



System i  
Lucrul în rețea Telnet

*Versiunea 6 Ediția 1*







System i  
Lucrul în rețea Telnet

*Versiunea 6 Ediția 1*

**Notă**

Înainte de a utiliza aceste informații și produsul pe care îl suportă, citiți informațiile din “Observații”, la pagina 99.

Această ediție se aplică versiunii 6, ediția 1, modificare 0 a IBM i5/OS (număr de produs 5761-SS1) și tuturor edițiilor și modificărilor următoare până când nu se indică altfel în ediții noi. Această versiune nu rulează pe toate modelele RISC și nici pe modelele CISC.

© Copyright International Business Machines Corporation 1998, 2008. Toate drepturile rezervate.

# Cuprins

<b>Telnet.</b>	<b>1</b>	INIT0100: Formatul informațiilor de descriere utilizator	42
Fișier PDF pentru Telnet	1	INIT0100: Formatul informațiilor de descriere a dispozitivului	43
Scenarii Telnet	1	INIT0100: Formatul informației de descriere a conexiunii	45
Scenariu Telnet: Configurarea serverului Telnet	1	Program de ieșire pentru terminare dispozitiv	46
Scenariu Telnet: Sesiuni Telnet în cascadă	3	Exemple: Programe de ieșire Telnet	47
Scenarii de procesare a cererilor sistem	5	Gestionarea clientului Telnet	48
Folosirea unui job de grup	6	Controlarea funcțiilor server Telnet de la client	48
Scenariu Telnet: Securizare Telnet cu SSL	8	Sesiunile client Telnet 5250	49
Detalii de configurare pentru securizarea Telnet cu SSL	10	Pornirea unei sesiuni client Telnet	49
Planificarea pentru serverul Telnet	14	Sesiunile client Telnet 3270	51
Descrierile de dispozitiv virtual	14	Pornirea unei sesiuni client 3270 Telnet	51
Securitatea Telnet	15	Considerente pentru 3270 tot-ecranul	52
Împiedicare acces Telnet	15	Folosirea unei stații de afișare	54
Controlare acces Telnet	16	Maparea tastaturii 3270 pentru serverele Telnet	55
Configurarea serverului Telnet	19	Sesiuni client Telnet VTxxx	57
Pornirea serverului Telnet	19	Pornirea unei sesiuni client VTxxx	57
Setarea numărului de dispozitive virtuale	20	Considerente tot-ecranul VTxxx	58
Configurare automată a dispozitivelor virtuale	20	Opțiuni de emulare VTxxx	62
Crearea propriilor dumneavoastră dispozitive virtuale	21	Valori cheie VTxxx	63
Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare	22	Suport limbă națională VTxxx	68
Setarea parametrului de ținare în viață a sesiunii	23	Mod național VTxxx	69
Asignare dispozitive la subsisteme	23	Tastatura numerică	71
Activarea subsistemului QSYSWRK	24	Editarea blocului de taste (keypad)	73
Crearea de profiluri utilizatori	24	Valori de taste VTxxx prin funcție 5250	75
Tipuri de emulare suportate i5/OS	24	Moduri de operare ale stațiilor de lucru VT220	78
Configurarea serverului Telnet pentru modul tot-ecranul 5250	25	Tastele funcționale din linia de sus la VT220	78
Configurare server Telnet pentru modul tot-ecranul 3270	25	Cuvintele cheie pentru caracterele de control VT100 și VT220	79
Tipurile de terminal 3270 suportate	27	Stabilirea unei sesiuni cascade Telnet	80
Configurare server Telnet pentru mod tot-ecranul VTxxx	27	Mutarea între sesiuni cascade Telnet	81
Securizare Telnet cu SSL	30	Terminarea unei sesiuni client Telnet	82
Configurarea SSL pe serverul Telnet	30	Depanarea problemelor Telnet	82
Înlăturare restricții de port	30	Determinarea problemelor cu Telnet	82
Asignarea unui certificat la serverul Telnet	31	A face ping serverului dumneavoastră gazdă	85
Activare autentificare client pentru serverul Telnet	32	Tipuri de depanare emulare	85
Activare SSL în serverul Telnet	34	Depanarea serverului dumneavoastră SSL Telnet	88
Inițializare și dialog de confirmare (handshake) SSL	35	Verificarea stării sistemului	88
Gestionarea serverului Telnet	36	Căutarea unui ascultător SSL activ	89
Configurare sesiuni Telnet de imprimantă	36	Verificarea istoricului de joburi Telnet	89
Necesitățile pentru sesiunile de imprimantă Telnet	37	Coduri de retur SSL	90
Suport tipărire pentru server Telnet la clientul Telnet System i Access pentru Windows	37	Ieșiri ale programului serviciu TRCTCPAPP	92
Oprirea sesiunii server Telnet	38	Materialele necesare pentru raportarea problemelor Telnet	95
Terminare joburi manager dispozitiv	38	Informații de diagnoză generate automat	96
Folosirea programelor cu punct de ieșire Telnet	39	Informațiile înrudite pentru Telnet	97
Program de ieșire inițializare dispozitiv	40	<b>Anexa. Observații</b>	<b>99</b>
Formatul punctului de ieșire Telnet INIT0100: Grupul de parametri necesari	41	Informații despre interfața de programare	100
		Mărci comerciale	100
		Termenii și condițiile	101



---

## Telnet

Telnet este un protocol care vă permite să vă logați și să folosiți un calculator de la distanță ca și cum ați fi conectați direct la acesta din interiorul rețelei locale.

Sistemul (de obicei un PC) pe care îl aveți fizic în față este clientul Telnet. Serverul Telnet este calculatorul de la distanță la care este atașat clientul. TCP/IP 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, tipul preferat este emularea 5250. Telnet suportă de asemenea tipurile 3270 și VTxxx de stații de lucru cât și
- | moduri de suport imprimantă RFC (Request for Comments) 4777 (TN5250E). Acest subiect introduce Telnet și oferă
- | informații despre administrarea Telnet în sistemul dumneavoastră.

**Notă:** Prin utilizarea exemplurilor de coduri, sunteți de acord cu termenii din “Informații referitoare la licența de cod și declinarea responsabilității” la pagina 97.

---

## Fișier PDF pentru Telnet

Puteți vizualiza și tipări un fișier PDF cu aceste informații.

Pentru vizualizarea sau descărcarea versiunii PDF a acestui document, selectați Telnet (aproximativ 1300 KB).


### Salvarea fișierelor PDF

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

1. Faceți clic dreapta pe legătura PDF din browser-ul dumneavoastră.
2. Faceți clic pe opțiunea care salvează PDF-ul în plan local.
3. Navigați la directorul în care doriți să salvați PDF-ul.
4. Faceți clic pe **Save**.

### Descărcarea Adobe Reader

Aveți nevoie ca Adobe Reader să fie instalat în sistemul dumneavoastră pentru a vizualiza sau tipări aceste PDF-uri.

Puteți descărca o copie gratuită de pe situl Web Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

#### Referințe înrudite

“Informațiile înrudite pentru Telnet” la pagina 97

Publicațiile IBM Redbooks și siturile web conțin informații înrudite cu colecția de subiecte Telnet. Puteți vedea sau tipări oricare din fișierele PDF.

---

## Scenarii Telnet

Scenariile oferă exemple de utilizare Telnet pentru a introduce concepte de bază și operații de configurare.

### Scenariu Telnet: Configurarea serverului Telnet

Scenariul descrie cum un administrator configurează un server Telnet, inclusiv obiectivele, cerințele preliminare și presupunerile și detaliile de configurare.

## Situația

Ken Harrison este administratorul unui nou mediu i5/OS pentru compania fictivă Culver Pharmaceuticals.

## Obiectivele

El trebuie să configureze serverul Telnet pentru a îndeplini următoarele specificații:

- Permitearea de creare automată de până la 100 de dispozitive virtuale.
- Afișarea permanentă a ferestrei de semnare.
- Restricționarea utilizatorilor privilegiați la anumite dispozitive.
- Limitarea fiecărui utilizator la o sesiune de dispozitiv.

## Cerințele preliminare și supozițiile

Acest scenariu face următoarele supoziții:

- Culver Pharmaceuticals rulează sistemul de operare i5/OS.
- TCP/IP este configurat.
- Ken are autorizare \*IOSYSCFG.

## Detalii de configurare

Puteți urmări pași configurării serverului dumneavoastră Telnet în Navigator System i.

1. Porniți serverul Telnet:
  - a. În Navigator System i, selectați **sistemul dumneavoastră** → **Rețea** → **Servere** → **TCP/IP**.
  - b. În panoul din dreapta, în coloana Nume server, localizați **Telnet**.
  - c. Confirmați că apare **Pornit** în coloana Stare.
  - d. Dacă serverul nu rulează, faceți clic dreapta pe **Telnet** și apoi clic pe **Pornire**.
2. Setări numărul dispozitivelor virtuale:
  - a. Selectați **sistemul dumneavoastră** → **Configurare și Service** → **Valori de sistem**.
  - b. În panoul din dreapta, faceți clic dreapta pe **Dispozitive** și selectați **Proprietăți**.
  - c. În pagina Valori sistem dispozitive, activați **Dispozitive pass-through și TELNET** și setați **Numărul maxim de dispozitive** la 100.
3. Configurare proprietăți server Telnet:
  - a. Selectați **sistemul dumneavoastră** → **Rețea** → **Servere** → **TCP/IP**.
  - b. În panoul din dreapta, faceți clic dreapta pe **Telnet** și selectați **Proprietăți**.

Tabela 1. Setările proprietăților Telnet

Faceți clic pe această fișă...	Și ...
Semnare sistem	Selecția: <ul style="list-style-type: none"><li>• Restricționarea utilizatorilor privilegiați la anumite dispozitive.</li><li>• Limitarea fiecărui utilizator la o sesiune de dispozitiv.</li></ul>
Semnare la distanță	Specificați numărul permis de încercări de semnare și acțiunea care să fie efectuată dacă se atinge numărul maxim de încercări de semnare.
La distanță	Selecția opțiunea <b>Afișarea întotdeauna a semnării</b> pentru <b>Utilizare Telnet pentru semnare la distanță</b> .



Tabela 1. Setările proprietăților Telnet (continuare)

Faceți clic pe această fișă...	Și ...
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 și joburilor interactive din sistemul dumneavoastră, nu doar Telnet.

4. Alocarea dispozitivelor la subsisteme.

La interfața în mod text, introduceți:

ADDWSE SBS(D(QINTER) WRKSTNTYPE(\*ALL)

5. Activați subsistemul QSYSWRK:

Verificarea stării subsistemului QSYSWRK:

a. În interfața pe bază de caractere, tastați **WRKSBS** (Work with Subsystems - lucru cu subsisteme).

b. Verificați că sunt afișate următoarele sisteme:

- QSYSWRK
- QINTER
- QSPL

Dacă subsistemul QSYSWRK nu este activ, efectuați următorii pași:

a. În interfața pe bază de caractere, tastați **STRSBS** (Start Subsystem - pornire subsistem).

b. Tastați **QSYSWRK** pentru descrierea subsistemului și **QSYS** pentru Bibliotecă, apoi apăsați **Enter**.

c. Repetați pentru Nume subsistem **QINTER** cu Biblioteca **QSYS** și pentru Nume subsistem **QSPL** cu Biblioteca **QSYS**.

6. Creați profiluri utilizator Telnet:

a. Porniți Navigator System i și expandați **sistemul dumneavoastră**.

b. Faceți clic dreapta pe **Utilizatori și grupuri** și selectați **Utilizator nou**.

c. Introduceți numele utilizatorului, descrierea și parola.

d. Pentru a specifica descrierea unui job, faceți clic pe **Joburi** și introduceți descrierea jobului.

e. Faceți clic pe **OK**.

7. Verificați dacă Telnet funcționează.

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

**Concepte înrudite**

“Tipuri de emulare suportate i5/OS” la pagina 24

Emularea preferată pentru sistem este emularea 5250. Totuși, sistemul suportă de asemenea emulare 3270 și VTxxx.

**Operații înrudite**

“Configurarea serverului Telnet” la pagina 19

Subiectul conține informații despre cum să vă configurați serverul dumneavoastră Telnet pentru diverse tipuri de emulare.

## Scenariu Telnet: Sesiuni Telnet în cascadă

Scenariul demonstrează abilitatea de a porni sesiuni Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați fost conectat, puteți comuta între sisteme prin folosirea valori de cerere sistem.

În acest scenariu, utilizatorul stabilește sesiuni Telnet cu mai multe servere. Aceasta este cunoscută ca *sesiuni Telnet în cascadă*. Prin folosirea acestei metode, veți putea să:

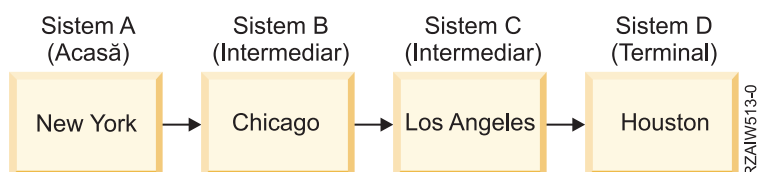
- Stabiliți sesiunii Telnet între biroul de acasă și Chicago.
- Se conecteze la servere Telnet suplimentare fără a termina sesiunea inițială.
- Comute între sesiuni pentru a se întoarce la un job pe sistemul din New York.

## Situația

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. După ce Janice a stabilit o sesiune client cu serverul Telnet din Chicago, ea își dă seama că are nevoie să lucreze cu unele fișiere de la biroul din Los Angeles.

## Obiectivele

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.



Această figură descrie conexiunile pe care le face Janice. Sistemul de la care pornește din New York este numit sistemul gazdă. 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.

## Cerințele preliminare și supozițiile

Acest scenariu face următoarele supoziții:

- Server Telnet rulează pe toate sistemele.
- Janice are o semnătură pe toate sistemele.
- Toate sistemele rulează i5/OS V4R5, sau mai nou.

## Detalii de configurare

Janice finalizează următorii pași pentru a se conecta la serverele Telnet:

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

După ce s-a conectat la sistemul din Houston, ea dorește să efectueze o operație pe sistemul (principal) 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.

După terminarea lucrului pe sistemul din New York, ea se poate întoarce la sistemul din Houston prin parcurgerea operațiilor următoare:

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. Această comandă oprește sesiunea curentă și o întoarce la afișajul de semnare al sistemului gazdă.

### Referințe înrudite

“Stabilirea unei sesiuni cascadeate Telnet” la pagina 80

Puteți stabili o altă sesiune Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați stabilit o sesiune cascadeată, vă puteți deplasa între diferitele sisteme.

“Mutarea între sesiuni cascadeate Telnet” la pagina 81

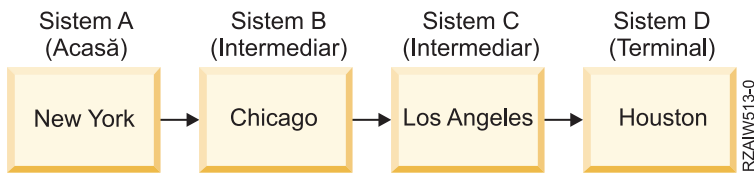
După ce ați pornit o sesiune cascadeată Telnet, apăsați tasta SysRq, și apăsați Enter pentru a afișa meniul Cerere sistem.

## Scenarii de procesare a cererilor sistem

Scenariile explică cum funcționează procesarea cererilor sistem cu multiple tipuri de sisteme.

