați să vă conectați, veți primi un mesaj (TCP2504) indicând că sesiunea client Telnet s-a terminat și că conexiunea este închisă. În plus, jobul QTCPIP din serverul iSeries la distanță trimite un mesaj (CPF8940) indicând că un dispozitiv virtual nu poate fi selectat automat.

Dacă schimbați Numărul maxim de dispozitive la 10, următoarea încercare de conexiune Telnet va determina serverul Telnet să creeze un dispozitiv virtual. Telnet creează acest dispozitiv virtual pentru că numărul dispozitivelor virtuale atașate controlerului (0) este mai mic decât numărul specificat de Numărul maxim de dispozitive (10). Chiar dacă schimbați numărul specificat la 0 din nou, următorul utilizator care încearcă o conexiune va reuși. Când o încercare de conexiune Telnet eșuează deoarece serverul iSeries nu este capabil să creeze un dispozitiv virtual, mesajul CPF87D7 este trimis cozii de mesaje operator a sistemului pe serverul Telnet.

Notă:

Serverul Telnet nu șterge dispozitivele virtuale configurate automat sau dispozitivele denumite, chiar dacă numărul dispozitivelor atașate la controlerul virtual depășește Numărul maxim de dispozitive.

Valorile de sistem ale dispozitivelor specifică dacă dispozitivele virtuale Pass-through sau Telnet pe tot ecranul, care sunt atașate la un controler QPACTLnn, sunt configurate automat. Această valoare de sistem nu afectează dispozitivele care sunt atașate la controlere QPACTLnn, deoarece nu sunt dispozitive implicite de sistem. De obicei, dispozitivele QPADEVnnnn sunt atașate la controlere QPACTLnn, în timp ce dispozitivele cu nume, precum NEWYORK001, sunt atașate unui controler QVIRCDnnnn.

Pentru instrucțiuni pentru a seta această valoare în Navigator iSeries, faceți referire la Setarea numărului de dispozitive virtuale.

Crearea propriilor dumneavoastră dispozitive virtuale

Puteți crea controlere și dispozitive virtuale. Dacă creați propriile dumneavoastră dispozitive virtuale și permiteți serverului dumneavoastră iSeries^(TM) să selecteze automat numele dispozitivului, trebuie să fiți atenți la următoarele:

- Controlerul virtual trebuie numit QPACTLnn, unde nn reprezintă numărul zecimal 01 sau mai mare.
- Dispozitivul virtual va fi numit QPADEV xxxx, unde xxxx este un caracter alfanumeric de la 0001 la ZZZZ. Dispozitivul virtual ar trebui să aibă clasa de dispozitive *VRT. Locul unui dispozitiv virtual este sub un controler virtual.

Dacă alegeți să creați propriile dumneavoastră dispozitive, trebuie să fiți familiar cu Convențiile de numire descrieri dispozitiv virtual folosite de serverul Telnet. Dacă doriți să selectați propriile dumneavoastră nume de dispozitive (folosind un client RFC 2877 sau API-urile terminal virtual) atunci controlerul virtual va avea numele QVIRCDnnnn, unde nnnn este un număr zecimal 01 sau mai mare.

Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare

Restricționarea utilizatorilor privilegiați la anumite dispozitive



Programul licențiat OS/400^(R) utilizează valorile sistem semnare-în pentru a restricționa sau limita dispozitivele la care se poate semna un utilizator. Autorizarea la toate obiectele (*ALLOBJ), permite accesul utilizatorului la oricare dintre resursele sistemului. Autorizarea specială service (*SERVICE) permite utilizatorului să efectueze anumite funcții de service pe sistem. De exemplu, utilizatorul cu acest tip de autorizare va putea să depaneze un program și să efectueze funcții de afișare și de service alternativ. Pentru a seta aceste valori utilizând Navigator iSeries^(TM), urmați pașii următori:

1. În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, —> **Rețea** —> **Servere** —> **TCP/IP**.
2. În panoul din dreapta, faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.
3. În pagina **Proprietăți Telnet - Semnare în sistem**, selectați următoarele:

Restricționarea utilizatorilor privilegiați la anumite dispozitive.

Aceasta indică faptul că toți utilizatorii cu autorizări speciale pentru toate obiectele (*ALLOBJ) și service (*SERVICE) au nevoie de autorizare explicită pentru stațiile de lucru specifice.

Limitarea fiecărui utilizator la o sesiune de dispozitiv.

Specifică dacă un utilizator se poate înregistra la mai mult de o stație de lucru. Aceasta nu împiedică utilizatorul să folosească joburi grup sau să facă o cerere sistem la stația de lucru. Aceasta reduce probabilitatea de partajare a parolelor și de nesupraveghere a dispozitivelor.

Limitarea încercărilor de semnare

Folosiți valorile sistem de semnare pentru a defini numărul încercărilor de semnare la sistem permise. Numărul încercărilor permise de semnare Telnet crește dacă aveți dispozitive virtuale configurate automat.

1. În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, —> **Rețea** —> **Servere** —> **TCP/IP**.
2. În panoul din dreapta, faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.
3. În pagina **Proprietăți Telnet**, faceți clic pe fișa **Semnare în sistem**.
4. În pagina **Proprietăți Telnet - Semnare în sistem**, puteți specifica numărul încercărilor de semnare permise și acțiunea care să fie luată dacă numărul maxim de încercări de semnare este atins.
5. Faceți clic pe fișa **La distanță**.
6. În pagina **Proprietăți Telnet - Semnare la distanță**, selectați o opțiune pentru **Folosire Telnet pentru semnarea la distanță**. Opțiunile sunt:
 - **Afișează întotdeauna semnarea** - Toate sesiunile de semnare la distanță sunt necesare pentru a parcurge procesul normal de semnare.
 - **Permite ocolirea semnării** - Sistemul permite utilizatorului să ocolească panoul de semnare. Utilizatorul este încă semnat în sistem, dar panoul de semnare nu este afișat.

Notă:

Dacă este activată **Folosirea Pass-through pentru semnarea la distanță**, opțiunile sunt selectate automat pe baza setărilor pe care le specificați pentru **Folosire Pass-through pentru semnarea la distanță**. Telnet este încă disponibil pentru semnările la distanță dacă selectați Pass-through.

Ce să faceți în continuare:

Setarea parametrului păstrare în viață al sesiunii



Setarea parametrului păstrare-în-viață al sesiunii

Puteți seta timpul maxim de inactivitate pe care protocolul TCP îl va permite înainte de a trimite o probă pentru a testa o sesiune inactivă folosind parametrul de activitate (keep-alive) TCP. Protocolul va trimite cererile de rămânere în activitate clientului la distanță la orice moment când sesiunea este inactivă pentru a perioadă mai mare decât valoarea de rămânere în activitate. Perioada inactivă este definită prin parametrul timeout de menținere-în-viață sesiune din proprietățile Telnet din Navigator iSeries^(TM) sau parametrul din comanda CHGTELNA. Când o sesiune se constată a fi inactivă (nici un răspuns la nici o probă de verificare a activității clientului la distanță), acea sesiune este terminată, dispozitivul virtual asociat cu sesiunea este returnat grupului de dispozitive virtuale libere și sistemul de operare iSeries realizează setarea acțiunii în valoarea sistem QDEVRCYACN a jobului interactiv ce rulează pe dispozitivul virtual. Aceasta afectează doar dispozitivele virtuale cu nume. Pentru dispozitivele virtuale auto-selectate (QPADEVxxxx), jobul interactiv este oprit întotdeauna.

Serverul Telnet setează menținere-în-viață la 600 secunde.

Setarea are efect la pornirea serverului. În plus față de parametrul timeout menținere-în-viață sesiune, puteți de asemenea dori să revedeți setările intervalului de timeout din Valori sistem joburi inactive în Navigator iSeries. Acest parametru de timeout este folosit pentru limitarea perioadei de timp în care orice job interactiv are permisiunea de a fi inactiv înainte ca sistemul de operare iSeries să realizeze acțiunea setată în valoarea sistem QINACTMSGQ a jobului interactiv. În cazul joburilor interactive conectate Telnet, o acțiune *DSCJOB este onorată pentru dispozitivele virtuale numite. Pentru dispozitivele virtuale selectate automat(QPADEVxxxx), acțiunea *DSCJOB va cauza terminarea jobului interactiv.



Pentru setarea parametrului menținere-în-viață pentru Telnet în Navigator iSeries, urmați acești pași:

1. În Navigator iSeries, selectați **serverul dumneavoastră iSeries**, —> **Rețea** —> **Servere** —> **TCP/IP**.
2. În panoul din dreapta, faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.
3. În pagina **Proprietăți Telnet**, faceți clic pe fișa **Timeout**.
4. În pagina **Proprietăți Telnet - Timeout**, specificați acțiunea care să fie luată când joburile ating timeout-ul. Puteți specifica de asemenea cât timp să acordați unei operații înainte ca jobul să intre în timeout. Puteți specifica informații atât pentru joburile inactive, cât și pentru joburile deconectate.



Ce să faceți în continuare:

Asocierea dispozitivelor la subsisteme

Asocierea de dispozitive la subsisteme

Înainte ca un utilizator să se poată semna pe serverul iSeries^(TM), stația de lucru trebuie să fie definită la un subsistem. Stația de lucru, de exemplu, ar fi dispozitivul virtual de afișare selectat sau creat automat de către serverul Telnet.

Numele stație de lucru sau tipul stației de lucru trebuie specificat în descrierea de subsistem pe serverul iSeries. Utilizați comanda Afișare descriere subsistem (Display Subsystem Description - DSPSBSD) pentru a vizualiza intrările de stații de lucru definite la subsistem.

Comanda următoare poate fi utilizată pentru adăugarea tuturor tipurilor de stații de lucru la un subsistem denumit QINTER:

```
ADDWSE SBSB(QINTER) WRKSTNTYPE(*ALL)
```

Dispozitivele de tipărire sunt întotdeauna direcționate către subsistemul QSPL.

Comanda Adăugare intrare stație de lucru (Add Workstation Entry - ADDWSE) poate fi executată când subsistemul este activ. Dar modificările pot avea sau nu efect imediat. S-ar putea să fie nevoie să opriți și să reporniți subsistemul.

Ce să faceți în continuare:

Activarea subsistemului QSYSWRK

Activarea subsistemului QSYSWRK

Jobul de server pentru o aplicație TCP/IP trebuie pornit în subsistemul QSYSWRK. Subsistemul de spool, QSPL, trebuie să fie activ pentru a rula sesiuni de imprimantă Pass-through.

Pentru a verifica starea subsistemului QSYSWRK, completați următorii pași:

1. În interfața bazată-pe-caracter din serverul iSeries^(TM), tipăriți WRKSBS (Gestionare subsisteme active).
2. Verificați că sunt afișate următoarele sisteme:
 - QSYSWRK
 - QINTER
 - QSPL

Dacă subsistemul QSYSWRK nu este activ, efectuați următorii pași:

1. În interfața caracter a serverului iSeries, introduceți STRSBS (Start subsystem - Pornire subsistem).
2. Introduceți QSYSWRK pentru descrierea de subsistem și QSYS pentru bibliotecă, apoi apăsați pe Enter.
3. Repetați pentru Nume subsistem QINTER cu Biblioteca QSYS și pentru Nume subsistem QSPL și Biblioteca QSYS.

Dacă nu știți ce subsisteme să folosiți pentru joburile interactive, introduceți WRKSBSD *ALL la interfața caracter iSeries. Intrările Tip stație de lucru vă indică dispozitivul care este alocat unui subsistem.

Ce să faceți în continuare:

Crearea profilurilor de utilizator

Crearea profilurilor de utilizator

Pe serverul Telnet puteți crea utilizator Telnet utilizând Navigator iSeries^(TM).

Pentru a crea profiluri utilizatori Telnet, completați următorii pași:

1. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries**.
2. Faceți clic dreapta pe **Utilizatori și grupuri** și selectați **Utilizator nou**.
3. Introduceți numele utilizatorului, descrierea și parola.
4. Pentru a specifica descrierea unui job, faceți clic pe **Joburi** și introduceți descrierea jobului.
5. Apăsați **OK**.

Ce să faceți în continuare:

Selectați și configurați tipul dumneavoastră de emulare

Tipurile de emulare suportate de iSeries^(TM)

Pentru iSeries, tipul preferat este emularea 5250. Totuși, iSeries suportă de asemenea emularea 3270 și VTxxx. Selectați tipul de emulare pentru care doriți să configurați serverul Telenet:

- Modul 5250 tot-ecranul

- Modul 3270 tot-ecranul
- Modul VTxxx tot-ecranul

Configurarea serverului Telnet pentru modul 5250 tot-ecranul



Trebuie să completați acești pași înaintea stabilirii sesiunii dumneavoastră client Telnet:

1. Trebuie să porniți serverul Telnet pe sistemul la distanță (sistemul la care doriți să vă conectați utilizând Telnet).
2. (Opțional) Setați serverul iSeries^(TM) pentru configurarea automată a controlerelor și dispozitivelor virtuale. Verificați că joburile QTVTELNET și QTVDEVICE în subsistemul QSYSWRK sunt active efectuând următorii pași:
 - a. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Control funcționare**.
 - b. Faceți clic dreapta pe **Subsisteme** și apoi pe **Deschidere**.
 - c. Verificați dacă subsistemul este activ.
3. Verificați valoarea sistem QAUTOVRT. Ar trebui să fie egală cu numărul maxim de utilizatori înscriși pe sistem, utilizând dispozitive virtuale configurate automat, în orice moment. QAUTOVRT suportă valorile numerice între 0 și 32500 și o valoare specială *NOMAX.



Configurarea serverului Telnet pentru modul eran plin 3270



Supportul 3270 tot-ecranul permite utilizatorilor clientului Telnet să se semneze și să ruleze aplicații tot-ecranul iSeries^(TM), chiar dacă s-a negociat un suport 3270 tot-ecranul. Serverul negociază suport 3270 tot-ecranul cu orice aplicație client Telnet care suportă aplicații 3270 tot-ecranul, mai degrabă decât aplicațiile 5250 tot-ecranul. Un exemplu de sistem care negociază suport 3270 tot-ecranul este cel din familia S/390^(R).

Telnet 5250 (TN5250) trimite fluxul de date între două sisteme ca EBCDIC. Deoarece șirurile de date 3270 sunt translatate în șiruri de date 5250, dispozitivele stație de lucru operează ca un terminal 5250 la distanță pe serverul iSeries și programele aplicație.

După ce ați terminat configurarea generală a serverului Telnet, sunt câțiva pași adiționali pentru a activa suportul pentru modul 3270 tot-ecranul. Modul tot-ecranul este un mod “bloc” în opoziție cu modul “linie”. “Modul linie” este când datele sunt transmise câte o linie o dată, în timp ce modul “bloc” sau tot-ecranul transmite o dată întregul ecran.

Pentru informații despre capacitățile dispozitiv 3270 suportate, faceți referire la Tipurile de terminale 3270 suportate.

Pentru informații despre 3270 tot-ecranul cum ar fi dimensiunea ecranului, maparea tastaturii, tasta de selectare cursor și mesajele de eroare și caracterele null, consultați Sesiunile client Telnet 3270.

Completați următoarele task-uri pentru a configura serverul Telnet pentru modul 3270 tot-ecranul:

1. Verificați valoarea sistem QKBDTYPE (page 26)
2. Setați maparea de tastatură implicită (page 27)
3. Modificați maparea unei tastaturi (opțional) (page 27)
4. Modificați coada de mesaje (opțional) (page 27)

Verificarea valorii sistem QKBDTYPE

Când serverul Telnet iSeries 400 creează automat dispozitive virtuale de afișare, folosește valoarea sistem QKBDTYPE pentru a determina tipul de tastatură pentru dispozitivul virtual.

Dacă crearea inițială a dispozitivului virtual eșuează folosind comanda QKBDTYPE, serverul Telnet folosește valoarea USB a tastaturii pentru a încerca să creeze dispozitivul. Dacă a doua încercare de creare a dispozitivului de afișare

virtual eșuează folosind valoarea USB, atunci un mesaj (CPF87D7) este trimis cozii de mesaje a operatorului sistemului. Acest mesaj indică faptul că sistemul nu poate selecta automat dispozitivul virtual.

Setarea mapării implicite de tastatură

O stație terminal 3270 conectată la un server iSeries care folosește Telnet apare unui server iSeries ca fiind o stație terminal 5251. Tastatura stației de afișare 3270 are o mapare de tastatură echivalentă 5251 asociată cu ea care îi permite să aibă toate funcțiile echivalent-5251 pe un server iSeries.

Când un utilizator sistem client Telnet se înregistrează pentru prima dată în mod 3270 tot-ecranul, serverul iSeries asociază automat maparea de tastatură implicită tastaturii 3277, 3278 sau 3279 a utilizatorului. Evitați acest lucru incluzând o mapare de tastatură definită de utilizator în profilul utilizator a procedurii de semnare. Aceasta furnizează maparea necesară tastaturilor 3270 pentru a realiza aproximativ aceleași funcții precum tastaturile echivalente 5250.

Afișarea unei mapări de tastatură

Puteți folosi comanda Afișare mapare tastatură (DSPKBDMAP) pentru a vedea maparea curentă a tastaturii. Sau, puteți folosi opțiunea 6 (Afișare mapare tastatură 3270) din Meniul de Configurare TCP/IP Telnet, în timp ce terminalul este în modul de emulare 3270.

Modificarea unei mapări de tastatură

Folosiți comanda Modificare mapare tastatură (CHGKBDMAP) dacă vreți să faceți schimbări minore mapării de tastatură implicite. Această comandă este disponibilă din meniul de Configurare Telnet TCP/IP ca opțiunea 7 (Modificare mapare de tastatură 3270).

Pentru a seta o nouă mapare de tastatură, folosiți comanda Setare mapare tastatură (SETKBDMAP). Această comandă este disponibilă din meniul de Configurare Telnet TCP/IP. Asignările de taste pe care le specificați au efect până când folosiți aceste comenzi din nou pentru a specifica noi asignări de taste sau pînă când vă deconectați.

Notă:

Diferența dintre CHGKBDMAP și SETKBDMAP este aceea că, în cazul SETKBDMAP, sistemul aplică valorile implicite și apoi modificările din SETKBDMAP. Cu CHGKBDMAP, sistemul aplică valorile implicite plus orice schimbări pe care le-ați făcut anterior în timpul acestei sesiuni și apoi sunt aplicate modificările CHGKBDMAP.

Pentru informații suplimentare despre maparea tastaturii consultați [Maparea tastaturii 3270](#)

Modificați coada de mesaje

O coadă de mesaje este ca o căsuță poștală pentru mesaje. Serverul iSeries are mai multe cozi de mesaje care păstrează mesajele ce furnizează informații ajutătoare la găsirea și raportarea problemelor. Când coada de mesaje a stației de lucru este în modul break, apar mesaje pe dispozitivul 3270 la fel cum apar și pe un ecran 5250. Pentru a primi mesaje în modul break, trebuie să specificați *BREAK în comanda de schimbare a cozii de mesaje (CHGMSGQ). Când stația dumneavoastră de lucru nu este în modul break, veți primi mesajul următor: un mesaj a sosit în coada de mesaje.

Pentru a găsi acest mesaj și să continuați folosirea stației de lucru, urmați acești pași:

1. Apăsați tasta funcțională asignată tastei de ajutor sau tasta funcțională asignată funcției de resetare eroare.
2. Introduceți comanda Afișare mesaj (DSPMSG) sau tasta funcțională care este asignată funcției SysReq (cerere sistem) urmată de opțiunea 4 (Afișare mesaj) pentru a vedea mesajul în așteptare.
3. Setati coada de mesaje a stației de lucru în modul întrerupere pentru a vedea mesajele imediat cum ajung.

Resetarea indicatorului luminos al ecranului de inhibare intrare

La folosirea unui server iSeries de pe un terminal tip 5250, apăsarea anumitor taste în anumite situații face ca introducerea să fie inhibată. Când apare acest lucru, terminalul 5250 afișează indicatorul inhibare intrare.

Doă asteriscuri afișate în colțul din dreapta-jos a ecranului indică semnalizarea de inhibare intrare. Când tastatura este inhibată, orice taste mapate la tastele funcționale iSeries sunt ignorate.

Pentru a reseta tastatura apăsați tasta Enter sau apăsați tasta mapată la tasta Reset iSeries.



Tipurile de terminal 3270 suportate: Următoarea tabelă enumeră capacitățile pentru dispozitivele 3270 suportate de Telnet. Asigurați-vă că clientul 3270 își negociază unul din tipurile de terminal suportate de 3270. Următorul tabel arată tipurile de terminal suportate.

Tabelul 1. Mapări stații de lucru în modul tot-ecranul

Tip dispozitiv	Capacități dispozitiv
3277	Această stație de afișare suportă fluxuri de date generice 3270. Atribute extinse, precum sublinierea, clipirea, imaginea inversată sau culori nu sunt suportate.
3278	Această stație suportă atribute suplimentare, ca clipire, imagine inversată și sublinierea dacă sunt cerute de cuvintele cheie ale sistemului OS/400 ^(R) DDS (data description specifications). Notă: <ul style="list-style-type: none">Atributele extinse nu sunt suportate de unele implementări client ale Telnet 3270 mod tot-ecranul (TN3270).Terminalele DBCS care tratează tipul de terminal 3278-2-E sunt suportate.
3279	Această stație de afișare suportă atribute de culori și atribute de fluxuri de date extinse trimise pentru un dispozitiv 3278. Atributele de culoare sunt determinate (în același fel ca la 5292 Full Color Display) interpretând atributele DDS ale cuvintelor cheie DDS pentru clipire, intensitate mare sau culori.

Configurarea serverului Telnet pentru modul VTxxx tot-ecranul



Suportul serverului VTxxx permite utilizatorilor clientului Telnet să se semneze și să ruleze aplicații iSeries^(TM) 5250 tot-ecranul, chiar dacă s-a negociat modul VTxxx tot-ecranul. Aplicația client Telnet trebuie să fie capabilă să negocieze suport pentru terminal VTxxx. Când este negociat modul VTxxx tot-ecranul, serverul Telnet iSeries este responsabil pentru maparea funcțiilor 5250 la tastele VTxxx și vice versa.

Cu toate că serverul Telnet iSeries suportă clienți VTxxx, acesta nu este modul preferat de folosit deoarece terminalul VTxxx este un dispozitiv orientat caracter. Serverul iSeries este un sistem mod bloc. Majoritatea implementărilor Telnet suportă clienți TN3270 sau TN5250 care trebuie folosiți la conectarea la un server Telnet iSeries.

În general, când o tastă la un terminal VTxxx este apăsată, codul hexazecimal asociat tastei este imediat transmis serverului Telnet. Serverul Telnet trebuie să analizeze apăsarea unei taste și apoi să trimită caracterul înapoi la terminalul VTxxx unde este afișat. Aceasta implică un activitate mărită (overhead) asociată fiecărei apăsări de tastă. În mod diferit, dispozitivele orientate bloc 5250 și 3270 înregistrează toate apăsările de taste ale clientului până când o tastă identificator atenție (AID) este apăsată. Când este apăsată o tastă AID, clientul trimite intrarea buffer-ată la server pentru procesare. Dispozitivele orientate bloc implică mai puțin 'overhead' pe tastă apăsată și, în general, furnizează performanțe mai bune decât dispozitivele orientate caracter, precum terminalele VTxxx.

VTxxx trimite datele ca ASCII între 2 sisteme.

După ce ați terminat configurarea generală a serverului Telnet, sunt câțiva pași adiționali pentru a activa suportul pentru modul VTxxx tot-ecranul.

Modul tot-ecranul este un mod “bloc” în opoziție cu modul “linie”. “Modul linie” este când datele sunt transmise câte o linie o dată, în timp ce modul “bloc” sau tot-ecranul transmite o dată întregul ecran.

Pentru informații despre VTxxx tot-ecranul, opțiuni de emulare și valori taste, consultați Sesiunile client Telnet VTxxx.

Completați următoarele task-uri pentru a configura serverul Telnet pentru modul VTxxx tot-ecranul:

1. Verificați valoarea sistem QKBDTYPE (page 29)
2. Setări maparea de tastatură implicită (page 29)
3. Setări tipul terminalului virtual de rețea implicit (opțional) (page 30)
4. Setări tabelele de mapare ASCII/EBCDIC (opțional) (page 30)

Verificarea valorii sistem QKBDTYPE

Când serverul Telnet iSeries 400 creează automat dispozitive virtuale de afișare, folosește valoarea sistem QKBDTYPE pentru a determina tipul de tastatură pentru dispozitivul virtual.

Dacă crearea inițială a dispozitivului virtual eșuează folosind valoarea sistem QKBDTYPE, serverul Telnet încearcă să creeze dispozitivul din nou, folosind valoarea USB pentru tipul de tastatură. Dacă a doua încercare de a crea tipul de tastatură eșuează, atunci sistemul trimite un mesaj (CPF87D7) istoricului job QTCPIP. Acest mesaj indică faptul că sistemul nu poate selecta automat dispozitivul virtual. Sistemul trimite, de asemenea, un mesaj cozii de mesaje a operatorului sistemului.

Setarea mapării implicite de tastatură

Când sesiunea Telnet negociază în modul VTxxx tot-ecranul, sistemul folosește o mapare de tastatură implicită. Pentru afișarea mapării implicite de tastatură pentru VTxxx, folosiți comanda DSPVTMAP (Display VT Keyboard Map - Afișare mapare de tastatură VT). Pentru modificarea mapării de tastatură VTxxx, folosiți comanda CHGVMTMAP (Change VT Keyboard Map - Modificare mapare tastatură VT) sau comanda SETVTMAP (Set VT Keyboard Map - Setarea mapării de tastatură VT). Faceți referire la Opțiuni de emulare VTxxx pentru informații despre lucrul cu mapările de tastatură.

Pentru a găsi valorile speciale ale tastelor 5250, consultați tabela Valorile tastelor VTxxx după funcție.

Tabela de taste numerice arată tastele de pe blocul de taste (keypad) auxiliar care în mod normal transmit coduri pentru cifre, punct zecimal, semnul minus și virgula.

Tabela de editare arată tastele care transmit coduri pentru tastele de editare.

Deoarece tastatura VTxxx nu are aceleași taste cu tastatura 5250, trebuie să existe o mapare de tastatură între tastele VTxxx și funcțiile iSeries. Serverul iSeries asociază o mapare de tastatură implicită când este stabilită pentru prima dată o sesiune VTxxx. În unele cazuri pot fi mai mult de o tastă sau secvență de taste care mapează o anumită funcție server iSeries. În aceste cazuri, puteți folosi oricare din tastele definite pentru apelarea funcției server iSeries dorite.

Notă:

1. Fiecare caracter de control este o valoare pe un octet generată de la o tastatură VTxxx ținând tasta CTRL apăsată în timp ce apăsați una din tastele alfanumerice. Caracterele de control generează aceleași valori hexazecimale, dacă este și dacă nu este apăsat SHIFT.
2. Secvențele escape sunt coduri de mai mulți octeți care sunt generate de apăsarea tastei ESC urmată de caractere care formează secvența dorită.
3. Serverul iSeries ignoră semnificația tuturor caracterelor alfabetice într-o secvență escape. Puteți tasta caractere alfabetice litere mari și litere mici în secvențe escape.
4. Funcțiile F1-F12 ale serverului iSeries sunt mapate la tasta Esc urmată de una din tastele de pe rândul de sus al tastaturii VTxxx. O tastă ESC urmată de o tastă din linia de sus a tastaturii VTxxx, în combinație cu SHIFT, mapează funcțiile F13-F24.
5. Unele sisteme client Telnet VTxxx folosesc Ctrl-S și Ctrl-Q cu scopul de a controla fluxul. Acest lucru este în general cunoscut ca și control de flux XON/XOFF. Dacă folosiți un sistem client care are activat XON/XOFF, nu trebuie să folosiți valorile *CTLS și *CTLQ în maparea tastaturii dumneavoastră.

Setarea tipului de terminal virtual de rețea implicit

Parametrul tip de terminal virtual de rețea implicit specifică modul de utilizare când serverul Telnet nu poate să negocieze unul din tipurile de terminal suportate.

Pentru a seta valoarea Terminal virtual de rețea implicit fie la modul *VT100 pentru VT100/VT220, fie la modul linie *NVT pentru ASCII, efectuați următorii pași:

1. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
2. Faceți clic dreapta pe **TELNET** și selectați **Proprietăți**.
3. Faceți clic pe fișa **General** și selectați valoarea corespunzătoare de lângă **Terminal virtual de rețea implicit**.
4. Apăsați **OK**.

Setarea tabelor de mapare ASCII/EBCDIC

Serverul Telnet iSeries folosește implicit tabelele de mapare ASCII-la-EBCDIC și EBCDIC-la-ASCII bazate pe parametrul CCSID din atributele Telnet TCP/IP. Implicit este folosit setul de caractere multinațional DEC (*MULTINAT). Alte CCSID-uri ASCII pe 7 și 8 biți și oricare din seturile de caractere de înlocuire naționale DEC sunt, de asemenea, acceptate pentru folosire.

Notă:

Pentru VT220 modul 8-biți, tabelele de mapare nu sunt disponibile. În acest mod, sistemul folosește seturile de caractere de înlocuire DEC. Pentru VT220 modul 7-biți, puteți folosi ori tabelele de mapare ori seturile de caractere de înlocuire DEC.

Există trei modalități de a schimba implicitul. Puteți schimba parametrul CCSID, specificați valori diferite pentru tabelele de ieșire VTxxx (TBLVTOUIT) și de intrare (TBLVTIN) sau schimbați tabelele implicite pentru sesiunea curentă.

- Pentru modificarea valorilor pentru tabele, efectuați pașii următori:
 1. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
 2. Faceți clic dreapta pe **TELNET** și selectați **Proprietăți**.
 3. Apăsați **Mapări**.
 4. Selectați casuța de validare **Folosirea tabelor de mapare specificate** și faceți clic pe **Tabele**.

5. Selectați **Folosirea tabelii de mapare de ieșire și Folosirea tabelii de mapare de intrare pentru a schimba parametrul CCSID.**
 6. Apăsați **OK**.
 7. Apăsați **OK**.
- Pentru a schimba tabelele implicite pentru sesiunea curentă, folosiți comanda SETVTTBL (Setare tabele de mapare VT).

O altă modalitate de accesare a acestei comenzi este să folosiți opțiunea 2 pentru comanda CHGTCPTELN.



Securizarea Telnet cu SSL

Cu protocolul SSL (Secure Sockets Layer), puteți stabili conexiuni sigure între aplicația server Telnet și clienții Telnet care furnizează autentificarea unuia sau ambelor puncte finale ale sesiunii de comunicații. SSL furnizează de asemenea secretul și integritatea datelor schimbate între server și client.

Configurarea SSL pe serverul Telnet

Acest subiect furnizează instrucțiuni pentru activarea SSL pe serverul dumneavoastră iSeries^(TM).

Dialog de confirmare și inițializare SSL

Acest subiect furnizează detalii despre interacțiunile dintre servere Telnet, clienți și SSL.

Pentru mai multe informații despre SSL, faceți referire la următoarele subiecte:

- Secure Sockets Layer (SSL)
- Depanarea serverului Telnet SSL

Configurarea SSL pe serverul Telnet

Puteți configura serverul OS/400^(R) Telnet pentru a securiza sesiunile cu SSL (Secure Sockets Layer). Factorul cel mai important care trebuie luat în considerare la activarea SSL pe serverul Telnet este sensibilitatea informațiilor care sunt implicate în sesiunile client. Dacă informația este sensibilă sau privată atunci este o bună idee de a securiza serverul Telnet iSeries^(TM) cu SSL.

Pentru configurarea SSL pe serverul Telnet, urmați acești pași:

1. Instalați software-ul următor pentru suportul SSL Telnet și pentru gestionarea certificatelor digitale:
 - TCP/IP Connectivity Utilities pentru iSeries, 5722-TC1
 - Digital Certificate Manager, 5722-SS1 - Boss Option 34
 - Cryptographic Access Provider, 5722-AC x
 - IBM^R HTTP Server for iSeries, 5722-DG1
 - Developer Kit for JavaTM, 5722-JV1
2. Asigurați-vă că ați înlăturat restricțiile de port și ați permis SSL să pornească.
3. Asignați un certificat serverului Telnet
4. Activarea autentificării clientului pentru serverul Telnet (pas opțional)
5. Activarea SSL pe serverul Telnet
6. Porniți serverul Telnet.

Pentru informații suplimentare despre rezolvarea problemelor SSL legate de serverul Telnet, consultați Rezolvarea problemelor serverului dumneavoastră Telnet SSL. Uneori, a înțelege ceea ce se întâmplă în timpul procesării SSL vă poate ajuta, de asemenea, la determinarea locului în care a apărut o problemă. Revedeți Dialog de configurare și inițializare SSL pentru informații suplimentare despre procesarea SSL.

Înlăturarea restricțiilor de port: Înainte de V5E1, restricțiile de port au fost utilizate deoarece suportul SSL (Secure Sockets Layer) nu a fost disponibil pentru Telnet. Acum puteți specifica dacă să pornească SSL, non-SSL sau ambele.

Prin urmare nu mai este nevoie de restricții de port. Dacă ați definit restricții de port în edițiile anterioare, va trebui să înlăturați restricțiile de port pentru a putea folosi parametrul SSL. Pentru a elimina restricțiile, urmăriți acești pași:

1. Pentru afișarea restricțiilor de port, efectuați pașii următori:
 - a. Porniți Navigator iSeries^(TM) și expandați serverul dumneavoastră de rețea **Series** —> .
 - b. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Proprietăți**.
 - c. Faceți clic pe fișa **Restricții port**.
2. Pentru înlăturarea restricțiilor de port, continuați de la pasul de mai sus:
 - a. Selectați restricția de port pe care vreți să o ștergeți.
 - b. Faceți clic pe **Înlăturare**.
 - c. Faceți clic pe **OK**

Setarea implicită este de a porni SSL pe portul 992 și non-SSL pe portul 23. Serverul Telnet folosește intrarea pentru Telnet din tabela de servicii ca să afle portul non-SSL și Telnet-SSL ca să afle portul SSL.

Ce să faceți în continuare:

Asignați un certificat serverului Telnet

Asignarea unui certificat serverului Telnet: Când activați serverul Telnet pe sistemul dumneavoastră pentru a utiliza SSL, puteți stabili conexiuni Telnet sigure către sistemul dumneavoastră de la iSeries^(TM) Access pentru Windows^(R) sau de la alt client cu server Telnet activat, cum este un emulator Personal Communications. Înainte de a putea configura serverul Telnet pentru a folosi SSL, trebuie să fie instalate programele necesare și să setați certificatele digitale pe sistemul dumneavoastră.

1. Porniți IBM^(R) Digital Certificate Manager (DCM).

Notă:

Dacă aveți întrebări despre cum se completează un formular specific în timpul utilizării DCM, selectați semnul întrebării (?) de la începutul paginii pentru a accesa Ajutor online.

2. În cadrul de navigare, faceți clic pe **Selectarea unui depozit de certificate** și selectați fie ***OBJECTSIGNING** sau ***SYSTEM** ca depozit de certificate de deschis.
3. Introduceți o parolă pentru depozitul de certificate și faceți clic pe **Continuare**.
4. După împrăștierea cadrului de navigare, selectați **Gestionare certificate** pentru afișarea unei liste de task-uri.
5. Din lista de task-uri, selectați **Asignare certificat** pentru afișarea unei liste de certificate pentru depozitul de certificate curent.
6. Selectați un certificat din listă și faceți clic pe **Asignare la aplicații** pentru afișarea unei liste de definiții de aplicații pentru depozitul de certificate curent.
7. Selectați Telnet din listă și faceți clic pe **Continuare**. Se afișează o pagină fie cu un mesaj de confirmare pentru asignarea selecției dumneavoastră sau o eroare dacă a apărut o problemă.

Notă:

Baza de date chei clienți iSeries Access pentru Windows trebuie să conțină copia tuturor certificatelor Certificate Authority (CA) cerute. În acest caz, un certificat CA trebuie să existe în baza de date chei pentru certificatul asignat de dumneavoastră aplicației server Telnet. Baza de date chei este preconfigurată cu copii ale certificatelor CA de la aproximativ toate CA-urile cunoscute. Dacă alegeți să asigurați un certificat ce aparține unui CA local, atunci va trebui să adăugați o copie a certificatului la baza de date a clientului. Pentru a învăța să adăugați o copie a unui certificat CA Local, vedeți Pasul 5: Activați SSL pe clientul Telnet (page 13) din subiectul Telnet: Securitatea Telnet cu SSL - Detalii de configurare.

Serverul OS/400^(R) Telnet suportă autentificarea client ca o componentă opțională în configurația SSL. Autentificarea clientului apare când serverul verifică identitatea clientului prin autentificarea certificatului client transmis aplicației server.

Ce să faceți în continuare:

Activarea autentificării de client pentru serverul Telnet (pas opțional)

sau

Activarea SSL pe serverul Telnet

Activarea autentificării de client pentru serverul Telnet (pas opțional): Serverul Telnet suportă autentificarea certificatelor client Telnet. Aceasta înseamnă că în timpul negocierii SSL, serverul nu va genera numai certificatul pentru client, ci va căuta, opțional, un certificat client valid în funcție de cum este configurat Digital Certificate Manager (DCM). DCM vă va permite să configurați dacă Certificatele Client SSL sunt necesare pentru sesiuni Telnet.

Pentru a activa acest suport, administratorul de sistem va indica cum se lucrează cu suportul SSL. Utilizați panoul General din Proprietăți Telnet din Navigator iSeries^(TM) pentru a indica dacă SSL, non-SSL sau suportul pentru ambele va începe la pornirea serverului Telnet. Implicit, suporturile SSL și non-SSL pornesc întotdeauna.

Administratorul de sistem are posibilitatea de a indica dacă sistemul cere autentificare client SSL pentru toate sesiunile Telnet. Când SSL este activ și sistemul cere autentificarea clientului, prezența unui certificat client valid înseamnă că clientul este de încredere.

Sistemul aplică orice variabile negociate RFC 2877 și variabile de ieșire ale utilizatorului Telnet după îndeplinirea controalelor SSL.

Pentru a actualiza specificațiile aplicației din IBM^(R) DCM și pentru a activa autentificarea clientului pentru serverul Telnet, urmăriți pașii de mai jos:

1. Pornire IBM^(R) Digital Certificate Manager (DCM). Dacă aveți nevoie să obțineți sau să creați certificate, sau altfel să setați sau să modificați sistemul dumneavoastră de certificare, faceți asta acum. Vedeți Configurarea DCM pentru informații despre setarea unui sistem de certificare.
2. Faceți clic pe butonul **Selectarea unui depozit certificate**.
3. Selectați ***SYSTEM**. Selectați **Continuare**.
4. Introduceți parola corespunzătoare pentru depozitul de certificate ***SYSTEM**. Selectați **Continuare**.
5. Când meniul de navigare din stânga se reîncarcă, expandați **Gestiune aplicații**.
6. Faceți clic pe **Actualizare definiție aplicație**.
7. În ecranul următor, selectați aplicația **Server**. Selectați **Continuare**.
8. Selectați serverul **OS/400^(R) TCP/IP Telnet**.
9. Faceți clic pe **Actualizare definiție aplicație**.
10. În tabelul care este afișat, selectați **Da** pentru a cere autentificarea clientului.
11. Faceți clic pe **Aplicare**.
12. DCM se reîncarcă în pagina **Actualizare definiție aplicație** cu un mesaj de confirmare. Când ați terminat actualizarea definiției aplicației pentru serverul Telnet, faceți clic pe **Oprire**.

Pentru un exemplu despre ce are nevoie un client să facă pentru a activa autentificarea clientului prin certificat pentru o aplicație Telnet, consultați Activare autentificare client pentru o sesiune PC5250.

Ce să faceți în continuare:

Activarea SSL pe serverul Telnet

Exemplu: Activare autentificare client pentru o sesiune PC5250: După ce ați configurat SSL pentru serverul Telnet și ați specificat folosirea autentificării client, utilizatorilor li se va cere să furnizeze un certificat client valid și de încredere serverului Telnet pentru fiecare încercare de conexiune.

Clienții trebuie să creeze un certificat utilizator și să importe acel certificat către baza de date IBM^(R) Key Management database înainte ca clientul să se autentifice.

Crearea unui certificat utilizator în DCM

1. Pornire IBM^(R) Digital Certificate Manager (DCM). Dacă aveți nevoie să obțineți sau să creați certificate, sau altfel să setați sau să modificați sistemul dumneavoastră de certificare, faceți asta acum. Vedeți Configurarea DCM pentru informații despre setarea unui sistem de certificare.
2. Expandați **Creare certificat**.
3. Selectați **Certificat utilizator**. Selectați **Continuare**.
4. Completați formularul **Certificat utilizator**. Doar acele câmpuri marcate prin "Necesar" trebuie completate. Selectați **Continuare**.
5. În funcție de browser-ul pe care îl utilizați, vi se va cere să generați un certificat care va fi încărcat în browser-ul dumneavoastră. Urmați instrucțiunile furnizate de browser.
6. Când pagina **Creare certificat utilizator** se reîncarcă, faceți clic pe **Instalare certificat**. Aceasta va instala certificatul în browser.
7. Exportați certificatul pe PC-ul dumneavoastră. Trebuie să memorați certificatul într-un fișier protejat prin parolă.

Notă:

Se cer Microsoft^(R) Internet Explorer 5 sau Netscape 4.5 pentru utilizarea funcțiilor de exportare și importare.

Importarea certificatului în IBM Key Management

Trebuie să adăugați Autoritatea de certificare care a creat certificatul client în baza de date de chei a PC-ului, altfel importarea certificatului client nu va funcționa.

1. Faceți clic pe **Start** —> **Programs** —> **IBM iSeries^(TM) Access pentru Windows^(R)** —> **Proprietăți iSeries^(TM) Access pentru Windows^(R)**.
2. Selectați fișa **Secure Sockets**.
3. Faceți clic pe **IBM Key Management**.
4. Vi se va cere parola dumneavoastră pentru baza de date chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, ca400. Este afișat un mesaj de confirmare. Apăsați **OK**.
5. Din meniul derulant, selectați **Certificate personale**.
6. Faceți clic pe **Importare**.
7. În ecranul **Importare cheie**, introduceți numele fișierului și calea pentru certificat. Apăsați **OK**.
8. Introduceți parola pentru fișierul protejat. Aceasta este aceeași parolă pe care ați creat-o în Pasul 7 din Crearea unui certificat utilizator în DCM. Apăsați **OK**. Când certificatul a fost adăugat cu succes la certificatele dumneavoastră personale în IBM Key Management, puteți folosi emulatorul PC5250 sau orice altă aplicație Telnet.

Porniți o sesiune emulator PC5250 din Navigator iSeries

1. Deschideți Navigator iSeries.
2. Faceți clic pe numele sistemului dumneavoastră pe care ați setat autentificarea client pentru Telnet.
3. Selectați **Emulator terminal**.
4. Selectați meniul **Comunicație**, apoi selectați **Configurare**.
5. Faceți clic pe **Proprietăți**.
6. În dialogul **Conexiune**, selectați **Utilizare SSL (Secure Sockets Layer)**.

7. Dacă aveți mai mult de un certificat client, selectați fie **Selectare certificat la conectare** fie **Utilizare implicită** pentru a determina care certificat client să fie folosit.
8. Apăsați **OK**.
9. Apăsați **OK**.

Activare SSL pe serverul Telnet: Pentru a activa SSL pe serverul Telnet, urmați acești pași:

1. Deschidere Navigator iSeries^(TM).
2. Expandați **Serverul meu iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
3. Faceți clic dreapta pe **Telnet**.
4. Selectați **Proprietăți**.
5. Selectați fișa **General**.
6. Alegeți una din aceste opțiuni pentru suportul SSL:
 - **Numai securizat**
Selectați aceasta pentru a permite numai sesiunile SSL cu serverul Telnet.
 - **Numai non-securizat**
Selectați aceasta pentru a interzice sesiunile securizate cu serverul Telnet. Încercările de semnare la un port SSL nu se vor conecta.
 - **Atât securizat, cât și non-securizat**
Permite ambele sesiuni securizate și non-securizate cu serverul Telnet.

Ce să faceți în continuare:

Porniți serverul Telnet

Inițializare și dialog de confirmare (handshake) SSL

Uneori, a înțelege ceea ce se întâmplă în timpul procesării SSL vă poate ajuta la determinarea locului în care a apărut o problemă.

Ce se întâmplă în timpul inițializării SSL?

Serverul Telnet încearcă să inițializeze SSL la fiecare pornire a serverului. În timpul inițializării, serverul Telnet verifică informațiile de certificat din aplicația QIBM_QTV_TELNET_SERVER. Puteți spune că inițializarea SSL a avut succes atunci când apar mai multe joburi active QTVTELNET în subsistemul QSYSWRK. Bineînțeles, dacă câmpul cu numărul de joburi de pornit din pagina General a proprietăților este setat la 1, vedeți un singur job QTVTELNET activ.

Serverul Telnet nu inițializează SSL atunci când aveți un port telnet-ssl restricționat. Serverul Telnet trimite mesajul TCP2550 Accesul la portul 992 este restricționat istoricului jobului QTVTELNET și cozii de mesaje QSYSOPR.

Când un certificat este incorect sau expirat, inițializarea eșuează și serverul Telnet trimite mesajul CPDBC nn către istoricul jobului QTVTELNET.

Chiar dacă nici un certificat sau un certificat expirat nu este în aplicația QIBM_QTV_TELNET_SERVER, serverul Telnet inițializează cu succes SSL. Oricum, dialogul de confirmare (handshake) SSL eșuează atunci când clientul încearcă să se conecteze la serverul Telnet. Serverul Telnet trimite mesajul CPDBC nn către istoricul jobului QTVTELNET.

Ce se întâmplă în timpul reinițializării SSL?

Când certificatul din aplicația QIBM_QTV_TELNET_SERVER se modifică, serverul Telnet reinițializează SSL, dacă apare o modificare DCM. Aceasta înseamnă că puteți recupera un certificat expirat sau să adăugați și să înlăturați certificate utilizator și Telnet-ul va alege automat modificările. Procesul este același ca inițializarea SSL. Sesiunile

client Telnet SSL noi folosesc noul certificat. Sesiunile client Telnet SSL care sunt deja stabilite folosesc certificatul original. Odată ce serverul Telnet este oprit și apoi repornit, toate sesiunile client Telnet SSL folosesc noul certificat.

Dacă reinițializarea SSL eșuează, sesiunile SSL stabilite folosesc certificatul original care a fost inițializat când serverul a pornit și noile sesiuni sunt blocate pentru conectare. Data următoare când porniți serverul Telnet, inițializarea SSL eșuează, chiar dacă va mai fi încă un ascultător SSL activ. Totuși, nici o nouă conexiune SSL nu va fi cu succes până când o modificare în DCM nu forțează serverul Telnet să se reinițializeze cu succes.

Ce se întâmplă în timpul unui dialog de confirmare (handshake) SSL?

Un dialog de confirmare (handshake) SSL apare atunci când clientul Telnet SSL se conectează la portul TCP 992 și încearcă o negociere SSL cu serverul. În timp ce clientul se conectează la server, afișează numere de stare sau mesaje în bara de stare a ferestrei deschise.

Dacă dialogul de confirmare (handshake) SSL nu reușește, sesiunea Telnet nu se stabilește. De exemplu, un ecran de semnare în sistem nu apare în fereastra client Telnet SSL. Consultați ghidul utilizatorului sau ajutorul online al clientului Telnet SSL pentru informații despre anumite numere de stare sau mesaje. Serverul Telnet trimite mesajul CPDBC nn către istoricul jobului QTVTELNET.

Gestionarea serverului Telnet

Serverul Telnet iSeries^(TM) permite unui utilizator TCP/IP de pe un sistem client Telnet de la distanță să se semneze și să ruleze aplicații pe serverul iSeries. Suportul server Telnet iSeries negociază transmisia datelor cu aplicația client Telnet de la distanță pentru diverse moduri de operare.

Aplicațiile server și client Telnet negociază aceste moduri de operare. Funcțiile disponibile depind de tipul de terminal care este negociat.

Cu schimbări minime la valorile sistemului, serverul Telnet poate suporta conexiuni Telnet când pornește TCP/IP. Pentru toate modurile de operare cu excepția modului linie ASCII, serverul iSeries trimite automat ecranul de semnare iSeries când este făcută o conexiune Telnet. Pentru modul linie ASCII, trebuie să fie activă o aplicație a beneficiarului care afișează date.

Revedeți următoarele subiecte pentru a învăța cum să gestionați cu succes serverul Telnet:

Configurarea sesiunii de imprimare Telnet

Această secțiune furnizează instrucțiuni pentru legarea la imprimante pe serverul iSeries de pe locațiile de la distanță din rețea.

Terminarea sesiunii server

Acest subiect furnizează instrucțiuni pentru terminarea unei sesiuni Telnet. Terminarea sesiunii Telnet eliberează dispozitivul virtual pentru a fi folosit de o nouă sesiune Telnet.

Terminarea joburilor Device Manager

Uneori este necesar să opriți și să reporniți joburile Device manager, la aplicarea unui PTF programului. Acest subiect furnizează instrucțiuni pentru oprirea și repornirea joburilor Device Manager.

Folosirea programelor de ieșire Telnet

Găsiți informații despre utilizarea programelor de ieșire pentru serverul dumneavoastră Telnet.

Configurarea sesiunilor de imprimare Telnet

Pentru a funcționa emulatorul pentru imprimantă Telnet este nevoie de crearea unui dispozitiv imprimantă virtual iSeries^(TM) (va fi un dispozitiv 3812 sau 5553). Un astfel de dispozitiv este necesar pentru generarea șirurilor de date pentru imprimare trimise pentru sesiunea de imprimare. Imprimantele folosite pentru imprimare Telnet pot fi atașate

PC-ului sau atașate aceleași rețele cu PC-ul. Sesiunile de imprimantă Telnet negociază cu un client Telnet la distanță de pe un sistem care suportă emularea de imprimantă Telnet. Vedeți Cerințe pentru sesiunile de imprimare Telnet.

Sesiunile de imprimantă Telnet furnizează fluxul de date pentru imprimantă dintre două sisteme, fie în format EBCDIC, fie ASCII, în funcție de preferințele clientului solicitant.

Sesiunile de imprimantă Telnet sunt active imediat după inițializarea Telnet. Funcțiile de tipărire nu necesită profiluri de utilizator și parole. Totuși, dacă setările dumneavoastră de securitate o cer, puteți folosi programele punct de ieșire Telnet pentru blocarea pornirii sesiunilor de imprimare.

Când folosiți sesiuni de imprimantă Telnet, toate datele pentru imprimantă sunt păstrate într-o coadă de scriere pentru imprimantă. Nu puteți tipări direct la un dispozitiv de imprimantă. Comenzile pentru fișierul de imprimantă, de creare fișier de imprimantă (CRTPRTF), de modificare fișier de imprimantă (CHGPRTF) și de suprascriere fișier de imprimantă (OVRPRTF) trebuie să utilizeze parametrul implicit SPOOL(*YES). De asemenea, Telnet setează coada de ieșire sau scriitorul imprimantei la același nume ca și imprimanta.

Pentru a seta sesiunile de imprimantă Telnet, urmați acești pași:

1. Verificați pentru a fi sigur că stiva TCP este activă. Dacă nu, lansați comanda STRTCP pentru a porni stiva TCP.
2. Porniți serverul Telnet.
3. Setări numărului de dispozitive virtuale
4. Setări parametrul menținere-în-viață sesiune Telnet.
5. Creați controlere și dispozitive virtuale.
6. Activați subsistemul QSPL.
7. Testați configurarea cu un fișier de tipărire de test.
8. Tipăriți un fișier dintr-o sesiune de imprimantă Telnet.

Notă:

Subsistemul QSYSWRK pornește când pornește stiva TCP.

Necesitățile pentru sesiunile de imprimantă Telnet

Dacă intenționați să utilizați sesiunile de imprimantă Telnet, consultați furnizorul clientului Telnet pentru a vedea dacă asigură suport pentru funcția de sesiune imprimantă. Următorii clienți suportă funcția de sesiune imprimantă:

- IBM^(R) iSeries^(TM) Access pentru Windows^(R)
- Personal Communications
- IBM Host OnDemand

Sesiunile de imprimantă Telnet suportă următoarele imprimante generice EBCDIC:

- IBM-3812-1 pentru setul de caractere pe un octet (SBCS)
- IBM-5553-B01 pentru setul de caractere pe dublu octet (DBCS)

Puteți specifica fiecare din tipurile de dispozitive generice prin cererea funcției iSeries HPT (Host Print Transform) și selectarea tipului de fabricație specific. Dacă folosiți iSeries Access pentru Windows, puteți folosi PDT (Printer Definition Table) sau GDI (Graphical Device Interface) pentru a defini hardware-ul specific. Serverul iSeries trimite șirul de date pentru imprimare în ASCII.

Îmbunătățirea API-ului sistem API-ul sistem QDCRDEVD (Retrieve Device Description), furnizează adresa IP a clientului Telnet. Există câteva câmpuri pentru dispozitive de afișare (*DSP) și de tipărire (*PRT) : protocol de Rețea, adresa protocolului de Rețea și adresa internet IP în forma cu puncte. Aceste câmpuri furnizează informații, la nivelul socket-urilor, aplicației dumneavoastră, despre conexiunea TCP/IP a clientului.

Pentru mai multe informații consultați:

Suportul de imprimare al serverului Telnet pentru clientul Telnet iSeries Access pentru Windows

Terminarea sesiunii server

Când sunteți conectat la un server iSeries^(TM), făcând sing-off nu înseamnă neapărat că ați terminat sesiunea pe serverul Telnet. Ecranul virtual sau dispozitivul imprimantă este încă activ și nu poate fi folosit de către altă sesiune Telnet. Pentru a închide această sesiune, trebuie să introduceți o tastă sau o secvență de taste pentru a poziționa clientul Telnet în modul comandă locală. Puteți apoi tasta comanda pentru închiderea sesiunii. Folosiți următoarea secvență de taste pentru a termina o sesiune server Telnet.

- Din serverul iSeries, apăsați tasta **Attn** și selectați opțiunea **99** (End Telnet session - QUIT).
- Din cele mai multe alte sisteme, deconectați-vă.

Dacă nu știți ce tastă sau ce secvență de taste să apăsați pentru a determina clientul să intre în modul comandă, consultați administratorul de sistem sau documentația pentru clientul Telnet.

Puteți utiliza și parametrul terminare conexiune (ENDCNN) al comenzii SIGNOFF pentru a închide sesiunea de pe sistemul server și pentru a termina conexiunea Telnet. De exemplu, SIGNOFF ENDCNN(*YES) vă întoarce pe sistemul client (dacă ați stabilit numai o sesiune Telnet). Sau vă întoarce pe sistemul anterior (dacă ați stabilit mai multe sesiuni Telnet).

Terminare joburi Device Manager

Pornirea și oprirea Telnetului termină joburile serverului Telnet, dar nu și pe cele Device Manager. Aceasta se întâmplă deoarece natura joburilor Device Manager cere ca ele să ruleze tot timpul sau cel puțin până la o nouă repornire a sistemului. Pentru a face ciclul de joburi Device Manager, trebuie să completați pașii speciali 2 și 3. Apoi, următoarea dată când porniți Telnet, va observa că nu sunt joburi Device Manager care rulează și le va porni. Completați următorii pași pentru a termina joburi din Device Manager:

1. Terminați joburile server Telnet active, efectuând următorii pași:
 - a. Porniți Navigator iSeries^(TM) și expandați serverul dumneavoastră de rețea **iSeries** → → **Servers** → **TCP/IP**.
 - b. Faceți clic dreapta pe **Telnet** și selectați **Oprire**.
2. Găsiți toate joburile manager dispozitive Telnet active efectuând următorii pași:
 - a. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** → **Control funcționare**.
 - b. Selectați **Joburi active**.
 - c. Căutați QTVDEVICE.
3. Terminați toate joburile găsite la pasul 2 făcând clic dreapta și selectând **Ștergere/Oprire**. Trebuie să așteptați ca toate joburile să iasă înainte de a trece la pasul următor.
4. Porniți serverul Telnet și joburile managerului de dispozitive din panoul **Ștergere/Oprire**.
Orice dispozitive virtuale Telnet care sunt încă în procesul de terminare când toate joburile Device Manager s-au terminat, pot deveni inaccesibile până la o nouă repornire a sistemului.

Utilizarea programelor punct de ieșire Telnet

Cu folosirea programelor de ieșire, programatorul experimentat poate crea procesări proprii în timpul unei aplicații. Dacă serverul Telnet găsește un program înregistrat la unul din punctele de ieșire pentru server, el apelează acel program folosind parametrii definiți de acel punct de ieșire.

Un **punct de ieșire** este un punct specific în programul Telnet unde controlul poate trece la un program de ieșire. Un **program de ieșire** este un program căruia punctul de ieșire îi pasează controlul.

Pentru fiecare punct de ieșire, există un API numit **interfață punct de ieșire**. Punctul de ieșire folosește această interfață pentru a pasa informații între aplicația Telnet și programul de ieșire. Fiecare punct de ieșire are un nume unic. Fiecare interfață punct de ieșire are un format de punct de ieșire care definește cum este transmisă informația între aplicația Telnet și programul de ieșire scris de utilizator.

Diferite puncte de ieșire pot împărți aceeași interfață punct de ieșire. Când se întâmplă acest lucru, puncte de ieșire multiple pot apela un singur program de ieșire.

Pentru mai multe informații despre folosirea programelor de ieșire, consultați:

Program de ieșire inițializare dispozitiv Telnet

Vă permite să asociați programul dumneavoastră de ieșire personalizat cu puncte de ieșire pe serverul Telnet iSeries^(TM).

Program de ieșire terminare dispozitiv Telnet

Vă permite să înregistrați informații de terminare sesiune.

Exemple de programe de ieșire Telnet

Puteți descărca exemple de programe de ieșire TELNET pentru a vă asista la scrierea programelor de ieșiri.

Performanță punct de ieșire

Timpul de răspuns al serverului Telnet pentru cererea inițială de sesiune va include tot timpul necesar serverului să apeleze, să proceseze și să returneze programul de ieșire QIBM_QTG_DEVINIT. Dacă programul dumneavoastră de ieșire procesează semnificativ, va rezulta o așteptare mai mare înainte ca sesiunea dumneavoastră să fie stabilă. Dacă doriți să modificați valoarea timeout implicită de 60 de secunde pentru programele de ieșire utilizator, puteți folosi comanda ADDEXITPGM pentru a adăuga date utilizator care vor fi citite ca valoare timeout. În următorul exemplu, parametrul PGMDTA rescrie timeout-ul implicit de 60 de secunde la 10 secunde:

```
ADDEXITPGM EXITPNT(QIBM_QTG_DEVINIT) FORMAT(INIT0100)
PGMNBR(1) PGM(USEREXIT/DEVINIT2) REPLACE(*YES)
CRTEXITPNT(*NO) PGMDTA(*JOB *CALC 10)
```

O dată ce programul Telnet este stabilit de un panou de semnare sau alt panou server iSeries, nu este afectată performanța. Când acesta apare, programul de ieșire nu mai este în calea Telnet. Sesiunile Telnet stabilite nu au nici o întârziere datorită programului de ieșire QIBM_QTG_DEVINIT.