### Scenariul 1

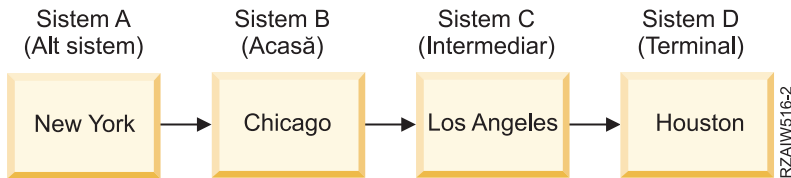
Imaginea descrie setarea următoare: Sistemul principal A din New York se conectează la sistemul intermediar B din Chicago, care se conectează la sistemul intermediar C din Los Angeles, care se conectează la sistemul terminal D din Houston.



### Scenariul 2

Sistemul New York folosește Telnet 3270 sau VTxxx. Este un sistem altul decât System i.

Imaginea descrie următoarea setare: Sistemul A din New York se conectează la sistemul gazdă B din Chicago, care se conectează la sistemul intermediar C din Los Angeles, care se conectează la sistemul terminal D din Houston.

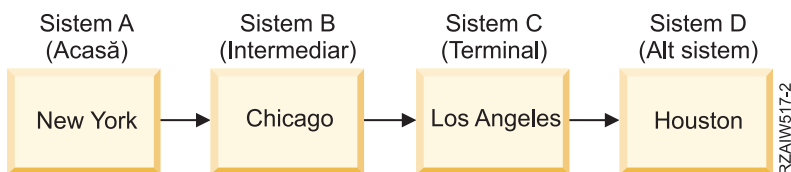


Procesarea cererii sistem funcționează ca în primul scenariu, cu excepția faptului că Chicago este considerat ca fiind sistemul principal. Toate cererile sistem trimise sistemului gazdă se procesează pe sistemul Chicago.

### Scenariul 3

Sistemul Houston folosește Telnet 3270 sau VTxxx. Este un sistem altul decât System i.

Imaginea descrie următoarea setare: Sistemul gazdă A din New York se conectează la sistemul intermediar B din Chicago, care se conectează la sistemul intermediar C din Los Angeles, care se conectează la sistemul terminal D din Houston.

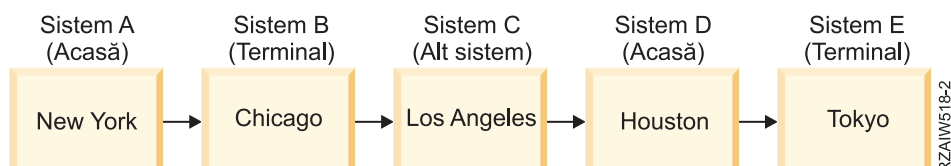


Procesarea cererii sistem funcționează ca în primul scenariu, cu excepția faptului că Los Angeles este considerat ca fiind sistemul terminal pentru întreaga procesare a cererii sistem. Dacă apăsați tasta System Request (Cerere sistem), iar apoi apăsați tasta Enter, se afișează meniul Cerere sistem pentru Los Angeles.

#### Scenariul 4

Sistemul Los Angeles folosește Telnet 3270 sau VTxxx. Este un sistem altul decât System i.

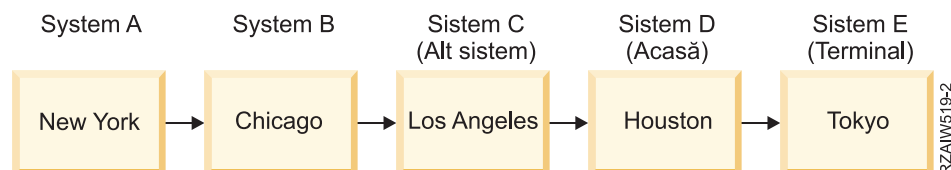
Sistemul gazdă din New York se conectează la sistemul terminal B din Chicago, care se conectează la sistemul C din Los Angeles, care se conectează la sistemul gazdă D din Houston, care se conectează la sistemul terminal E din Tokyo.



Procesarea cererii sistem funcționează ca în primul scenariu, cu excepția faptului că sistemul din Chicago este considerat ca fiind sistemul terminal pentru procesarea cererii sistem. Dacă apăsați tasta Cerere sistem iar apoi apăsați tasta Enter, meniul Cerere sistem pentru Chicago este afișat.

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.

Imaginea descrie următoarea setare: Sistemul A din New York se conectează la sistemul B din Chicago, care se conectează la sistemul C din Los Angeles, care se conectează la sistemul gazdă D din Houston, care se conectează la sistemul terminal E din Tokyo.



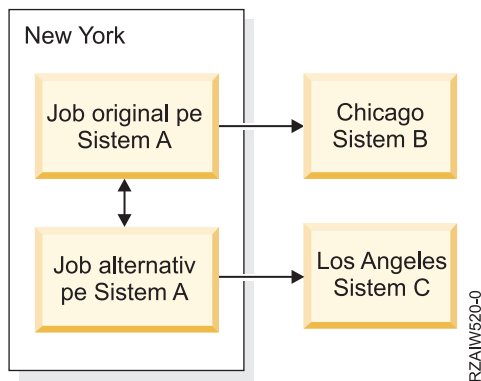
Ca un exemplu al acestei funcții de mapare pentru un server Telnet 3270, maparea implicită de tastatură identifică tasta Cerere sistem ca pe o tastă 3270 PF11. Pentru un client Telnet 3270, tasta F11 este mapată la tasta 3270 PF11. Dacă sistemul din Los Angeles folosește fluxul de date 3270, atunci prin apăsarea tastei F11 se mapează sistemul Los Angeles la tasta Cerere sistem din sistemul 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 mai ales dacă folosiți fluxul de date VTxxx și mapați între date bloc și date caracter.

#### Folosirea unui job de grup

Aceste exemple conțin informații despre cum să folosiți Telnet, joburi alternative și joburi de grup pentru a lucra cu sisteme multiple.

Puteți folosi Telnet și jobul alternativ pentru a vă conecta la sisteme multiple de la sistemul de acasă, luați în considerare următoarele exemple:



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, utilizând opțiunea 11 din Cerere de 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 jobul 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 setarea unui job de grup, parcurgeți acești pași:

1. Modificați jobul curent într-un job de grup utilizând comanda CHGGRPA (Change Group Attributes - Modificare atribute 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.

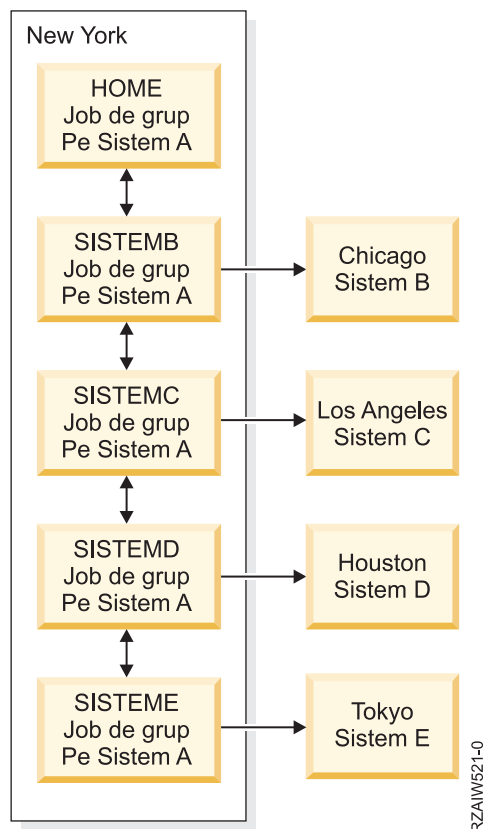
Puteți folosi comanda TFRGRPJOB GRPJOB(\*SELECT) pentru a selecta jobul de grup pe care îl doriți. De exemplu, dacă joburile de grup cu numele CHICAGO, LOSANGELES, HOUSTON și TOKYO pornesc, comanda TFRGRPJOB GRPJOB(\*SELECT) arată următorul ecran:

```

Transfer la Job de grup                               Sistem:  SYS198
Job de grup activ . . . : ACASĂ
Text . . . . . :
Type option, press Enter.
  1=Transfer la job de grup
-----Joburi de grup suspendate-----
Opt  Job de grup  Text
-    -          TOKYO
-    -          HOUSTON
-    -          LOSANGELES
-    -          CHICAGO
Bottom F3=Ieșire F5=Reîmprospătare F6=Pornirea unui nou job de grup F12=Anulare

```

Puteți folosi Telnet pentru a stabili o sesiune cu fiecare sistem de la jobul corespunzător. Exemplul următor prezintă un scenariu de job de grup:



Sistemul A din New York conține jobul de grup Acasă în sistemul A, cu săgeți bidirecționale de-a lungul unui lanț care se conectează la, în ordine: jobul de grup Sistem B în Sistem A, jobul de grup Sistem C în Sistem A, jobul de grup Sistem D în Sistem A și jobul de grup Sistem E în Sistem A. Fiecare job de grup al unui sistem în A are o săgeată care indică sistemul la distanță aflat în corelație (B, C, D și E).

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

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

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

## Scenariu Telnet: Securizare Telnet cu SSL

Acest exemplu de configurare descrie cum să folosiți SSL (Secure Sockets Layer) pentru a securiza Telnet în sistemul dumneavoastră.

### Situația

Bob este în cursul creării unei afaceri de brokeraj. Se retrage din funcția sa de agent la bursă în cadrul unei mari firme comerciale, și dorește să continue să ofere servicii de brokeraj unui număr mai mic de clienți de la domiciliul său. Își conduce firma de pe un sistem mic, pe care ar dori să îl folosească pentru a oferi acces prin cont clienților săi, prin intermediul sesiunilor 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 respectivii clienți să utilizeze sesiuni Telnet 5250 pentru a-și accesa conturile, însă este îngrijorat atât pentru securitatea serverului său, cât și pentru cea a sesiunilor clienților săi. După cercetarea opțiunilor de securitate Telnet, Bob se decide să folosească SSL (Secure

Sockets Layer) pentru a asigura confidențialitatea datelor în timpul sesiunilor Telnet 5250 între serverul și clienții săi.

## Obiectivele

În acest scenariu, Bob dorește să securizeze sesiunile Telnet 5250 ale clienților săi de brokeraj la conturile lor de acționari din sistemul său. Bob dorește să activeze SSL pentru a proteja integritatea datelor client pe măsură ce acestea sunt transmise prin Internet. Mai vrea de asemenea să activeze certificate pentru autentificare client pentru a se asigura că sistemul său verifică faptul că doar clienții lui își accesează conturile. După ce Bob a configurat serverul Telnet pentru SSL și a activat autentificarea client și server, poate prezenta această nouă opțiune de accesibilitate a contului clienților săi, asigurându-i că sesiunile lor Telnet 5250 sunt în siguranță:

- Securizare server Telnet cu SSL.
- Activare server pentru autentificare client.
- Obținere certificat privat de la un CA (certificate authority) local și asignați-l la Telnet.

## Detaliile

În acest scenariu, setarea pentru afacerea de brokeraj este după cum urmează:

- Sistemul rulează i5/OS V5R4, sau mai nou, și oferă acces la conturile acționarilor prin sesiuni Telnet 5250.
- Aplicația server Telnet este pornită în sistem.
- 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.

## Cerințele preliminare și supozițiile

Acest scenariu face următoarele supoziții:

- Sistemul rulează OS/400 V5R2, sau i5/OS V5R3, sau mai nou.
- TCP/IP este configurat.
- Bob are autorizare \*IOSYSCFG.
- Bob adresează problema în Configurarea serverului Telnet.
- Bob adresează problema în Cerințe preliminare SSL.
- Bob crează o autoritate de certificare locală în sistemul său.

## Pașii operației

Există două seturi de operații pe care Bob trebuie să le finalizeze pentru a-și implementa scenariul: un set de operații îi permit să își seteze sistemul să folosească SSSL și necesită certificate pentru autentificare utilizator; celălalt set de operații permite utilizatorilor de pe clienți Telnet să participe în sesiuni SSL cu serverul Telnet al lui Bob și să obțină certificate pentru autentificare de utilizator.

Bob realizează următorii pași pentru a completa acest scenariu:

### Pașii de operație pentru serverul Telnet

Pentru a implementa acest scenariu, Bob trebuie să realizeze aceste operații în sistemul său:

1. Înlăturare restricții de port. Consultați Înlăturare restricții de port.
2. Creare și operare autoritate de certificare locală. Consultați Creare și operare autoritate de certificare locală.
3. Configurare server Telnet pentru a cere certificate pentru autentificare client. Consultați Configurare server Telnet pentru a cere certificate pentru autentificare client.
4. Activare și pornire SSL pe server Telnet. Consultați Activarea și pornirea SSL pe un server Telnet.

### Pașii operației de configurare client

Pentru a implementa acest scenariu, fiecare utilizator care accesează serverul Telnet de pe sistemul lui Bob trebuie să realizeze aceste operații:

1. Activare SSL pe clientul Telnet. Consultați Activarea SSL pe clientul Telnet.
2. Activare client Telnet pentru a prezenta certificat de autentificare. Consultați Activare client Telnet pentru a prezenta certificat pentru autentificare.

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 pentru securizarea Telnet cu SSL

Aici sunt pași detaliați de configurare pentru securizarea Telnet cu SSL (Secure Sockets Layer).

### Pasul 1: Înlăturare restricții de port

În edițiile anterioare V5R1, restricțiile de port erau utilizate deoarece suportul SSL (Secure Sockets Layer - Nivel securizat de socket-uri) nu era 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 definiți restricții de port în edițiile anterioare, este nevoie 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 vedea orice restricție curentă de port, porniți Navigator System i și expandați *sistemul dumneavoastră* → **Rețea**.
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**.

În mod implicit, setarea este de pornire a sesiunilor SSL pe portul 992 și a sesiunilor 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 DCM-ul (Digital Certificate Manager) pentru a crea și opera un CA (certificate authority) local în sistem, 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. Există un formular pentru fiecare din operațiile pe care sunteți nevoie să le realizați pentru a crea și opera un CA local în sistem. Completarea acestor formulare vă permite să:



- a. Alegeți cum să memorați cheia privată pentru certificatul CA local. Acest pas este inclus doar dacă aveți un IBM 4758-023 PCI Cryptographic Coprocessor instalat în sistem. Dacă sistemul dumneavoastră nu are un coprocesor criptografic, DCM memorează automat certificatul și cheia lui primară în depozitul de certificate CA local.
- b. Furnizați informații de identificare pentru CA-ul local.
- c. Instalați certificatul CA local pe PC-ul dumneavoastră sau în browser-ul dumneavoastră. Aceasta permite software-ului să recunoască CA-ul local și să valideze certificatele emise de CA.
- d. Alegeți datele de politică pentru CA-ul dumneavoastră local.
- e. Folosiți noul CA local pentru a emite un certificat de server sau client pe care aplicațiile îl pot folosi pentru conexiuni SSL. Dacă aveți un IBM 4758-023 PCI Cryptographic Coprocessor instalat în sistem, acest pas vă permite să selectați cum să stocați chei private pentru certificatul de server sau client. 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.
- f. Selectați aplicațiile care pot folosi certificatul client sau server pentru conexiuni SSL.

**Notă:** Asigurați-vă că ați selectat ID-ul aplicației pentru serverul Telnet (QIBM\_QTV\_TELNET\_SERVER).

- g. Utilizați noul CA local pentru emiterea unui certificat de semnare obiect pe care aplicațiile îl pot folosi pentru semnarea digitală a obiectelor. Aceasta creează depozitul de certificate \*OBJECTSIGNING, pe care îl folosiți pentru a gestiona certificatele de semnare obiect.

**Notă:** Deși acest scenariu nu utilizează certificate de semnare obiecte, asigurați-vă că ați parcurs acest pas. Dacă anulați în acest punct din operație, aceasta se oprește și trebuie să efectuați operații separate pentru terminarea configurării certificatului dumneavoastră SSL.

- h. Selectați aplicațiile pe care doriți să le alocați CA-ului local.

**Notă:** Asigurați-vă că ați selectat ID-ul aplicației pentru serverul Telnet (QIBM\_QTV\_TELNET\_SERVER).

După ce ați completat formularele pentru această operație ghidată, puteți să configurați Serverul Telnet pentru a cere autentificarea clientului.

### Pasul 3: Configurare server Telnet pentru a cere certificate pentru autentificare client

Pentru a activa acest suport, administratorul de sistem indică felul în care este tratat suportul SSL. Folosiți panoul general Proprietăți Telnet din Navigator System i pentru a indica dacă suport SSL, non-SSL sau suport pentru ambele pornește o dată cu 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 i5/OS**.
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 să ceară certificate pentru autentificarea clientului, puteți activa și porni SSL pentru serverul Telnet.

#### **Pasul 4: Activare și pornire SSL pentru server Telnet**

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

1. Deschideți Navigator System i.
2. Expandați *sistemul dumneavoastră* → **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 nesecurizat**  
Selectați aceasta pentru ca un port SSL să nu se conecteze.
  - **Atât securizate, cât și nesecurizate**  
Permite atât sesiunile securizate, cât și cele nesecurizate cu serverul Telnet.

Pentru a porni serverul Telnet prin folosirea Navigator System i, urmați acești pași:

1. Expandați *sistemul dumneavoastră* → **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 pentru 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 CA în baza de date de chei i5/OS. Când serverul Telnet folosește un certificat de la un CA local, clientul Telnet trebuie să obțină o copie a certificatului CA local și să îl instaleze în baza de date de chei i5/OS.

Pentru a adăuga un certificat CA local de la sistem astfel încât clientul Telnet să poată participa în sesiuni SSL cu servere Telnet care folosesc un certificat de la CA-ul local, urmați acești pași::

1. Deschideți Navigator System i.
2. Faceți clic dreapta pe numele *sistemului dumneavoastră*.
3. Selectați **Proprietăți**.
4. Selectați fișa **Securizare Socket-uri**.
5. Faceți clic pe **Descărcare**. Aceasta descarcă certificatul CA i5/OS automat în baza de date de chei certificate.
6. Vi se cere parola bazei de date de chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, ca400. Este afișat un mesaj de confirmare. Faceți clic pe **OK**.

Butonul de descărcare actualizează automat baza de date de chei PC IBM Toolbox for Java.

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

Ați configurat SSL pentru serverul Telnet, specificat că serverul ar trebui să aibă încredere în certificatele emise de CA-ul prezent și ați specificat că este nevoie de autentificare a 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-ul local pentru a obține un certificat pentru autentificare la serverul Telnet și să importe acel certificat în baza de date IBM Key Management înainte ca autentificarea clientului să intre în funcțiune.

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**. Trebuie completate doar acele câmpuri marcate prin "Necesar". Selectați **Continuare**.
5. În funcție de browserul pe care îl folosiți, sunteți rugat să generați un certificat care este încărcat în browser-ul dumneavoastră. Urmați instrucțiunile furnizate de browser.
6. Când pagina browser-ului **Creare certificat utilizator** se reîncarcă, apăsați **Instalare certificat**. Acesta instalează certificatul în browser.
7. Exportați certificatul pe PC-ul dumneavoastră. Trebuie să memorați certificatul într-un fișier protejat prin parolă.

**Notă:** Sunt necesare Microsoft Internet Explorer 5 sau Netscape 4.5 pentru utilizarea funcțiilor de exportare și importare.

Apoi, trebuie să importați certificatul în baza de date IBM Key Management astfel încât clientul Telnet să îl poată folosi pentru autentificarea certificatului în cheia IBM prin urmarea acestor pași:

Trebuie să adăugați clientul importat care crează certificatul de client în baza de date de chei a PC-ului; altfel, operația de importare a certificatului clientului nu funcționează.

1. Faceți clic pe **Pornire** → **Programe** → **IBM System i Access pentru Windows** → **System i Access pentru Windows Proprietăți**.
2. Selectați fișa **Securizare Socket-uri**.
3. Faceți clic pe **IBM Key Management**.
4. Vi se cere parola bazei de date de chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, ca400. Este afișat un mesaj de confirmare. Faceți clic pe **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. Faceți clic pe **OK**.
8. Introduceți parola pentru fișierul protejat. Aceasta este aceeași parolă pe care ați specificat-o când ați creat un certificat utilizator în DCM. Faceți clic pe **OK**. Când certificatul este adăugat cu succes în certificatele dumneavoastră personale din 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.

### Operații înrudite

Pornire Digital Certificate Manager

“Asignarea unui certificat la serverul Telnet” la pagina 31

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

---

## Planificarea pentru serverul Telnet

Puteți determina numărul de dispozitive virtuale pe care să le asociați cu stații de lucru care sunt conectate la sistemul dumneavoastră. Acest subiect furnizează de asemenea proceduri de securitate pentru controlarea sau împiedicarea accesului la 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 doriți să fie create automat de către Telnet sau dacă doriți 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. De asemenea, ar trebui să luați în considerare alte măsuri de securitate, cum ar fi setarea serverului Telnet pentru detectarea conexiunilor pierdute.

## Descrierile de dispozitiv virtual

Telnet folosește descrierile de dispozitiv virtual pentru a menține informațiile de stație de lucru client pentru sesiuni Telnet deschise. Aici sunt detaliile despre configurarea și numirea descrierilor de dispozitiv virtual.

O stație de lucru *dispozitiv virtual* atașată este o descriere de dispozitiv care este folosită pentru a forma o conexiune între un utilizator și o stație de lucru fizică atașată unui sistem la distanță. Dispozitivele virtuale furnizează informații despre dispozitivul dumneavoastră fizic (ecran sau imprimantă) programelor din sistem. Sistemul caută protocolul client/server atașat pentru a specifica un dispozitiv virtual. Dacă sistemul nu poate găsi un dispozitiv virtual specificat, atunci caută pentru un dispozitiv virtual desemnat într-un program de ieșire înregistrat. Dacă sistemul nu poate găsi un dispozitiv virtual, atunci încearcă să potrivească o descriere de dispozitiv virtual cu un tip și model de dispozitiv similar cu dispozitivul din sistemul dumneavoastră local.

## Convențiile de numire Telnet pentru controlere și dispozitive virtuale

Serverul Telnet folosește următoarele convenții pentru numirea dispozitivelor și controlerelor virtuale create automat, conform standardelor i5/OS:

- Pentru controlerul virtual, serverul utilizează numele QPACTL *nn*, unde *nn* reprezintă un număr zecimal de 01 sau mai mare.
- Pentru dispozitive virtuale, serverul folosește numele QPADEV *xxxx*, unde *xxxx* este un caracter alfanumeric de la 0001 la *zzzzz*, fără vocale.
- Pentru dispozitive virtuale cu nume, serverul dă controlerelor virtuale numele QVIRCD *nnnn*.

### Note:

1. Conform convenției de numire i5/OS, controlerul virtual trebuie să aibe numele QPACTL *nn*.
2. Dispozitivul virtual are numele de QPADEV *xxxx*.
3. Trebuie să acordați profilului utilizator QTCP autorizarea la dispozitivele virtuale create de utilizator.
4. Convențiile de denumire pot fi modificate pentru dispozitivele virtuale create automat folosind opțiunea \*REGFAC din QAUTOVRT.

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 de sistem de semnare definesc numărul de încercări 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 modele și tipuri de dispozitive care să se potrivească, dar există încă dispozitivele virtuale disponibile, atunci tipul și modelul de dispozitiv sunt modificate pentru a se potrivi cu dispozitivul și modelul client care au fost negociate. Acest lucru este adevărat atât pentru dispozitivele virtuale create automat (QPADEV *xxxx*), 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 dispozitiv și orice nume de controler doriți,

ținând cont ca numele să se conformeze regulilor de numire obiecte i5/OS.

#### Concepte înrudite

“Crearea propriilor dumneavoastră dispozitive virtuale” la pagina 21

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

#### Operații înrudite

“Setarea numărului de dispozitive virtuale” la pagina 20

Puteți activa serverul Telnet să confugreze automat un număr de dispozitive și controlere virtuale prin folosirea valorilor de sistem dispozitive QAUTOVRT. Puteți de asemenea să limitați numărul de încercări de înscriere permise.

#### Referințe înrudite

Valori de sistem dispozitive: Dispozitive pass-through și Telnet

## Securitatea Telnet

Când porniți Telnet într-o conexiune TCP, trebuie să luați în considerare măsurile de securitate care împiedică sau permit accesul utilizatorilor la sistem 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.

### Împiedicare acces Telnet

Dacă nu doriți ca cineva să folosească Telnet pentru a vă accesa sistemul, trebuie să împiedicați serverul Telnet să ruleze. Pentru a împiedica accesul prin Telnet la sistemul dumneavoastră, completați operațiile din acest subiect.

### Împiedicarea Telnet de a porni automat

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

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

### Împiedicarea accesului porturi Telnet

Pentru a împiedica pornirea Telnet și pentru a împiedica pe cineva să își asocieze o aplicație de utilizator, cum ar fi o aplicație de socket, cu portul pe care sistemul îl folosește în mod normal pentru Telnet, urmați acești pași:

1. În Navigator System i, selectați **sistemul dumneavoastră** → **Rețea** → **Servere** → **TCP/IP**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Proprietăți**.
3. În fereastra Proprietăți de configurare TCP/IP, faceți clic pe fișa **Restricții port**.
4. În pagina Restricții port, faceți clic pe **Adăugare**.
5. În pagina Adăugare restricție port, specificați valorile următoare:
  - **Nume utilizator:** Specificați un profil de utilizator care este protejat în sistemul dumneavoastră. (Un profil de utilizator protejat este un profil de utilizator care nu deține programe care adoptă autorizare și care nu are o parolă cunoscută de alți 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 tabela WRKSRVTBLE (Work with Service Table Entries) sub numele de servicii Telnet și Telnet-ssl. Este posibil ca acestea să fie mapate la porturi altele decât 23 și 992.

Repetăți acest proces pentru fiecare port pe care doriți să îl restricționați. IANA (Internet Assigned Numbers Authority - Autoritatea pentru numerele alocate pe Internet) furnizează informații despre alocările obișnuite de numere de port.

6. Faceți clic pe **OK** pentru adăugarea restricției.
7. În pagina Restricții port, faceți clic pe **Adăugare** și repetați procedura pentru protocolul UDP (User Datagram Protocol).
8. Faceți clic pe **OK** pentru salvarea restricțiilor dumneavoastră de port și pentru închiderea ferestrei Proprietăți de 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.

#### Informații înrudite

 [IANA \(Internet Assigned Numbers Authority\)](#)

## Controlare acces Telnet

Trebuie să țineți cont de considerentele de securitate când doriți ca clienții Telnet să acceseze sistemul dumneavoastră.

## Autentificarea de client

Serverul Telnet suportă autentificare client în plus față de autentificarea SSL a serverului. Când este activată, serverul Telnet autentifică atât certificatele de server cât și de client când clienții Telnet se conectează la portul SSL Telnet. Clienții Telnet care nu trimit un certificat valid de client când încearcă să se conecteze la portul SSL Telnet, nu vor reuși să stabilească o sesiune de imprimantă sau afișare.

## Protejarea parolelor

Parolele Telnet nu sunt codate când sunt trimise între clientul tradițional și server. În funcție de metodele dumneavoastră de conectare, sistemul dumneavoastră poate fi vulnerabil la furtul parolelor prin ascultarea liniei. (Monitorizarea unei linii prin folosirea echipamentelor electrice este des întâlnită sub numele de sniffing (adulmecare).) Parolele Telnet sunt codate dacă se utilizează negocieri TN5250E pentru schimbul unei parole codate. 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; este necesar SSL pentru codarea întregului trafic.

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 care limitează numărul de încercări de semnare. Cu toate că valoarea sistem QMAXSIGN se aplică la Telnet, este posibil să reduceți eficacitatea acestei valori sistem dacă vă setați sistemul să configureze 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 dintre 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. O privire generală a capacității programului de ieșire Telnet oferă o privire generală a capacității programului de ieșire Telnet.

**Notă:** Ca alternativă, puteți utiliza programul dumneavoastră de ieșire Telnet pentru furnizarea de înregistrări în istoric. Mai degrabă decât să faceți programul dumneavoastră să ia decizii asupra eventualelor încercări de pătrundere, puteți utiliza posibilitatea de înregistrare în istoric pentru monitorizarea încercărilor de pornire a sesiunilor Telnet.

## Oprirea sesiunilor inactice

Sesiunile Telnet sunt incluse în procesarea sistemului pentru QINACTITV. Valoarea sistem QINACTMSGQ definește acțiunea pentru sesiunile Telnet interactive care sunt inactice 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 termină mai degrabă decât să se deconecteze. Sesiunile Telnet care continuă să folosească descrieri de dispozitiv cu numele QPADEVxxx nu permit utilizatorilor să se deconecteze de la aceste 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.

## Limitarea încercărilor de semnare

Numărul încercărilor permise de semnare Telnet crește dacă aveți dispozitive virtuale configurate automat. Valoarea de sistem dispozitiv din Navigator System i definește numărul de dispozitive virtuale pe care Telnet le poate crea.

Utilizați valorile sistem de semnare pentru definirea numărului încercărilor permise de semnare la sistem. Pentru instrucțiuni pentru setarea acestei valori în Navigator System i, consultați “Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare” la pagina 22.

## Restricționarea profilurilor de utilizatori puternici

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. Mai degrabă decât să împiedicați toți utilizatorii Telnet care au autorizarea specială \*ALLOBJ, ați putea să restricționați utilizatorii Telnet puternici în funcție de locație. Cu punctul de ieșire de inițiere Telnet, puteți crea un program de ieșire care asignează o anumită descriere de dispozitiv unei cereri de sesiune pe baza adresei IP a solicitantului.

## Controlare funcție după locație

S-ar putea să doriți să controlați ce funcții permiteți sau ce meniu vede utilizatorul pe baza locației de unde cererea Telnet a fost făcută. API-ul (application programming interface) QDCRDEVD vă oferă acces la adresa IP a solicitantului. Aici sunt câteva sugestii pentru folosirea acestui suport:

- Puteți folosi API-ul într-un program inițial pentru toți utilizatorii (dacă activitatea Telnet este semnificativă în mediul dumneavoastră).
- Puteți să setați meniul pentru utilizator sau chiar să comutați 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. De exemplu, puteți seta meniul inițial pentru utilizator, seta programul inițial pentru utilizator sau să specificați sub care profil de 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 returnează de asemenea și adrese IP de imprimantă, cât și pentru afișaje. Selectați formatul DEVD1100 pentru imprimante și DEVD0600 pentru terminalele de afișare.