Nu există nici un impact asupra performanțelor vizibil utilizatorului care este asociat cu deconectarea sesiunii. Deconectare înseamnă că închideți sesiunea de emulare terminal, nu că faceți sign-off și vă întoarceți la panoul de semnare. Dacă vă deconectați, atunci este apelat programul de ieșire QIBM_QTG_DEVTERM, care va realiza procedura de deconectare pentru sesiunea dumneavoastră. Utilizatorii nu vor vedea acest lucru deoarece apare după ce conexiunea s-a întrerupt.

Controlul funcționării

Puteți rezolva probleme cheie de control al funcționării folosind programul de ieșire Telnet. Aceste probleme includ posibilitatea de a cere descrieri de dispozitive altele decât QPADEVxxxx, deschizând ușa pentru controlul de către Work Management (Control funcționare) a joburilor stații de lucru virtuale interactive și rutarea acestor joburi subsistemelor specifice.

Rutarea subsistem și selecția numelui de dispozitiv

Recomandarea curentă este ca orice subsistem dat, de exemplu, QBASE, QCMN sau QINTER, să servească cel mult 300 de utilizatori.

Utilizatorii pot folosi avantajos numele de dispozitive virtuale Telnet mai bune și configura subsistemele lor interactive pentru a diviza munca, dacă este necesar. Aceasta este realizată folosind comanda Adăugare intrare stație de lucru (ADDWSE). Această comandă vă permite să specificați căror dispozitive un subsistem trebuie sau nu trebuie să le aloce nume particulare de dispozitive terminale virtuale.

Următoarea comandă face ca QINTER să aloce toate stațiile de lucru QPADEV*, ceea ce înseamnă că toate dispozitivele de acel fel sunt rutate spre subsistemul QINTER:

```
ADDWSE SBS(D(QINTER) WRKSTN(QPADEV*) AT(*SIGNON)
```

Următoarea comandă face ca QINTER să nu aloce toate stațiile de lucru QPADEV*, ceea ce înseamnă că aceste dispozitive pot fi alocate unui alt subsistem:

```
ADDWSE SBS(D(QINTER) WRKSTN(QPADEV*) AT(*ENTER)
```

Utilizatorii pot dezvolta propriile convenții de denumire a dispozitivelor pentru a diviza munca. De exemplu, un tip de subdiviziune este de a ruta anumite dispozitive subsistemelor legate de NLS în două locații.

Exemplu

Pentru scopul acestui exemplu, cei doi utilizatori sunt în Chicago și New York. Utilizatorii sunt asociați subsistemelor iSeries CHICAGO și NEWYORK, respectiv, în funcție de localizarea lor geografică. Caracteristicile acestui exemplu include:

- Adresele IP pentru Chicago încep cu 1.2.3.* .
- Adresele IP pentru New York încep cu 2.3.4.* .
- Pentru ca toate sesiunile Telnet din Chicago să ruleze în subsistemul CHICAGO, este folosit programul de ieșire al utilizatorului. Programul de ieșire creează un nume de dispozitiv virtual care începe cu 'CHICAGO' pentru toate conexiunile Telnet de la 1.2.3. Programul de ieșire utilizator creează, de asemenea, nume de dispozitiv virtual care începe cu 'NEWYORK' pentru toate conexiunile de la 2.3.4.
- Programul de ieșire utilizator asignează numele de dispozitiv virtual 'CHICAGO01' pentru adresa IP 1.2.3.47. Programul asignează un numele de dispozitiv virtual 'NEWYORK01' pentru adresa IP 2.3.4.48. Programul atașează o parte variabilă ('01', '02', etc.) numelui rădăcină 'CHICAGO' și verifică dacă dispozitivul nu este deja în folosință înainte de a-l asigna utilizatorului curent.

Pentru a vă asigura că dispozitivele virtuale CHICAGO01 și NEWYORK01 sunt în subsistemele Chicago și respectiv New York, setați intrările stațiilor de lucru după cum urmează:

```
ADDWSE SBS(D(QINTER) WRKSTN(CHICAGO*) AT(*ENTER)
ADDWSE SBS(D(QINTER) WRKSTN(NEWYORK*) AT(*ENTER)
ADDWSE SBS(D(CHICAGO) WRKSTN(CHICAGO*) AT(*SIGNON)
ADDWSE SBS(D(NEWYORK) WRKSTN(NEWYORK*) AT(*SIGNON)
```

Program de ieșire inițializare dispozitiv

Aplicația server Telnet include puncte de ieșire care vă permit să intrați în logica Telnet de semnare și terminare. Puteți folosi comenzile iSeries^(TM) WRKREGINF (Work with Registration Information - Gestionare informații de înregistrare) sau ADDEXITPGM (Add Exit Program - Adăugare program de ieșire) pentru a asocia programul dumneavoastră de ieșire personalizat la un punct de ieșire. Dacă serverul Telnet găsește un program înregistrat la unul din punctele de ieșire pentru server, el apelează acel program folosind parametrii definiți de acel punct de ieșire. Acești parametrii includ adresa IP, numele utilizatorului și numele dispozitivului virtual. Programul personal de ieșire procesează apoi această informație, de exemplu, înregistrează un mesaj și returnează controlul serverului Telnet. La revenire, programul dumneavoastră de ieșire spune serverului să accepte sau să respingă acest client și orice utilizator opțional sau parolă pe care o suprascrise.

Orice punct de ieșire are un nume și o interfață punct de ieșire. Interfața punct de ieșire este o listă de parametrii de intrare și ieșire pe care serverul Telnet îi schimbă cu programul dumneavoastră de ieșire. Există două puncte de ieșire pentru serverul Telnet:

- QIBM_QTG_DEVINIT
- QIBM_QTG_DEVTERM

Grup de parametri necesari:

1	Informația de descriere a utilizatorului	I/O	Char(*)
---	--	-----	---------

2	Informația de descriere a dispozitivului	I/O	Char(*)
3	Informația de descriere a conexiunii	Intrare	Char(*)
4	Opțiunii de mediu	Intrare	Char(*)
5	Lungimea opțiunilor de mediu	Intrare	Binary(4)
6	Permite conexiune	Ieșire	Char(1)
7	Permite semnarea automată	Ieșire	Char(1)

Numele membrului QSYSINC : ETGDEVEX
Numele punctului de ieșire: QIBM_QTG_DEVINIT
Numele formatului punctului de ieșire: INIT0100

Serverul Telnet furnizează opțional numele dispozitivului pentru selectare sau setare, pentru a fi folosit în timpul sesiunii Telnet și permite unui client TELNET să treacă peste inițializările tradiționale de dispozitive. Administratorii pot controla aceste noi facilități în timpul folosirii unui nou program de ieșire, care va porni opțional chiar după stabilirea sesiunii client. Mai mulți parametri vor fi furnizați programului de ieșire pentru a fi folosiți în procesul de decizie și programul de ieșire poate seta sau modifica diverși parametri înainte de a se reveni la serverul Telnet. Puteți să înregistrați opțional un al doilea program de ieșire pentru a porni chiar înainte de a se termina sesiunea. Puteți folosi al doilea program de ieșire pentru controlul sesiunii sau gestionarea dispozitivelor virtuale.

Formatul punctului de ieșire Telnet INIT0100:

- Grup de parametri necesar
- Informații descriere utilizator
- Informații descriere dispozitiv
- Informații descriere conexiune

Formatul punctului de ieșire Telnet INIT0100: Grup de parametri necesari: Informații de descriere utilizator
I/O; CHAR(*) Informație despre utilizator pe care sistemul o va folosi ca parte în procesul de semnare automată.

Informații de descriere dispozitiv

I/O; CHAR(*) Informație despre utilizator pe care sistemul o va folosi pentru a crea sau schimba dispozitivul pe care-l va folosi în această sesiune Telnet.

Informații de descriere conexiune

I/O; CHAR(*) Informația despre conexiunea client pe care programul de ieșire o poate folosi.

Opțiuni mediu

INPUT; CHAR(*) Un vector care conține toate opțiunile mediului RFC 2877 negociate de către client. Acestea vor fi în formatul exact în care erau când au fost recepționate de la client și specificate de RFC 2877. Șirul va fi, în general, constituit din una sau mai multe perechi de nume de variabile de mediu și valorile asociate. RFC-ul specifică faptul că fiecare nume de variabilă va fi precedat fie de X'01' fie de X'03' dacă este un VAR definit RFC 2877 sau un USERVAR definit de o anumită aplicație. Dacă o valoare va fi asociată cu VAR (sau USERVAR), acea valoare va apare următoarea în șir precedată de caracterul VALUE X'01' definit de RFC 1572. Secvența de perechi VAR/VALUE se va repeta până la maxim 1024 octeți de date negociate.

RFC 2877 și RFC-urile de negociere Telnet mult mai generale permit de asemenea caracterelor de control să apară în numele de variabile VAR/USERVAR sau în valorile lor asociate. Aceasta este permisă prin utilizarea caracterului ESC X'02' și a regulilor care se aplică atunci când caracterul ESC sau caracterele de control Telnet IAC trebuie să apară în secvența de negociere. Consultați RFC 1572 pentru o descriere mai completă a regulilor privind caracterele de control ESC.

În timp ce buffer-ul opțiunilor de mediu va arăta negocierile în funcție de client, incluzând parole, Telnet va suprapune întotdeauna orice text în clar sau valori parolă criptate în buffer pentru a evita problemele de securitate.

Lungimea opțiunilor de mediu

Lungimea opțiunilor de mediu referite în paragraful precedent este de obicei de 1024 de octeți. Cum negocierile de opțiune sunt de lungime nedefinită, orice negociere care depășește lungimea specificată poate fi trunchiată pentru a se potrivi în buffer-ul opțiunilor de mediu.

Permiterea conexiunii

OUTPUT; CHAR(1) Se aplică tuturor dispozitivelor și indică serverului Telnet dacă ar trebui să permită clientului conectarea. Dacă tipul de dispozitiv este DISPLAY și aveți activată opțiunea conectare automată, atunci acest client poate de asemenea să treacă de panoul de semnare de pe serverul iSeries^(TM). Valori valide sunt următoarele:

- 0 - Refuzarea cererii de la client
- 1 - Acceptarea cererii de la client

Permiterea semnării automate

OUTPUT; CHAR(1) Se aplică tipurilor de dispozitive DISPLAY și indică serverului Telnet dacă ar trebui să permită acestui client operația de semnare automată. Dacă este permisă semnarea automată, atunci acest client poate ocoli panoul de semnare pe serverul iSeries. Valori valide sunt următoarele:

- 0 - Refuzarea cererii pentru aplicație de la client. Sistemul va ignora profilul utilizatorului, biblioteca curentă, programul de apelat, meniul inițial și parametrii de ieșire ai numelui dispozitivului.
- 1 - Acceptarea cererii pentru aplicație de la client. Sistemul va considera profilul utilizatorului, biblioteca curentă, programul de apelat, meniul inițial și parametrii de ieșire ai numelui dispozitivului valide dacă programul de ieșire le returnează.

INIT0100: Formatul informației de descriere a utilizatorului: Procesul de semnare automată va folosi informația despre utilizator.

Următoarea tabelă arată formatul informației de descriere a utilizatorului:

Tabela 1. Formatul Informațiilor de descriere utilizator

Offset zecimal	Offset hexazecimal	Tip	Câmp
0	0	INT(4)	Lungimea informațiilor de descriere utilizator
4	4	CHAR(10)	Profil utilizator
14	E	CHAR(10)	Biblioteca curentă
24	18	CHAR(10)	Programul de apelat
34	22	CHAR(10)	Meniul inițial

Descrierile câmpului informații de descriere utilizator

Biblioteca curentă

Numele bibliotecii care va fi biblioteca curentă dacă activați stegulețul de semnare automată. Acest parametru este opțional, dar dacă îl furnizați, trebuie să-l aliniați la stânga și să-l mărginiți cu blankuri. Valori valide sunt următoarele:

Nume bibliotecă

Numele bibliotecii pe care ai vrea ca sistemul să o desemneze ca bibliotecă curentă

Meniu inițial

Numele meniului inițial pentru afișare dacă ați activat stegulețul de semnare automată. Valori valide sunt următoarele:

Nume meniu

Numele meniului de afișat

Lungimea informațiilor de descriere utilizator

Lungimea structurii informației de descriere a utilizatorului

Programul de apelat

Numele programului pe care-l va apela sistemul dacă ați activat stegulețul de semnare automată. Acest parametru este opțional, dar dacă îl furnizați, trebuie să-l aliniați la stânga și să-l mărginiți cu blankuri. Valori valide sunt următoarele:

nume program

Numele unui program pe care serverul îl va porni

Profil de utilizator

Profilul utilizatorului pe care sistemul îl folosește în procedura de semnare dacă ați activat stegulețul de semnare automată. Sistemul necesită acest parametru, trebuie să-l aliniați la stânga și să-l completați cu blankuri.

INIT0100: Formatul informației de descriere a dispozitivelor: Informații care vor fi folosite pentru a crea sau modifica dispozitivul folosit pentru această sesiune Telnet.

Următoarea tabelă arată formatul informației de descriere a dispozitivului, care specifică caracteristicile dispozitivului asociat cu aceasta sesiune.

Tabela 1. Formatul informațiilor de descriere dispozitiv

Offset zecimal	Offset hexazecimal	Tip	Câmp
0	0	CHAR(10)	Numele dispozitivului
10	A	CHAR(8)	Formatul dispozitivului
18	12	CHAR(2)	Rezervat
20	14	BINARY(4)	Offset la structura atributelor dispozitivului
24	18	BINARY(4)	Lungimea structurii atributelor dispozitivului
28	1C	CHAR(*)	Structura atributelor dispozitivului

Descrierile câmpului cu informații de descriere conexiune

Nume dispozitiv

Dispozitivul virtual specific pentru a fi asociat cu această sesiune Telnet. Pentru dispozitive de afișare (DISPLAY), dacă valoarea de sistem a dispozitivului de auto-creare QAUTOVRT îi permite, dispozitivul va fi auto-creat de sistem, dacă nu există deja, și în continuare activat (vary on). Pentru dispozitive de tipărire (PRINT), sistemul va auto-crea dispozitive dacă nu există deja. Dacă programul de ieșire nu furnizează nici o valoare, serverul Telnet va folosi automat metodele de selecție tradiționale ale dispozitivelor virtuale Telnet. Ar trebui să fie un DISPLAY valid sau un nume descriptiv de dispozitiv PRINT și trebuie să se conforme denumirii convenționale ale obiectului OS/400.^(R)

Formatul dispozitivului

Tipul dispozitivului virtual specific care este asociat cu această sesiune Telnet. În mod curent, doar dispozitivele de afișare pe care sistemul le suportă.

DSPD0100

Dispozitivul este de afișare. Sistemul returnează atributele dispozitivului de afișare.

Rezervat

Rezervat pentru folosire în viitor.

Offset la structura de atribute a dispozitivului

Offset-ul de la începutul informației de descriere a dispozitivului până la începutul structurii atributelor dispozitivului.

Lungimea structurii de atribute a dispozitivului

Lungimea în spațiul utilizatorului a structurii atributelor dispozitivului.

INIT0100: Formatul informațiilor de descriere a dispozitivului de afișare (DSPD0100)

Următoarea tabelă arată formatul informației de descriere a dispozitivului, care specifică caracteristicile dispozitivului asociat cu aceasta sesiune.

Tabela 2. Formatul informațiilor de descriere a dispozitivului de afișare (DSPD0100)

Offset zecimal	Offset hexazecimal	Tip	Câmp
0	0	CHAR(3)	Identificator de tastatură
3	3	CHAR(1)	Rezervat
4	4	BINARY(4)	Pagină de cod
8	8	BINARY(4)	Setul de caractere

DSPD0100 Descrieri câmp

Set caracter

Specifică setul de caractere pe care sistemul le folosește pentru acest job interactiv. Puteți găsi valori valide în Suportul pentru limbi naționale. Acest câmp este identic cu parametrul Set de caractere din API-ul Open Virtual Terminal Path QTVOPNVT.

Pagină de cod

Specifică pagina de cod pe care sistemul o folosește pentru acest job interactiv. Puteți găsi valori valide în Suportul pentru limbi naționale. Acest câmp este identic cu parametrul Pagină de cod din API-ul Open Virtual Terminal Path QTVOPNVT.

Identificator tastatură

Specifică identificatorul de tastatură pe 3 caractere pe care sistemul le folosește pentru acest job interactiv. Identificatorul de tastatură specifică implicit pagina de cod și setul de caractere care trebuie folosit, dacă nu sunt suprascrise ca parte a parametrilor Pagină de cod și Set de caractere. Puteți găsi identificatorii valizi în Suportul pentru limbi naționale. Acest câmp este identic cu parametrul Tip limbă tastatură din API-ul Open Virtual Terminal Path QTVOPNVT.

Rezervat

Rezervat pentru folosire în viitor.

INIT0100: Formatul informației de descriere a conexiunii: Informații despre conexiunea client pe care programul de ieșire o poate folosi.

Următoarea tabelă arată formatul informației de descriere a conexiunii, care descrie clientul și informația despre conexiune pentru această sesiune.

Tabela 1. Formatul informației de descriere conexiune

Offset zecimal	Offset hexazecimal	Tip	Câmp
0	0	INT(4)	Lungimea informației de descriere a conexiunii
4	4	CHAR(20)	Adresa internet a clientului
24	18	CHAR(1)	Parola client validată
25	19	CHAR(12)	Tipul stației de lucru
39	27	CHAR(1)	Conexiune SSL

Offset zecimal	Offset hexazecimal	Tip	Câmp
40	28	CHAR(20)	Adresă internet (locală) server
60	3C	CHAR(1)	Nivel de autentificare client
61	3D	CHAR(3)	Rezervat
64	40	INT(4)	Certificat client valid
68	44	INT(4)	Offset la certificat client
72	48	INT(4)	Lungime certificat client

Descrierile câmpului de informații de descriere conexiune

Lungimea informației de descriere conexiune

Lungimea structurii de descriere a conexiunii

Adresă internet client

Aceasta este adresa IP (sau structura tip) a clientului și este totdeauna furnizată programului de ieșire. Structura câmpurilor noi este :

Tabela 2. Macheta adresei IP client

Nume	Dimensiune	Descriere
sin_len	CHAR(1)	Dimensiunea structurii sockaddr_in
sin_family	CHAR(1)	Familie sau protocol. IP (Versiunea 4) este hex 02.
sin_port	CHAR(2)	Numărul fără semn al portului pe 16 biți.
sin_addr	CHAR(16)	4 octeți fără semn

Parola client validată

Specifică dacă Telnet a validat parola codată a clientului (dacă a fost recepționată una). Sistemul va seta această valoare dacă ClientiiTN5250E trimite parola codată pentru validare. Parola va fi verificată folosind apelurile funcțiilor serviciu. Aceasta permite programului de ieșire să garanteze un proces de semnare client sigur.

- Valoare = 0, Parola/formula de acces client (sau tichetul Kerberos) nu a fost validată sau nu a fost recepționat nimic.
- Valoare = 1, Parola/formula de acces client în text în clar a fost validată
- Valoare = 2, Parola/formula de acces client codată (sau tichetul Kerberos) a fost validată

Tipul stației de lucru

Tipul stației de lucru cerut de client și va fi una din Specificațiile internet menționate în tabela Stație de lucru și mapare imprimantă (page 83).

SSL (Secure socket layer)

Aceasta indică dacă conexiunea este o conexiune SSL.

- **0** - Conexiunea nu folosește SSL (Secure Sockets Layer).
- **1** - Conexiunea folosește SSL (Secure Sockets Layer).

Adresă internet server

Aceasta este adresa IP (sau structura tip) a interfeței de rețea a gazdei (locală) și este totdeauna furnizată programului punctului de ieșire. Structura câmpurilor noi este :

Tabela 3. Macheta adresei IP client

Nume	Dimensiune	Descriere
sin_len	CHAR(1)	Dimensiunea structurii sockaddr_in
sin_family	CHAR(1)	Familia protocolului IP este 02h, IPX este 06h
sin_port	CHAR(2)	Numărul fără semn al portului pe 16 biți
sin_addr	CHAR(16)	Adresa de rețea fără semn pe 4 octeți

Nivelul de autentificare client

Indică dacă certificatele SSL ale clientului sunt necesare pentru conectarea la server.

0 - Nici un certificat client nu este necesar.

1 - Un certificat client valid este necesar.

Cod retur valid certificat client

Indică codul return primit în timpul negocierii SSL când se validează certificatul client.

Offset la certificat client

Indică offset-ul de la începutul structurii conexiunii până la primul octet al certificatului client.

Lungime certificat client

Indică lungimea certificatului client care a fost primit. Dacă nici un certificat nu a fost primit, lungimea este 0.

Program de ieșire pentru terminare dispozitiv

Punctul de ieșire QIBM_QTG_DEVTERM apare când un client Telnet termină o sesiune Telnet. Aceasta dă clienților posibilitatea de a înregistra în istoric (log) informația de terminare a sesiunii și a face operațiile de resetare și curățare dispozitiv.

Următoarea tabelă arată parametrii pentru punctul de ieșire QIBM_QTG_DEVTERM.

1	Numele dispozitivului	Intrare	Char(10)
---	-----------------------	---------	----------

Numele membrului QSYSINC : NONE

Numele punctului de ieșire: QIBM_QTG_DEVTERM

Numele formatului punctului de ieșire: TERM0100

Nume dispozitiv

Dispozitivul virtual specific pentru a fi asociat cu această sesiune Telnet.

Serverul Telnet va furniza opțional pentru oprirea dispozitivului, activități de auditare a sesiunii, gestionarea dispozitivelor virtuale care sunt legate de dispozitivul asociat cu sesiunea Telnet terminată.

Grup de parametri necesari

Nume dispozitiv

Intrare; CHAR(10) Dispozitivul virtual specific asociat cu această sesiune Telnet.

Exemple de programe de ieșire Telnet



Programele exemplu sunt disponibile pentru a vă ajuta să folosiți punctele de ieșire Telnet pe serverul dumneavoastră.

Notă: Citiți Declinarea responsabilității pentru exemplul de cod pentru informații juridice importante.

Descărcarea cu exemplu conține următoarele resurse:

- **Exemplu de cod utilitar CL program de ieșire Create Telnet (TELCRT)**
Acesta este un cod de exemplu funcțional pentru programul utilitar ce crează, instalează și înregistrează programele de ieșire Telnet. Este scris în limbajul de programare CL (Command Language) OS/400^(R).
- **Exemplu de cod utilitar CL program de ieșire Delete Telnet (TELDTL)**
Acesta este un cod de exemplu funcțional pentru programul utilitar ce dezinstalează și șterge programele de ieșire Telnet. Este scris în limbajul de programare CL OS/400.
- **Exemplu simplu de program de ieșire inițializare Telnet (DEVINIT1)**
Programul de ieșire inițializare Telnet (DEVINIT1) vă lasă să filtrați clienții Telnet. Dumneavoastră decideți cine poate să se conecteze la serverul Telnet și cine nu. Acest exemplu este simplu deoarece nu este conceput să beneficieze de multe alte funcții disponibile pentru programele de ieșire Telnet. Programul avansat de ieșire Telnet este conceput să beneficieze de aceste funcții.
Este recomandabil să începeți cu programul simplu de ieșire inițializare Telnet, pentru a înțelege cum lucrează și apoi migrați la programul avansat de ieșire inițializare Telnet, dacă aveți nevoie de maparea Virtual Device sau alte funcții avansate.
- **Exemplu avansat de program de ieșire inițializare Telnet (DEVINIT2)**
Programul avansat de ieșire inițializare (logon) Telnet folosește listele de acces MAP și DISALLOW. Folosind lista MAP, în locul listei mai simple ALLOW, programul avansat de inițializare exploatează mai mult din interfața punctelor de ieșire, decât versiunea simplă. Vă permite să setați sau să înlocuiți setările sesiunii Telnet, o funcție pe care o vedeți în mod normal în mediile Client Access. Mai jos sunt câteva exemple de setări de sesiune pe care le puteți face:
 - Selectarea unui dispozitiv Terminal virtual pentru această sesiune
 - Ocolirea panoului de semnare
 - Setarea suportului NLS
- **Exemplu de program de ieșire terminare Telnet (DEVTERM)**
DEVTERM QCSRC este un program de înregistrare în istoric care înregistrează mesajul de deconectare.
Acesta este un program de acompaniere atât pentru DEVINIT1 QCSRC, cât și pentru DEVINIT2 QCSRC. Mesajele de terminare pe care le înregistrează pot fi comparate cu mesajele de inițializare pentru a determina durata sesiunii Telnet.

Fișierele cu exemplele de programe de ieșire Telnet

Există două tipuri de formate de fișier disponibile la descărcare: ZIP și SAVF. Ambele formate conțin aceleași fișiere.

Fișierele .zip sunt într-un format care este compatibil cu PC-urile. Alegeți fișierul .zip ca să descărcați fișierele de program și de informații pe PC, dezarhivați-le, apoi transferați-le ul pe serverul iSeries^(TM). Va fi nevoie să redenumiți, odată ajunse pe serverul iSeries.

Un fișier .savf este un fișier de salvare OS/400. Descărcați-l pe PC, apoi transferați-l pe serverul iSeries. IBM recomandă să creați o bibliotecă temporară pe iSeries și transferați fișierul de salvare în ea. Despachetați fișierul de salvare din biblioteca temporară și urmați instrucțiunile din fișierul READ.ME.

Faceți clic pe legătura pentru formatul de fișier pe care-l doriți, apoi alegeți **Save**.

- telnet.zip (924 KB)
- telnet.savf (5.45 MB)



Gestionarea clientului Telnet

Clientul Telnet iSeries^(TM) permite unui utilizator iSeries TCP/IP să se semneze și să folosească aplicații pe un sistem la distanță cu o aplicație server Telnet.

Telnet vă permite să vă conectați la un calculator la distanță și să îl folosiți ca și cum ați fi direct conectat la el. Puteți rula programe, schimba configurații sau pur și simplu orice ați putea face dacă ați sta chiar dumneavoastră în fața calculatorului la distanță.

Telnet face calculatorul dumneavoastră să pară o stație de lucru a unui calculator mainframe. Cu alte cuvinte, când folosiți Telnet, calculatorul dumneavoastră (clientul) pretinde a fi sau emulează, un terminal direct conectat la calculatorul la distanță (serverul Telnet).

Clientul Telnet suportă de asemenea RFC 2877. Clienții RFC 2877 au mai mult control peste dispozitivul virtual server Telnet pe iSeries prin câțiva noi parametri la comanda STRTCPTELN (TELNET). Noii parametri sunt:

- Terminal virtual la distanță (RMTVRTDSP)
- Utilizatorul la distanță (RMTUSER)
- Parolă la distanță (RMTPWD) (incluzând suport pentru parole noi pe 128 octeți dacă severul Telnet le suportă)
- Criptarea parolei la distanță (RMPWENC) (incluzând criptările DES7 și SHA1)
- Program inițial la distanță (RMTINLPGM)
- Meniu inițial la distanță (RMTINLMNU)
- Biblioteca curentă la distanță (RMTCURLIB)
- Tipul de tastatură la distanță (RMTKBDTYPE)
- Setul de caractere la distanță (RMTCHRSET)
- Pagina de cod la distanță (RMTCODPAG)

Pentru mai multe informații despre lucrul cu clientul Telnet, consultați următoarele:

Serverul Telnet de control funcționează de pe client

Controlați procesarea pe stația de lucru de pe serverul Telnet, atunci când vă aflați într-o sesiune client.

Sesiunile client Telnet 5250

Această secțiune furnizează informații despre folosirea acestui tip de emulare pentru conectare și folosire aplicații pe un sistem la distanță care are o aplicație server Telnet.

Sesiunile client Telnet 3270

Această secțiune furnizează informații despre folosirea acestui tip de emulare pentru conectare și folosire aplicații pe un sistem la distanță care are o aplicație server Telnet. Această secțiune furnizează de asemenea informații suplimentare despre emularea 3270.

Sesiunile client Telnet VTxxx

Această secțiune furnizează informații despre folosirea acestui tip de emulare pentru conectare și folosire aplicații pe un sistem la distanță care are o aplicație server Telnet. Această secțiune furnizează de asemenea informații suplimentare despre emularea VTxxx.

Stabilirea unei sesiuni Telnet în cascadă

Învățați cum să stabiliți o altă sesiune Telnet în timpul unei sesiuni Telnet. O dată ce stabiliți o sesiune cascadata, învățați cum să vă mutați pe diferitele sisteme.

Terminarea unei sesiuni client

Învățați cum să terminați complet o sesiune Telnet.

Controlul funcțiilor server Telnet de pe client

Clientul Telnet iSeriesTM deține funcții de control care vă permit controlul procesării stației de lucru pe sistem când sunteți într-o sesiune client. Funcțiile de control Telnet vă permit să apelați comenzi client către server ce pot influența sesiunea pornită deja.

Atât numele serverului iSeries, cât și numele TCP/IP sunt afișate pentru fiecare din funcțiile de comandă.

Pentru a selecta funcțiile serverului pe care doriți să le controlați, trebuie să accesați meniul **Funcții control Telnet**. Pentru a ajunge la acest meniu, apăsați tasta **Attention** a tastaturii dumneavoastră 5250.

Lista următoare vă oferă o scurtă descriere a fiecărei dintre funcțiile control client Telnet:

Întreruperea unui proces din sistem

Întrerupere proces sau **IP**: Această funcție anulează, întrerupe sau suspendă un proces pornit pe server. De exemplu, puteți utiliza IP când un proces pare a fi intrat într-o buclă permanentă sau dacă ați pornit un proces din greșeală.

Interogarea stării conexiunii când sistemul devine inactiv

Cerere stare conexiune sau **AYT**: Această funcție furnizează un mesaj de la server care vă anunță că sistemul merge în continuare. Puteți utiliza această funcție de control atunci când sistemul server devine în mod neașteptat inactiv pentru o perioadă lungă de timp.

Rejectarea ieșirii de la distanță înainte de a ajunge la stația de lucru

Rejectarea datelor de ieșire de la distanță sau **AO**: Această funcție permite unui proces care generează date la ieșire să fie executat până la sfârșit fără a trimite ieșirea la stația dumneavoastră de lucru. Această funcție elimină ieșirea sistem server deja produsă, dar care nu a fost încă afișată pe stația de lucru.

Curățarea căii de date între sistemul dumneavoastră și server

Curățare cale de date sau **SYNCH**: Această funcție abandonează toate caracterele (în afară de comenzile Telnet) dintre sistemul dumneavoastră și sistemul server. Puteți utiliza această funcție atunci când mecanismele de control al fluxului rețelei determină ca alte funcții, cum ar fi **IP** sau **AO**, să fie trecute în buffer.

Oprirea sesiunii Telnet

Oprire sesiune Telnet sau **QUIT**: Această funcție termină sesiunea Telnet și închide conexiunea TCP/IP la sistemul server (sistemul de la distanță). Puteți solicita această funcție în orice moment în timpul sesiunii Telnet, dar ar trebui să închideți sistemul de la distanță înainte de selectarea acestei funcții. Dacă nu închideți sesiunea, veți rămâne conectat la sistemul server deoarece protocolul Telnet nu asigură o secvență de terminare sesiune.

Folosirea tastei Attn pentru opțiunea gazdă la distanță

Tasta ATTN pentru gazdă la distanță: Apăsați tasta Attn pentru a afișa meniul Funcții control Telnet.

Note:

Această opțiune se aplică doar pentru modul 5250.

Dacă rulați modul VTxxx (VT100 sau VT220), atunci există două selecții adiționale în acest meniu:

- Pentru sesiuni VT100, Opțiunea 6 (Modificare mapare tastatură principală VT100) și Opțiunea 7 (Modificare mapare tastatură alternativă VT100).
- Pentru sesiuni VT220, Opțiunea 8 (Modificare mapare tastatură principală VT220) și Opțiunea 9 (Modificare mapare tastatură alternativă VT220).

Sesiunile client Telnet 5250

Suportul client Telnet 5250 permite utilizatorilor iSeries^(TM) să se autentifice pe alte sisteme și să acceseze 5250 tot-ecranul. Suportul pentru 5250 tot-ecranul poate fi negociat doar cu o aplicație server Telnet care rulează pe un server iSeries pe un sistem care suportă serverul Telnet 5250. Negocierea suportului pentru stația de lucru 525x cu aplicația server Telnet la distanță activează suportul 5250 tot-ecranul.

Faceți referire la Pornirea unei sesiuni Telnet 5250 pentru a folosi emularea 5250.

Pornirea unei sesiuni client Telnet 5250

Notă: Ar trebui să cunoașteți numele sau adresa Internet a sistemului la distanță cu care doriți să porniți sesiunea Telnet. Pentru a afișa adresa Internet și numele gazdelor, completați următorii pași:

1. Porniți Navigator iSeries^(TM) și expandați **serverul dumneavoastră de rețea iSeries** —>
2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele Internet și numele gazdă.

Pornirea unei sesiuni client Telnet

1. Introduceți comanda STRTCPTELN sau introduceți TELNET în linia de comandă iSeries și apăsați pe **Enter**.
2. Tastați numele sistemului la distanță, dacă vreți să folosiți parametrii opționali, apăsați F10. Altfel, apăsați **Enter**. Dacă ați introdus *INTERNETADR pentru câmpul **Sistem la distanță**, serverul va afișa câmpul pentru **Adresă Internet**.
3. Tastați adresa Internet a sistemului la distanță, dacă vreți să folosiți parametrii opționali, apăsați F10. Altfel, apăsați **Enter**. Ecranul afișează valori ale parametrilor opționali și informațiile privind adresa Internet.
4. Pentru a folosi valorile implicite ale parametrilor, apăsați **Enter**.
5. În timpul sesiunii 5250 modul tot-ecranul, următorii parametrii opționali sunt, de asemenea, aplicabili:

- Timp de așteptare pentru gazdă (INZWAIT)
- Tip limbă tastatură (KBDTYPE)
- Numărul portului aplicației server gazdă la distanță (PORT)
- Terminal virtual la distanță (RMTVRTDSP)
- Utilizatorul la distanță (RMTUSER)
- Parola la distanță (RMTPWD)
- Criptarea parolei la distanță (RMTPWDENC)
- Program inițial la distanță (RMTINLPGM)
- Meniu inițial la distanță (RMTINLMNU)
- Biblioteca curentă la distanță (RMTCURLIB)
- Tipul de tastatură la distanță (RMTKBDTYPE)
- Setul de caractere la distanță (RMTCHRSET)
- Pagina de cod la distanță (RMTCODPAG)

Următorul ecran reprezintă un ecran pentru deschidere de sesiune pe sistemul la distanță.

Notă:

- Panoul de semnare va fi afișat dacă nici unul din parametrii de semnare automată nu sunt introduși la comanda STRTCPTELN (RMTUSER, RMTPWD, RMTPWDENC) sau dacă s-a întâmpinat o eroare când au fost introduși acești parametri. Dacă aceste valori sunt introduse corect, nici un panou de semnare nu va fi afișat. Utilizatorul este automat semnat și orice ecran inițial definit pentru utilizator va fi afișat.
- În plus, următoarele sunt de asemenea adevărate:
 - Dacă comanda STRTCPTELN furnizează parametrii corecți RMTUSER, RMTPWD, RMTPWDENC și RMTINLPGM, atunci utilizatorul va fi semnat. De asemenea, programul inițial furnizat va fi rulat.
 - Totuși, dacă parametrul RMTINLPGM este furnizat invalid, utilizatorul va fi semnat, dar va fi afișat un mesaj 'job terminat anormal'. Aceleași acțiuni sunt adevărate și pentru parametrul RMTINLMNU.
- Pentru parametrul RMTCURLIB, o valoare corectă va rezulta în semnarea utilizatorului. De asemenea, orice program inițial sau meniu cum sunt definite în profilul utilizatorului sau un comanda STRTCPTELN, se va executa. În plus biblioteca curentă va fi setată la valoarea parametrului. Dacă este furnizat un parametru RMTCURLIB invalid, atunci un panou de semnare va fi afișat cu un mesaj care spune că valoarea bibliotecă curentă este invalidă.
- De asemenea, pentru toate chestiunile de mai sus, dacă parametrii RMTKBDTYPE, RMTCHRSET sau RMTCODPAG sunt furnizați cu valori valide, vor avea efect pentru încercările reușite de semnare automată. Nu vor avea efect asupra încercărilor invalide.

Notă: Dacă sistemul nu găsește sau nu configurează serverul SOCKS sau dacă nu apar erori folosind serverul SOCKS, atunci o conexiune directă este stabilită.

Dimensiunea ecranului TN5250

Modul Telnet 5250 tot-ecranul suportă următoarele dimensiuni de ecrane:

- 1920-caractere (24 x 80) pe toate stațiile de afișare 5250.

- 3564-caractere (27 x 132) pe toate 3180 Modelul 2; 3197 Modele D1, D2, W1, W2 și 3477 Modele FA, FC, FD, FE, FG, FW.

Pentru a controla funcțiile server în timp ce sunteți într-o sesiune client, consultați Controlul funcțiilor server Telnet.

Sesiunile client Telnet 3270

Deoarece fluxurile de date 3270 sunt translatate în fluxuri de date 5250, dispozitivele stație de lucru se comportă ca un terminal la distanță 5251 la serverul iSeries^(TM) și la programele aplicație.

Următoarele subiecte furnizează mai multe informații despre emularea 3270:

Pornirea unei sesiuni 3270

Pornirea unei sesiuni client folosind emularea 3270.

Considerații 3270 tot-ecranul

Trebuie să cunoașteți problemele prezentate în acest subiect când folosiți emularea 3270.

Folosirea unei stații de afișare

Acest subiect descrie tastatura și diferențele de ecran pentru utilizarea unei stații de afișare pe parcursul unei sesiuni Telnet 3270 tot-ecranul.

Maparea tastaturii 3270 pentru serverele Telnet

Acest subiect furnizează mapări de tastatură pentru suportul emulării 3270.

Pornirea unei sesiuni client Telnet 3270

Când clientul Telnet negociază suport pentru stație de lucru 327x cu aplicația server la distanță Telnet, sistemul activează modul 3270 tot-ecranul. Clientul negociază suport 3270 tot-ecranul cu orice aplicație server Telnet care suportă aplicații 3270 (în locul celor 5250) tot-ecranul. Aplicația sistem la distanță controlează stația dumneavoastră de afișare. Primiți aceleași ecrane și introduceți date în același fel în care ați introduce pentru alte dispozitive 3270 atașate local la sistemul la distanță.

Trebuie să porniți serverul Telnet pe sistemul la distanță (sistemul server la care doriți să vă conectați utilizând Telnet).

Ar trebui să cunoașteți numele sau adresa IP a sistemului la distanță cu care doriți să porniți sesiunea Telnet. Pentru a afișa adresa IP și numele gazdelor, completați următorii pași:

1. Porniți Navigator iSeries^(TM) și expandați **serverul dumneavoastră de rețea iSeries** —>
2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele IP și numele gazdă.

Pornirea unei sesiuni client Telnet

1. Tastați comanda STRTCPTLN sau tastați TELNET în linia de comandă și apăsați **Enter**.
2. Tastați numele sistemului la distanță. Dacă vreți să folosiți parametrii opționali, apăsați F10, altfel apăsați **Enter** . Dacă introduceți *INTNETADR pentru numele **Sistem la distanță** și apăsați pe **Enter**, serverul vă va afișa câmpul **Adresa IP**.
3. Tastați adresa IP a sistemului la distanță. Pentru a folosi parametrii opționali, apăsați F10, altfel apăsați **Enter** . Ecranul afișează valori ale parametrilor opționali și informațiile privind adresa IP.
4. Pentru a folosi valorile implicite ale parametrilor, apăsați Enter. Conexiunea cu serverul Telnet va porni.
5. În timpul unei sesiuni mod 3270 tot-ecranul, se pot folosi de asemenea următorii parametri opționali:
 - Timp de așteptare pentru gazdă (INZWAIT)
 - Tip limbă tastatură (KBDTYPE)
 - Tasta Page Up (roll down) (PAGEUP)
 - Tasta Page Down (roll up) (PAGEDOWN)

- Tasta selectare cursor (CSRSLT)
- Tabela de traducere 3270 de ieșire (TBL3270OUT)
- Tabela de traducere 3270 de intrare (TBL3270IN)
- Blocarea tastaturii numerice (NUMLCK)
- Modificarea modului de tratare pentru valorile nule (NULLS)
- Numărul portului aplicației server gazdă la distanță (PORT)

Următorul ecran reprezintă un ecran pentru deschidere de sesiune pe sistemul la distanță.

Pentru a controla funcțiile server în timp ce sunteți într-o sesiune client, consultați Controlul funcțiilor server Telnet.

Pentru informații despre maparea tastaturii, consultați Maparea tastaturii 3270 pentru serverele Telnet.

Pentru informații despre utilizarea 3270 în modul tot-ecranul, consultați Considerații 3270 tot-ecranul

Considerații 3270 tot-ecranul

La folosirea modului 3270 tot-ecranul pentru clientul dumneavoastră Telnet, trebuie să fiți atenți la următoarele considerații:

- Dimensiunea ecranului 3270
- Tasta de selectare a cursorului 3270
- Mesaje de eroare 3270
- Caractere nule 3270

Mărimea ecranului TN3270

Cerințele modului Telnet 3270 tot-ecranul:

- Dacă tipul de dispozitiv 3270 negociat necesită 1920 de caractere, codul clientului Telnet iSeries^(TM) va rula cu orice tip de dispozitiv 5250 ca client terminal.
- Dacă tipul de dispozitiv 3270 negociat cere 3564 caractere, codul client Telnet iSeries cere tipurile de dispozitive 3180 Model 2, 3197 Model D1, D2, W1, W2, 3477 Model FA, FC, FD, FE, FG sau 5250 FW ca și terminal pentru client.
- Este un ecran de 27x132 când se negociază un tip de dispozitiv 3180 Model 2, 3197 Mode D1, D2, W1, W2 sau 3477 Model FA, FC, FD, FE, FG sau FW. În versiunile anterioare era necesară o zonă de date pentru a obține acest suport.
- Pentru a obține un ecran 24x80, executați comanda CRTDTAARA DTAARA(libname/QTVNO32785) TYPE(*CHAR) VALUE('1').

Tasta de selectare cursor TN3270

Tasta existentă de selectare a cursorului (Cursor Select) este dezactivată dacă alegeți să o emulați. Specificând unul din următorii parametrii pentru comanda STRTCPTLN veți emula tasta de selectare cursor:

Parametru	Valoare
Tasta Page Up (Roll Down)	*CSRSLT
Tasta Page Down (Roll Up)	*CSRSLT
Tasta Cursor Select	Tasta *F (specifică o tastă funcțională de la *F1 la *F24)

Mesaje TN3270

Când folosiți modul Telnet 3270 tot-ecranul, mai multe tipuri de mesaje de eroare pot să apară.

- Erori de introducere taste apar ca un număr pe 4 digiți în colțul din stânga-jos al ecranului. Apăsați tasta Help sau F1 (Help) pentru a obține mai multe informații despre acest mesaj. Consultați cartea pentru operarea sistemului dacă nu puteți corecta eroarea.
- Mesajele sistem includ mesaje Telnet care sunt provenite de la serverul iSeries.
- Pentru informații despre mesajele trimise de sistemul la distanță, consultați documentația sistemului la distanță.

Tratarea caracterelor null TN3270

Când o stație de afișare 3270 trimite un flux de date, toate caracterele nule sunt șterse. Specificați una din valorile următoare pentru lucrul cu parametrii nuli (NULLS) în comanda STRTCPTELN:

***REMOVE**

Șterge caracterele nule de la început și sfârșit

***BLANK**

Valoarea implicită; șterge caracterele nule de la început și sfârșit în blancuri. De exemplu, presupunem că datele sunt alcătuite din următoarele (0 indică un nul):

```
0x0yz000
```

Fluxul de date trimis de la o stație de afișare 5250 care rulează Telnet 3270 tot-ecranul cu implicitul *BLANK va conține următoarele:

```
bxbyz
```

Fluxul de date trimis de la o stație de afișare 3270 sau de la una 5250 care rulează Telnet 3270 tot-ecranul când valoarea *REMOVE este specificată, va conține următoarele:

```
xyz
```

Valoarea *REMOVE este validă pentru următoarele dispozitive:

- Orice dispozitiv atașat local
- Terminale atașate la un controler 5394 la distanță
- Monitoare PC folosind funcția stație de lucru

Folosirea unei stații de afișare

Când folosiți o stație de afișare în timpul unei sesiuni TELNET tot-ecranul, trebuie să cunoașteți diferențele între tastaturi și între ecrane. Alte considerente speciale despre modul Telnet 3270 includ numărul de câmpuri de intrare, mesaje de eroare și oprirea unei sesiuni.

Specificarea tastaturii și a setului de caractere

Tipul de limbă pentru tastatură pe care îl specificați pentru stația de lucru, folosind parametrul din comanda STRTCPTELN, trebuie să fie același cu parametrul tip de limbă pentru tastatură al stației atașate de la distanță. Dacă specificați un tip de limbă pentru tastatură care nu se potrivește, câteva dintre caractere nu vor fi afișate cum trebuie.

Tastaturile 5250 și 3270

Așezarea și funcțiile tastelor sunt diferite la tastatura 5250 (3196G, 3180 Model 2 sau 5291) decât la tastatura 3278.

Notă:

Pentru un client Telnet care operează în modul 3270 tot-ecranul, funcția Curățare de la 3270 poate fi apelată implicit cu secvența de taste Shift-Cmd-Backspace.

Cartea System Operation for New Users prezintă diferențele dintre următoarele tastaturi:

- Tastatura IBM^(R) îmbunătățită

- Tastatura tip mașină de scris cu 122 taste
- Tastatura 5250
- Tastatura stil PC sau PC AT^(R)
- Tastatura stil 5250 PC sau PC AT^(R)
- Tastatura IBM îmbunătățită PC

Tastaturi pentru calculatorul personal

În cazul în care calculatorul dumneavoastră personal utilizează WSF (Workstation Function) iSeries^(TM) Access pentru Windows^(R), puteți afișa imaginea tastaturii 5250 utilizând comanda WSFKEYS (Taste funcționale stație de lucru). Puteți schimba stilul folosind comanda CFGWSF (Configure Workstation Function). Aceste comenzi sunt explicate în cartea 'Client Access/400 for DOS with Extended Memory Setup'. Dacă calculatorul dumneavoastră personal nu utilizează funcția stație de lucru, referiți-vă la documentația corespunzătoare pentru emulatorul dumneavoastră (de exemplu, OS/2^(R) CM/2) pentru a vizualiza și schimba stilul tastaturii.

TN3270—Semnul minus

Dacă specificați valoarea *YES pentru parametrul blocare numerică a tastaturii din comanda STRTCPTLN, când folosiți date de la tastatură și dacă cursorul este aflat în câmpuri doar numerice, atunci faceți următoarele pentru a afișa semnul minus.

Pentru a afișa un semn minus la 5250:

1. Apăsați tasta Num (Numeric).
2. Apăsați tasta minus (-).

Pentru a afișa un semn minus la 3278, apăsați tasta semn minus.

TN3270—Page Down și Page Up

Dacă aplicația 3270 are un ecran care nu permite vizualizarea tuturor câmpurilor din datele de intrare, folosiți tastele de la 5250 Page Down și Page Up pentru a introduce date când numărul maxim de câmpuri de intrare este depășit.

Puteți asigna, de asemenea, funcțiile PF și PA tastelor Page, specificând folosirea lor în comanda STRTCPTLN.

Cursorul apare întotdeauna subliniat pe ambele ecrane 3270 și 5250.

Maparea tastaturii 3270 pentru serverele Telnet

Următoarea tabelă arată asignările implicite pentru tastele PF pentru a realiza diferite funcții 5250. Puteți folosi comanda Afișare mapare tastatură (DSPKBDMAP) pentru a vedea maparea curentă a tastaturii. Sau, puteți folosi opțiunea (Afișare mapare tastatură 3270) din meniul de configurare Telnet TCP/IP, în timp ce terminalul este în modul de emulare 3270.

Tastă funcțională 5250	Taste 3270 implicite pentru selectarea funcției
Ajutor	PF1
Ajutor 3270	PF2
Clear (Curățare)	PF3
Print	PF4
Afișare attribute înglobate	PF5
Cerere test	PF6
Roll Down	PF7
Roll Up	PF8
Resetare eroare	PF10 sau Enter
Sys Req	PF11
Record Backspace	PF12

Tastă funcțională 5250	Taste 3270 implicite pentru selectarea funcției
F1 până la F12	Apăsați PA1, apoi una dintre: PF1 până la PF12
F13 până la F24	Apăsați PA2, apoi una dintre: PF1 până la PF12 sau PF13 până la PF14 (dacă există)
Ieșire din câmp	Erase EOF, apoi Field Tab
Attn	Pentru 3277 folosiți Test Request, apoi apăsați PA1. Pentru 3278/3279 folosiți tasta ATTN

Următorul exemplu de program CL setează maparea tastaturii pentru o stație de lucru 327x-type care utilizează Telnet pentru a merge la un server iSeries^(TM). Acest program mapează tastele funcționale iSeries la tastele funcționale echivalente de pe stația de lucru 327x. Dacă încercați să lansați o comandă CHGKBDMAP de pe o stație de lucru care nu e în modul de emulare 3270, veți primi un mesajul CPF8701. Prin monitorizarea pentru el, restul programului devine nefolosit în aceste circumstanțe.

PGM

```

MONMSG      MSGID(CPF8701 CPF0000)
CHGKBDMAP  PF1(*F1) PF2(*F2) PF3(*F3) PF4(*F4) PF5(*F5)
PF6(*F6) PF7(*DOWN) PF8(*UP) PF9(*F9)
PF10(*F10) PF11(*F11) PF12(*F12)
PA1PF1(*HELP) PA1PF2(*HLP3270)
PA1PF3(*CLEAR) PA1PF4(*PRINT)
PA1PF5(*DSPATR) PA1PF6(*TEST) PA1PF7(*F7)
PA1PF8(*F8) PA1PF9(*ATTN) PA1PF10(*RESET)
PA1PF11(*SYSREQ) PA1PF12(*BCKSPC)
ENDPGM

```

Înregistrând această sursă CL ca parte a fișierului QCLSRC în biblioteca TCPLIB ca membru CHGKBD, puteți crea programul CL CHGKBD în biblioteca TCPLIB folosind următoarea comandă CL:

```

CRTCLPGM PGM(TCPLIB/CHGKBD) SRCFILE(TCPLIB/QCLSRC)
TEXT('Schimbă maparea tastaturii pentru terminale 327x')

```

Programul CHGKBD poate fi apelat de orice utilizator Telnet pe un server iSeries. El poate fi apelat automat la conectare specificând programului CHGKBD pentru parametrii inițiali ai programului la comanda CHGUSRPRF sau programul CHGKBD poate fi apelat de programul inițial al profilului.

Tastetele PA1 și PA2 pe o tastatură PC

Tastele PA1 și PA2 nu apar pe tastatură PC. O mapare de tastatură din emulatorul dumneavoastră 3270 furnizează funcția acestor taste 3270 pe o tastatură PC.

Maparea de tastatură Telnet implicită pentru 3270 utilizează aceste taste. De aceea, este important să știți unde sunt aceste taste pe tastatură înainte de începe o sesiune Telnet 3270. Aceasta este important, în special când plănuiți să începeți o sesiune fără să schimbați maparea de tastatură. Ar trebui să consultați documentația emulatorului pentru tastele sau apăsarile de taste necesare producerii acestor funcții.

Există câteva secvențe de taste 5250 pentru care nu există secvențe 3270 suportate, și de aceea, nu este posibil să setați aceste comenzi de tastatură pe 3270. Secvențele de taste sunt:

- Field Plus
- Minus în câmp
- Șterge toate câmpurile de intrare

Funcția tastei 5250 Field Exit (Ieșire câmp) este realizată pe o tastatură 3270 folosind tasta Erase EOF (Ștergere EOF) și apoi tasta Tab.

Circumstanțe speciale

Când folosiți modul Telnet 3270 tot-ecranul pe un terminal 3270 și înainte ca maparea implicită pentru terminal să fie modificată, tastele de la PF1 la PF12 pot fi emulate de secvența de taste PA1 PFX. De aceea, instrucțiunile precum Apasă PF3 sau Apasă PF4 se vor citi: Apasă PA1 PF3 și Apasă PA1 PF4, înainte de a crea o nouă mapare de tastatură.

În funcție de instalarea client Telnet pentru gazdă, de exemplu client VM Telnet, la apăsarea PA1 utilizatorul poate primi instrucțiunea comandă TELNET: pe linia de jos a ecranului. Dacă sistemul arată acest tip de instrucțiune: PA1, apăsați tasta Enter, mută cursorul la linia de comandă și apăsați tasta PF dorită. În acest caz comenzile următoare pot fi emulate de PF1 până la PF12:

1. Apăsați PA1, se primește instrucțiunea Telnet comandă TELNET :
2. Tastați PA1, apăsați tasta Enter
3. Mutați cursorul la linia de comandă.
4. Apăsați tasta PF dorită.

Pentru informații adiționale despre maparea tastaturii, consultați Anexa D. Mapări de tastatură 3270 TELNET.

Notă: Host Command Facility (HCF) este o caracteristică disponibilă pe sistemul System/370^(TM), 43xx și sistemele gazdă 30xx. Această caracteristică dă posibilitatea unui utilizator de pe un server gazdă să folosească aplicații pe un server iSeries. Dacă folosiți HCF pentru a vă conecta la serverul iSeries și apoi folosiți Telnet pentru conectare la un alt server iSeries, sunteți într-o sesiune 3270 tot-ecranul. Tastatura este mapată de două ori, o dată pentru sesiunea inițială HCF și o dată pentru sesiunea Telnet. Pentru a folosi tastele PF în felul în care le-ai folosi de obicei, trebuie să schimbi maparea tastaturii pe ambele servere iSeries. Aveți grijă să folosiți aceeași mapare de tastatură pe fiecare server iSeries.

Sesiunile client Telnet VTxxx

Suportul Telnet VTxxx permite utilizatorilor iSeries^(TM) să se autentifice pe servere non-iSeries dacă aceștia se află pe un terminal local VTxxx atașat la sistem. Suportul client VTxxx permite unui utilizator iSeries să se conecteze pe orice sistem la distanță într-o rețea TCP/IP care suportă șirul de octeți Vtxxx. Ca un utilizator Telnet iSeries, trebuie să fiți atent la diferențele operaționale și fizice între sesiunile 5250 și VTxxx.

Subiectele următoare furnizează mai multe informații despre emularea VTxxx:

Pornirea unei sesiuni VTxxx

Pornirea unei sesiuni client Telnet folosind emularea VTxxx.

Considerații VTxxx tot-ecranul

Trebuie să cunoașteți problemele prezentate în acest subiect când folosiți emularea VTxxx.

Opțiuni emulare VTxxx

Acest subiect furnizează informații despre opțiunile de personalizare pentru tipul de emulare VTxxx.

Valorile tastelor VTxxx

Acest subiect furnizează mapări de tastatură pentru suportul emulării VTxxx.

Pornirea unei sesiuni client Telnet VTxxx

Trebuie să porniți serverul Telnet pe sistemul la distanță (sistemul server la care doriți să vă conectați utilizând Telnet).

Notă:

Ar trebui să cunoașteți numele sau adresa IP a sistemului la distanță cu care doriți să porniți sesiunea Telnet. Pentru a afișa adresa IP și numele gazdelor, completați următorii pași:

1. Porniți Navigator iSeries^(TM) și expandați **serverul dumneavoastră de rețea iSeries** —>
2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele IP și numele gazdă.

Pornirea unei sesiuni client Telnet

1. Introduceți comanda STRTCPTELN sau introduceți TELNET în linia de comandă iSeries și apăsați pe **Enter**.
2. Tastați numele sistemului la distanță sau tastați *INTERNETADR dacă preferați utilizarea adresei IP. Dacă vreți să folosiți parametrii opționali, apăsați F10. Altfel, apăsați **Enter**.

Dacă ați introdus *INTERNETADR pentru câmpul **Sistem la distanță**, iSeries va afișa câmpul **Adresa IP**.

3. Tastați adresa IP a sistemului la distanță. Pentru folosirea parametrilor opționali, apăsați pe **F10**, altfel apăsați pe **Enter**. Ecranul afișează valori ale parametrilor opționali și informațiile privind adresa IP.
4. Pentru a folosi valorile implicite ale parametrilor, apăsați **Enter**.
5. În timpul sesiunii VTxxx modul tot-ecranul, următorii parametrii opționali sunt, de asemenea, aplicabili:
 - Tabela de traducere ASCII de intrare (TBLVTIN)
 - Tabela de traducere ASCII de ieșire (TBLVTOUR)
 - Tabelă specială ieșire (TBLVTDRWO)
 - Tabelă specială intrare (TBLVTDRWI)
 - Opțiuni selectate (VTOPT)
 - Afișare atributele caracterului (DSPCHRATTR)
 - Caracteristica defilare pagină (PAGESEROLL)
 - Caracteristica de răspuns (ANSWERBACK)
 - Stopuri Tab (TABSTOP)
 - Timp de așteptare pentru gazdă (INZWAIT)
 - Identificator set de caractere codate (CCSID)
 - Mod de operare ASCII (ASCOPRMOD)— se aplică doar la inițializarea unei sesiuni VT220 (nu are nici un efect asupra negocierilor)
 - Numărul portului aplicației server gazdă la distanță (PORT)
 - Caractere de control (CTLCHAR)

Notă:

Caractere neașteptate pot apărea datorită configurării incorecte a sistemului la distanță. Dacă acest lucru se întâmplă, verificați că valoarea tip stație de lucru este o valoare corespunzătoare pentru stația de lucru VTxxx modul tot-ecranul. Puteți folosi, de asemenea, comanda set term pentru a schimba modul tot-ecranul al acestei conexiuni.

Următorul ecran reprezintă un ecran pentru deschidere de sesiune pe sistemul la distanță.

Dacă plănuieți folosirea VTxxx modul tot-ecranul, consultați Considerații despre VTxxx tot-ecranul .

Pentru a controla funcțiile server în timp ce sunteți într-o sesiune client, consultați Controlul funcțiilor server Telnet.