## Controlare semnare automată

Telnet suportă capacitatea ca un utilizator System i Access pentru Windows să ocolească ecranul Semnare prin trimiterea unui nume și parole de profil de utilizator 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. Tabela următoare prezintă opțiunile. Aceste opțiuni se aplică numai când cererea Telnet include un ID utilizator și o parolă.

Tabela 2. Opțiunile QRMTSIGN de setare sistem

Opțiune	Modul de lucru QRMTSIGN cu Telnet
*REJECT	Sesiunile Telnet care cer semnare automată nu sunt permise.
*VERIFY	Dacă combinația de profil utilizator și parolă este validă, sesiune Telnet pornește. <sup>1</sup>
*SAMEPRF	Dacă combinația profil utilizator și parolă este validă, sesiune Telnet pornește. <sup>1</sup>
*FRCSIGNON	Sistemul ignoră profilul utilizator și parola. Utilizatorul vede ecranul de Semnare.

<sup>1</sup> - Un program înregistrat de ieșire Telnet poate să nu țină seama de setarea QRMTSIGN, alegând dacă să permită sau nu semnarea automată pentru un solicitant (probabil pe baza adresei IP).

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

- Valoare = 0, Parola/formula de acces (sau tichetul Kerberos) clientului nu a fost validată sau nu a fost primită nici una.
- Valoare = 1, Parola/formula de acces text în clar a clientului a fost validată.
- Valoare = 2, Parola/formula de acces cifrată (sau tichetul Kerberos) a fost validată.

## Activare semnare anonimă

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 de la o organizație din afară, puteți asigura sesiunii Telnet unui profil de utilizator care are autoritate limitată în sistemul dumneavoastră și un meniu specific. Puteți ocoli ecranul Semnare astfel încât vizitatorul are oportunitatea să folosească un alt profil de utilizator mai puternic. Cu această opțiune, utilizatorul nu are nevoie să furnizeze un ID utilizator și parolă.

## Privire generală a capacității 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. Puteți realiza următoarele acțiuni la pornirea unui program de ieșire:

- Folosiți certificatul de client SSL pentru a asocia un profil de utilizator certificatului și pentru a asigura acel profil de utilizator sesiunii Telnet, prin ocolirea ecranului Semnare.
- Folosiți adresa IP a sistemului (locală) pe sisteme multihome pentru a ruta conexiuni la diferite subsisteme pe baza interfeței rețelei (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.
- Asignați o descriere de dispozitiv i5/OS specifică pentru sesiune. Aceasta permite rutarea jobului interactiv către orice subsistem setat să primească acele dispozitive.
- Asignați valori de limbă națională specifice pentru sesiune, cum ar fi tastatură și set de caractere.
- Asocierea unui anumit profil utilizator pentru sesiune.
- Înregistrați automat solicitantul (fără afișarea ecranului de Semnare).



- Setăți înregistrarea în istoricul de auditare pentru sesiune.

#### Concepte înrudite

“Configurare automată a dispozitivelor virtuale” la pagina 20

Puteți activa serverul Telnet să vă configureze automat dispozitivele și controlerele virtuale prin folosirea valorilor de sistem dispozitive QAUTOVRT în Navigator System i.

“Folosirea programelor cu punct de ieșire Telnet” la pagina 39

Prin folosirea programelor de ieșire, programatorul experimentat poate crea o procesare personalizată în timpul unei aplicații. Dacă serverul Telnet găsește un program înregistrat la unul din punctele de ieșire pentru server, acesta apelează acel program prin folosirea parametrilor care sunt definiți prin punctul de ieșire.

#### Operații înrudite

Digital Certificate Manager (DCM)

“Setarea parametrului de ținere în viață a sesiunii” la pagina 23

Puteți folosi parametrul ținere în viață TCP pentru a seta timpul maxim de inactivitate pe care îl permite protocolul TCP înainte de a trimite o sondă pentru a testa inactivitatea unei sesiuni.

#### Referințe înrudite

Valori de sistem: Privire generală dispozitive

valori de sistem: Privire generală semnare

#### Informații înrudite



Technical Studio: Telnet Exit Programs

---

## Configurarea serverului Telnet

Subiectul conține informații despre cum să vă configurați serverul dumneavoastră Telnet pentru diverse tipuri de emulare.

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. Vă stau la dispoziție mai multe tipuri de emulare diferite pentru negocierea cererilor și convertirea acestora într-o ieșire. Sistemul poate suporta stații de lucru tip 3270 și stații de lucru VTxxx, dar tipul preferat este emularea 5250.

Pentru configurarea serverului dumneavoastră Telnet pentru utilizarea cu unul dintre celelalte tipuri de emulare suportate, completați următoarele operații de legătură care conțin pași de operație.

După ce ați configurat Telnet, ar fi bine să securizați Telnet cu SSL (Secure Sockets Layer).

#### Concepte înrudite

“Scenariu Telnet: Configurarea serverului Telnet” la pagina 1

Scenariul descrie cum un administrator configurează un server Telnet, inclusiv obiectivele, cerințele preliminare și presupunerile și detaliile de configurare.

## Pornirea serverului Telnet

Serverul Telnet activ are una sau mai multe instanțe de aceste joburi care rulează în subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

Pentru a porni serverul Telnet prin folosirea Navigator System i, urmați acești pași:

1. Expandați *sistemul dumneavoastră* → **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**.

#### Concepte înrudite

“Oprirea sesiunii server Telnet” la pagina 38

Prin oprirea unei sesiuni Telnet, faceți ca dispozitivul virtual să fie disponibil unei noi sesiuni Telnet.

### Operații înrudite

“Activarea subsistemului QSYSWRK” la pagina 24

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

“Activare SSL în serverul Telnet” la pagina 34

Urmați acești pași pentru a înțelege cum să activați SSL (Secure Sockets Layer) în serverul Telnet.

“Verificarea stării sistemului” la pagina 88

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

## Setarea numărului de dispozitive virtuale

Puteți activa serverul Telnet să configureze automat un număr de dispozitive și controlere virtuale prin folosirea valorilor de sistem dispozitive QAUTOVRT. Puteți de asemenea să limitați numărul de încercări de înscriere permise.

Puteți specifica numărul de dispozitive care sunt pornite automat și numărul maxim de dispozitive pe care sistemul le configurează automat. Sistemul configurează sau crează câte un dispozitiv pe rând, dacă este nevoie, până la o anumită limită.

1. În Navigator System i, selectați **sistemul dumneavoastră** → **Configurare și Service** → **Valori sistem**.
2. În panoul din dreapta, faceți clic dreapta pe **Dispozitive** și selectați **Proprietăți**.
3. La pagina Valori de 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
  - **Numărul maxim de dispozitive (1-32 500)** - Specificați o valoare între 1 și 32 500 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.

### Concepte înrudite

“Descrierile de dispozitiv virtual” la pagina 14

Telnet folosește descrierile de dispozitiv virtual pentru a menține informațiile de stație de lucru client pentru sesiuni Telnet deschise. Aici sunt detaliile despre configurarea și numirea descrierilor de dispozitiv virtual.

“Configurare automată a dispozitivelor virtuale”

Puteți activa serverul Telnet să vă configureze automat dispozitivele și controlerele virtuale prin folosirea valorilor de sistem dispozitive QAUTOVRT în Navigator System i.

### Referințe înrudite

Valori de sistem dispozitive: Dispozitive pass-through și Telnet

### Informații înrudite



Technical Studio: Telnet Exit Programs

## Configurare automată a dispozitivelor virtuale

Puteți activa serverul Telnet să vă configureze automat dispozitivele și controlerele virtuale prin folosirea valorilor de sistem dispozitive QAUTOVRT în Navigator System i.

Puteți specifica numărul de dispozitive care sunt pornite automat, și puteți specifica numărul maxim de dispozitive pe care sistemul le configurează automat. Sistemul configurează sau crează câte un dispozitiv pe rând, dacă este nevoie, până la o anumită limită.

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 modifică atributele unui dispozitiv existent pentru a satisface cererea clientului dacă acel dispozitiv virtual este cerut după nume.

Dacă nu ați permis niciodată configurarea automată a dispozitivelor virtuale în sistemul dumneavoastră, Valoare de sistem dispozitive: Număr maxim de dispozitive este 0. O încercare de conexiune Telnet eșuează când numărul de dispozitive în folosință depășește Numărul maxim de dispozitive. Un dispozitiv aflat în folosire are afișatăstarea activ sau semnat. Dacă încercați să vă semnați, veți primi un mesaj (TCP2504) care indică faptul că sesiune client Telnet s-a terminat și conexiunea a fost închisă. În plus, jobul QTCPIP de pe sistemul de la distanță trimite un mesaj (CPF8940) care indică faptul că un dispozitiv virtual nu poate fi selectat în mod 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 sistemul nu este capabil să creeze un dispozitiv virtual, mesajul CPF87D7 este trimis coada de mesaje operator de sistem de pe serverul Telnet.

**Note:**

1. Serverul Telnet nu șterge automat dispozitive virtuale configurate sau dispozitive cu nume, chiar dacă numărul de dispozitive atașat la controlerul virtuale depășește numărul maxim de dispozitive.
2. Valorile de sistem dispozitive specifică dacă dispozitivele virtuale pass-through și dispozitivele virtuale tot-ecranul Telnet care sunt atașate la controlerul QPACTLnn sunt configurate automat. Această valoare de sistem nu afectează dispozitivele care sunt atașate la controlerul QVIRCDnnnn, deoarece nu sunt dispozitive implicite de sistem. De obicei, dispozitivele QPADEVnnnn sunt atașate la controlerul QPACTLnn în timp ce dispozitivele cu nume, cum ar fi NEWYORK001, sunt atașate la controlerul QVIRCDnnnn controller.

**Concepte înrudite**

“Controlare acces Telnet” la pagina 16

Trebuie să țineți cont de considerentele de securitate când doriți ca clienții Telnet să acceseze sistemul dumneavoastră.

**Operații înrudite**

“Setarea numărului de dispozitive virtuale” la pagina 20

Puteți activa serverul Telnet să confugreze automat un număr de dispozitive și controlerul virtual prin folosirea valorilor de sistem dispozitive QAUTOVRT. Puteți de asemenea să limitați numărul de încercări de înscriere permise.

**Referințe înrudite**

Valori de sistem dispozitive: Dispozitive pass-through și Telnet

## Crearea propriilor dumneavoastră dispozitive virtuale

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

Dacă vă creați propriul dispozitiv virtual și permiteți sistemului dumneavoastră să selecteze automat numele dispozitivului, trebuie să țineți cont de următoarele reguli:

- Controlerul virtual are numele QPACTL nn, unde nn este un număr zecimal 01 sau mai mare.
- Dispozitivul virtual are numele 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 vă creați propriile dumneavoastră dispozitive, ar trebui să fiți familiarizați cu convențiile de numire a descrierilor de dispozitive virtuale folosite de către serverul Telnet. Dacă doriți să vă selectați propriile nume de dispozitive (prin folosirea unui client RFC 4777 sau a API-urilor Terminal virtual), atunci controlerul virtual are numele QVIRCD nnnn, unde nnnn este un număr zecimal 01 sau mai mare.

**Concepte înrudite**

“Descrierile de dispozitiv virtual” la pagina 14

Telnet folosește descrierile de dispozitiv virtual pentru a menține informațiile de stație de lucru client pentru sesiuni Telnet deschise. Aici sunt detaliile despre configurarea și numirea descrierilor de dispozitiv virtual.

## Restricționarea utilizatorilor privilegiați la anumite dispozitive și limitarea încercărilor de semnare

Valorile de sistem de semnare sunt utilizate atât pentru restricționarea sau limitarea dispozitivelor la care se poate semna un utilizator, cât și pentru definirea numărului încercărilor permise de semnare la sistem.

### Restricționarea utilizatorilor privilegiați la anumite dispozitive

Programul cu licență i5/OS folosește valorile de sistem de semnare pentru a restricționa sau limita dispozitivele la care un utilizator se poate semna. Valoarea \*ALLOBJ (*All object authority - Autorizare la toate obiectele*) permite utilizatorului să acceseze oricare dintre resursele de pe sistem. Valoarea \*SERVICE (*Service special authority - Autorizare specială de service*) permite utilizatorului să realizeze anumite funcții de service pe sistem. De exemplu, utilizatorul având acest tip de autoritate va fi capabil să depaneze un program și să execute funcții de afișare și de modificare de service. Pentru a seta aceste valori prin folosirea Navigator System i, urmați acești pași:

1. Selectați **sistemul dumneavoastră** → **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 opțiunile următoare:
  - **Restricționați utilizatorii privilegiați la anumite dispozitive.** Această selecție indică faptul că toți utilizatorii cu autorizare specială \*ALLOBJ (all object - toate obiectele) și \*SERVICE (service) au nevoie de autorizare explicită pentru anumite stații de lucru.
  - **Limitați fiecare utilizator la o singură sesiune de dispozitiv.** Această selecție indică faptul că un utilizator poate semna doar pe o singură 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 parolilor și de nesupraveghere a dispozitivelor.

### Limitarea încercărilor de semnare

Utilizați valorile sistem de semnare pentru definirea numărului încercărilor permise de semnare la sistem. Numărul încercărilor permise de semnare Telnet crește dacă aveți dispozitive virtuale configurate automat. Pentru setarea acestor valori, parcurgeți acești pași:

1. În Navigator System i, selectați **sistemul dumneavoastră** → **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 permise de semnare și acțiunea care să fie luată dacă se atinge numărul maxim de încercări de semnare.
5. Faceți clic pe fișa **La distanță**.
6. În pagina Proprietăți Telnet - Semnare la distanță, selectați o opțiune pentru **Utilizare Telnet pentru semnare 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 Utilizarea pass-through pentru semnarea la distanță, atunci opțiunile sunt selectate automat pe baza setărilor pe care le specificați pentru Utilizarea pass-through pentru semnarea la distanță. Telnet este încă disponibil pentru semnările la distanță dacă selectați Pass-through.

#### Concepte înrudite

Valori de sistem: Privire generală semnare

## Setarea parametrului de ținere în viață a sesiunii

Puteți folosi parametrul ținere în viață TCP pentru a seta timpul maxim de inactivitate pe care îl permite protocolul TCP înainte de a trimite o sondă pentru a testa inactivitatea unei sesiuni.

Protocolul trimite cereri de ținere în viață către clientul la distanță de fiecare dată când sesiunea rămâne nefolosită pentru perioade de timp mai lungi decât valoare de ținere în viață. Perioada de nefolosire este definită de către parametrul Timeout ținere în viață sesiune din Proprietăți Telnet din Navigator System i, sau un parametru din comanda CHGTELNA. Când o sesiune pare a fi inactivă (nu se primește nici un răspuns de la clientul la distanță de la nici o sondă ținere în viață) acea sesiune este încheiată, dispozitivul virtual asociat cu sesiunea este returnat pool-ului liber de dispozitive virtuale, iar sistemul de operare i5/OS realizează acțiunea setată în valoarea de sistem QDEVRCYACN din jobul interactiv care rulează în dispozitivul virtual. Această acțiunea afectează doar dispozitivele virtuale numite. Pentru dispozitivele virtuale selectate automat (QPADEVxxx), jobul interactiv se termină mereu.

Serverul Telnet definește implicit setarea ținere-în-viață la 600 de secunde.