Pentru informații suplimentare despre maparea tastaturii, vedeți Valorile tastelor VTxxx.

Considerații VTxxx tot-ecranul

Ca la orice tip de emulare, trebuie să Țineți seama de câteva considerații înainte de a folosi modul VTxxx tot-ecranul cu serverul dumneavoastră Telnet. Aceste considerații includ probleme de securitate, precum și condiții de eroare posibile și indicatoare luminoase. Deveniți familiar cu aceste considerații pentru a înțelege mai bine cum să folosiți modul VTxxx tot-ecranul.

În plus față de preocupările pentru securitate, există multe alte lucruri de care să Țineți seama când folosiți modul VTxxx tot-ecranul cu serverul dumneavoastră Telnet. Când folosiți modul VTxxx tot-ecranul, trebuie să aveți în vedere următoarele:

- Considerații de securitate pentru Modul VTxxx tot-ecranul (page 58)
- Considerații Telnet și SNA 5250 Pass-through pentru modul VTxxx tot-ecranul (page 58)
- Procesarea cererii sistem pentru sesiunile VTxxx (page 58)
- Condiții de eroare la tastatura 5250 (page 58)
- Stații de afișare și suport VTxxx (page 59)
- Diferențe operaționale (page 59)
- Caracteristici tastatură (page 59)
- Caracteristici ecran (page 60)
- Dimensiunea ecranului VTxxx (page 60)
- Atribute caractere VTxxx (page 61)

Considerații de securitate pentru Modul VTxxx tot-ecranul

Numărul de încercări de semnare permis crește o dată cu dispozitivele virtuale configurate automat. Numărul total de încercări de semnare este egal cu numărul de încercări de semnare la sistem permise, înmulțit cu numărul dispozitivelor virtuale care pot fi create.

Valoarea sistem QMAXSIGN definește numărul de încercări de semnare permise. Numărul de dispozitive virtuale ce pot fi create de Telnet este definit de variabila sistem QAUTOVRT.

Considerații Telnet și SNA 5250 Pass-through pentru modul VTxxx tot-ecranul

Serverul iSeries^(TM) suportă 5250 Pass-through. 5250 Pass-through este similar cu Telnet, dar rulează pe un protocol de rețea SNA (Systems Network Architecture) și nu pe TCP/IP. 5250 Pass-through folosește dispozitive virtuale pentru afișarea directă la dispozitivele fizice la fel cum face Telnet. În 5250 Pass-through, serverul iSeries creează automat dispozitive virtuale în același mod în care o face pentru Telnet. De aceea, valorile sistem pentru dispozitive controlează numărul dispozitivelor configurate automat și pentru 5250 Pass-through și pentru Telnet.

Procesarea cererii sistem pentru sesiunile VTxxx

Procesarea cererilor sistem pentru sesiuni VTxxx este puțin diferită de cea a unei stații de lucru normale 5250.

Când tasta SysReq (Cerere sistem) este apăsată pe o stație de lucru 5250, o linie de comandă pentru cererea de sistem apare în josul ecranului. Dacă apăsați tasta Enter, apare meniul Cerere sistem.

Pentru sesiuni VTxxx când apăsați o funcție cerere de sistem, meniul Cerere sistem este afișat imediat.

Condiții de eroare la tastatura 5250

Câteva condiții de eroare cauzează blocarea tastaturii 5250 și afișarea unui cod de eroare pe linia de mesaje. Un exemplu pentru o astfel de condiție este tastarea când cursorul nu este într-un câmp de introducere de date. Pentru sesiuni VTxxx, aceste erori cauzează producerea unui sunet pe stația de lucru VTxxx și tastatura rămâne deblocată.

Anumite aplicații iSeries blochează de asemenea tastatura 5250 și aprind indicatorul luminos de intrare 5250 inhibată. Utilizatorul trebuie să apese tasta de resetare eroare (Error Reset) înainte de a debloca tastatura. Pentru sesiuni VTxxx, blocarea tastaturii 5250 cauzează producerea unui sunet pe terminalul VTxxx de fiecare dată când este apăsată o tastă. Pentru a debloca tastatura, trebuie să fie apăsată tasta VTxxx care este mapată pentru tasta Error Reset. În maparea de tastatură VTxxx implicită, tasta CTL-R mapează tasta de resetare eroare.

Stații de afișare și suportul VTxxx

Când sistemul negociază suport VTxxx, serverul Telnet transmite ecrane cu maxim 24 linii și 80 coloane. Sistemul client VTxxx vede aceste ecrane în aproape același fel în care ele apar pe o stație de lucru 5251 Model 11. Totuși, există câteva diferențe.

O stație de lucru 5251 are indicatoare luminoase partea dreaptă care indică : Sistem disponibil, Mesaj în așteptare, Shift tastatură, Mod inserare și Intrare-inhibată.

Suportul pentru serverul VTxxx emulează indicatorul luminos Sistem disponibil, punând un asterisc în coloana 80 a liniei 9. Pentru indicatoarele Mesaj în așteptare, Mod inserare și Intrare-inhibată asteriscul apare în coloana 80 a liniilor 11, 13 și respectiv 15. Când apare asteriscul, el este scris peste caracterul care era afișat anterior în acea locație a ecranului. Implicit, serverul VTxxx nu afișează indicatoarele luminoase. Puteți activa sau dezactiva acești indicatori tastând secvența de taste care este mapată pe funcția de activare a indicatoarelor luminoase. Secvența implicită de taste pentru această funcție este ESC-T.

Notă:

- Când folosiți un client VTxxx pentru a vă atașa la serverul Telnet iSeries, rețineți că indicatorul Mod inserare și Intrare-inhibată pot să nu funcționeze cum au fost descrise mai sus. 5250 suportă atașarea ca o funcție locală în timp ce VTxxx nu are această facilitare. Indicatoarele Sistem disponibil și Mesaj în așteptare, vor fi totuși, afișate corect.
- Un ecran 5251 suportă un atribut de ecran cunoscut sub numele de separator de coloane. **Separatorul de coloane** este o linie verticală afișată între caractere. Această linie nu ocupă spațiul unui caracter. VTxxx nu suportă un astfel de atribut. Dacă o aplicație iSeries generează un ecran care folosește atributul separato de coloane, acel ecran este afișat pe sistemul client VTxxx cu separatorul de coloane mapat pe atributul VTxxx de subliniere.

Diferențe operaționale

Ca utilizator Telnet iSeries, trebuie să fiți atent la diferențele operaționale și fizice între terminalele VTxxx și 5250.

5250 este un terminal orientat bloc. Datele tastate la 5250 sunt acumulate într-un buffer și trimise serverului iSeries doar când este apăsată tasta AID (attention identifier). Tasta AID pe o tastatură 5250 este tasta care inițiază o funcție. Următoarele sunt taste AID pe o tastatură 5250:

- Clear (Curățare)
- Command Function de la 1 până la 24
- Enter/Rec Adv
- Help
- Print
- Record Backspace Function
- Roll Down (Page Up)
- Roll Up (Page Down)

Terminalele VTxxx operează în modul caracter. Caracterele sunt transmise gazdei imediat ce o tastă este apăsată.

O altă diferență este felul în care datele sosesc pe ecran. Sistemul scrie date pe un terminal VTxxx caracter cu caracter și tu vei vedea datele venind ca fluxuri de caractere. La 5250, sistemul scrie datele în blocuri și tot sau doar o parte din ecran, se schimbă odată.

Caracteristici tastatură

Ar trebui să evitați folosirea tastelor de mutare a cursorului. În loc, folosiți tastele funcționale asociate cu cuvintele cheie *CSRUP, *CSRDOWN, *CSRRIGHT și *CSRLEFT. Implicit acestea sunt tastele F13, F14, F15 și respectiv F16. Dacă folosiți tastele de mutare a cursorului 5250, aplicația VTxxx pe care o folosiți s-ar putea să nu meargă așa cum vă așteptați. Aceasta se întâmplă deoarece rezultatele folosirii acestor taste nu sunt transmise sistemului la distanță până când tasta AID nu este apăsată.

De exemplu, utilizând Telnet către RS/6000^(R) și obținând emulare VT220, comanda SMIT furnizează un meniu de control al interfeței către AIX^(R). Aici tastele funcționale asociate cu cuvintele cheie *CSRxx realizează așa cum vă așteptați mutarea cursorului, la fel ca tastele. Totuși, tastele de mutare a cursorului 5250, în timp ce mișcă fizic cursorul în josul ecranului și selectează opțiunea SMIT, nu produce luminarea (highlight) opțiunii selectate. Luminată în imagine inversată rămâne prima opțiune a meniului SMIT, indiferent de poziția tastelor.

Tastarea unui caracter de control pe o tastatură iSeries este diferită de tastarea unui caracter de control pe un terminal VTxxx real. Pe un terminal VTxxx, apăsați și țineți apăsată tasta de control în timp ce apăsați pe caracterul asociat cu funcția de control.

Când folosiți suport Telnet iSeries, echivalentul este obținut tastând două indicatoare de caractere de control urmate de apăsarea tastei funcționale asociate cu funcția implicită de trimitere fără CR (Carriage Return) (*SENDWOCR) (tasta F11). De exemplu, dacă maparea de tastatură implicită și parametrii implicați ai comenzii STRTCPTELN sunt efectivi, funcția VTxxx Control-C poate fi obținută tastând &C urmat de apăsarea tastei F11. <F12> poate de asemenea să introducă această funcție, folosind maparea de tastatură implicită. În cazul în care folosiți o aplicație unde <F12> este mapată din nou, acest exemplu este inclus și ilustrează rolul tastei *SENDWOCR.

Folosiți parametrul CTLCHAR din comanda STRTCPTELN pentru a selecta caracterul folosit pentru a indica un caracter de control. Implicit este &. Caracterele &C trebuie să fie ultimile caractere introduse înaintea apăsării tastei funcționale *SENDWOCR sau &C-ul nu este interpretat drept un caracter de control. Un caracter de control se transmite doar atunci când tasta funcțională *SENDWOCR este apăsată. Puteți asigna caracterele de control VTxxx folosite curent unei taste funcționale. Următorul este un exemplu descriptiv al unei comenzi Ctrl-C. Când folosiți un client Telnet pentru a vă conecta la un sistem RS/6000, sistemul negociază, de obicei, emularea VT220. Secvența Ctrl-C este una importantă în AIX pentru a termina comenzi care rulează mult, precum PING. Este, de aceea, important să știți cum să faceți acest lucru înainte de a iniția comenzi RS/6000. Implicit secvența este &C<F11>. Observați că trebuie să tastați aceste taste repede și poate e nevoie de câteva încercări înainte ca task-ul RS/6000 să accepte intrarea.

Apăsați tasta funcțională care este asociată cu funcția *HIDE, (F6 pe o mapare de tastatură implicită) dacă nu vreți să afișați caracterele tastate. Folosiți această funcție când tastați o parolă.

Dacă vreți să trimiteți caracterele tastate sistemului la distanță pentru procesare fără a apăsa tasta Enter, trebuie să apăsați tasta funcțională asociată cu funcția *SENDWOCR (F11 pe maparea de tastatură implicită).

Este folositor, de obicei, să poți să reapelezi comenzi introduse anterior. Pe serverul iSeries, F9 furnizează des această funcție. Pe AIX, aceasta poate fi activată tastând comanda `set -o vi` și apăsând Enter. După aceasta, puteți începe să găsiți comenzi cu secvența Esc-K. Pentru a realiza acest lucru folosind maparea de tastatură implicită în emularea VTxxx, trebuie să folosiți secvența <F5>k<F11>. Caracterul Esc începe căutarea comenzii. Apoi folosiți k pentru a extrage alte comenzi. Când operați în acest mod, se aplică comenzile H pentru dreapta, L pentru stânga, X pentru ștergere, I pentru inserare și R pentru înlocuire. Secvența <F5>i<F11> oprește această facilități.

Caracteristici ecran

Caracterul dinaintea poziției cursorului va fi întotdeauna blanc. Caracterul de fapt se salvează intern și este arătat când se face reîmprospătare la ecran cu cursorul în altă poziție.

O aplicație VTxxx care folosește rândul 1, coloana 1 a ecranului nu funcționează la fel când folosește suportul client Telnet iSeries. Majoritatea stațiilor de afișare tip-5250 nu permit scrierea pe linia 1, coloana 1. Dacă aplicația VTxxx poziționează cursorul pe linia 1, coloana 1, serverul iSeries pune automat cursorul pe linia 2, coloana 2.

Datorită diferențelor arhitecturale, sistemul ignoră anumite comenzi și secvențe nesuportate. Un exemplu sunt seturile de caractere descărcabile pe flux în jos (downstream loadable).

Dimensiunea ecranului VTxxx

Modul Telnet VTxxx tot-ecranul suportă următoarele dimensiuni de ecran:

- Pe stațiile de afișare 3180:
 - Ecranele 24 x 80 VTxxx ar trebui să arate ca 24 x 80.

- Ecranele 24 x 132 VTxxx ar trebui să arate ca 24 x 132.
- Pe stațiile de afișare 5250:
 - Ecranele 24 x 80 VTxxx ar trebui să arate ca 24 x 80.
 - Ecranele 24 x 132 cer ca tasta funcțională asignată pentru *SHIFTDSP (F10 pe maparea de tastatură implicită) să mute informația de pe ecran la stânga sau la dreapta.

Atribute caracter VTxxx

Un terminal VTxxx suportă următoarele atribute:

- Clipire
- Îngroșare
- Inversare imagine
- Subliniere
- Orice combinație de mai sus

Fluxul de date 5250 suportă atributele anterioare pentru ca o stație de afișare 5250 să poată reprezenta toate atributele VTxxx. Totuși, există câteva limitări:

- Fluxul de date 5250 poate suporta doar 3 din atributele caracterului în același timp. Atributele subliniere, clipire și imagine inversată sunt afișate când sistemul la distanță selectează toate atributele VTxxx în același timp. O stație de afișare 5250 nu poate afișa combinația de subliniere, îngroșare și imagine inversată. Sublinierea și imaginea inversată sunt afișate când aplicația VTxxx selectează această combinație.
- Octetul de atribute ocupă spațiu pe stațiile de lucru 5250 care nu suportă atribute extinse. Atributele nu ocupă spațiu pe un terminal VTxxx. Aceasta înseamnă că dacă selectați atributele caracterului, nu vedeți toate datele afișate pe un ecran 5250. Când primiți date VTxxx care trebuie afișate cu atributele caracterelor, octetul de atribute 5250 ocupă poziția dinaintea datelor. Caracterul care era tipărit acolo este pierdut. Dacă un caracter trebuie afișat la linia 1, coloana 1 cu atributele setate, acel caracter nu este afișat. Puteți alege să nu afișați atributele caracterului specificând DSPCHRATTR(*NO) la comanda STRTCPTELN. Aceasta vă permite să vedeți toate datele de pe ecran fără atribute.

Notă:

Această restricție nu este aplicabilă pentru terminale care suportă atribute extinse precum terminalul 3477.

Indicator tastatură VT100

Un terminal VT100 are indicatorul L1 care poate fi programat pentru diferite aplicații. Acest indicator nu este emulat de suportul Telnet iSeries.

Opțiuni de emulare VTxxx

Când folosiți modul VTxxx tot-ecranul cu serverul dumneavoastră Telnet, există câteva proceduri suplimentare pe care puteți să le faceți pentru a personaliza tipul de emulare. Puteți afișa maparea curentă de tastatură și apoi decide dacă vreți s-o schimbați sau nu. Puteți, de asemenea, schimba caracterele de control când folosiți modul VT220 tot-ecranul.

Afișarea unei mapări de tastatură VTxxx

Pentru a afișa maparea de tastatură curentă pentru VTxxx, folosiți comanda Afișare mapare tastatură VT (DSPVTMAP). Această comandă nu are parametri. Afișați cheile VTxxx care sunt mapate la funcțiile server iSeries^(TM).

Comanda DSPVTMAP este validă doar când este apelată dintr-o sesiune server Telnet iSeries care operează în modul VTxxx tot-ecranul.

Tastați DSPVTMAP pentru a vedea următorul ecran și apoi apăsați tasta Page Down pentru a vedea ecranele suplimentare. Puteți afișa maparea de tastatură VT folosind opțiunea 3 din meniul Configurare Telnet TCP/IP.

Setarea unei mapări de tastatură VTxxx

Pentru a schimba maparea de tastatură implicită, folosiți comanda Setare mapare tastatură VT (SETVTMAP). (Această comandă este, de asemenea disponibilă folosind opțiunea 5 (Setare mapare de tastatură VT) din meniul de Configurare TCP/IP Telnet.) Maparea de tastatură implicită pe care ați dorit s-o schimbați, este pusă la loc după lansarea comenzii fără nici un parametru specificat de utilizator. Puteți specifica până la patru din valorile speciale definite pentru fiecare parametru. O valoare specială nu poate fi folosită pentru a specifica mai mult de o funcție server iSeries.

Modificarea unei mapări de tastatură VTxxx

Ca și SETVTMAP, comanda Modificare mapare tastatură VT (CHGVTMAP) vă permite să vă configurați maparea de tastatură când sunteți conectat la un server Telnet iSeries în modul VTxxx. Parametrii pentru comanda SETVTMAP sunt, implicit, valorile pe care vreți să le schimbați. În timp ce parametrii pentru comanda CHGVTMAP sunt, implicit, valorile setate în acel moment. Exceptând această diferență, cele două comenzi sunt identice.

Pentru informații suplimentare despre modificarea mapării de tastatură VT, consultați Valorile tastelor VTxxx.

Acoperire automată VTxxx

Serverul iSeries VTxxx necesită ca clientul VTxxx să aibă opțiunea acoperirea automată (autowrap) pornită. Când autowrap este pornită, un caracter scris pe coloana 80 VTxxx cauzează mutarea cursorului pe coloana 1 a liniei următoare. Consultați documentația client VTxxx pentru detalii despre cum se setează această opțiune.

Caractere de control VT220

Când este negociată emularea pe 8-biți VT220, intervalul de caractere între X'80' până la X'9F' sunt protejate drept caractere de control C1 după cum sunt definite arhitectural în DEC VT220 Programmer Reference Manual. Aceasta poate cauza interpretarea caracterelor succesive de către sistem ca date în relație cu aceste caractere. Dacă sistemul negociază VT220 7-biți sau VT100, atunci intervalul întreg de caractere de la X'80' până la X'F' este disponibil pentru translatarea caracterelor. Interpretați X'80' până la X'9F' ca și caractere de control C1, doar în modul VT220 8-biți.

Aceasta are o importanță particulară pentru NLS, deoarece mai multe limbi diferite de engleză folosesc aceste valori pentru caracterele specifice limbii. În aceste cazuri, modul de emulare VT220 8-biți poate să nu funcționeze așa cum v-ați așteptat.

Valorile tastelor VTxxx

Suportul sesiunii client pentru ambele moduri VT100 și VT220 furnizează o mapare de tastatură principală și alternativă. Pentru a adapta capacitățile blocului de taste (keypad) VT220, puteți să vă salvați maparea tastaturii. Folosind tasta F6 din ecranul Modificare mapare tastatură VTxxx, puteți salva toate schimbările la aceste mapări de tastaturi pentru sesiunile ulterioare. Datele sunt salvate în profilul utilizatorului și odată salvate, se vor aplica automat următoarea dată când emulatorul Telnet VTxxx este activat.

Opțiunea tastatură pe care o selectați din meniul Trimitere funcții de control Telnet determină care mapare de tastatură trebuie folosită. Figurile de la 2 la 9 arată funcțiile VTxxx care corespund tastei 5250 AID. Lista următoare dă numărul opțiunii și figurile corespunzătoare :

- Figura 2 și Figura 3 ilustrează opțiunea 6 (Modificare mapare tastatură principală VT100).
- Figura 4 și Figura 5 ilustrează opțiunea 7 (Modificare mapare tastatură alternativă VT100).
- Figura 6 și Figura 7 ilustrează opțiunea 8 (Modificare mapare tastatură principală VT220).
- Figura 8 și Figura 9 ilustrează opțiunea 9 (Modificare mapare tastatură alternativă VT220).

Nivelul suportului negociat între serverul iSeries^(TM) și serverul Telnet determină ce opțiuni sunt afișate în meniul Send Telnet Control Functions. Meniul afișează opțiunile 6 și 7 dacă modul VT100 tot-ecranul este negociat inițial. Meniul afișează opțiunile 8 și 9 dacă modul VT220 tot-ecranul este negociat inițial.

Notă:

Nu există diferențe între valorile implicite ale mapărilor VT100 principale și alternative.

Următoarele figuri arată mapările implicite ale tastaturii. Puteți schimba oricare dintre valori. Dacă apăsați tasta Enter, schimbările dumneavoastră se vor salva doar pentru sesiunea curentă. Dacă apăsați F6 (Salvare), schimbările dumneavoastră se vor salva permanent și sunt valabile și următoarea dată când porniți o sesiune Telnet VTxxx.

Figura 1. Modificare mapare tastatură principală VT100 (Ecran 1)

```
-----+-----
                                Change VT100 Primary Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC
Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT
                                More...

F3=Exit  F6=Save  F12=Cancel
-----+-----
```

Figura 2. Modificare mapare tastatură principală VT100 (Ecran 2)

```
-----+-----
                                Change VT100 Primary Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 17 . . *CTLD
Function Key 18 . . *CTLE
Function Key 19 . . *CTLF
Function Key 20 . . *CTLG
Function Key 21 . . *CTLH
Function Key 22 . . *CTLI
Function Key 23 . . *CTLJ
Function Key 24 . . *CTLK
Rollup key . . . . *CTLL
Rolldown key . . . *CTLM

                                Bottom

F3=Exit  F6=Save  F12=Cancel
-----+-----
```

Figura 3. Modificare mapare tastatură alternativă VT100 (Ecran 1)

```
-----+-----
                                Change VT100 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT100 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
-----+-----
```

```

Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC
Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT
                        More...

F3=Exit  F6=Save  F12=Cancel

```

Figura 4. Modificare mapare tastatură alternativă VT100 (Ecran 2)

```

Change VT100 Alternate Keyboard Map

Type changes, press Enter:
5250 key          VT100 function
Function Key 17 . . *CTLD
Function Key 18 . . *CTLE
Function Key 19 . . *CTLF
Function Key 20 . . *CTLG
Function Key 21 . . *CTLH
Function Key 22 . . *CTLI
Function Key 23 . . *CTLJ
Function Key 24 . . *CTLK
Rollup key . . . . *CTLL
Rolldown key . . . *CTLM

Bott

F3=Exit  F6=Save  F12=Cancel

```

Puteți schimba între mapările principală și alternativă, în timpul unei sesiuni VTxxx, folosind tasta funcțională asignată cuvintelor cheie *KEYPRI și *KEYALT. Puteți asigura aceste cuvinte cheie oricăror taste funcționale 5250 disponibile. Este recomandat să asigurați *KEYPRI la tasta funcțională 5250 Page Up și *KEYALT la tasta funcțională 5250 Page Down pentru ambele mapări de tastatură: principală și alternativă.

Figura 5. Modificare mapare tastatură principală VT220 (Ecran 1)

```

Change VT220 Primary Keyboard Map

Type changes, press Enter:
5250 key          VT220 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . *SHIFTDSP
Function Key 11 . . *SENDWOCR
Function Key 12 . . *CTLC

```

```

Function Key 13 . . *CSRUP
Function Key 14 . . *CSRDOWN
Function Key 15 . . *CSRRIGHT
Function Key 16 . . *CSRLEFT
                    More...

F3=Exit  F6=Save  F12=Cancel

```

Figura 6. Modificare mapare tastatură principală VT220 (Ecran 2)

```

Change VT220 Primary Keyboard Map
Type changes, press Enter:
5250 key          VT220 function
Function Key 17 . . *CTLD
Function Key 18 . . *CTLE
Function Key 19 . . *CTLF
Function Key 20 . . *CTLG
Function Key 21 . . *CTLH
Function Key 22 . . *CTLI
Function Key 23 . . *CTLJ
Function Key 24 . . *CTLK
Page up (rolldown) . *KEYPRI
Page down (rollup) . *KEYALT

Bottom

F3=Exit  F6=Save  F12=Cancel

```

Figura 7. Modificare mapare tastatură alternativă VT220 (Ecran 1)

```

Change VT220 Alternate Keyboard Map
Type changes, press Enter:
5250 key          VT220 function
Function Key 1 . . . *PF1
Function Key 2 . . . *PF2
Function Key 3 . . . *PF3
Function Key 4 . . . *PF4
Function Key 5 . . . *ESC
Function Key 6 . . . *HIDE
Function Key 7 . . . *TAB
Function Key 8 . . . *CTLA
Function Key 9 . . . *CTLB
Function Key 10 . . . *SHIFTDSP
Function Key 11 . . . *SENDWOCR
Function Key 12 . . . *CTLC
Function Key 13 . . . *CSRUP
Function Key 14 . . . *CSRDOWN
Function Key 15 . . . *CSRRIGHT
Function Key 16 . . . *CSRLEFT
                    More...

F3=Exit  F6=Save  F12=Cancel

```

Figura 8. Modificare mapare tastatură alternativă VT220 (Ecran 2)

```

+-----+
|                                     Change VT220 Alternate Keyboard Map
|
| Type changes, press Enter:
| 5250 key          VT220 function
| Function Key 17 . . *CTLD
| Function Key 18 . . *FINDKEY
| Function Key 19 . . *INSERTKEY
| Function Key 20 . . *REMOVEKEY
| Function Key 21 . . *SELECTKEY
| Function Key 22 . . *PREVSCN
| Function Key 23 . . *NEXTSCN
| Function Key 24 . . *CTLK
| Rollup key . . . . *KEYPRI
| Rolldown key . . . . *KEYALT
|
|                                     Bottom
|
| F3=Exit  F6=Save  F12=Cancel
+-----+

```

Puteți introduce mai multe tipuri de informație VTxxx pentru a schimba maparea tastaturii. Urmează câteva exemple:

Date caracter

Puteți asigna un șir de caractere unei taste funcționale. Spre exemplu, dumneavoastră sunteți pe serverul iSeries și utilizați Telnet pentru a stabili o conexiune cu sistemul RS/6000^(R). Pentru a asigna șirul de caractere `set term=vt100` următoarei taste funcționale:

```
Tasta funcțională 24 . . *CTLK
```

De la iSeries va trebui să tastați:

```
Function Key 24 . . 'set term=vt100'
```

Aceasta vă permite să apăsați o tastă funcțională, decât să tastați tot timpul un șir de caractere.

Când apăsați tasta funcțională în timpul unei sesiuni VTxxx, șirul de caractere asignat tastei funcționale va fi transmis sistemului de la distanță cu caracterele CR(carriage return) și LF(line feed) adăugate. Dacă tastați date înainte de a apăsa tasta funcțională, sistemul adaugă șirul de caractere la datele pe care le-ați tastat. Aceasta vă permite să asignați șirul de caractere corespunzător unei comenzi des folosite la o tastă funcțională. Datele caracter pe care le tastați vor fi mapate din EBCDIC în ASCII înainte de a fi transmise sistemului la distanță.

Cuvinte cheie tastă de control Puteți asocia apăsarea unei taste control VTxxx unei taste funcționale folosind un cuvânt cheie definit. De exemplu, dacă vroiți să asignați o tastă de control VTxxx diferită pentru următoarea tastă funcțională :

```
Tasta funcțională 24 . . *CTLK
```

Ați tasta:

```
Function Key 24 . . *CTLZ
```

Când apăsați tasta funcțională, noul caracter de control asignat tastei funcționale este transmis sistemului la distanță. Dacă tastați date înainte de a apăsa tasta funcțională, sistemul adaugă caracterul de control la datele pe care le-ați tastat și le trimite sistemului la distanță.

Date hexazecimale

Puteți asigna un șir hexazecimal unei taste funcționale. Când apăsați tasta funcțională, datele hexazecimale sunt transmise sistemului la distanță. Caracterele CR și CF nu sunt adăugate datelor hexazecimale. Dacă tastați date înainte de a apăsa tasta funcțională, sistemul adaugă datele hexazecimale la datele pe care le-ați tastat și le trimite sistemului la

distanță. Aceasta vă permite să tastați un caracter care nu este pe tastatura 5250 (de exemplu, paranteze drepte). Pentru a asigna un șir hexazecimal, tastați X urmat de un șir de caractere hexazecimale între apostroafe, de exemplu, X'1A1A'. Datele hexazecimale nu sunt mapate înainte de a fi trimise sistemului la distanță.

Funcții de control iSeries locale

Puteți asocia un cuvânt cheie pentru a fi tratat local în sesiunea client Telnet iSeries. Aceste asignări sau mapări nu vor rezulta în traficul de flux de date ASCII transmis sesiunii sever Telnet la distanță. Aceste funcții de control local sunt *HIDE, *SHIFTDSP, *KEYPRI și *KEYALT. Funcția de trimis fără CR (*SENDWOOCR) este, de asemenea, o funcție locală, dar în acest caz, fluxurile de date ASCII sunt transmise sesiunii server Telnet la distanță.

Pentru informații suplimentare despre valorile tastelor VTxxx, faceți referire la următoarele subiecte:

- Suport limbă națională VTxxx
- Mod național VTxxx
- Tastatura numerică
- Editarea tastaturii numerice
- Valorile taste VTxxx după funcția 5250
- Moduri de operare stație de lucru VT220
- Tastele funcționale VT220 din rândul de sus
- Cuvinte cheie caractere de control VT100 și VT220

Supportul pentru limba națională VTxxx: Există câteva metode alternative de selectare a mapărilor de caractere între sisteme client și server cu emulări VTxxx. Acestea sunt:

- Identificator set de caractere codate (CCSID)
- Mod multinațional
- Mod național

Dacă nici unul nu este potrivit, puteți seta și specifica tabele de mapare definite de utilizator.