Această setare are efect la pornirea serverului. În plus față de parametrul de ținere în viață a sesiunii, s-ar putea să doriți să examinați Setări interval timeout din Valori de sistem joburi inactice din Navigator System i. Acest Parametru timeout limitează durata în care i se permite unui job interactiv să fie nefolosit înainte ca sistemul de operare i5/OS să realizeze acțiunea setată în valoarea de sistem QINACTMSGQ din jobul interactiv. În cazul joburilor interactive conectate Telnet, o acțiune \*DSCJOB este onorată doar pentru dispozitive virtuale numite. Pentru dispozitive virtuale selectate automat (QPADEVxxx), o acțiune \*DSCJOB duce la terminarea jobului interactiv.

Pentru a seta parametrul de ținere în viață pentru Telnet din Navigator System i, urmați acești pași:

1. În Navigator System i, selectați **sistemul dumneavoastră** → **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 de luat când joburile ajung la un timeout. Puteți specifica de asemenea cât timp să acordați unei operații înainte ca jobul să intre în timeout. Puteți specifica informații atât pentru joburile inactice, cât și pentru cele deconectate.

### Concepte înrudite

“Controlare acces Telnet” la pagina 16

Trebuie să țineți cont de considerentele de securitate când doriți ca clienți Telnet să acceseze sistemul dumneavoastră.

### Referințe înrudite

Valori de sistem: Privire generală joburi

## Asignare dispozitive la subsisteme

Înainte ca un utilizator să se poate semna în sistem, stația de lucru trebuie să fie definită unui subsistem. Stația de lucru este dispozitivul virtual de afișare care este selectat sau creat automat de către serverul Telnet.

Numele stației de lucru sau tipul stației de lucru ar trebui specificate în descrierea subsistemului din sistem. 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 SBSD(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. Totuși, modificările pot avea sau nu efect imediat. S-ar putea să fie nevoie să opriți și să reporniți subsistemul.

## Activarea subsistemului QSYSWRK

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

Pentru a verifica starea subsistemului QSYSWRK, completați următorii pași:

1. În interfața pe bază de caractere, tastați WRKSBS (Work with active subsystems - lucru cu subsisteme active).
2. Verificați că sunt afișate următoarele sisteme:
  - QSYSWRK
  - QINTER
  - QSPL

Dacă subsistemul QSYSWRK nu este activ, efectuați următorii pași:

1. În interfața pe bază de caractere, tastați STRSBS (Start subsystem - pornire subsistem).
2. Tastați QSYSWRK pentru descrierea subsistemului și QSYS pentru Bibliotecă, apoi apăsați Enter.
3. Repetați pentru Nume subsistem QINTER cu Biblioteca QSYS și pentru Nume subsistem QSPL și Biblioteca QSYS.

Dacă nu știți ce subsistem să folosiți pentru joburi interactive, tastați WRKSBSD \*ALL în interfața pe bază de caractere. Intrările Tip stație de lucru vă indică dispozitivul care este alocat unui subsistem.

### Ce să faceți în continuare:

Crearea profilurilor de utilizator

#### Operații înrudite

“Pornirea serverului Telnet” la pagina 19

Serverul Telnet activ are una sau mai multe instanțe de aceste joburi care rulează în subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

## Crearea de profiluri utilizatori

În serverul Telnet, puteți crea porfilul utilizatori Telnet prin folosirea Navigator System i.

Pentru a crea profiluri utilizatori Telnet, completați următorii pași:

1. Porniți Navigator System i și expandați *sistemul dumneavoastră*.
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. Faceți clic pe **OK**.

## Tipuri de emulare suportate i5/OS

Emularea preferată pentru sistem este emularea 5250. Totuși, sistemul suportă de asemenea emulare 3270 și VTxxx.

Selectați tipul de emulare pe care doriți să îl configurați pentru utilizare de către serverul dumneavoastră Telnet.

#### Concepte înrudite

“Scenariu Telnet: Configurarea serverului Telnet” la pagina 1

Scenariul descrie cum un administrator configurează un server Telnet, inclusiv obiectivele, cerințele preliminare și presupunerile și detaliile de configurare.



## Configurarea serverului Telnet pentru modul tot-ecranul 5250

Modul tot-ecranul 5250 permite utilizatorilor client Telnet să se înscrie și să ruleze aplicații cu tot-ecranul 5250.

Trebuie să parcurgeți acești pași înainte de stabilirea sesiunii dumneavoastră de client Telnet:

1. Trebuie să porniți serverul Telnet pe sistemul la distanță (sistemul la care doriți să vă conectați utilizând Telnet).
2. Setări platforma System i să configureze automat dispozitive și controlere virtuale. Verificați că joburile QTVTELNET și QTVDEVICE din subsistemul QSYSWRK sunt active prin parcurgerea pașilor următori:
  - a. Porniți Navigator System i și expandați **sistemul dumneavoastră** → **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 valori numerice de la 0 la 32 500 și o valoare specială \*NOMAX.

## Configurare server Telnet pentru modul tot-ecranul 3270

Utilizatorii client Telnet se pot înscrie și rula aplicații tot-ecranul 5250 prin folosirea modului tot-ecranul 3270.

Sistemul negociază suport tot-ecranul 3270 cu orice aplicație client Telnet care suportă aplicații tot-ecranul 3270, mai degrabă decât cu aplicații tot-ecranul 5250. Un exemplu de sistem care negociază suport tot-ecranul 3270 este familia IBM System z family.

Telnet 5250 (TN5250) trimite fluxul de date între două sisteme ca EBCDIC. Deoarece fluxurile de date 3270 sunt translatate în fluxuri de date 5250, dispozitivele stației de lucru funcționează ca o stație de afișare 5251 la distanță pentru sistem și programele de aplicație.

După ce ați finalizat configurarea generală a serverului Telnet, mai sunt câțiva pași adiționali pentru a activa suportul pentru modul tot-ecranul 3270. Modul tot-ecranul este un mod bloc opus modului linie. Mod linie este atunci când datele sunt transmise linie cu linie, în timp ce modul bloc sau tot-ecranul transmite întregul ecran o dată.

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

1. Verificați valoare de sistem QKBDTYPE. Consultați “Verificarea valorii de sistem QKBDTYPE”
2. Setări mapare implicită de tastatură. Consultați “Setarea mapării implicite de tastatură”
3. Modificarea unei mapări de tastatură. Consultați “Modificare unei mapări de tastatură” la pagina 26
4. Modificare coadă de mesaje. Consultați “Modificare coadă de mesaje” la pagina 26

## Verificarea valorii de sistem QKBDTYPE

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

Dacă crearea inițială a dispozitivului virtual eșuează utilizând valoarea de sistem QKBDTYPE, serverul Telnet folosește valoarea de tastatură USB 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 de afișare 3270 conectată la un model System i care folosește Telnet apare ca fiind o stație de afișare 5251 unei platforme System i. Tastatura stație de afișare 3270 are asociată o mapare de tastatură 5251 echivalentă. Maparea de tastatură 5251 echivalentă permite tastaturii stației de afișare 3270 să finalizeze funcții 5251 echivalente în sistem.

Când un utilizator de sistem client Telnet se înscrie pentru prima dată în modul tot-ecranul 3270, sistemul automat asignează maparea implicită de tastatură pentru tastatura 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.

## Modificare 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. Alocările de taste pe care le specificați au efect până când folosiți aceste comenzi din nou pentru a specifica alocări noi de taste sau până 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.

## Modificare coadă de mesaje

O coadă de mesaje este ca o căsuță poștală pentru mesaje. Sistemul are mai multe cozi de mesaje care rețin mesajele care oferă informații ajutătoare în cautarea și raportarea problemelor. Când coada de mesaje a stației de lucru este în modul întrerupere, apar mesaje pe dispozitivul 3270 la fel cum apar și pe un ecran 5250. Pentru a primi mesaje în modul întrerupere, trebuie să specificați \*BREAK în comanda de schimbare a cozii de mesaje (CHGMSGQ). Când stația dumneavoastră de lucru nu se află în modul întrerupere, primiți mesajul următor: A sosit un mesaj într-o coadă de mesaje.

Ca să recuperați acest mesaj și să continuați utilizarea stației de lucru, parcurgeți acești pași:

1. Apăsați tasta funcțională alocată funcției de ajutor sau tasta funcțională care este alocată funcției de resetare eroare.
2. Introduceți comanda Afișare mesaj (DSPMSG) sau tasta funcțională care este alocată 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 luminii de inhibare intrare a ecranului

La folosirea unui model System i de la un terminal de tip 5250, apăsarea anumitor taste în unele situații duce la inhibarea intrării. Când apare acest lucru, terminalul 5250 afișează indicatorul inhibare intrare.

Două asteriscuri afișate în colțul din dreapta-jos a ecranului indică semnalizarea de inhibare intrare. Când tastatura este inhibată, orice taste mapate tastelor funcționale i5/OS sunt ignorate.

Pentru a reseta tastatura, apăsați tasta Enter sau apăsați tasta mapată pentru tasta Resetare.

### Concepte înrudite

“Sesiunile client Telnet 3270” la pagina 51

Tipul de emulare 3270 vă permite să accesați un sistem la distanță care are o aplicație server Telnet.

“Maparea tastaturii 3270 pentru serverele Telnet” la pagina 55

Subiectul conține informații despre maparea tastaturii pentru suport al emulării 3270.

### Referințe înrudite



“Tipurile de terminal 3270 suportate”

Subiectul descrie capacitățile dispozitivelor 3270 pe care Telnet le suportă. Asigurați-vă că clientul dumneavoastră Telnet negociază unul din tipurile suportate de terminal 3270.

### Tipurile de terminal 3270 suportate:

Subiectul descrie capacitățile dispozitivelor 3270 pe care Telnet le suportă. Asigurați-vă că clientul dumneavoastră Telnet negociază unul din tipurile suportate de terminal 3270.

Următorul tabel arată tipurile de terminal suportate.

Tabela 3. Mapările stației de lucru tot-ecranul

Tipul de dispozitiv	Capabilitățile dispozitivului
3277	Această stație de afișare suportă fluxuri de date generice 3270. Atribute extinse, precum sublinierea, clipirea intermitentă, imaginea inversată sau culoarea nu sunt suportate.
3278	Această stație suportă atribute extinse, cum ar fi intermitența, video invers și sublinierea dacă sunt cerute de cuvintele cheie DDS (Data Description Specifications) i5/OS. <b>Note:</b> 1. Atributele extinse nu sunt suportate de unele implementări client ale Telnet 3270 mod tot-ecranul (TN3270). 2. Tipurile de terminale DBCS (Double-byte character set - set de caractere pe doi octeți) sunt terminale care negociază un tip 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 mod ca un Ecran 5292 cu culori complete) prin interpretarea atributelor DDS drept clipire intermitentă, intensitate înaltă sau cuvintele cheie DDS de culoare.

### Concepte înrudite

“Configurare server Telnet pentru modul tot-ecranul 3270” la pagina 25

Utilizatorii client Telnet se pot înscrie și rula aplicații tot-ecranul 5250 prin folosirea modului tot-ecranul 3270.

### Configurare server Telnet pentru mod tot-ecranul VT<sub>xxx</sub>

Suportul pentru server VT<sub>xxx</sub> permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacă suportul tot-ecranul VT<sub>xxx</sub> este negociat.

Aplicația client Telnet trebuie să poată negocia suportul pentru terminal VT<sub>xxx</sub>. Când este negociat modul tot-ecranul VT<sub>xxx</sub>, serverul Telnet este responsabil pentru maparea funcțiilor 5250 în taste VT<sub>xxx</sub> și invers.

Deși serverul Telnet suportă clienți VT<sub>xxx</sub>, acesta nu este modul preferat de folosire pentru că terminalul VT<sub>xxx</sub> este un dispozitiv orientat caracter. Sistemul de operare i5/OS este un sistem orientat bloc. Majoritatea implementărilor Telnet suportă un client TN3270 sau TN5250 care ar trebui folosit la conectarea cu un server Telnet.

În general, când o tastă de la un terminal VT<sub>xxx</sub> este apăsată, codul hexazecimal asociat cu acea tastă este transmis imediat către serverul Telnet. Serverul Telnet trebuie să proceseze acea apășare de tastă și apoi să trimită înapoi acel caracter către terminalul VT<sub>xxx</sub> unde este afișat. Aceasta implică o activitate mărită (overhead) asociată fiecărei apășări de tastă. În mod diferit, dispozitivele orientate bloc 5250 și 3270 înregistrează toate apășările 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 au o activitate mai puțin mărită la fiecare apășare de tastă și, în general, au o mai bună performanță decât un dispozitiv orientat caracter, cum este terminalul VT<sub>xxx</sub>.

VT<sub>xxx</sub> livrează datele între cele două sistem ca ASCII.

După ce ați finalizat configurarea generală a serverului Telnet, este nevoie să finalizați câțiva pași suplimentari pentru a activa suportul pentru modul tot-ecranul VTxxx.

Modul tot-ecranul este un mod bloc opus unui mod linie. Mod linie este atunci când datele sunt transmise linie cu linie, în timp ce modul bloc sau tot-ecranul transmite întregul ecran o dată.

Finalizați următoarele operații pentru a configura serverul pentru modul tot-ecranul VTxxx:

1. “Verificarea valorii de sistem QKBDTYPE”
2. “Setarea mapării implicite de tastatură”
3. “Setarea tipului de terminal virtual de rețea implicit” la pagina 29
4. “Setarea tabelului de mapare ASCII/EBCDIC” la pagina 29

## Verificarea valorii de sistem QKBDTYPE

Când serverul Telnet crează automat dispozitive virtuale de afișare, folosește valoarea de 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 USB ca valoare 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 o sesiune Telnet negociază în modul tot-ecranul VTxxx, sistemul folosește o mapare implicită de tastatură. Pentru a afișa maparea implicită de tastatură pentru VTxxx, folosiți comanda DSPVTMAP (Display VT Keyboard Map - afișare mapare tastatură VT). Pentru a modifica maparea de tastatură VTxxx, folosiți comanda CHGVVTMAP (Change VT Keyboard Map - modificare mapare de tastatură VT) sau comanda SETVTMAP (Set VT Keyboard Map - setare mapare de tastatură VT).

Tabela cu blocul numeric de taste prezintă tastele de pe blocul auxiliar de taste care transmit în mod normal codurile pentru cifre, punct zecimal, semnul minus și virgulă.

Tabela de editat cu blocul de taste prezintă tastele care transmit coduri pentru tastele din blocul de taste de editat.

Deoarece tastatura VTxxx nu are aceleași taste ca tastatura 5250, o mapare de tastatură trebuie să existe între tastele VTxxx și funcțiile i5/OS. Sistemul asignează o mapare implicită de tastatură când o sesiune VTxxx este stabilă pentru prima dată. În unele cazuri, pot fi mai mult de o tastă sau secvență de taste care mapează o anumită funcție i5/OS. În aceste cazuri, puteți folosi oricare din tastele definite pentru apelarea funcției i5/OS cerute.

### Note:

1. Fiecare caracter de control este o valoare de 1 octet generată de la o tastatură VTxxx prin ținerea apăsată a tastei CTRL în timp ce se apasă una din tastele alfabetice. Caracterele de control generează aceleași valori hexazecimale, dacă este și dacă nu este apăsat SHIFT.
2. Secvențele escape reprezintă coduri de mai mulți octeți care sunt generate prin apăsarea tastei Esc, urmată de caracterele care formează secvența dorită.
3. Sistemul ignoră cazul tuturor caracterelor alfabetice într-o secvență escape. Puteți tasta caractere alfabetice litere mari și litere mici în secvențe escape.
4. Funcțiile de sistem F1-F12 sunt mapate la tasta Esc urmată de una din tastele din rândul de sus al tastaturii VTxxx. Tasta Esc urmată de o tastă deviată (shift) plus una din tastele din rândul de sus al unei tastaturi VTxxx mapează funcțiile F13-F24.

5. Unele sisteme client Telnet VTxxx folosesc Ctrl-S și Ctrl-Q în scopuri de control al fluxului. 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 terminalului virtual de rețea implicit fie la \*VT100 pentru modul VT100/VT220, fie la \*NVT pentru modul linie ASCII, finalizați următorii pași:

1. Porniți Navigator System i și expandați *sistemul dumneavoastră* → **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. Faceți clic pe **OK**.

## Setarea tabelelor de mapare ASCII/EBCDIC

Serverul Telnet folosește tabele implicite de mapare ASCII-în-EBCDIC și EBCDIC-în-ASCII pe baza parametrului CCSID (coded character set identifier) 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 modul VT220 7-biți, puteți utiliza fie tabelele de mapare, fie seturile de caractere de înlocuire DEC.

Există trei modalități de a schimba implicitul. Puteți modifica parametrul CCSID, specificați valori diferite pentru tabelele de ieșiri (TBLVTOU) și intrări (TBLVTIN) VTxxx, sau modifica tabelele implicite pentru sesiune curentă.

- Pentru modificarea valorilor pentru tabele, efectuați pașii următori:
  1. Porniți Navigator System i și expandați *sistemul dumneavoastră* → **Rețea** → **Servere** → **TCP/IP**.
  2. Faceți clic dreapta pe **TELNET** și selectați **Proprietăți**.
  3. Apăsați **Mapări**.
  4. Selectați caseta de bifare **Folosire tabele de mapare specificate** și faceți clic pe **Tabele**.
  5. Selectați casetele de bifare **Folosire tabelă de mapare ieșiri** și **Folosire tabelă de mapare intrări** pentru a modifica parametrul CCSID.
  6. Faceți clic pe **OK**.
  7. Faceți clic pe **OK**.
- Pentru a schimba tabelele implicite pentru sesiunea curentă, folosiți comanda SETVTTBL (Setare tabele de mapare VT).

O altă modalitate pentru accesarea acestei comenzi este utilizarea opțiunii 2 în comanda CHGTCPTELN.

### Concepte înrudite

“Sesiuni client Telnet VTxxx” la pagina 57

Sesiunile client Telnet VTxxx furnizează informații despre folosirea aceluiași tip de emulare pentru înscrierea și folosirea aplicațiilor pe un sistem la distanță care are o aplicație server Telnet. Această secțiune furnizează de asemenea informații suplimentare despre emularea VTxxx.

### Referințe înrudite

“Tastatura numerică” la pagina 71

Aici sunt tastele din blocul auxiliar de taste care în mod normal transmit codurile pentru zecimale, punct zecimal, semne minus și virgule.

“Editarea blocului de taste (keypad)” la pagina 73

Tabela arată tastele care transmit coduri pentru tasta editare bloc de taste.

“Opțiuni de emulare VTxxx” la pagina 62

Când folosiți modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet, sunt câteva proceduri opționale pe care le puteți aplica pentru a personaliza tipul de emulare. Puteți să afișați maparea curentă de tastatură și apoi să vă decideți dacă doriți să o modificați. Puteți de asemenea să modificați caracterele de control când folosiți modul tot-ecranul VT220.

“Valori de taste VTxxx prin funcție 5250” la pagina 75

Tabela descrie valoarea tastei VTxxx prin funcția 5250.

## Securizare Telnet cu SSL

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

### Concepte înrudite

SSL (Secure Sockets Layer)

### Operații înrudite

“Depanarea serverului dumneavoastră SSL Telnet” la pagina 88

Aici sunt pașii detaliați pentru depanarea serverului SSL (Secure Sockets Layer) inclusiv coduri de retur sistem SSL și o listă cu problemelor SSL obișnuite.

## Configurarea SSL pe serverul Telnet

Cel mai important factor de luat în considerare când activați SSL pe serverul Telnet este sensibilitatea informației care este implicată în sesiunile client. Dacă informațiile sunt sensibile, sau private, atunci este recomandată securizarea serverului Telnet cu SSL.

Pentru configurarea SSL pe serverul Telnet, urmați acești pași:

1. Instalați software-urile următoare pentru suportarea Telnet SSL și gestionarea certificatelor digitale:
  - IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
  - Manager de certificat digital
  - IBM HTTP Server for i5/OS (5761-DG1)
  - IBM Developer Kit for Java (5761-JV1)
2. Asigurați-vă că ați înlăturat restricțiile de port și ați permis SSL să pornească.
3. Alocați un certificat la serverul Telnet.
4. Activați autentificarea client pentru serverul Telnet (pas opțional).
5. Activați SSL pe serverul Telnet.
6. Porniți serverul Telnet.

### Concepte înrudite

“Inițializare și dialog de confirmare (handshake) SSL” la pagina 35

Aici sunt detaliile despre interacțiunile dintre servere Telnet, clienți și SSL (Secure Sockets Layer).

### Operații înrudite

“Depanarea serverului dumneavoastră SSL Telnet” la pagina 88

Aici sunt pașii detaliați pentru depanarea serverului SSL (Secure Sockets Layer) inclusiv coduri de retur sistem SSL și o listă cu problemelor SSL obișnuite.

“Verificarea stării sistemului” la pagina 88

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

## Înlăturare restricții de port:

În edițiile anterioare V5R1, restricțiile de port erau utilizate deoarece suportul SSL (Secure Sockets Layer - Nivel securizat de socket-uri) nu era 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 elimina restricțiile, urmăriți acești pași:

1. Pentru listarea restricțiilor de port, parcurgeți pașii următori:
  - a. Porniți Navigator System i și expandați **sistemul dumneavoastră** → **Rețea**.
  - b. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Proprietăți**.
  - c. Faceți clic pe fișa **Restricții port**.
2. Pentru înlăturarea Restricției de port, continuați să parcurgeți pașii următori:
  - a. Selectați restricția de port pe care vreți să o ștergeți.
  - b. Faceți clic pe **Înlăturare**.
  - c. Apăsăți **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.

#### **Operații înrudite**

“Asignarea unui certificat la serverul Telnet”

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

#### **Asignarea unui certificat la serverul Telnet:**

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

Înainte de a putea configura serverul Telnet să folosească SSL, este necesar să instalați programele de cerințe preliminare și să setați certificate digitale în sistemul dumneavoastră.

1. Porniți IBM 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 cadrul listei de operații, selectați **Asignare certificat** pentru afișarea unei liste cu 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 alocarea selecției dumneavoastră sau o eroare dacă a apărut o problemă.

**Notă:** Bazele de date de chei clienți System i Access pentru Windows trebuie să conțină o copie a oricărui certificat CA (certificate authority) cerut. În acest caz, un certificat CA trebuie să existe în baza de date chei pentru certificatul alocat de dumneavoastră aplicației server Telnet. Baza de date chei este preconfigurată cu copii ale certificatelor CA de la aproximativ toate CA-urile cunoscute. Dacă, totuși, alegeți să asignați un certificat serverului Telnet emis de un CA local atunci este nevoie să adăugați o copie a certificatului CA-ului local în

baza de date de chei client. Pentru a învăța cum să adăugați o copie a unui certificat CA local, consultați Pasul 5: Activarea SSL la clientul Telnet din subiectul Scenariu Telnet: Securizare Telnet cu SSL - Detalii configurare.

Serverul Telnet suportă autentificare client ca pe o componentă opțională în configurarea SSL. Autentificarea clientului survine atunci când serverul verifică identitatea clientului prin autentificarea certificatului de client transmis aplicației server.

### **Ce să faceți în continuare:**

Activarea autentificării clientului pentru serverul Telnet (pas opțional) sau Activarea SSL pe serverul Telnet.

#### **Concepte înrudite**

Planificare SSL

“Detalii de configurare pentru securizarea Telnet cu SSL” la pagina 10

Aici sunt pași detaliați de configurare pentru securizarea Telnet cu SSL (Secure Sockets Layer).

#### **Operații înrudite**

“Înlăturare restricții de port” la pagina 30

În edițiile anterioare V5R1, restricțiile de port erau utilizate deoarece suportul SSL (Secure Sockets Layer - Nivel securizat de socket-uri) nu era disponibil pentru Telnet. Acum puteți specifica dacă să pornească SSL, non-SSL sau ambele. Prin urmare, nu mai este nevoie de restricțiile de port.

Configurare certificate pentru prima dată

Pornire Digital Certificate Manager

“Activare autentificare client pentru serverul Telnet”

Serverul Telnet suportă autentificarea de certificate de client Telnet. Aceasta înseamnă că în timpul dialogului de confirmare SSL (Secure Sockets Layer), serverul nu numai că poate genera un certificat de server pentru client, dar poate de asemenea să verifice opțional pentru un certificat valid de client, în funcție de cum este configurat DCM-ul (Digital Certificate Manager).

“Activare SSL în serverul Telnet” la pagina 34

Urmați acești pași pentru a înțelege cum să activați SSL (Secure Sockets Layer) în serverul Telnet.

“Verificarea stării sistemului” la pagina 88

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

### **Activare autentificare client pentru serverul Telnet:**

Serverul Telnet suportă autentificarea de certificate de client Telnet. Aceasta înseamnă că în timpul dialogului de confirmare SSL (Secure Sockets Layer), serverul nu numai că poate genera un certificat de server pentru client, dar poate de asemenea să verifice opțional pentru un certificat valid de client, în funcție de cum este configurat DCM-ul (Digital Certificate Manager).

DCM-ul vă permite să configurați dacă Certificatele de client SSL sunt necesare pentru sesiuni Telnet.

Pentru a activa acest suport, administratorul de sistem indică în ce fel este tratat suportul SSL. Folosiți panoul Proprietăți generale Telnet din Navigator System i pentru a indica dacă suportul SSL, non-SSL sau suportul pentru ambele va porni o dată cu pornirea serverului Telnet. Implicit, suporturile SSL și non-SSL pornesc întotdeauna.

Administratorul de sistem are abilitatea de a indica dacă sistemul are nevoie de 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 oricare variabile RFC 4777 negociate, iar utilizatorul Telnet părăsește variabilele după satisfacerea controalelor SSL.

Pentru actualizarea specificațiilor de aplicație din IBM DCM și activarea autentificării de client pentru serverul Telnet, parcurgeți pașii de mai jos:

1. Porniți IBM DCM. Dacă trebuie să obțineți sau să creați certificate sau altfel să vă setați sau să vă modificați sistemul dumneavoastră de certificate, faceți aceasta acum.
2. Faceți clic pe **Selectare memorie certificat**.
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 panoul următor, selectați aplicația **Server**. Selectați **Continuare**.
8. Selectați **Serverul Telnet TCP/IP i5/OS**.
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-ul se reîncarcă la pagina Actualizare definiție aplicație cu un mesaj de confirmare. Când reîncărcarea DCM-ului a terminat de reîncărcat și actualizat definiția aplicației pentru serverul Telnet, faceți clic pe **Gata**.

#### Operații înrudite

“Asignarea unui certificat la serverul Telnet” la pagina 31

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

Pornire Digital Certificate Manager

“Activare SSL în serverul Telnet” la pagina 34

Urmați acești pași pentru a înțelege cum să activați SSL (Secure Sockets Layer) în serverul Telnet.

#### Informații înrudite



Configurare DCM

*Exemplu: Activare autentificare client pentru o sesiune PC5250:*

După ce ați configurat SSL (Secure Sockets Layer) pentru serverul Telnet și ați specificat folosirea autentificării client, utilizatorii sunt nevoiți să furnizeze un certificat de client vali și de încredere serverului Telnet la fiecare încercare de conectare.

Clienții sunt nevoiți să creeze un certificat de utilizator și să importe acel certificat în baza de date IBM Key Management înainte ca autentificare de client să funcționeze.

#### Crearea unui certificat de utilizator în DCM

1. Porniți IBM Digital Certificate Manager (DCM). Dacă trebuie să obțineți sau să creați certificate sau altfel să vă setați sau să vă modificați sistemul dumneavoastră de certificate, faceți aceasta acum.
2. Expandați **Creare certificat**.
3. Selectați **Certificat utilizator**. Selectați **Continuare**.
4. Completați formularul Certificat de utilizator. Trebuie completate doar acele câmpuri marcate prin "Necesar". Selectați **Continuare**.
5. În funcție de browser-ul pe care îl folosiți, veți fi rugat să generați un certificat care este încărcat în browser-ul dumneavoastră. Urmați instrucțiunile furnizate de browser.
6. La reîncărcarea paginii Creare certificat de utilizator, faceți clic pe **Instalare Certificat**. Acesta instalează certificatul în browser.
7. Exportați certificatul în sistemul dumneavoastră. Trebuie să memorați certificatul într-un fișier protejat prin parolă.

**Notă:** Sunt necesare Microsoft Internet Explorer 5 sau Netscape 4.5 pentru utilizarea funcțiilor de exportare și importare.



### Importarea certificatului în IBM Key Management

1. Faceți clic pe **Pornire** → **Programe** → **IBM System i Access pentru Windows** → **System i Access pentru Windows Proprietăți**.
2. Selectați fișa **Securizare Socket-uri**.
3. Faceți clic pe **IBM Key Management**.
4. Vi se cere parola bazei de date de chei. Doar dacă nu ați modificat anterior parola de la cea implicită introduceți, ca400. Este afișat un mesaj de confirmare. Faceți clic pe **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. Faceți clic pe **OK**.
8. Introduceți parola pentru fișierul protejat. Aceasta este aceeași parolă pe care ați creat-o în Pasul 7 la pagina 33 din Crearea unui certificat de utilizator în DCM. Faceți clic pe **OK**. Când certificatul a fost adăugat cu succes la certificatele dumneavoastră personale din IBM Key Management, puteți utiliza emulatorul PC5250 sau orice altă aplicație Telnet.

### Pornirea unei sesiuni de emulator PC5250 din Navigator System i

1. Deschideți Navigator System i.
2. Faceți clic dreapta pe numele sistemului dumneavoastră pe care l-ați setat pentru autentificarea de 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. Faceți clic pe **OK**.
9. Faceți clic pe **OK**.

#### Operații înrudite

Pornire Digital Certificate Manager

Configurare DCM

#### Informații înrudite



Configurare DCM

### Activare SSL în serverul Telnet:

Urmați acești pași pentru a înțelege cum să activați SSL (Secure Sockets Layer) în serverul Telnet.

1. Deschideți Navigator System i.
2. Expandați **sistemul dumneavoastră** → **Rețea** → **Servere** → **TCP/IP**.
3. Faceți clic dreapta pe **Telnet**.
4. Selectați **Proprietăți**.
5. Selectați fișa **General**.
6. Alegeți una dintre 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**

Selectați aceasta pentru a permite atât sesiunile securizate, cât și cele non-securizate cu serverul Telnet.