Notă:

Supportul VTxxx este limitat la un subset aparținând unor limbi cu set de caractere pe un octet (SBCS). O listă a limbilor suportate este prezentată mai târziu în această secțiune. Oricare din aceste tabele suportate de traducere limbă pe un singur octet, poate fi modificată pentru a mapa orice limbă pe un octet care este preferată, apoi identificată în parametrul corespunzător pentru a porni clientul Telnet.

Selecția modului este realizată cu parametrul CCSID din comanda Pornire TCP/IP Telnet (STRTCPTELN). Parametrii tabelă de intrare ASCII/EBCDIC (TBLVTIN) și de ieșire EBCDIC/ASCII (TBLVTOUT) ai acestei comenzi permit specificarea de tabele de mapare definite de utilizator. Dacă aceștia nu sunt necesari, valoarea implicită a *CCSID permite maparea caracterelor folosind modul specificat în parametrul CCSID.

Mod multinațional VTxxx

Modul multinațional suportă setul de caractere multinațional DEC, care este un set de caractere pe 8 biți care conține majoritatea caracterelor folosite în marile limbi Europene. Setul de caractere ASCII este inclus în setul de caractere multinațional DEC. Setul de caractere multinațional DEC este folosit implicit.

Modul național VTxxx: Modul național suportă setul de caractere de înlocuire național, care este un grup de seturi de caractere pe 7 biți. Doar unul din seturile de caractere din grup este disponibil pentru folosire la un moment dat. VT220 suportă, de asemenea, setul de caractere standard ASCII pe 7 biți ca parte a modului național. Terminalul VT220 suportă următoarele limbi naționale în seturi de caractere ASCII pe 7 biți:

- Englez
- Danez

- Olandez
- Finlandez
- Francez
- Francez/Canadian
- German
- Italian
- Norvegian
- Spaniol
- Suedez
- Elvețian
- Englez US

Pentru a folosi modul național, sistemul are nevoie de tabele de mapare pentru a mapa datele ASCII de intrare în EBCDIC și datele de ieșire EBCDIC în ASCII când operați în modul VTxxx tot-ecranul.

Folosiți parametrul CCSID la comanda Telnet pentru a selecta modul național, care este o tabelă de mapare NLS. Consultați Pornirea unei sesiuni VTxxx.

Introducând o valoare numerică care reprezintă o valoare CCSID înregistrată în intervalul 1-65553, este o cale pentru a identifica tabela de mapare corespunzătoare. Cartea *International Application Development* conține detalii despre valorile CCSID înregistrate.

Tabelele de mapare NLS sunt construite dinamic, pentru un sistem la distanță, prima dată când Telnet este folosit și sunt bazate pe seturile de caractere de înlocuire naționale DEC. Deoarece seturile de caractere sunt pe 7 biți, ele pot conține doar caractere unice pentru o singură țară. Deoarece setul de caractere multinațional DEC este pe 8 biți, el permite includerea caracterelor unice pentru un grup de țări.

Identificarea obiectelor tabelă

Puteți identifica obiectele tabelă (*TBL) folosind comanda Gestionare obiecte: WRKOBJ OBJ(QUSRSYS/Q*) OBJTYPE(*TBL)

Toate obiectele tabelă ale sistemului sunt conținute de biblioteca QUSRSYS.

Obiectele tabelă sunt denumite Qxxxxyzzz unde xxx este pagina de cod DE LA, yyy este setul de caractere LA și zzz este pagina de cod LA.

Pentru tabela de ieșire (EBCDIC-la-ASCII):

- ID-ul paginii de cod DE LA este luat din ID-ul paginii de cod din QCHRID a descrierii mesajului CPX8416 (folosiți WRKMSGD CPX8416 pentru afișare), 037 în figura de mai jos dintr-un sistem bazat pe Engleză US.
- Setul de caractere și pagina de cod LA sunt derivate din parametrul CCSID folosit cu comanda Telnet.

Pentru tabela de intrare (ASCII-la-EBCDIC):

- ID-ul paginii de cod DE LA este derivat din parametrul CCSID folosit cu comanda Telnet.
- Setul de caractere și pagina de cod LA sunt luate din ID-ul setului caractere și ID-ul paginii de cod din QCHRID a descrierii mesajului CPX8416 (folosiți WRKMSGD CPX8416 pentru afișare), 697 și 037 în figura de mai jos dintr-un sistem bazat pe engleza US.

Figura 1. Exemplu mesaj CPX8416

```

+-----+
|                                     System: SYSNAM01
| Message ID . . . . . : CPX8416
| Message file . . . . . : QCPFMSG
| Library . . . . . : QSYS
|
| Message . . . . . :
| QCHRID      697 37      QCURSYM      $ QDATFMT      MDY QDATSEP /
| QDECFMT     QLEAPADJ  0 QCCSID 37      QTIMSEP      : QLANGID ENU
| QCNTRYID    US QIGCCDEFNT *NONE
+-----+

```

CCSID	ID set de caractere real	ID set de caractere tabelă	ID pagină de caractere real	ID pagină de caractere real
MULTINAT	1290	A05	1100	A5U
ENGLEZ	1291	A06	1101	A5V
1292	A07	1102	A5W	
1293	A08	1103	A5X	
289	289	1104	A5Y	
1192	A8E	1020	A3M	
265	265	1011	A3D	
293	293	1012	A3E	
1297	BAB	1107	A52	
1195	A8H	1023	A3P	
1296	BAA	1106	A51	
1193	A8F	1021	A3N	

De exemplu, pe un sistem britanic cu QCHRID 697 285 (setul de caractere 697 pagina de cod 285) în mesajul CPX8416 care folosește Telnet cu CCSID(*BRITISH), tabelele vor avea următoarele nume:

- Ieșire (EBCDIC-to-ASCII) Q285A06A5V
- Intrare (ASCII-to-EBCDIC) QA5V697285

Tabele de mapare definite utilizator (Mod ASCII)

Unde tabelele de mapare multinaționale sau NLS nu coincid cu cerințele unui utilizator, pot fi create și folosite tabele de mapare a caracterelor definite de utilizator.

Aveți, de asemenea, posibilitatea de a specifica tabele de mapare definite de utilizator, folosind parametrii tabelor de ieșire ASCII-la-EBCDIC (TBLVTOUT) și intrare ASCII-la-EBCDIC (TBLVTIN) ai comenzii STRTCPTELN. Puteți specifica o tabelă de mapare definită de utilizator pentru ambele tabele de mapare de intrare și ieșire și apoi să folosiți valoarea sistem implicită pentru celelalte.

Tastatura numerică: Următoarea tabelă arată tastele de pe blocul de taste (keypad) auxiliar care, în mod normal, transmit coduri pentru cifre, punct zecimal, semnul minus și virgulă.

Cuvânt cheie	Mod	Caracter hexa Transmis	Descrierea caracterelor de control
*NUM0	Mod VT52	X'30' sau X'1B3F70' ¹	Tasta 0 a tastaturii numerice
*NUM0	Modul pe 7 biți VT100 sau VT220	X'30' sau X'1B4F70' ¹	Tasta 0 a tastaturii numerice
*NUM0	Modul pe 8 biți VT220	X'30' sau X'8F70' ²	Tasta 0 a tastaturii numerice

Cuvânt cheie	Mod	Caracter hexa Transmis	Descrierea caracterelor de control
*NUM1	Mod VT52	X'31' sau X'1B3F71' ¹	Tasta 1 a tastaturii numerice
*NUM1	Modul pe 7 biți VT100 sau VT220	X'31' sau X'1B4F71' ¹	Tasta 1 a tastaturii numerice
*NUM1	Modul pe 8 biți VT220	X'31' sau X'8F71' ²	Tasta 1 a tastaturii numerice
*NUM2	Mod VT52	X'32' sau X'1B3F72' ¹	Tasta 2 a tastaturii numerice
*NUM2	Modul pe 7 biți VT100 sau VT220	X'32' sau X'1B4F72' ¹	Tasta 2 a tastaturii numerice
*NUM2	Modul pe 8 biți VT220	X'32' sau X'8F72' ²	Tasta 2 a tastaturii numerice
*NUM3	Mod VT52	X'33' sau X'1B3F73' ¹	Tasta 3 a tastaturii numerice
*NUM3	Modul pe 7 biți VT100 sau VT220	X'33' sau X'1B4F73' ¹	Tasta 3 a tastaturii numerice
*NUM3	Modul pe 8 biți VT220	X'33' sau X'8F73' ²	Tasta 3 a tastaturii numerice
*NUM4	Mod VT52	X'34' sau X'1B3F74' ¹	Tasta 4 a tastaturii numerice
*NUM4	Modul pe 7 biți VT100 sau VT220	X'34' sau X'1B4F74' ¹	Tasta 4 a tastaturii numerice
*NUM4	Modul pe 8 biți VT220	X'34' sau X'8F74' ²	Tasta 4 a tastaturii numerice
*NUM5	Mod VT52	X'35' sau X'1B3F75' ¹	Tasta 5 a tastaturii numerice
*NUM5	Modul pe 7 biți VT100 sau VT220	X'35' sau X'1B4F75' ¹	Tasta 5 a tastaturii numerice
*NUM5	Modul pe 8 biți VT220	X'35' sau X'8F75' ²	Tasta 5 a tastaturii numerice
*NUM6	Mod VT52	X'36' sau X'1B3F76' ¹	Tasta 6 a tastaturii numerice
*NUM6	Modul pe 7 biți VT100 sau VT220	X'36' sau X'1B4F76' ¹	Tasta 6 a tastaturii numerice
*NUM6	Modul pe 8 biți VT220	X'36' sau X'8F76' ²	Tasta 6 a tastaturii numerice
*NUM7	Mod VT52	X'37' sau X'1B3F77' ¹	Tasta 7 a tastaturii numerice
*NUM7	Modul pe 7 biți VT100 sau VT220	X'37' sau X'1B4F77' ¹	Tasta 7 a tastaturii numerice
*NUM7	Modul pe 8 biți VT220	X'37' sau X'8F77' ²	Tasta 7 a tastaturii numerice
*NUM8	Mod VT52	X'38' sau X'1B3F78' ¹	Tasta 8 a tastaturii numerice
*NUM8	Modul pe 7 biți VT100 sau VT220	X'38' sau X'1B4F78' ¹	Tasta 8 a tastaturii numerice
*NUM8	Modul pe 8 biți VT220	X'38' sau X'8F78' ²	Tasta 8 a tastaturii numerice
*NUM9	Mod VT52	X'39' sau X'1B3F79' ¹	Tasta 9 a tastaturii numerice
*NUM9	Modul pe 7 biți VT100 sau VT220	X'39' sau X'1B4F79' ¹	Tasta 9 a tastaturii numerice
*NUM9	Modul pe 8 biți VT220	X'39' sau X'8F79' ²	Tasta 9 a tastaturii numerice
*NUMMINUS	Mod VT52	X'2D' sau X'1B3F6D' ¹	Tasta minus a tastaturii numerice
*NUMMINUS	Modul pe 7 biți VT100 sau VT220	X'2D' sau X'1B4F6D' ¹	Tasta minus a tastaturii numerice
*NUMMINUS	Modul pe 8 biți VT220	X'2D' sau X'8F6D' ²	Tasta minus a tastaturii numerice
*NUMCOMMA	Mod VT52	X'2C' sau X'1B3F6C' ¹	Tasta virgulă a tastaturii numerice
*NUMCOMMA	Modul pe 7 biți VT100 sau VT220	X'2C' sau X'1B4F6C' ¹	Tasta virgulă a tastaturii numerice
*NUMCOMMA	Modul pe 8 biți VT220	X'2C' sau X'8F6C' ²	Tasta virgulă a tastaturii numerice
*NUMBERIOD	Mod VT52	X'2E' sau X'1B3F6E' ¹	Tasta punct a tastaturii numerice
*NUMBERIOD	Modul pe 7 biți VT100 sau VT220	X'2E' sau X'1B4F6E' ¹	Tasta punct a tastaturii numerice
*NUMBERIOD	Modul pe 8 biți VT220	X'2E' sau X'8F6E' ²	Tasta punct a tastaturii numerice
*PF1	Mod VT52	X'1B50'	Tasta PF1 a tastaturii numerice
*PF1	Modul pe 7 biți VT100 sau VT220	X'1B4F50'	Tasta PF1 a tastaturii numerice
*PF1	Modul pe 8 biți VT220	X'8F50' ²	Tasta PF1 a tastaturii numerice
*PF2	Mod VT52	X'1B51'	Tasta PF2 a tastaturii numerice

Cuvânt cheie	Mod	Caracter hexa Transmis	Descrierea caracterelor de control
*PF2	Modul pe 7 biți VT100 sau VT220	X'1B4F51'	Tasta PF2 a tastaturii numerice
*PF2	Modul pe 8 biți VT220	X'8F51' ²	Tasta PF2 a tastaturii numerice
*PF3	Mod VT52	X'1B52'	Tasta PF3 a tastaturii numerice
*PF3	Modul pe 7 biți VT100 sau VT220	X'1B4F52'	Tasta PF3 a tastaturii numerice
*PF3	Modul pe 8 biți VT220	X'8F52' ²	Tasta PF3 a tastaturii numerice
*PF4	Mod VT52	X'1B53'	Tasta PF4 a tastaturii numerice
*PF4	Modul pe 7 biți VT100 sau VT220	X'1B4F53'	Tasta PF4 a tastaturii numerice
*PF4	Modul pe 8 biți VT220	X'8F53' ²	Tasta PF4 a tastaturii numerice

¹ - Este transmis un singur caracter în modul numeric tastatură numerică; o secvență de 3 caractere este trimisă în modul aplicație tastatură numerică.

² - Această secvență este o versiune scurtată a secvenței pe 7 biți. Ea poate fi ori prezentată când operați în modul 8-biți, care poate fi apelat de gazda sau serverul VT220 la distanță sau poate fi specificată în parametrul ASCOPRMOD din comanda STRTCPTELN CL.

Editarea keypad: Următoarea tabelă arată tastele care transmit coduri pentru tastele de editare ale blocului de taste (keypad).

Cuvânt cheie	Mod	Caracter hexa Transmis	Descrierea caracterelor de control
*CSRUP	Mod VT52	X'1B41'	Tasta cursor-sus
*CSRUP	Resetarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B5B41'	Tasta cursor-sus
*CSRUP	Resetarea modului tastă cursor pe 8 biți VT220	X'9B41'	Tasta cursor-sus
*CSRUP	Setarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B4F41'	Tasta cursor-sus
*CSRUP	Setarea modului tastă cursor pe 8 biți VT220	X'8F41'	Tasta cursor-sus
*CSRDOWN	Mod VT52	X'1B42'	Tasta cursor-jos
*CSRDOWN	Resetarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B5B42'	Tasta cursor-jos
*CSRDOWN	Resetarea modului tastă cursor pe 8 biți VT220	X'9B42'	Tasta cursor-jos
*CSRDOWN	Setarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B4F42'	Tasta cursor-jos
*CSRDOWN	Setarea modului tastă cursor pe 8 biți VT220	X'8F42'	Tasta cursor-jos
*CSRRIGHT	Mod VT52	X'1B43'	Tasta cursor dreapta
*CSRRIGHT	Resetarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B5B43'	Tasta cursor dreapta
*CSRRIGHT	Resetarea modului tastă cursor pe 8 biți VT220	X'9B43'	Tasta cursor dreapta
*CSRRIGHT	Setarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B4F43'	Tasta cursor dreapta

Cuvânt cheie	Mod	Caracter hexa Transmis	Descrierea caracterelor de control
*CSRRIGHT	Setarea modului tastă cursor pe 8 biți VT220	X'8F43'	Tasta cursor dreapta
*CSRLEFT	Mod VT52	X'1B44'	Tasta cursor-stânga
*CSRLEFT	Resetarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B5B44'	Tasta cursor-stânga
*CSRLEFT	Resetarea modului tastă cursor pe 8 biți VT220	X'9B44'	Tasta cursor-stânga
*CSRLEFT	Setarea modului tastă cursor pe 7 biți VT100 sau VT220	X'1B4F44'	Tasta cursor-stânga
*CSRLEFT	Setarea modului tastă cursor pe 8 biți VT220	X'8F44'	Tasta cursor-stânga
*FINDKEY	Modul pe 7 biți VT220	X'1B5B317E'	Editarea tastei Găsire a tastaturii numerice
*FINDKEY	Modul pe 8 biți VT220	X'9B317E' ¹	Editarea tastei Găsire a tastaturii numerice
*INSERTKEY	Modul pe 7 biți VT220	X'1B5B327E'	Editarea tastei Inserare aici a tastaturii numerice
*INSERTKEY	Modul pe 8 biți VT220	X'9B327E' ¹	Editarea tastei Inserare aici a tastaturii numerice
*REMOVEKEY	Modul pe 7 biți VT220	X'1B5B337E'	Editarea tastei Înlăturare a tastaturii numerice
*REMOVEKEY	Modul pe 8 biți VT220	X'9B337E' ¹	Editarea tastei Înlăturare a tastaturii numerice
*SELECTKEY	Modul pe 7 biți VT220	X'1B5B347E'	Editarea tastei Selectare a tastaturii numerice
*SELECTKEY	Modul pe 8 biți VT220	X'9B347E' ¹	Editarea tastei Selectare a tastaturii numerice
*PREVSCN	Modul pe 7 biți VT220	X'1B5B357E'	Editarea tastei Ecranul anterior a tastaturii numerice
*PREVSCN	Modul pe 8 biți VT220	X'9B357E' ¹	Editarea tastei Ecranul anterior a tastaturii numerice
*NEXTSCN	Modul pe 7 biți VT220	X'1B5B367E'	Editarea tastei Ecranul următor a tastaturii numerice
*NEXTSCN	Modul pe 8 biți VT220	X'9B367E' ¹	Editarea tastei Ecranul următor a tastaturii numerice

Notă: Această secvență este versiunea scurtată a secvenței pe 7 biți. Ea doar prezentată când operați în modul 8-biți, care poate fi apelat de gazda sau serverul VT220 de la distanță sau poate fi specificată în parametrul ASCOPRMOD din comanda CL, STRTCPTLN.

Valorile tastelor VTxxx prin funcția 5250:

Funcția implicită 5250	Valoare specială	Taste VTxxx	Valoare hexazecimală ¹
Attn	*CTLA	<CTRL-A>	X'01'
Attn	*ESCA	<ESC><A>	X'1B41'
Backspace	*BACKSPC	<Backspace sau CTRL-H>	X'08'
Curăță Ecranul	*ESCC	<ESC><C>	X'1B43'

Funcția implicită 5250	Valoare specială	Taste VTxxx	Valoare hexazecimală ¹
Cursor în jos	*CSRDOWN	<Săgeată în jos>	X'1B5B42'
Stânga cursor	*CSRLEFT	<Săgeată la stânga>	X'1B5B44'
Dreapta cursor	*CSRRIGHT	<Săgeată la dreapta>	X'1B5B43'
Cursor în sus	*CSRUP	<Săgeată în sus>	X'1B5B41'
Ștergere	*DLT	<Ștergere>	X'7F'
Ștergere	*RMV	<Înlăturare>	X'1B5B337E' ²
Ștergere	*RMV	<Înlăturare>	X'9B337E' ³
Duplicare	*ESCD	<ESC><D>	X'1B44'
Enter	*RETURN	<Return sau CTRL-M>	X'0D'
Ștergere intrare	*CTLE	<CTRL-E>	X'05'
Resetare eroare	*CTLR	<CTRL-R>	X'12'
Resetare eroare	*ESCR	<ESC><R>	X'1B52'
Avans câmp	*TAB	<TAB sau CTRL-I>	X'09'
Înapoi câmp	*ESCTAB	<ESC><Tab sau CTRL-I>	X'1B09'
Ieșire din câmp	*CTLK	<CTRL-K>	X'0B'
Ieșire din câmp	*CTLX	<CTRL-X>	X'18'
Ieșire din câmp	*ESCX	<ESC><X>	X'1B58'
Minus în câmp	*ESCM	<ESC><M>	X'1B4D'
Help	*CTLQST	<CTRL-Question Mark>	X'1F'
Help	*ESCH	<ESC><H>	X'1B48'
Home	*CTLO	<CTRL-O>	X'0F'
Inserare	*ESCI	<ESC><I>	X'1B49'
Inserare	*ESCDLT	<ESC><Delete>	X'1B7F'
Inserare	*INS	<Inserează aici>	X'1B5B327E' ²
Inserare	*INS	<Inserează aici>	X'9B327E' ³
Linie nouă	*ESCLF	<ESC> <Line Feed sau CTRL-J>	X'1B0A'
Page Down (Roll Up)	*CTLD	<CTRL-D>	X'04'
Page Down (Roll Up)	*CTLF	<CTRL-F>	X'06'
Page Down (Roll Up)	*NXTSCR	<Ecranul următor>	X'1B5B367E' ²
Page Down (Roll Up)	*NXTSCR	<Ecranul următor>	X'9B367E' ³
Page Up (Roll Down)	*CTLB	<CTRL-B>	X'02'
Page Up (Roll Down)	*CTLU	<CTRL-U>	X'15'
Page Up (Roll Down)	*PRVSCR	<Ecranul precedent>	X'1B5B357E' ²
Page Up (Roll Down)	*PRVSCR	<Ecranul precedent>	X'9B357E' ³
Print	*CTLP	<CTRL-P>	X'10'
Print	*ESCP	ESC	X'1B50'
Redesenare ecran	*CTLL	<CTRL-L>	X'0C'
Redesenare ecran	*ESCL	<ESC><L>	X'1B4C'
SysReq (Cerere sistem)	*CTLC	<CTRL-C>	X'03'
SysReq (Cerere sistem)	*ESCS	<ESC><S>	X'1B53'

Funcția implicită 5250	Valoare specială	Taste VTxxx	Valoare hexazecimală ¹
Cerere test	*CTLT	<CTRL-T>	X'14'
Comutare indicatoare luminoase	*ESCT	<ESC><T>	X'1B54'
F1	*ESC1	<ESC><1>	X'1B31'
F1	*F1	<F1> ⁵	X'1B5B31317E' ²
F1	*F1	<F1> ⁵	X'9B31317E' ³
F1	*PF1	<PF1>	X'1B4F50' ²
F1	*PF1	<PF1>	X'8F50' ³
F2	*ESC2	<ESC><2>	X'1B32'
F2	*F2	<F2> ⁵	X'1B5B31327E' ²
F2	*F2	<F2> ⁵	X'9B31327E' ³
F2	*PF2	<PF2>	X'1B4F51' ²
F2	*PF2	<PF2>	X'8F51' ³
F3	*ESC3	<ESC><3>	X'1B33'
F3	*F3	<F3> ⁵	X'1B5B31337E' ²
F3	*F3	<F3> ⁵	X'9B31337E' ³
F3	*PF3	<PF3>	X'1B4F52' ²
F3	*PF3	<PF3>	X'8F52' ³
F4	*ESC4	<ESC><4>	X'1B34'
F4	*F4	<F4> ⁵	X'1B5B31347E' ²
F4	*F4	<F4> ⁵	X'9B31347E' ³
F4	*PF4	<PF4>	X'1B4F53' ²
F4	*PF4	<PF4>	X'8F53' ³
F5	*ESC5	<ESC><5>	X'1B35'
F5	*F5	<F5> ⁵	X'1B5B31357E' ²
F5	*F5	<F5> ⁵	X'9B31357E' ³
F6	*ESC6	<ESC><6>	X'1B36'
F6	*F6	<F6>	X'1B5B31377E' ²
F6	*F6	<F6>	X'9B31377E' ³
F7	*ESC7	<ESC><7>	X'1B37'
F7	*F7	<F7>	X'1B5B31387E' ²
F7	*F7	<F7>	X'9B31387E' ³
F8	*ESC8	<ESC><8>	X'1B38'
F8	*F8	<F8>	X'1B5B31397E' ²
F8	*F8	<F8>	X'9B31397E' ³
F9	*ESC9	<ESC><9>	X'1B39'
F9	*F9	<F9>	X'1B5B32307E' ²
F9	*F9	<F9>	X'9B32307E' ³
F10	*ESC0	<ESC><0>	X'1B30'
F10	*F10	<F10>	X'1B5B32317E' ²
F10	*F10	<F10>	X'9B32317E' ³

Funcția implicită 5250	Valoare specială	Taste VTxxx	Valoare hexazecimală ¹
F11	*ESCMINUS	<ESC><Minus>	X'1B2D'
F11	*F11	<F11>	X'1B5B32337E' ²
F11	*F11	<F11>	X'9B32337E' ³
F12	*ESCEQ	<ESC><Equal>	X'1B3D'
F12	*F12	<F12>	X'1B5B32347E' ²
F12	*F12	<F12>	X'9B32347E' ³
F13	*ESCEXCL	<ESC><Exclamație>	X'1B21'
F13	*F13	<F13>	X'1B5B32357E' ²
F13	*F13	<F13>	X'9B32357E' ³
F14	*ESCAT	<ESC><La semn>	X'1B40'
F14	*F14	<F14>	X'1B5B32367E' ²
F14	*F14	<F14>	X'9B32367E' ³
F15	*ESCPOUND	<ESC><Pound>	X'1B23'
F15	*F15	<F15>	X'1B5B32387E' ²
F15	*F15	<F15>	X'9B32387E' ³
F16	*ESCDOLLAR	<ESC><Dollar>	X'1B24'
F16	*F16	<F16>	X'1B5B32397E' ²
F16	*F16	<F16>	X'9B32397E' ³
F17	*ESCPCT	<ESC><Procent>	X'1B25'
F17	*F17	<F17>	X'1B5B33317E' ²
F17	*F17	<F17>	X'9B33317E' ³
F18	*ESCCFX	<ESC><Accent circumflex>	X'1B5E' ¹
F18	*F18	<F18>	X'1B5B33327E' ²
F18	*F18	<F18>	X'9B33327E' ³
F19	*ESCAMP	<ESC><Ampersand>	X'1B26'
F19	*F19	<F19>	X'1B5B33337E' ²
F19	*F19	<F19>	X'9B33337E' ³
F20	*ESCAST	<ESC><Asterisc>	X'1B2A'
F20	*F20	<F20>	X'1B5B33347E' ²
F20	*F20	<F20>	X'9B33347E' ³
F21	*ESCLPAR	<ESC><Paranteză stânga>	X'1B50'
F22	*ESCRPAR	<ESC><Paranteză dreapta>	X'1B51'
F23	*ESCUS	<ESC><Linie de subliniere>	X'1B5F'
F24	*ESCPLUS	<ESC><Plus>	X'1B2B'
Vezi nota 4	*FIND	<Căutare>	X'1B5B317E'
Vezi nota 4	*FIND	<Căutare>	X'9B317E'
Vezi nota 4	*SELECT	<Selectare>	X'1B5B347E'
Vezi nota 4	*SELECT	<Selectare>	X'9B347E'

Notă:

- ¹ - Doar dacă nu este identificată valoarea hexazecimală este în modul VT100.
² - Mod de control VT220 pe 7 biți.
³ - Nu este nici o tastă funcțională 5250 care mapează această tastă VT.
⁴ - Tastele de la F1 la F5 nu sunt disponibile pe terminalul VT220. Totuși, multe emulatoare trimit aceste valori hexazecimale când una din tastele de la F1 până la F5 este apăsată.

Moduri de operare ale stațiilor de lucru VT220: Când sistemul negociază tipul stației de lucru VT220, există câteva moduri de operare care sunt suportate:

- Modul VT200 cu controale pe 7 biți este modul implicit și folosește funcții standard ANSI. Acest mod furnizează toată gama de capacități VT220 într-un mediu de comunicare pe 8 biți cu controale pe 7 biți. Acest mod suportă setul de caractere multinațional DEC sau seturile de caractere de înlocuire naționale (NRC), în funcție de setul de caractere al modului selectat.
- Modul VT200 cu controale pe 8 biți folosește funcții standard ANSI și furnizează toată gama de capacități VT220 într-un mediu de comunicație pe 8 biți cu controale pe 8 biți. Acest mod suportă setul de caractere multinațional DEC sau seturile NRC, în funcție de setul de caractere al modului selectat.
- Modul VT100 folosește funcții standard ANSI. Acest mod restricționează folosirea tastaturii doar la tastele VT100. Toate datele au o restricție pe 7 biți și se generează doar caractere ASCII, NRC sau grafice speciale.
- Modul VT52 folosește funcții private DEC (nu ANSI). Acest mod restricționează folosirea tastaturii doar la tastele VT52.

Dacă modul VT220 este negociat, atunci un mod de operare inițial pentru clientul Telnet este selectat folosind parametrul modului de operare ASCII (ASCOPRMOD) de la pornirea TCP/IP Telnet (STRTCPTLN) sau comanda TELNET.

Tastele funcționale din linia de sus la VT220: Următoarea tabelă arată tastele care transmit coduri pentru tastele funcționale de pe linia de sus a tastaturii VT220 în **modul 7 biți**.