### **Operații înrudite**

“Asignarea unui certificat la serverul Telnet” la pagina 31

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

“Activare autentificare client pentru serverul Telnet” la pagina 32

Serverul Telnet suportă autentificarea de certificate de client Telnet. Aceasta înseamnă că în timpul dialogului de confirmare SSL (Secure Sockets Layer), serverul nu numai că poate genera un certificat de server pentru client, dar poate de asemenea să verifice opțional pentru un certificat valid de client, în funcție de cum este configurat DCM-ul (Digital Certificate Manager).

“Pornirea serverului Telnet” la pagina 19

Serverul Telnet activ are una sau mai multe instanțe de aceste joburi care rulează în subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

## **Inițializare și dialog de confirmare (handshake) SSL**

Aici sunt detaliile despre interacțiunile dintre servere Telnet, clienți și SSL (Secure Sockets Layer).

### **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 să vă dați seama dacă inițializarea SSL s-a realizat cu succes atunci când în subsistemul QSYSWRK apare mai mult de un job QTVTELNET activ. 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 în aplicația QIBM\_QTV\_TELNET\_SERVER nu există nici un certificat sau certificatul existent este expirat, serverul Telnet inițializează SSL cu succes. 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 re-inițializării SSL?**

Când certificatul din aplicația QIBM\_QTV\_TELNET\_SERVER se modifică, serverul Telnet re-inițializează SSL-ul dacă apare o modificare DCM. Aceasta înseamnă că puteți restaura un certificat expirat sau să adăugați sau înlăturați certificate de utilizator și Telnet efectuează modificările automat. 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 de client Telnet SSL vor utiliza certificatul nou.

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 dialogului de confirmare 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 pentru clientul dumneavoastră Telnet SSL pentru informații despre starea caracteristică a numerelor sau mesajelor. Serverul Telnet trimite mesajul CPDBC nn către istoricul jobului QTVTELNET.

### Operații înrudite

“Configurarea SSL pe serverul Telnet” la pagina 30

Cel mai important factor de luat în considerare când activați SSL pe serverul Telnet este sensibilitatea informației care este implicată în sesiunile client. Dacă informațiile sunt sensibile, sau private, atunci este recomandată securizarea serverului Telnet cu SSL.

“Verificarea istoricului de joburi Telnet” la pagina 89

Când inițializarea și dialogul de confirmare SSL (Secure Socket Layer) eșuează, serverul Telnet trimite un mesaj de diagnostic CPDBC nn la jobul QTVTELNET.

---

## Gestionarea serverului Telnet

Trebuie să luați la cunoștință de cum să lucrați cu serverul dumneavoastră Telnet și cum să folosiți programele de ieșire pentru a controla accesul utilizatorilor.

Serverul Telnet permite unui utilizator TCP/IP de pe un client Telnet să se înscrie pe și să ruleze aplicații pe platforma System i. Suportul server Telnet negociază transmisia de date cu aplicația client Telnet la distanță pentru diverse moduri de operare.

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

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

## Configurare sesiuni Telnet de imprimantă

Subiectul conține instrucțiuni pentru atașarea la imprimante din sistem de la locații la distanță din rețea.

Trebuie să creați un dispozitiv imprimantă virtual 3812 sau 5553 pentru a folosi emularea de imprimantă Telnet. Un astfel de dispozitiv este necesar pentru a genera fluxurile de date imprimantă trimise pentru sesiune de imprimantă. Imprimantele folosite pentru imprimare Telnet pot fi atașate PC-ului sau atașate aceleiași 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.

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. La folosirea comenzilor fișier de imprimantă CRTPRTF (create printer file - creere fișier imprimantă), CHGPRTF (change printer file - modificare fișier

imprimantă) și OVRPRTF (overwrite printer file - suprascrieri fișier imprimantă) trebuie să folosiți 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. Consultați Pornirea serverului Telnet.
3. Setează numărul de dispozitive virtuale. Consultați Setarea numărului de dispozitive virtuale.
4. Setează parametrul ținere în viață sesiune Telnet. Consultați Setarea parametrului de ținere în viață a sesiunii Telnet.
5. Creați dispozitive și controlere virtuale. Consultați Crearea de dispozitive și controlere virtuale.
6. Activați subsistemul QSPL. Consultați Activarea subsistemului QSPL.
7. Testați setarea cu un fișier imprimantă de test.
8. Tipăriți un fișier dintr-o sesiune de imprimantă Telnet.

**Notă:** Subsistemul QSYSWRK pornește atunci 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 System i Access pentru Windows
- 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 oricare din tipurile de dispozitive generice prin cererea funcției HPT (Host Print Transform) și selectarea tipului specific de manufacturare. Dacă folosiți System i Access pentru Windows, puteți folosi PDT (Printer Definition Table) sau GDI (Graphical Device Interface) pentru a defini un anumit hardware. Sistemul trimite imprimantei flux de date în ASCII.

### Îmbunătățirea API-ului de sistem

API-ul de sistem QDCRDEVD (Retrieve Device Description - Extragere descriere dispozitiv) furnizează adresa IP a clientului Telnet. Sunt mai multe câmpuri pentru dispozitive de afișare (\*DSP) și tipărire (\*PRT): Protocol de rețea, Adresă protocol de rețea și Adresă IP în formă zecimal punctată. Aceste câmpuri furnizează informații, la nivelul socket-urilor, aplicației dumneavoastră, despre conexiunea TCP/IP a clientului.

### Suport tipărire pentru server Telnet la clientul Telnet System i Access pentru Windows:

Clientul IBM System i Access pentru Windows furnizează atât emulare de afișare, client Telnet tot-ecranul 5250 cât și emulare de imprimantă.

Selectați una dintre următoarele pentru pornirea unei sesiuni de imprimantă:

1. **System i Access pentru Windows** → **Emulatoare** → **Pornire sau configurare sesiune** din meniul pornire program.
2. Selectați numele unui model System i la care să vă conectați.
3. Folosiți câmpul **ID stație de lucru** pentru a cere în mod specific un nume de dispozitiv virtual. Puteți lăsa câmpul blank și serverul Telnet selectează automat un dispozitiv virtual compatibil (QPADEVxxxx) și returnează numele panoul de control imprimantă.

#### 4. Pentru tipul emulării:

- a. Selectați o imprimantă.
- b. Faceți clic pe caseta **Setare** pentru a porni dialogul de setare emulare imprimantă PC5250.

Din dialogul de setare, puteți configura lucruri ca, font, coadă de mesaje și funcția gazdă HPT. Funcțiile gazdă HPT includ transformarea datelor de tipărire în ASCII în sistemul de operare i5/OS. Selectarea HTP (host print transform) activează alte elemente de configurare, cum ar fi model de imprimantă și opțiuni de selectare tavă media. De asemenea există o opțiune de reconectare automată și o opțiune de înlocuire a numărului implicit de port Telnet (23).

Pentru a termina sesiunea, faceți clic pe **Comunicație** → **Deconectare de la bara de meniuri**.

## Oprirea sesiunii server Telnet

Prin oprirea unei sesiuni Telnet, faceți ca dispozitivul virtual să fie disponibil unei noi sesiuni Telnet.

Când sunteți conectat la un sistem, deconectarea nu închide în mod necesar sesiunea server 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 una din următoarele secvențe de taste pentru a opri o sesiune server Telnet.

- Din sistemul de operare i5/OS, apăsați tasta **Atenție** iar apoi selectați opțiunea **99** (Oprire sesiune TELNET - IEȘIRE).
- Pentru marea parte a celorlalte sisteme de operare, delogați-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). Dacă aveți stabilită mai mult de o sesiune Telnet, comanda vă întoarce la sistemul anterior.

### Operații înrudite

“Pornirea serverului Telnet” la pagina 19

Serverul Telnet activ are una sau mai multe instanțe de aceste joburi care rulează în subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

## Terminare joburi manager dispozitiv

Uneori este necesară oprirea și repornirea joburilor manager dispozitiv; de exemplu, la aplicarea unui PTF (program temporary fix) programului. Acest subiect oferă instrucțiuni pentru oprirea și repornirea joburilor manager dispozitiv.

Pornirea și oprirea Telnet oprește joburile de server Telnet, dar nu joburile manager dispozitiv. Aceasta se întâmplă deoarece natura joburilor manager dispozitiv necesită ca acestea să ruleze mereu, sau cel puțin până la următoarea repornire a sistemului. Pentru a face joburile manager dispozitiv să cicleze, este nevoie să efectuați pașii speciali 2 și 3. Apoi, următoarea dată când porniți Telnet, va vedea că nu rulează nici un job manager dispozitiv și le va porni. Finalizați următorii pași pentru a opri joburi manager dispozitiv:

1. Terminați joburile active de server Telnet prin parcurgerea pașilor următori:
  - a. Porniți Navigator System i și expandați **sistemul dumneavoastră** → **Rețea** → **Servere** → **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 System i și expandați **sistemul dumneavoastră** → **Control funcționare**.
  - b. Selectați **Joburi active**.
  - c. Căutați QTVDEVICE.

3. Opriți toate joburile întâlnite la pasul 2 făcând clic dreapta și prin selectarea **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 se află încă în procesul de oprire după ce toate joburile manager dispozitiv au fost oprite pot deveni inaccesibile până la următoarea repornire.

## Folosirea programelor cu punct de ieșire Telnet

Prin folosirea programelor de ieșire, programatorul experimentat poate crea o procesare personalizată în timpul unei aplicații. Dacă serverul Telnet găsește un program înregistrat la unul din punctele de ieșire pentru server, acesta apează acel program prin folosirea parametrilor care sunt definiți prin punctul de ieșire.

Un *punct de ieșire* reprezintă un punct specific din 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.

Pot exista puncte de ieșire diferite care să împartă aceeași interfață punct de ieșire. Când se întâmplă acest lucru, puncte de ieșire multiple pot apela un singur program de ieșire.

## Performanța punctului de ieșire

Timpul de răspuns al serverului Telnet pentru cererea dumneavoastră de sesiune inițială include orice durată necesară serverului pentru a apela, procesa și returna programul de ieșire QIBM\_QTG\_DEVINIT. Dacă programul dumneavoastră de ieșire realizează o procesare semnificativă, impactul asupra performanței ar putea avea ca rezultat o așteptare mai îndelungată înainte ca sesiunea dumneavoastră să fie stabilită. Dacă doriți să modificați valoare implicită a timeout-ului de 60 de secunde a programelor de ieșire utilizator, puteți folosi comanda ADDEXITPGM pentru a adăuga date de utilizator care sunt citite ca valori de timeout. În următorul exemplu, parametrul PGMDTA rescrie timeout-ul implicit de 60 de secunde la 10 secunde:

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

După ce programul Telnet este stabilit printr-o fereastră de semnare sau alt model System i, nu există nici un efect asupra performanței. 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. Deconectarea înseamnă că vă încheiați sesiunea de emulare terminal, nu că vă delogați și vă întoarceți la panoul de semnare. Dacă vă deconectați, atunci este apelat programul de ieșire QIBM\_QTG\_DEVTERM, care realizează procesul de deconectare a sesiunii dumneavoastră. Utilizatorii nu pot vedea asta deoarece are loc după ce conexiunea a fost întreruptă.

## Controlul funcționării

Puteți rezolva probleme cheie de control al funcționării folosind programul de ieșire Telnet. Aceste probleme includ posibilitatea de a cere descrieri de dispozitiv altele decât QPADEVxxxx, astfel se deschide ușa joburilor de control funcționare al stațiilor de lucru virtuale interactive, și rutarea acelor joburi către un subsistem specific.

## Rutarea în subsistem și selecția numelui dispozitivului

Utilizatorii pot profita de nume mai bune de dispozitiv virtual Telnet și își pot configura subsistemele interactive pentru a împărți munca. 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(DQINTER) 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(DQINTER) 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

Cei doi utilizatori sunt în Chicago și New York. Utilizatorii sunt asigurați subsistemelor CHICAGO sau NEWYORK, conform locațiilor lor geografice. 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 alocă numele de dispozitiv virtual 'CHICAGO01' pentru adresa IP 1.2.3.47. Programul alocă un nume 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 aloca utilizatorului curent.

Pentru a vă asigura că dispozitivele virtuale din CHICAGO01 ajung la subsistemul Chicago, iar cele din NEWYORK01 ajung la subsistemul New York, setați intrările stațiilor de lucru după cum urmează:

**Notă:** Prin utilizarea exemplurilor de coduri, sunteți de acord cu termenii din Informații despre licența asupra codurilor și declinarea responsabilității.

```
ADDWSE SBS(DQINTER) WRKSTN(CHICAGO*) AT(*ENTER)
ADDWSE SBS(DQINTER) WRKSTN(NEWYORK*) AT(*ENTER)
ADDWSE SBS(DCHICAGO) WRKSTN(CHICAGO*) AT(*SIGNON)
ADDWSE SBS(DNEWYORK) WRKSTN(NEWYORK*) AT(*SIGNON)
```

### Concepte înrudite

“Controlare acces Telnet” la pagina 16

Trebuie să țineți cont de considerentele de securitate când doriți ca clienții Telnet să acceseze sistemul dumneavoastră.

## Program de ieșire inițializare dispozitiv

Aplicația de server Telnet include puncte de ieșire care vă permit să conectați logica de semnare și terminare Telnet. Puteți folosi comenzile WRKREGINF (Work with Registration Information - lucru cu înregistrare informații) sau ADDEXITPGM (Add Exit Program - adăugare program de ieșire) pentru a vă asocia programul de ieșire unui 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 personalizat de ieșire apoi procesează informațiile. De exemplu, înregistrează în istoric un mesaj și returnează controlul serverului Telnet. La returnare, programul de ieșire spune sistemului dacă să accepte sau să refuze acest client și orice înlocuiri opționale de utilizator sau parolă.

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

*Tabela 4. Grup de parametri necesari*

Nu.	Interfața punct de ieșire	Intrare sau ieșire?	Parametri
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 asigură opțional pentru selectarea sau setarea numelui de dispozitiv care va fi folosit în sesiunea Telnet, și permite unui client Telnet să ocolească inițializarea tradițională de dispozitiv. Administratorii ar putea controla aceste noi caracteristici prin intermediul unui nou program de ieșire, care opțional pornește imediat după stabilirea sesiunii client. Mai mulți parametrii sunt livrați programului de ieșire pentru a fi folosiți în procesul decizional, și programul de ieșire poate seta sau modifica diverși parametrii înainte de a se întoarce la serverul Telnet. În mod opțional, puteți înregistra un al doilea program de ieșire care să pornească imediat înainte de terminarea sesiunii. Puteți folosi al doilea program de ieșire pentru controlul sesiunii sau gestionarea dispozitivelor virtuale.

#### **Formatul punctului de ieșire Telnet INIT0100: Grupul de parametri necesari:**

Aici se află descrierile detaliate ale grupului de parametri necesari.

##### **Informația de descriere a utilizatorului**

I/O; CHAR(\*)

Informații despre utilizator pe care sistemul le folosește ca parte a procesului de semnare automată.

##### **Informația de descriere a dispozitivului**

I/O; CHAR(\*)

Informații pe care sistemul le folosește pentru a crea sau modifica dispozitivul pe care îl folosește pentru această sesiune Telnet.

##### **Informația de descriere a conexiunii**

I/O; CHAR(\*)

Informații despre conexiunea client pe care o poate folosi programul de ieșire.