Cuvânt cheie	Caracter hexazecimal transmis
*F6	X'1B5B31377E'
*F7	X'1B5B31387E'
*F8	X'1B5B31397E'
*F9	X'1B5B32307E'
*F10	X'1B5B32317E'
*F11	X'1B5B32337E'
*F12	X'1B5B32347E'
*F13	X'1B5B32357E'
*F14	X'1B5B32367E'
*F15 or *HELP	X'1B5B32387E'
*F16 or *DO	X'1B5B32397E'
*F17	X'1B5B33317E'
*F18	X'1B5B33327E'
*F19	X'1B5B33337E'
*F20	X'1B5B33347E'

Următoarea tabelă arată tastele care transmit coduri pentru tastele funcționale de pe linia de sus a tastaturii VT220 în **modul 8 biți**.

Cuvânt cheie	Caracter hexazecimal transmis
*F6	X'9B31377E'

Cuvânt cheie	Caracter hexazecimal transmis
*F7	X'9B31387E'
*F8	X'9B31397E'
*F9	X'9B32307E'
*F10	X'9B32317E'
*F11	X'9B32337E'
*F12	X'9B32347E'
*F13	X'9B32357E'
*F14	X'9B32367E'
*F15 or *HELP	X'9B32387E'
*F16 or *DO	X'9B32397E'
*F17	X'9B33317E'
*F18	X'9B33327E'
*F19	X'9B33337E'
*F20	X'9B33347E'

Cuvinte Cheie Caractere de Control la VT100 și VT220:

Descrierea caracterelor de control	Tastă apăsată cu tasta CTRL apăsată	Cuvânt cheie	Caracter hexa Transmis
Null	Bara de spațiu	*NUL	X'00'
Început antet	A	*SOH,*CTLA	X'01'
Început text	B	*STX,*CTLB	X'02'
Sfârșit text	C	*ETX,*CTLC	X'03'
Sfârșit transmisie	D	*EOT,*CTLD	X'04'
Întrebare	E	*ENQ,*CTLE	X'05'
Aprobare	F	*ACK,*CTLF	X'06'
Sonerie	G	*BEL,*CTLG	X'07'
Backspace	H	*BS,*CTLH	X'08'
Tabulare orizontală	I	*HT,*CTLI	X'09'
Linie nouă (Line feed)	J	*LF,*CTLJ	X'0A'
Tabulare verticală	K	*VT,*CTLK	X'0B'
Pagina nouă (Form feed)	L	*FF,*CTLL	X'0C'
Început rând (Carriage return)	M	*CR,*CTLM	X'0D'
Shift afară	N	*SO,*CTLN	X'0E'
Shift apăsat	O	*SI,*CTLO	X'0F'
Data link escape	P	*DLE,*CTLP	X'10'
Control dispozitiv 1	Q	*DC1,*CTLQ	X'11'
Control dispozitiv 2	R	*DC2,*CTLR	X'12'
Control dispozitiv 3	S	*DC3,*CTLS	X'13'
Control dispozitiv 4	T	*DC4,*CTLT	X'14'
Confirmare negativă	U	*NAK,*CTLU	X'15'

Descrierea caracterelor de control	Tastă apăsată cu tasta CTRL apăsată	Cuvânt cheie	Caracter hexa Transmis
Pauză sincronă (Synchronous idle)	V	*SYN,*CTLV	X'16'
Sfârșit bloc transmisie	W	*ETB,*CTLW	X'17'
Abandon caracter sau cuvânt anterior	X	*CAN,*CTLX	X'18'
Sfârșit mediu	Y	*EM,*CTLY	X'19'
Înlocuitor	Z	*SUB,*CTLZ	X'1A'
Escape	[*ESC	X'1B'
Separator fișier	\	*FS	X'1C'
Separator grup]	*GS	X'1D'
Separator înregistrare	&eqv.	*RS	X'1E'
Separator unitate	?	*US	X'1F'
Ștergere		*DEL	X'7F'

Stabilirea unei sesiuni Telnet în cascadă

Puteți stabili o sesiune Telnet în timpul unei sesiuni Telnet. Sistemul gazdă este primul sistem client pe care îl folosiți. Sistemul terminal este ultimul sistem server Telnet pe care îl accesați. Sistemul prin care treceți pentru a ajunge de la sistemul inițial la sistemul terminal este un sistem intermediar. Pentru a înțelege mai bine cum să folosiți Telnet în cascadă, faceți referire la Scenariu sesiuni Telnet în cascadă.

Pornirea unei sesiuni în cascadă

Pentru pornirea sesiunii dumneavoastră în cascadă, înregistrați-vă la sistemul gazdă, apoi urmați pașii pentru stabilirea unei sesiuni client. Repetați pașii pentru fiecare sistem la care doriți să vă conectați.

Consultați Mutarea între sesiunile Telnet în cascadă pentru alte instrucțiuni despre cum să folosiți sesiunile în cascadă.

Întoarcerea la sistemul server

Comanda SIGNOFF termină sesiunea și vă returnează la ecranul de semnare al sistemului server. Când sunteți conectat la sistemul server, comanda SIGNOFF termină jobul server curent și vă returnează la ecranul de semnare al sistemului server.

Puteți utiliza și parametrul terminare conexiune (ENDCNN) al comenzii SIGNOFF pentru a închide sesiunea de pe sistemul server și pentru a termina conexiunea TELNET. De exemplu, `signoff endcnn(*yes)` vă readuce în sesiunea dumneavoastră inițială pe sistemul client sau în sesiunea anterioară dacă aveți stabilite mai mult de o sesiune Telnet.

Notă:

- Nu există nici o limitare pentru numărul de sisteme cu care puteți stabili o sesiune Telnet.
- Sistemul gazdă interceptează opțiunile 13 și 14 din Cererea Sistem dacă sunt introduse la linia de intrare a Cererii Sistem. Această funcție vă poate ajuta dacă stabiliți o sesiune Telnet cu un sistem la care nu vă puteți semna. În acest caz, puteți termina o sesiune la acel sistem făcând următoarele lucruri:
 - Apăsați tasta SysReq (Cerere sistem).
 - Tastați 13 (Pornire cerere sistem pe sistemul acasă) la linia de intrare a cererii de sistem.
 - Tastați 2 (Oprire cerere precedentă) în meniul Cerere sistem.

Trecerea între sesiunile Telnet în cascadă

Odată ce ați pornit o sesiune Telnet în cascadă, apăsați tasta **System Request** (Sys Req) și apoi **Enter** pentru a afișa meniul Cerere sistem (System Request).

Meniul Cerere sistem vă oferă următoarele opțiuni:

Opțiunea SysReq (Cerere sistem)	Acțiune	Descriere
10	Pornirea unei cereri sistem la un sistem client	Afișează meniul SysReq (Cerere sistem) în sistemul client anterior
11	Transferul la sistemul client	Vă transferă la un job alternativ pe sistemul client anterior
13	Pornirea unei cereri sistem la sistemul de bază	Vă duce de pe un sistem terminal sau intermediar la meniul SysReq (Cerere sistem) al sistemului de bază
14	Transferul la sistemul de bază	vă duce dintr-un sistem terminal sau intermediar la jobul alternativ de pe sistemul de bază
15	Transferul la sistemul terminal	vă duce dintr-un sistem de bază sau intermediar la sistemul terminal.

Pentru a ocoli meniul Cerere sistem (System Request), apăsați tasta **SysReq** și introduceți 10 în linia de comandă. Această scurtătură este aplicabilă doar între serverele iSeries^(TM).

Pentru clienți Telnet non-IBM^(R)

Este posibil să pierdeți o sesiune Telnet în cascadă atunci când încercați să folosiți Cererea Sistem, opțiunile 10, 11, 13 sau 14. Pentru opțiunile 10 și 11, PC-ul client este sistemul anterior. Pentru opțiunile 13 și 14, PC-ul client este sistemul acasă.

Clientul dumneavoastră Telnet este compatibil dacă trece aceste două teste:

- Vă întoarceți pe sistemul acasă după utilizarea opțiunilor 13 sau 14.
- Nu pierdeți o sesiune utilizând opțiunile 10 sau 11 de pe sistemul acasă.

Pentru clienți incompatibili, urmați acești pași în loc să folosiți Cererea Sistem, opțiunile 10, 11, 13 sau 14:

1. Folosiți Cererea Sistem, opțiunea 11 pentru a vă întoarce din sistem în sistem până la sistemul acasă. Sistemul acasă este primul iSeries la care s-a conectat clientul Telnet la începutul sesiunii.
2. De pe sistemul acasă, utilizați Cererea Sistem, opțiunea 1, pentru a înainta din sistem în sistem.

Terminarea unei sesiuni client Telnet

Când sunteți conectat la un server iSeries^(TM), făcând sing-off nu înseamnă neapărat că ați terminat sesiunea pe serverul Telnet. Pentru a închide această sesiune, trebuie să introduceți o tastă sau o secvență de taste pentru a poziționa clientul Telnet în modul comandă locală. Puteți apoi tasta comanda pentru închiderea sesiunii. Acest tabel furnizează secvențe de taste pentru terminarea unei sesiuni pe serverul Telnet.

Terminarea unei sesiuni client Telnet

- Din serverul iSeries, apăsați tasta **Attn** și selectați opțiunea 99 (End Telnet session - QUIT).
- Din cele mai multe alte sisteme, deconectați-vă.

Dacă nu știți ce tastă sau ce secvență de taste să apăsați pentru a determina clientul să intre în modul comandă, consultați administratorul de sistem sau documentația pentru clientul Telnet.

Puteți utiliza și parametrul terminare conexiune (ENDCNN) al comenzii SIGNOFF pentru a închide sesiunea de pe sistemul server și pentru a termina conexiunea Telnet. De exemplu, SIGNOFF ENDCNN(*YES) vă întoarce pe sistemul client (dacă ați stabilit numai o sesiune Telnet). Sau vă întoarce pe sistemul anterior (dacă ați stabilit mai multe sesiuni Telnet).

Depanarea problemelor Telnet

Acest subiect furnizează informație folositoare pentru a vă ajuta în detectarea și rezolvarea problemelor cu Telnet. Acesta nu este un ghid complet, totuși, el poate fi un prim pas folositor. Acest subiect furnizează următoarele informații:

Determinarea problemelor cu Telnet

Această secțiune dă o informație de diagnosticare incluzând o diagramă pentru analiza problemelor serverului și o listă de materiale necesare când raportați probleme Telnet.

Depanarea tipurilor de emulare

Această secțiune dă o informație mai specifică despre determinarea problemelor cu tipul individual de emulare.

Depanarea serverului Telnet SSL

Această secțiune furnizează informație detaliată despre rezolvarea problemelor cu serverul SSL incluzând codurile return SSL și o listă cu problemele SSL obișnuite.

Ieșirile programului service TRCTCPAPP

Rulați o componentă de urmărire VTM cu câmpul de date al utilizatorului setat la Telnet.

Materialele necesare pentru raportarea problemelor

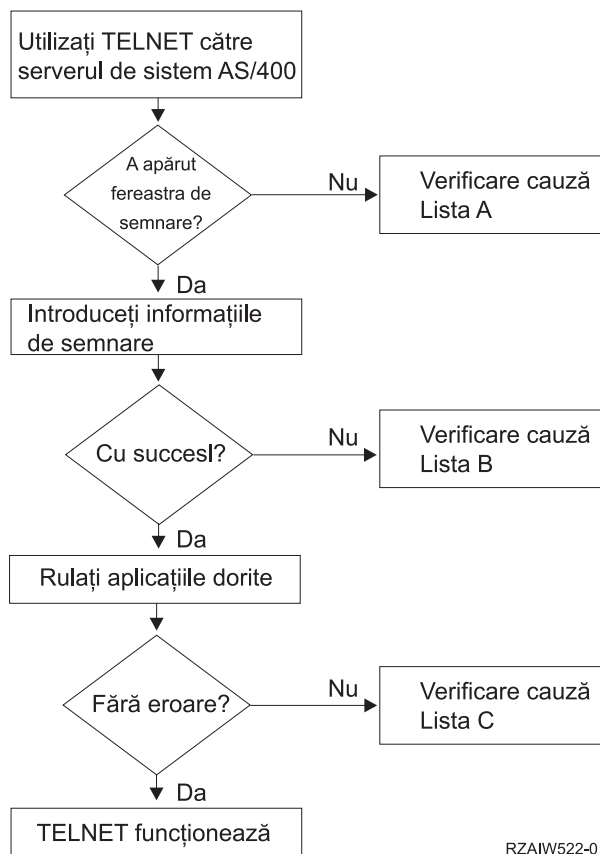
Această secțiune descrie de ce informații poate avea nevoie reprezentantul dumneavoastră de service.

Informații de diagnoză generate automat (FFDC)

Câteva erori de server Telnet vor genera automat informații de diagnosticare. Această secțiune descrie cum puteți extrage această informație.

Determinarea problemelor cu Telnet

Folosiți acest grafic după ce folosiți graficul pentru probleme generale TCP/IP . Dacă se detectează o problemă în timpul utilizării serverului Telnet iSeries^(TM), utilizați următoarea listă pentru a identifica cauza. Listele de cauze care urmează identifică potențialele probleme.



Descriere: Organigrama de analiză a problemelor Telnet

Lista de cauze A

1. Verificați dacă joburile serverului Telnet sunt active și dacă serviciul Telnet este asignat unui port valid nerestricționat.
 - a. Pentru a verifica dacă joburile QTVTELNET și QTVDEVICE sunt active în subsistemul QSYSWRK, urmați următorii pași:
 - 1) Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** → **Control funcționare**.
 - 2) Faceți clic dreapta pe **Joburi active** și uitați-vă dacă sunt active QTVTELNET și QTVDEVICE.
 - b. Dacă aceste joburi nu sunt active, efectuați următorii pași pentru a porni aceste joburi:
 - 1) Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** → **Rețea** → **Servere** → **TCP/IP**.
 - 2) Faceți clic dreapta pe **Telnet** și selectați **Pornire**.
 - c. Pentru a verifica dacă serviciul Telnet este asociat unui port valid, urmați următorii pași:
 - 1) Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** → **Rețea** → **Servere** → **TCP/IP**.
 - 2) Faceți clic dreapta pe **Conexiuni** și selectați **Deschidere**.
 - 3) Căutați Telnet.
 - d. Pentru imprimante, asigurați-vă că subsistemul QSPL este activ.
 - e. Verificați restricțiile porturilor mergând în meniul CFGTCP și selectând opțiunea 4 (Gestionare restricții porturi TCP/IP).
2. Verificați dacă Valoarea de sistem a dispozitivelor pe un server iSeries este setată corespunzător pentru a permite serverului TELNET să creeze automat dispozitive virtuale.

3. Verificați dacă conexiunea de rețea între serverul iSeries și clientul Telnet este activă folosind serviciul ping în Navigator iSeries. Dacă nu este activă, consultați administratorul de rețea.
4. Verificați dacă dispozitivele virtuale de pe serverele iSeries care sunt utilizate de Telnet sunt definite la un subsistem, unde trebuie să ruleze joburile Telnet interactive.
 - a. Pentru a vedea care intrări stație de lucru sunt definite unui subsistem, urmați următorii pași:
 - 1) Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Control funcționare**.
 - 2) Faceți dublu clic pe **Subsisteme** și selectați **Deschidere**.
 - b. Folosiți comanda de adăugare intrare stație de lucru (ADDWSE) pentru a defini stațiile de lucru unui subsistem. De exemplu, puteți folosi comanda următoare pentru a permite tuturor tipurilor de stații de lucru să ruleze sub subsistemul QINTER:


```
ADDWSE SBS(D(QINTER) WRKSTNTYPE(*ALL)
```
5. Verificați dacă subsistemul interactiv (QINTER) este activ. Conexiunile Telnet eșuează dacă subsistemele interactive nu sunt active. În această situație, sistemul nu scrie mesaje de eroare în istoricele de job QTVTELNET sau QTVDEVICE pentru a vă arăta problema.

Pentru a verifica dacă un subsistem este activ, completați următorii pași:

 - a. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Control funcționare**.
 - b. Faceți dublu clic pe **Subsisteme** și selectați **Deschidere**.
 - c. Verificați dacă subsistemul este activ.
6. Dacă operați în modul VTxxx tot-ecranul, verificați dacă configurarea locală a clientului VTxxx specifică autowrap. Când autowrap este pornită, sistemul va face wrap automat la coloana 80.
7. Căutați un program de ieșire Telnet înregistrat la punctul de ieșire QIBM_QTG_DEVINIT, formatul INIT0100, folosind comanda de lucru cu informațiile despre înregistrare (WRKREGINF). Dacă există un program de ieșire înregistrat pentru un utilizator, verificați istoricul de job al serverului Telnet, cu numele jobului QTVDEVICE, pentru orice erori legate de acel program. Dacă există erori, corectați erorile în programul de ieșire sau ștergeți programul de ieșire cu comanda de ștergere a programului de ieșire (RMVEXITPGM).
8. Asigurați-vă că clientul dumneavoastră încearcă să folosească portul corect pentru a se conecta la Telnet.

Pentru a determina portul pe care serviciul Telnet este asignat, completați următorii pași:

 - a. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Rețea** —> **Servere** —> **TCP/IP**.
 - b. Faceți clic dreapta pe **Conexiuni** și selectați **Deschidere**.
 - c. Căutați Telnet.
9. Folosiți comanda CFGTCP pentru a verifica dacă portul pe care clientul dumneavoastră încearcă să se conecteze nu este restricționat. De asemenea, cercetați istoricul de jobQTVTELNET pentru mesaje care indică dacă portul pe care încercați să-l folosiți nu este restricționat.
10. Când intenționați să vă conectați utilizând Telnet SSL, fiți siguri că aveți instalat Digital Certificate Manager (DCM) și unul dintre produsele criptografice furnizate de IBM.^(R). Aceasta este în plus față de cele enumerate mai sus. De asemenea, asigurați-vă că un certificat valid, neexpirat este asignat serverului Telnet (QIBM_QTV_TELNET_SERVER).

Lista de cauze B

1. Verificați-vă autorizarea asupra dispozitivelor virtuale de afișare. Dacă primiți mesajul CPF1110 când încercați să vă semnați la serverul iSeries, nu sunteți autorizați la dispozitivul de afișare virtual. Când serverul Telnet iSeries creează dispozitive virtuale, valoarea sistem QCRTAUT este folosită pentru a determina autorizarea acordată utilizatorului *PUBLIC. Această valoare sistem trebuie să fie *CHANGE pentru a permite oricărui utilizator să se semneze folosind Telnet.
2. Verificați dacă valoarea sistem QLMTSECOFR este corectă, în cazul în care sunteți responsabilul de securitate sau aveți autorizarea *SECOFR.

Lista de cauze C

1. Verificați-vă opțiunea în procesarea cuvintelor. Când întâlniți probleme în timpul utilizării OfficeVision^(R) sau comenzii WRKWFLR (Work with Folders), s-ar putea să fie nevoie să schimbați configurația dumneavoastră în așa

fel încât să fie folosit editorul Office Adapted Editor, în locul editorului standard. Pentru a face aceasta, puneți administratorul de sistem să schimbe opțiunea de procesare cuvinte (word processing) din informația de mediu asociată cu ID-ul de utilizator office.

2. Dacă operați în modul VTxxx tot-ecranul, verificați dacă configurarea locală a clientului VTxxx specifică autowrap. Când autowrap este pornită, sistemul va face wrap automat la coloana 80.
3. În cazul în care caracterele nu sunt afișate corect în sesiunea dumneavoastră VTxxx, verificați dacă sunt folosite tabelele de mapare corecte pentru sesiunea dumneavoastră
4. Dacă clientul VTxxx scoate sunete de fiecare dată când apăsați o tastă, tastatura dumneavoastră poate fi blocată. Consultați Condiții de eroare la tastatura 5250 (page 58).
5. Verificați istoricul jobului QTVTELNET și istoricul jobului QTVDEVICE pentru mesaje de eroare pe serverul iSeries.

Ping către serverul dumneavoastră gazdă

Utilizați comanda PING din Navigator iSeries^(TM) pentru a verifica conexiunea dumneavoastră TCP/IP.

Pentru a face ping sistemului dumneavoastră, completați următorii pași:

1. Porniți Navigator iSeries și expandați **serverul dumneavoastră iSeries** —> **Rețea**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Utilitare**.
3. Apăsați **Ping** pentru a afișa caseta de dialog Ping.
4. Tastați numele gazdă în caseta Ping (de exemplu, companyname.com).
5. Apăsați **Ping acum**.

Mesajele sunt afișate în caseta **Rezultate** pentru a vă spune starea conexiunii dumneavoastră.

Depanarea tipurilor de emulare

Când dezvoltați un client Telnet, este important să negociați tipul corect de emulare pentru stația de lucru. Funcțiile permise variază după tipul stației de lucru. Ceea ce urmează este un ghid pentru a înțelege tipul stației de lucru și capabilitățile de funcționare ale ei.

Negocierile și mapările tip stație de lucru

Tabela de mapări a stațiilor de lucru și a imprimantelor arată o listă de stații de afișare virtuale pe care serverul le folosește pentru a se potrivi cu stațiile fizice de afișare ale sistemului client.

Dacă nu sunteți sigur ce pachet de emulare folosiți, trebuie să aflați care vă este dispozitivul virtual de afișare. Puteți folosi comanda Lucrul joburi (WRKJOB) pentru a afla care este. Numele jobului este afișat sus. Acesta este numele dispozitivului virtual de afișare asociat cu jobul dumneavoastră Implicit, dispozitivul virtual va fi numit QPADEVxxxx, unde xxxx este un caracter alfanumeric.

Pentru a determina tipul dispozitivului, tastați:

```
WRKCFGSTS *DEV QPADEVxxxx
```

Puteți lucra cu descrierea dispozitivului dumneavoastră. Tastați un 8 (Gestionare descriere) lângă numele dispozitivului. Sistemul afișează tipul dispozitivului. Puteți determina din tipul dispozitivului dacă rulați în mod tot-ecranul pentru 3270, 5250, VT100 sau VT220.

Tabela 1. Mapările imprimantă și stație de lucru

Stația de lucru suportată și (model)	Tipul echivalent și (model)	Specificația Internet	Descriere
5251 (11)		IBM-5251-11	Monitor monocrom 24 X 80
5291 (1)	5291 (2)	IBM-5291-1	Monitor monocrom 24 X 80

Stația de lucru suportată și (model)	Tipul echivalent și (model)	Specificația Internet	Descriere
5292 (2)		IBM-5292-2	Monitor color 24 X 80; acest tip de stație de lucru este, de asemenea, emulat de o funcție grafică a stației de lucru.
3196 (A1)	3196 (A1) 3196(B1) 3196 (B2) 3476 (EA)	IBM-3196-A1	Monitor monocrom 24 X 80; acest tip de stație de lucru este, de asemenea, emulat de o funcție stație de lucru monocromă.
3486 (BA)		IBM-3486-BA	Monitor monocrom 24 X 80
3487(HA) ²	3487 (HG) ² 3487 (HW) ²	IBM-3487-HA	Monitor monocrom 24 X 80; acest tip de stație de lucru este, de asemenea, emulat de o funcție stație de lucru monocromă.
3487 (HC) ²		IBM-3487-HC	Monitor color 24 X 80; acest tip de stație de lucru este, de asemenea, emulat de o funcție stație de lucru color.
3179 (2)	3197 (C1) 3197 (C2) 3476 (EC)5292 (1)	IBM-3179-2	Monitor color 24 X 80; acest tip de stație de lucru este, de asemenea, emulat de o funcție stație de lucru color.
3180 (2)	3197 (D1) 3197 (D2) 3197 (W1) 3197 (W2)	IBM-3180-2	Monitor monocrom 27 X 132
5555 (B01)	5555 (E01)	IBM-5555-B01	Monitor monocrom 24 X 80 DBCS; acest tip de stație de lucru este emulat de o funcție stație de lucru care suportă ecrane DBCS.
5555 (C01)	5555 (F01)	IBM-5555-C01	Monitor color 24 x 80 DBCS; acest tip de stație de lucru este emulat de o funcție stație de lucru care suportă ecrane DBCS.
5555 (G01)		IBM-5555-G01	Monitor monocrom 24 X 80 DBCS, cu afișare grafică; acest tip de stație de lucru este emulat de o funcție a stației de lucru care suportă ecrane DBCS.
5555 (G02)		IBM-5555-G02	Monitor color 24 x 80 DBCS, cu afișare grafică; acest tip de stație de lucru este emulat de o funcție a stației de lucru care suportă ecrane DBCS.
3477 (FC)		IBM-3477-FC	Monitor color 27 X 132 ecran lat
3477 (FG)	3477 (FA) 3477 (FD) 3477 (FW)3477 (FE)	IBM-3477-FG	Monitor monocrom 27 X 132 ecran lat
3277 (0) ³	3277 (DHCF)	IBM-3277-2	Monitor monocrom 24 X 80

Stația de lucru suportată și (model)	Tipul echivalent și (model)	Specificația Internet	Descriere
3277 (0) ^{3,4}	3278 (DHCF)	IBM-3278-2	Monitor monocrom 24 X 80
3278 (0) ³		IBM-3278-2-E ⁵	Monitor monocrom 24 x 80
3278 (0) ³		IBM-3278-3	Monitor monocrom 24 x 80
3278 (0) ³		IBM-3278-4	Monitor monocrom 24 x 80
3278 (0) ³		IBM-3278-5	Monitor monocrom 24 x 80
3279 (0) ³	3279 (DHCF)	IBM-3279-2 IBM-3279-2-E ⁵	Monitor monocrom 24 X 80
3279 (0) ³		IBM-3279-3	Monitor color 24 x 80
3812 (1)		IBM-3812-1	Imprimantă 3812 (SBCS)
5553 (B01)		IBM-5553-B01	Imprimantă 5553 (DBCS)
VT100 (*ASCII) ⁶		DEC-VT100 VT100(7) VT102 DEC-VT102 DEC-VT200 DEC-VT220 VT200(7) VT220(7)	Monitor monocrom ASCII 24 x 80

Considerente:

¹ - Toate stațiile de lucru 5250, cu excepția 5555 (B01) și 5555 (C01), pot opera ca stații de lucru 5251-11.

² - Această stație de lucru poate fi configurată fie 24 x 80 fie 27 x 132. Trebuie să determinați modul stației de lucru înainte de a seta valoarea parametrului tip de stație de lucru.

³ - Serverele iSeries^(TM) suportă doar ecrane 24 X 80 în stațiile de lucru la distanță 327x. Stațiile de lucru de la distanță 3277 (cele cu DHCF și cele obișnuite) sunt mapate pe IBM-3277-2. Stațiile de la distanță 3278 sunt mapate pe IBM-3278-2. Stațiile de la distanță 3279 sunt mapate pe IBM-3279-2.

⁴ - Unele pachete de emulare Telnet 3270 tot-ecranul (TN3270) sau 3278-2 nu suportă corect câmpurile de scriere structurate. Din această cauză, dispozitivele tip 3278-2 sunt mapate la dispozitive 3277-2 de către implementarea serverului Telnet iSeries pentru a permite serverului iSeries să lucreze cu acele implementări TN3270.

⁵ - Evidențierea atributelor extinse este suportată. Sublinierea, clipirea și imaginea inversată sunt incluse. Procesarea 3270 DBCS este, de asemenea, suportată.

⁶ - Dispozitivul virtual VT100 suportă dispozitivele VT220.

⁷ - VT100, VT200 și VT220 nu sunt nume oficiale pentru tipurile de terminal. Toruși, câteva implementări negociază folosind aceste nume ca valoare pentru tipul de terminal.

Depanarea serverului Telnet SSL

Pentru a identifica problemele cu serverul Telnet, urmați acești pași:

1. Consultați starea sistemului pentru a verifica dacă este instalat software corespunzător și dacă serverele sunt pornite.
2. Faceți ping la serverul dumneavoastră gazdă pentru a verifica dacă TCP/IP este pornit și rețeaua este OK.
3. Verificați dacă severul Telnet este pornit .
4. Verificați dacă există un ascultător SSL folosind comanda NETSTAT *CNN.
5. Consultați istoricul jobuluiTelnet pentru a găsi codul de retur al SSL.
6. Consultați Probleme SSL și coduri de retur pentru sugestii în rezolvarea problemelor.

Certificate digitale incorecte pot cauza multe probleme cu SSL. DCM (Digital Certificate Manager) vă permite să modificați certificatele CA (Certificate Authority) sau sistem. Pentru a confirma faptul că aveți un certificat sistem valid, citiți cum să porniți Digital Certificate Manager și să vizualizați apoi certificatul sistem.

Verificarea stării sistemului

Pentru a confirma că serverul Telnet este pregătit pentru sesiuni SSL, urmați acești pași:

1. Verificați dacă aveți instalat software-ul corect pentru a suporta Telnet SSL și pentru a gestiona certificatele:

- TCP/IP Connectivity Utilities pentru iSeries^(TM), 5722-TC1
 - Digital Certificate Manager, 5722-SS1 - Boss Option 34
 - Cryptographic Access Provider, 5722-AC x
 - Serverul IBM^(R) HTTP pentru iSeries, 5722-DG1
 - Developer Kit pentru Java^(TM), 5722-JV1
2. Verificați dacă aveți un server Telnet sigurasociind un certificat cu aplicația server Telnet QIBM_QTV_TELNET_SERVER.
 3. Faceți ping la sistemul dumneavoastră gazdă pentru a verifica conexiunea dumneavoastră TCP/IP și starea rețelei.
 4. Determinați dacă serverul Telnet este pornit.
 5. Determinați dacă serverul Telnet este configurat pentru a permite conexiuni SSL.

Verificarea existenței unui ascultător SSL activ

Serverul Telnet trebuie să fie activ și pregătit pentru a recepționa tentativele de conectare. Pentru a căuta un ascultător SSL activ, urmați acești pași:

1. În interfața bazată-pe-caracter din iSeries^(TM) introduceți NETSTAT *CNN pentru a arăta cadrul cu ecranul de stări ale conexiunilor TCP/IP.
2. În coloana **Port local**, găsiți eticheta telnet- pentru telnet-ssl. Veți vedea numai telnet- deoarece câmpul nu este suficient de lung pe ecran.
 - Folosiți tasta F22 pentru a afișa complet câmpul Port local.
 - Folosiți tasta F14 pentru a vedea numerele de port. Intrarea telnet-ssl va fi portul 992.

Inițializarea SSL a eșuat dacă nu ați găsit telnet-ssl în coloana Port local. Pentru ajutor în rezolvarea problemei, verificați mesajele de diagnostică în istoricul de job QTVTELNET care rulează pe subsistemul QSYSWRK. Doar un singur job QTVTELNET va rula după o eroare de inițializare SSL.

Verificarea istoricului jobului Telnet

Când inițializarea SSL și dialogul de confirmare eșuează, serverul Telnet trimite mesajele de diagnosticare CPDBC nn către jobul QTVTELNET.(Un *dialog de confirmare (handshake)* este un schimb de mesaje la începutul unei sesiuni SSL care permite clientului să autentifice serverul folosind tehnici de cheie publică și, opțional, serverului să autentifice clientul.)

Pentru a verifica istoricul jobului pentru serverul Telnet, urmați acești pași:

1. În Navigator iSeries^(TM), expandați **serverul dumneavoastră de rețea iSeries** —> —> **Configurație TCP/IP** —> **IPv4**.
2. Faceți clic pe **Conexiuni**.
3. Faceți clic dreapta pe adresa IP a stației de lucru client care a eșuat și selectați **Joburi**. Notați numele jobului.
4. Extindeți **Management job** —> **Joburi server**.
5. Apăsați butonul drept al mouse-ului pe **QTVTELNET** din coloana Nume job.
6. Selectați **Istoric job**.
7. Căutați mesajul CPDBCnn în coloana ID mesaj.

Iată câteva lucruri care trebuie ținute minte în legătură cu joburile de server Telnet:

- Pornește un singur job QTVTELNET atunci când ascultătorul SSL nu reușește să se inițializeze.
- Joburile QTVDEVICE și QTVTELNET pornesc odată cu serverul Telnet după repornirea sistemului.
- Același număr de joburi QTVTELNET și QTVDEVICE sunt pornite atunci când serverul Telnet pornește un ascultător SSL.
- Joburile QTVTELNET sunt oprite prin comanda ENDTCPSVR *TELNET sau ENDTCP.
- Când subsistemul QSYSWRK se termină, jobul QTVDEVICE se termină.

Coduri de retur SSL

Următoarea tabelă de coduri return SSL prezintă cele mai întâlnite probleme care pot interveni în timpul unei inițializări SSL sau unui dialog de confirmare (handshake) SSL.

Înainte folosirii următoarei tabele de coduri de retur,

- Trebuie să aflați codul retur SSL în istoricul jobului QTVTELNET.
- În unele cazuri, va trebui să lucrați cu configurarea DCM pentru corectarea problemelor cu certificatele CA sau cu certificatele sistem.
- La copierea informațiilor din certificatele CA pentru clientul Telnet SSL, nu uitați să copiați liniile ce includ cuvintele BEGIN CERTIFICATE și END CERTIFICATE.

Coduri de retur obișnuite

Cod de retur	Descriere
-2	<p>Nici un certificat sistem nu este disponibil pentru procesarea SSL</p> <p>Serverul Telnet inițializează cu succes SSL, dar dialogul de confirmare (handshake) SSL eșuează. Nu există nici un panou de semnare în sistem în fereastra client SSL Telnet. Aplicația QIBM_QTV_TELNET_SERVER nu are asignată un certificat sistem.</p> <p>Vizualizați certificatul sistem și verificați dacă apare valoarea Da (Yes) în coloana Certificat asignat. Dacă valoarea este NU, creați un certificat sistem pentru aplicația QIBM_QTV_TELNET_SERVER. Consultați Gestionarea asignărilor de certificate unei aplicații pentru instrucțiuni.</p>
-4	<p>Certificatul CA sau certificatul sistem este rău</p> <p>Certificatul sistem nu este privat sau de încredere. Câmpurile Cheie privată și De încredere din certificatul de pe server sunt incorecte. Fereastra client Telnet SSL nu are nici un panou de semnare în sistem.</p> <p>Adăugați informații CA (Certificate Authority) în clientul dumneavoastră Telnet SSL. Dacă utilizați iSeriesTM Access pentru Windows^R ca și client Telnet SSL, vedeți Gestionare certificatele Internet public pentru sesiunile de comunicare SSL. Altfel, consultați Obținerea unei copii a certificatului CA privat pentru instrucțiuni.</p>
-16	<p>Sistemul pereche nu este recunoscut</p> <p>Această problemă este cea mai frecventă problemă atunci când un client Telnet SSL încearcă pentru prima oară să stabilească o sesiune SSL. Fereastra client Telnet SSL nu are nici un panou de semnare în sistem.</p> <p>Adăugați informații de certificat CA (Certificate Authority) clientului dumneavoastră Telnet SSL.</p>

Cod de retur	Descriere
-18	<p>Certificatul sistem este auto-semnat și serverul îl folosește drept certificat CA Certificatul sistem asignat aplicației QIBM_QTV_TELNET_SERVER trebuie să fie de încredere, semnat de o autoritate de certificate și folosit în perioada de validitate. Trebuie să creați un certificat CA și să îl asociați cu certificatul sistem. Serverul Telnet nu inițializează SSL dacă certificatul sistem este incorect.</p> <p>Creați un certificat CA și asociați-l cu certificatul sistem. Pentru instrucțiuni, consultați Crearea și operarea unui CA (Certificate Authority) local.</p>
-23	<p>Certificatul sistem nu este înregistrat de o autoritate de certificare de încredere Certificatul sistem asignat aplicației QIBM_QTV_TELNET_SERVER trebuie să fie de încredere, semnat de o autoritate de certificate și folosit în perioada de validitate.</p> <p>Modificați certificat CA la De încredere. Pentru instrucțiuni, consultați Gestionarea aplicațiilor în DCM.</p>
-24	<p>Perioada de timp validă a certificatului CA a expirat Utilizați un certificat expirat. Fereastra client Telnet SSL nu are nici un panou de semnare în sistem.</p> <p>Reînoiți certificatul CA care a fost utilizat pentru a construi certificatul sistem.</p>
-93	<p>SSL nu este disponibil pentru folosire Clienții Telnet SSL nu se pot conecta la o gazdă deoarece nu există nici un ascultător SSL activ.</p> <p>Instalați necesarul software care să sigure suportul pentru Telnet SSL și pentru administrarea certificatelor. Pentru instrucțiuni, consultați Verificarea stării sistemului.</p>

Alte coduri de retur SSL

Pentru codurile return SSL din acest tabel, folosiți Administrarea de certificate digitale pentru a verifica dacă certificatele digitale respectă necesitățile:

- Certificatul CA este valid și nu a expirat.
- Aplicația de server Telnet QIBM_QTV_TELNET_SERVER are valoarea Yes în coloana Certificate asignate.
- O autoritate de certificare semnează certificatul sistem.
- Certificatul sistem este de încredere.
- Certificatul sistem este folosit în cadrul de timp declarat în certificat.

Cod de retur	Descriere
-1	Nu sunt disponibile sau specificate cifruri
-6	OS/400 ^(R) nu suportă tipul de certificare
-10	A intervenit o eroare în procesarea SSL. În istoricul jobului, verificați mesajul CPExxxx unde xxxx este valoarea errno pentru socket.
-11	SSL a primit un mesaj formatat greșit

Cod de retur	Descriere
-12	A fost primit un cod de autentificare mesaj greșit
-13	Operația nu este suportată de SSL
-14	Semnătura certificatului nu este validă
-15	Certificatul este greșit
-17	S-a interzis permisiunea de acces la obiect
-20	Imposibil de alocat spațiu de stocare necesar procesării SSL
-21	SSL a detectat o stare greșită în sesiunea SSL
-22	Socket-ul folosit de către conexiunea SSL a fost închis
-25	Data din certificat are un format greșit
-26	Lungimea cheii este necorespunzătoare pentru export
-90	Nu este un fișier inel de chei
-91	Parola din baza de date de chei a expirat
-92	Certificatul este nevalid sau a fost rejectat de programul de ieșire
-94	SSL_Init() nu a fost invocat anterior pentru job
-95	Nu există inel de chei pentru inițializare SSL
-96	SSL nu este activat
-97	Secvența de cifru specificată nu este validă
-98	Sesiunea SSL s-a încheiat
-99	A intervenit o eroare necunoscută sau neașteptată în timpul procesării SSL
-1010	Criptarea dublă nu este permisă la utilizarea AC2 și IP-SEC

leșiri ale programului serviciu TRCTCPAPP

Pentru comanda de urmărire a aplicațiilor TCP/IP (TRCTCPAPP), listarea componentelor VTM de urmărire scoate în evidență un fișier spool, numit VTMTRACE cu câmpul de date al utilizatorului setat TELNET . Sistemul pune acest fișier în coada implicită de ieșire a profilului care rulează apelul TRCTCPAPP *TELNET *OFF. În același timp, toate 'cutiile negre' pentru joburile server sunt depozitate în fișierele spool numite QTOCTTRC cu datele utilizator setate laQTVnnnnnn.

Iată aici un exemplu a ceea ce vedeți în istoricul jobului interactiv când apăsați TRCTCPAPP *OFF

```

+-----+
| Command Entry                               SYSNAM03 |
| Request level: 1                             |
| All previous commands and messages:         |
| > trctcpapp *telnet *off                    |
| Spooled printer file 1 opened for output.   |
| Trace data for application TELNET formatted: Spooled VTMTRACE user data 'TELNET' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017231' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017230' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017229' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017232' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017233' |
| Trace data for application TELNET formatted: Spooled QTOCTTRC user data 'TV017234' |
|                                         More... |
| Type command, press Enter.                 |
| ==>                                         |
| F3=ExitF4=Prompt F9=Retrieve F10=Exclude detailed messages |
| F11=Display full F12=Cancel F13=Information Assistant F24=More keys |
+-----+

```

Iată aici un exemplu a ceea ce vedeți în coada implicită de ieșire a dumneavoastră.

```

-----+-----
                Work with All Spooled Files
Type options, press Enter.
1=Send 2=Change  3=Hold    4=Delete 5=Display    6=Release  7=Messages
8=Attributes      9=Work with printing status

Opt File          User          Queue          Device or      Sts  Total  Page
VTMTRACE         JEFF          JEFFSOUTQ     TELNET         HLD  46     1
QTOCTTRC         JEFF          JEFFSOUTQ     TV017231       HLD  4     1
QTOCTTRC         JEFF          JEFFSOUTQ     TV017231       HLD  2     1
QTOCTTRC         JEFF          JEFFSOUTQ     TV017231       HLD  2     1
QTOCTTRC         JEFF          JEFFSOUTQ     TV017231       HLD  2     1
QTOCTTRC         JEFF          JEFFSOUTQ     TV017231       HLD  2     1

Parameters for options 1, 2, 3 or command
==>
F3=Exit  F10=View 4  F11=View 2  F12=Cancel  F22=Printers  F24=More keys
-----+-----

```

Este creat doar un fișier cu numele VTMTRACE. Dacă modul Telnet SSL este operațional pe server, s-ar putea să aveți unul sau mai multe fișiere QTOCTTRC.

Iată un exemplu de fișier QTOCTTRC. Acest fișier spool este un job de server Telnet (QTVTELNET), opusul unui job QTVDEVICE.

```

-----+-----
                Display Spooled File
File . . . . . : TV017231          Page/Line  1/6
Control . . . . . Columns          1 - 78
Find . . . . .
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
TRCTCPAPP Attributes
  Application.....: Telnet Server
  Buffer size (KB).....: 0
    (Default of 0 means 16MB buffer)
  Trace full action.....: *WRAP
  Job id.....: 017231/QTCP /QTVTELNET
  Start date/time.....: Fri Dec 11 13:50:33 1998
  End date/time.....: Fri Dec 11 14:08:34 1998
  Trace buffer wrapped.....: No
Telnet Server Attributes
  AutoStart server.....: 'Y'
  Number servers.....: 2
  Session keep alive timeout..: 0
  Default NVT type.....: >*VT100<
  Outgoing EBCDIC/ASCII table.: >*CCSID <
  Incoming ASCII/EBCDIC table.: >*CCSID <
  Coded character set id.....: 84542
  Attributes version id.....: >V4R4M0 <
Trace common buffer structure:
80000000 00000000 161A8753 14001074 | .....g..... | Byte 16
80000000 00000000 161A8753 14FFFFE4 | .....g...U | Byte 48
80000000 00000000 161A8753 14005820 | .....g..... | Byte 80
00FFF000 00000084 F0F1F7F2 F3F1D8E3 | ..0....d017231QT | Byte 112
C3D74040 40404040 D8E3E5E3 C5D3D5C5 | CP QTVTELNE| | Byte 144
E340C699 8940C485 8340F1F1 40F1F37A | T Fri Dec 11 13: | Byte 176
F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017 | Byte 208
F2F3F140 |231 | | Byte 228
Flight Records:
qtvtnet: Job: QTVTELNET/QTCP/017231
(C) Copyright IBM Corporation, 1999
Licensed Material - Program Property of IBM.
-----+-----

```



```

Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Rel: V4R4M0 Vers: V4R4M0 PTR: P3684767
qvtvtnet: Program QVTVELNET dated 04 December 1998 running
qvtvtnet: Source file: qvtvtnet.plc
qvtvtnet: Last modified: Wed Dec 9 11:57:40 1998
qvtvtnet: Last compiled at 12:00:10 on Dec 9 1998
qvtvtnet: Arguments passed: 1
qvtvtnet: Time Started: Fri Dec 11 13:50:34 1998
qvtvtnet: sigaction() for SIGUSR1 is EndClientSession()
qvtvtnet: Set Telnet Server job identity for OpNav
qvtvtnet: Need to setup SSL_Init_Application()
qvtvtnet: SSL_Init_Application() successful
qvtvtnet: Find Telnet Server control block
qvtvtnet: Lock Telnet Server control block
qvtvtnet: Open driver to stream
qvtvtnet: First Telnet Server Job...

```

```
F3=Exit F12=Cancel F19=Left F20=Right F24=More keys
```

Iată un exemplu de alt fișier QTOCTTRC. Acesta este un fișier spool Device Manager, opusul jobului server QVTVELNET:

```

-----+-----
Display Spooled File
File . . . . . : TV017230 Page/Line 1/6
Control . . . . . Columns 1 - 78
Find . . . . .
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
TRCTCPAPP Attributes
  Application.....: Telnet Server
  Buffer size (KB).....: 0
    (Default of 0 means 16MB buffer)
  Trace full action.....: *WRAP
  Job id.....: 017230/QTCP /QTVDEVICE
  Start date/time.....: Fri Dec 11 13:50:33 1998
  End date/time.....: Fri Dec 11 14:08:39 1998
  Trace buffer wrapped.....: No
Telnet Server Attributes
  AutoStart server.....: Y
  Number servers.....: 2
  Session keep alive timeout.: 0
  Default NVT type.....: >*VT100<
  Outgoing EBCDIC/ASCII table.: >*CCSID <
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...
  Incoming ASCII/EBCDIC table.: >*CCSID <
  Coded character set id.....: 84542
  Attributes version id.....: >V4R4M0 <
Trace_common buffer structure:
  80000000 00000000 3DA86C25 5F001074 | .....y... | Byte 16
  80000000 00000000 3DA86C25 5F001074 | .....y... | Byte 16
  80000000 00000000 3DA86C25 5F002F64 | .....y... | Byte 80
  00FFF000 00000084 F0F1F7F2 F3F0D8E3 | ..0....d017230QT | Byte 112
  C3D74040 40404040 D8E3E5C4 C5E5C9C3 | CP QTVDEVIC | Byte 144
  C540C699 8940C485 8340F1F1 40F1F37A | E Fri Dec 11 13: | Byte 176
  F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017 | Byte 208
  F2F3F040 |230 | Byte 228
Flight Records:
qvtvtnesh: >>>> entry
(C) Copyright IBM Corporation, 1999.
Licensed Material - Program Property of IBM.
Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Release: V4R4M0 Version: V4R4M0 PTR: P3684767
qvtvtnesh: Program QVTVNCSSH dated 04 December 1998 running
qvtvtnesh: iActiveLogLevel: 0
qvtvtnesh: Source file: qvtvtnesh.c

```

```

qvtvncsh: Last modified: Wed Dec 9 11:48:33 1998
qvtvncsh: Last compiled at 11:59:42 on Dec 9 1998
qvtvncsh: SignalHandler() registered with signal()
qvtvncsh: Arguments passed: 4
qvtvncsh: argc: 4
qvtvncsh: argv[0]: >QSYS/QTVTNCSSH<
qvtvncsh: argv[1]: >>
qvtvncsh: argv[2]: >1p<
qvtvncsh: argv[3]: >s<
SignalHandler: >>>> entry
SignalHandler: Caught signal SIGSEGV

F3=Exit    F12=Cancel  F19=Left    F20=Right   F24=More keys

```

Materialele necesare pentru raportarea problemelor Telnet

Problemele raportate la IBM^(R) pot include una sau mai multe din următoarele așa cum au fost determinate de reprezentantul dumneavoastră de service:

- Istoricele jobului server Telnet:
 - Istoric job QTVTELNET
 - Istoric job QTVDEVICE
- Cîteva detalii despre scenariul problemei. De exemplu:
 - Tipul calculatorului gazdă la distanță pe care îl foloseați să faceți Telnet către sau de la, cum ar fi un server iSeries^(TM), zSeries^(TM) sau pSeries^(TM). Aceasta este în mod particular folositor dacă folosiți funcții Telnet cascade.
 - Tipul clientului ce intenționează să se conecteze la un server Telnet, cum este IBM^(R) Personal Communications și iSeries Access pentru Windows^(R).
- Istoricul jobului interactiv care rulează clientul Telnet (când clientul Telnet este sub investigare).
- Ieșirea jobului de urmărire (TRCJOB) a jobului interactiv eșuat (în special important dacă rulează client Telnet).

Notă:

Folosiți TRCJOB *ON pentru a începe această urmărire.
Rezultatul este un fișier spool QPSRVTRC în jobul interactiv.

- O urmărire comunicații pentru eșec, formatat și pentru ASCII și pentru EBCDIC, care conține numai date TCP/IP. Reprezentantul de service vă poate îndruma să includeți și mesaje broadcast în această urmărire. În plus, va trebui să filtrați această urmărire pe o adresă IP specifică dacă aveți o cantitate mare de trafic pe rețeaua dumneavoastră și știți adresa IP a clientului eșuat.
- Orice istorice pentru codul intern licențiat (LIC) cu codul major 0700 și codul minor 005x din timpul eșecului. În plus, pot să existe istorice de LIC informaționale pentru cod major 0701 și cod minor 005x care pot să fie de ajutor, dar nu sunt neapărat critice.
- O urmărire a componentei Virtual Terminal Manager (VTM) LIC. Puteți aduna această urmărire folosind comanda TRCTCPAPP a aplicației TCP/IP sau prin comanda de pornire a uneltelor de service ale sistemului (STRSST). Pentru toate detalii despre folosirea comenzii TRCTCPAPP, consultați Descrierea comenzii TRCTCPAPP.

Când rulează urmărirea VTM LIC se simte asupra performanței. Cîteva exemple de folosire a acestei comenzi sunt:

- Pentru a urmări toate activitățile VTM:
TRCTCPAPP APP(*TELNET) SET(*ON)
- Pentru a urmări activitatea pe un dispozitiv anume, când cunoașteți numele dispozitivului:
TRCTCPAPP APP(*TELNET) SET(*ON) DEVD(device name)
- Pentru a urmări activitatea pe un dispozitiv anume, când cunoașteți adresa clientului:
TRCTCPAPP APP(*TELNET) SET(*ON) RMTNETADR(*INET'www.xxx.yyy.zzz')
- Pentru a opri urmărirea și a genera un fișier spool de ieșire:
TRCTCPAPP APP(*TELNET) SET(*OFF)

Notă:

Ar trebui să primiți detalii specifice despre ce parametri să folosiți pentru problema dumneavoastră de la reprezentantul de service înainte de a lansa această comandă. Aceasta asigură strângerea de informații corecte despre problema dumneavoastră.

Informații de diagnoză generate automat

La apariția anumitor erori la serverul Telnet s-ar putea să fie produse niște informații de diagnosticare generate automat. Există situații când reprezentantul de service va cere aceste informații de diagnosticare pentru analiza corespunzătoare a problemelor serverului Telnet.

Dacă orice job Telnet sau Device Manager eșuează cu o eroare FFDC (first failure data capture), veți vedea fișierele spool cu WRKSPLF, profil QTCP. Când un job eșuează cu o eroare FFDC, fiecare job eșuat va avea automat două dump-uri. Unu este provocat de apelul DSPJOB *PRINT și DSPJOBLOG *PRINT îl provoacă pe celălalt. În acest fel, veți obține în dump atât istoricul jobului, cât și atributele de rulare ale jobului și veți avea ieșirea de la grupul de date al utilizatorului împreună cu numărul de identificare al jobului. Apoi, puteți să o comparați cu ieșirea oricărei componente VTM de urmărire.

Veți vedea un total de patru fișiere spool; două pentru jobul QTVTELNET și două pentru jobul QTVDEVICE. Când sistemul întâlnește o eroare FFDC, aceste fișiere se generează automat. Pentru un exemplu, vedeți figura de mai jos:

Figura 1. Ecranul Gestionarea tuturor fișierelor spool

```

+-----+
|                Work with All Spooled Files                |
|Type options, press Enter.                                |
| 1=Send 2=Change  3=Hold   4=Delete  5=Display  6=Release  7=Messages |
| 8=Attributes      9=Work with printing status            |
|Opt  File          User      Queue      Device or      Sts  Pages |
|      QPJOBLOG     QTCP      QEZJOBLOG  TV016868    HLD  4   |
|      QPDSPJOB     QTCP      QPRINT     TV016868    HLD  7   |
|      QPJOBLOG     QTCP      QEZJOBLOG  TV016955    HLD  3   |
|      QPDSPJOB     QTCP      QPRINT     TV016955    HLD  7   |
|      QPJOBLOG     QTCP      QEZJOBLOG  TV017231    HLD  3   |
|      QPJOBLOG     QTCP      QEZJOBLOG  TV017232    HLD  3   |
|      QPDSPJOB     QTCP      QPRINT     TV017232    HLD  7   |
|      QPDSPJOB     QTCP      QPRINT     TV017231    HLD  7   |
|Parameters for options 1, 2, 3 or command                |
|===>                                                     |
|F3=Exit   F10=View 4  F11=View 2  F12=Cancel  F22=Printers  F24=More keys |
+-----+

```

Informații înrudite despre Telnet

Dacă aveți nevoie de informații suplimentare despre Telnet, consultați următoarele surse:

V4 TCP/IP for AS/400^(R): More Cool Things Than Ever



(aproximativ 700 pagini)

Furnizează informații extinse despre TCP/IP, incluzând scenarii exemplu care demonstrează soluții comune cu exemple de configurații

Situl web Internet Engineering Task Force (IETF)



Citiți RFC (Request for Comments), cum ar fi RFC 2877 5250 Telnet Enhancements



Internet Assigned Numbers Authority (IANA)



Găsiți informații despre asignările numerelor de port uzuale

Anexa. Observații

Aceste informații au fost elaborate pentru produse și servicii oferite în S.U.A.

Este posibil ca IBM^(R) să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Consultați reprezentantul dumneavoastră local IBM pentru informații referitoare la produsele și serviciile curent disponibile în domeniul dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcțional și care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea și verificarea modului în care funcționează un produs, program sau serviciu non-IBM ține de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licență cu privire la aceste patente. Puteți trimite întrebări cu privire la licențe, în scris, la:

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

Pentru întrebări privind licența pentru informațiile DBCS (double-byte character set), contactați departamentul de proprietate intelectuală al IBM-ului din țara dumneavoastră sau trimiteți întrebările în scris la:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor țări unde asemenea prevederi nu sunt în concordanță cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPRESĂ SAU IMPLICITĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele sate nu acceptă declinarea responsabilității de exprimare sau garanțiile implicate în tranzacții sigure, de aceea acest articol nu se aplică pentru dumneavoastră.

Aceste informații pot include inexactități tehnice sau erori tipografice. Se efectuează modificări periodice la informațiile incluse aici; aceste modificări vor fi încorporate în noile ediții ale publicației. IBM poate aduce îmbunătățiri și/sau modificări produsului (produselor) și/sau programului (programelor) descrise în această publicație în orice moment fără vreun avertisment.

Referirile din aceste informații la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezența lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informațiile pe care le furnizați, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație pentru dumneavoastră.

Posesorii de licențe pentru acest program care doresc să aibă informații despre el în scopul de a permite: (I) schimbul de informații între programe create independent și alte programe (inclusiv acesta) și (II) utilizarea mutuală a informațiilor care au fost schimbate, vor contacta:

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

Aceste informații pot fi disponibile, să fie supuse unor termeni și condiții, inclusiv în unele cazuri, plata unor taxe.

Programul cu licență descris în aceste informații și toate materialele licențiate disponibile pentru el sunt furnizate de către IBM conform termenilor IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice acord echivalent între noi.

Aceste informații conțin exemple de date și rapoarte utilizate în operațiile din activitatea zilnică. Pentru a le arăta cât se poate de veridice, exemplele includ nume de indivizi, companii, brand-uri și produse. Toate aceste nume sunt fictive și orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidență.

LICENȚĂ - COPYRIGHT:

Aceste informații conțin exemple de programe de aplicații în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteți copia, modifica și distribui aceste exemple de programe sub orice formă fără să plătiți ceva IBM-ului, în scopul dezvoltării, folosirii, promovării și distribuirii programelor de aplicații conform cu interfața de programare aplicații pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate temeinic pentru toate condițiile. De aceea, IBM nu poate garanta sau sugera fiabilitatea, suportul pentru service sau funcționarea acestor programe.

EXCEPTÂND GARANȚIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ȘI FURNIZORII SĂI NU ACORDĂ NICI O GARANȚIE SAU CONDIȚIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE SAU CONDIȚIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAI DACĂ AU FOST INFORMAȚI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICIILE ECONOMICE DE CONSECINȚĂ; SAU
3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICIILE, REPUTAȚIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICȚII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.

Dacă vedeți aceste informații folosind o copie electronică, fotografiile și ilustrațiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale deținute de International Business Machines Corporation în Statele Unite, în alte țări sau ambele:

Application System/400

AS/400

e (logo)

IBM

iSeries

Operating System/400
OS/400
400

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci înregistrate deținute de Microsoft Corporation în Statele Unite, în alte țări sau ambele.

Java și toate mărcile comerciale bazate pe Java sunt mărci comerciale deținute de Sun Microsystems, Inc. în Statele Unite, în alte țări sau ambele.

Alte nume de companii, de produse și de servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termeni și condiții pentru descărcarea și tipărirea informațiilor

Permișiunile pentru folosirea informațiilor pe care le-ați selectat pentru descărcare sunt acordate în următorii termeni și condiții și cu indicarea acceptării lor de către dumneavoastră.

Uz personal: Puteți reproduce aceste informații pentru uzul dumneavoastră personal și necomercial cu condiția ca toate notele de proprietate să fie păstrate. Nu puteți distribui, afișa sau face lucrări derivate din aceste informații sau orice alte porțiuni din ele, fără acordul explicit al IBM.

Uz comercial: Puteți reproduce, distribui și afișa aceste informații doar în întreprinderea dumneavoastră cu condiția ca toate notele de proprietate să fie păstrate. Nu puteți face lucrări derivate ale acestor informații, sau să reproduceți, să distribuiți sau să afișați aceste informații sau orice alte porțiuni din ele în afara întreprinderii dumneavoastră, fără acordul explicit al IBM.

Cu excepția acestei permisiuni explicite, nici o altă permisiune, licență sau drepturi nu sunt acordate, fie explicite sau implicite, pentru informații sau alte date, software sau alte proprietăți intelectuale conținute în acestea.

IBM își păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreția sa, dacă folosirea Publicațiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau să re-exporta aceste informații, decât cu stricta respectare a legilor și a regulilor în vigoare, incluzând toate legile și regulile de export ale Statelor Unite. IBM NU ACORDĂ NICI O GARANȚIE PENTRU CONȚINUTUL ACESTOR INFORMAȚII. PUBLICAȚIILE SUNT FURNIZATE "AȘA CUM SUNT" ȘI FĂRĂ GARANȚIE DE NICI UN FEL, FIE EXPLICITĂ, FIE IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE SUBÎNȚELESE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Toate materialele au copyright IBM Corporation.

Prin descărcarea sau tipărirea de informații de pe acest sit, v-ați dat acordul pentru acești termeni și aceste condiții.

Informații de declinare a responsabilității pentru cod

IBM^(R) vă acordă o licență de copyright neexclusivă pentru a folosi toate exemplele de cod de programare din care puteți genera funcții similare adaptate nevoilor dumneavoastră specifice.

EXCEPTÂND GARANȚIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ȘI FURNIZORII SĂI NU ACORDĂ NICI O GARANȚIE SAU CONDIȚIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE SAU CONDIȚIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAI DACĂ AU FOST INFORMAȚI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICIILE ECONOMICE DE CONSECINȚĂ; SAU
3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAȚIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICȚII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.



Tipărit în S.U.A.