##### **Opțiunii de mediu**

INPUT; CHAR(\*)

Un șir care conține toate opțiunile de mediu RFC 4777 negociate de client. Acestea se află în același format în care se aflau când au fost primite de la client și specificate de RFC 4777. Șirul constă, în general, din una sau mai multe perechi de nume de variabile de mediu și valori asociate. RFC-ul specifică faptul că fiecare nume de variabilă este mereu precedat fie de un X'01' fie de X'03' depinde dacă este un RFC 4777 definit VAR sau o aplicație definită specific USERVAR. Dacă o valoare este asociată cu un VAR (sau USERVAR), acea valoare va apărea următoarea în șirul precedat de caracterul RFC 1572 definit VALUE - X'01'. Această secvență de perechi VAR/VALUE se repetă până la un maxim al unui total de 1024 octeți de date negociate.

RFC 4777 și mult mai generalele RFC-uri de negocieri Telnet permit de asemenea caracterelor de control să apară în numele variabilelor VAR/USERVAR sau în valorile asociate acestora. 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 de opțiuni de mediu arată negocierile clientului, inclusiv parole, Telnet suprapune întotdeauna orice valori de text în clar sau parolă criptată în buffer pentru a evita o expunere de securitate.

### Lungimea opțiunilor de mediu

Lungimea opțiunilor de mediu referite în paragraful precedent este de obicei de 1024 de octeți. Din cauza faptului că negocierile de opțiune au lungime nedefinită, orice negocieri care depășesc lungimea specificată ar putea fi trunchiate pentru a se potrivi în buffer-ul opțiunilor de mediu.

### Permite conexiune

OUTPUT; CHAR(1)

Se aplică tuturor dispozitivelor și indică serverului Telnet dacă toate dispozitivele ar trebui să permită clientului să se conecteze la serverul Telnet. Dacă tipul de dispozitiv este de afișare și ați activat semnarea automată, atunci acest client ar putea de asemenea să ocolească afișajul de semnare din sistem. Valorile Valide sunt după cum urmează:

- 0 Rejectarea cererii de la client
- 1 Acceptare cerere de la client

### Permiterea semnării automate

OUTPUT; CHAR(1)

Se aplică tipurilor de dispozitiv de afișare, și indică serverului Telnet dacă operația de semnare automată ar trebui să fie lasată să continue pentru acest client. Acest parametru se aplică tipurilor de dispozitiv de afișare. Dacă este permisă semnarea automată, atunci clientul poate ocoli dispozitivul de semnare din sistem. Valorile valide sunt după cum urmează:

- 0 Rejectarea cererii de aplicație de la client. Sistemul ignoră parametrii de ieșire Profil utilizator, Bibliotecă curentă, Program de apelat, Meniu inițial și Nume dispozitiv.
- 1 Acceptare cerere de aplicație de la client. Sistemul poate considera valizi parametrii de ieșire Profil utilizator, Bibliotecă curentă, Program de apelat, Meniu inițial și Nume dispozitiv dacă programul de ieșire îi returnează.

### INIT0100: Formatul informațiilor de descriere utilizator:

Procesul de semnare automată folosește informații despre utilizator.

Următoarea tabelă arată formatul informației de descriere a utilizatorului:

Tabela 5. Formatul informațiilor de descriere utilizator

Offset-ul zecimal	Offset-ul hexazecimal	Tip	Câmp
0	0	INT(4)	Lungimea informațiilor de descriere utilizator
4	4	CHAR(10)	Profil utilizator
14	E	CHAR(10)	Bibliotecă curentă



Tabela 5. Formatul informațiilor de descriere utilizator (continuare)

Offset-ul zecimal	Offset-ul hexazecimal	Tip	Câmp
24	18	CHAR(10)	Programul de apelat
34	22	CHAR(10)	Meniu inițial

## Descrierile câmpurilor cu informații despre descrierea utilizator

### Bibliotecă curentă

Numele bibliotecii care va fi biblioteca curentă dacă activați stegulețul de semnare automată. Acest parametru este opțional, dar dacă îl livrați, trebuie să vă asigurați că l-ați aliniat la stânga și că l-ați completat cu blancuri. Valoarea este după cum urmează:

#### nume bibliotecă

Numele bibliotecii pe care doriți ca sistemul să o desemneze ca bibliotecă curentă.

### Meniu inițial

Numele meniului inițial pentru afișare dacă ați activat stegulețul de semnare automată. Valoare validă este după cum urmează:

#### nume meniu

Numele unui meniu de afișat.

### Lungimea informațiilor de descriere utilizator

Lungimea structurii informațiilor de descriere utilizator.

### Programul de apelat

Numele unui program pe care sistemul îl apelează dacă aveți activat stegulețul de semnare automată. Acest parametru este opțional, dar dacă îl furnizați, trebuie să îl aliniați la stânga și să îl completați cu blancuri. Valoare este după cum urmează:

#### nume program

Numele unui program pe care sistemul îl va porni.

### Profil utilizator

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

## INIT0100: Formatul informațiilor de descriere a dispozitivului:

Aici este prezentarea generală a formaturilor pentru crearea sau modificarea dispozitivului folosit pentru o sesiune Telnet.

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

Tabela 6. Formatul informațiilor de descriere a dispozitivului

Offset-ul zecimal	Offset-ul 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

Tabela 6. Formatul informațiilor de descriere a dispozitivului (continuare)

Offset-ul zecimal	Offset-ul hexazecimal	Tip	Câmp
28	1C	CHAR(*)	Structura atributelor dispozitivului

## Descrierile câmpurilor cu informații de descriere a dispozitivului

### Numele dispozitivului

Dispozitivul virtual specific pentru a fi asociat cu această sesiune Telnet. Pentru dispozitivele DISPLAY (de afișare), dacă valoarea de sistem a dispozitivului de auto-creare QAUTOVRT îi permite, dispozitivul este auto-creat de sistem dacă nu există deja și variat pe activat. Pentru dispozitivele PRINT (de tipărire), sistemul auto-crează dispozitivul dacă acesta nu există deja. Dacă programul de ieșire nu va furniza nici o valoare, serverul Telnet se va întoarce la valoarea implicită de utilizare a metodelor de selecție tradiționale ale dispozitivelor virtuale Telnet. Acesta ar trebui să fie un nume valid de descriere dispozitiv DISPLAY sau PRINT și trebuie să adere la convențiile standard i5/OS de numire a obiectelor.

### 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 un ecran. Sistemul returnează atributele de afișare.

### Rezervat

Rezervat pentru folosire în viitor.

### Offset la structura atributelor dispozitivului

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

### Lungimea structurii atributelor 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 7. Formatul informațiilor de descriere a dispozitivului de afișare (DSPD0100)

Offset-ul zecimal	Offset-ul 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

## Descrierile câmpului DSPD0100

### Setul de caractere

Setul de caractere pe care sistemul îl folosește pentru acest job interactiv. Puteți găsi valori valide în NLS (national language support). Acest câmp este identic cu parametrul Set de caractere al API-ului QTVOPNVT (Open Virtual Terminal Path).

### Pagină de cod

Pagina de cod folosită de sistem pentru acest job interactiv. Puteți găsi valori valide în NLS. Acest câmp este identic cu parametrul Pagină de cod al API-ului QTVOPNVT (Open Virtual Terminal Path).

### Identificator de tastatură

Identificatorul de tastatură din 3 caractere folosit de sistem pentru acest job interactiv. Identificatorul de

tastatură specifică implicit pagina de cod și setul de caractere de folosit, doar dacă este înlocuit ca parte a parametrilor Pagină de cod și Set de caractere. Puteți găsi identificatori valizi în NLS. Acest câmp este identic cu parametrul de tastatură Tip limbă al API-ului QTVOPNVT (Open Virtual Terminal Path).

### Rezervat

Rezervat pentru folosire în viitor.

### Referințe înrudite

Deschiderea API-ului QTVOPNVT de cale terminală virtuală

### INT0100: Formatul informației de descriere a conexiunii:

Acest subiect conține informații despre conexiune 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 8. Formatul informației de descriere a conexiunii

Offset-ul zecimal	Offset-ul hexagonal	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
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 câmpurilor cu informații despre descrierea conexiunii

#### Lungimea informației de descriere a conexiunii

Lungimea structurii de descriere a conexiunii.

#### Adresa internet a clientului

Adresa IP (sau tipul de structură) a clientului care cere, care este întotdeauna furnizată programului de ieșire. Dispunerea noilor câmpuri este după cum urmează:

Tabela 9. Dispunerea adresei IP a clientului

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

Dacă Telnet a validat parola cifrată a clientului (dacă a fost primită una). Sistemul setează această valoare dacă

Clienții TN5250E transmit parola cifrată pentru validare. Parola este verificată prin apelarea funcțiilor de servicii. 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 text în clar a clientului a fost validată.
- Valoare = 2, Parola/formula de acces cifrată (sau tichetul Kerberos) a fost validată.

### Tipul stației de lucru

Tipul stației de lucru cerut de către client, care este una din Specificații Internet listate în Spațiu de lucru și tabela de mapare imprimantă.

### Secure Sockets Layer

Dacă conexiunea este o conexiune SSL (Secure Sockets Layer):

- 0** Conexiunea nu folosește SSL.
- 1** Conexiunea folosește SSL.

### Adresa Internet a serverului

Adresa IP (sau tipul de structură) a interfeței rețelei gazdă (locale), care este întotdeauna furnizată programului de ieșire punct. Disponibilitatea noilor câmpuri este după cum urmează.

Tabela 10. Disponibilitatea adresei IP a clientului

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

### Nivel de autentificare client

Dacă sunt cerute certificate client SSL pentru a se conecta la sistem.

- 0** Nu se cere certificat client.
- 1** Este nevoie de un certificat valid de client.

### Codul retur valid pentru certificatul de client

Codul retur primit în timpul operației de dialog de confirmare SSL la validarea certificatului de client.

### Offset la certificat client

Offsetul de la începutului Structurii de conexiune la primul octet al certificatului de client.

### Lungime certificat client

Lungimea certificatului client care este primit. Dacă nu se primește nici un certificat, atunci lungimea este 0.

#### Concepte înrudite

“Tipuri de depanare emulare” la pagina 85

Când dezvoltați un client Telnet, este important să negociați tipul corect de stație de lucru de emulare. Funcțiile permise variază o dată cu tipul stației de lucru. Următorul ghid vă ajută să înțelegeți tipul de stație de lucru și capabilitățile funcționale ale acelei stații de lucru.

### Program de ieșire pentru terminare dispozitiv

Punctul de ieșire QIBM\_QTG\_DEVTERM apare când un client Telnet oprește sesiunea Telnet. Acesta vă permite înregistrarea în istoric informații de terminare a sesiunii și să realizați operații de resetare sau curățare dispozitiv.

Tabela următoare prezintă 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

Serverul Telnet asigură uneori oprirea dispozitivului, activități de auditare sesiune și gestionare dispozitiv virtual legate de dispozitivul asociat cu sesiunea Telnet oprită.

## Grup de parametri necesari

### Numele dispozitivului

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

## Exemple: Programe de ieșire Telnet

Programe exemplu v-ar putea ajuta să folosiți punctele de ieșire Telnet în sistemul dumneavoastră.

Programele exemplu care pot fi descărcate conțin următoarele resurse:

- **Exemplu de cod utilitar CL pentru programul de ieșire TELCRT (Create Telnet - Creare Telnet)**

Utilizați acest exemplu de cod pentru crearea, instalarea sau înregistrarea programelor de ieșire Telnet. Este scris în limbajul de programare CL (Command Language)i5/OS.

- **Exemplu de cod utilitar CL pentru programul de ieșire TELDLT (Delete Telnet - Ștergere Telnet)**

Utilizați acest exemplu de cod pentru a dezinstala și șterge programe de ieșire Telnet din sistemul dumneavoastră. Este scris în limbajul de programare CL.

- **Exemplu elementar de program de ieșire pentru inițializarea 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 multele alte funcții disponibile pentru programele de ieșire Telnet. Programul avansat de ieșire Telnet este conceput să beneficieze de aceste funcții.

Se recomandă să începeți cu programul de ieșire din inițializarea Telnet elementar până când înțelegeți cum funcționează, și apoi treceți la programul de ieșire din inițializarea Telnet avansat dacă aveți nevoie de mapare Dispozitiv virtual sau alte funcții avansate.

- **Exemplu avansat de program de ieșire din inițializarea 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 feluri de setări pentru sesiune:

- Selectarea unui dispozitiv Terminal virtual pentru această sesiune
- Ocolirea panoului de semnare
- Setare NLS (national language support)

- **Exemplu program de ieșire închierie Telnet (DEVTERM)**

DEVTERM QCSRC este un simplu program de înregistrare în istoric care înregistrează un mesaj de deconectare.

Acesta este un program de acompaniere atât pentru DEVINIT1 QCSRC, cât și pentru DEVINIT2 QCSRC.

Mesajele de închierie pe care îl înregistrează poate fi comparat cu mesajele de inițializare pentru a determina durata sesiunii Telnet.

## Exemple de fișiere ale programului 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. Selectați fișierul .zip pentru a descărca fișierele de program și informații pe PC-ul dumneavoastră, dezarhivați-le, iar apoi transferați-le în sistemul dumneavoastră. Este nevoie să redenumiți majoritatea fișierelor după ce le salvați în sistemul dumneavoastră.

Un fișier .savf este un fișier de salvare i5/OS. Descărcați-l pe PC-ul dumneavoastră, iar apoi transferați-l în sistemul dumneavoastră. Puteți crea o bibliotecă temporară în sistem și să transferați fișierul de salvare acolo. Despachetați fișierul de salvare din biblioteca temporară și urmați instrucțiunile din fișierul readme.

Faceți clic pe legătură pentru formatul de fișier pe care îl doriți, iar apoi apăsați **Salvare**.

**Notă:** Prin utilizarea exemplelor de coduri, sunteți de acord cu termenii din “Informații referitoare la licența de cod și declinarea responsabilității” la pagina 97.

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

---

## Gestionarea clientului Telnet

Puteți porni o sesiune de client Telnet prin utilizarea de tipuri diferite de emulare. Acest subiect explică de asemenea cum se stabilește o sesiune cascadată Telnet.

Clientul Telnet permite unui utilizator TCP/IP să se înscrie și să folosească aplicații pe un sistem la distanță prin folosirea unei aplicații 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, modifica configurații sau să faceți aproape tot ce puteți să faceți.

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 (Request for Comments) 4777. Clienții RFC 4777 au mai mult control asupra dispozitivului virtual server Telnet pe platforma System i prin intermediul mai multor noi parametrii din comanda STRTCPTELN (TELNET). Noii parametrii 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 (RMTPWENC) (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)

## Controlarea funcțiilor server Telnet de la client

Puteți folosi clientul Telnet pentru a controla procesarea stației de lucru de pe serverul Telnet când vă aflați într-o sesiune client.

Atât numele i5/OS cât și numele TCP/IP sunt listate pentru fiecare din funcțiile de comandă.

Pentru a selecta care funcții de server doriți să le controlați, trebuie să accesați meniul Funcții de control Telnet. Pentru a ajunge la acest meniu, apăsați tasta **Attn** a tastaturii dumneavoastră 5250.

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

- **Înterupere proces pe sistem** **Înterupere 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.

- **Interogare stare conexiune când sistemul devine inactiv Interogare stare conexiune sau AYT:** Această funcție furnizează un mesaj de la server care vă anunță că sistemul rulează în continuare. Puteți utiliza această funcție de control atunci când sistemul server devine în mod neașteptat inactiv pentru o perioadă lungă de timp.
- **Ignorare date de ieșire la distanță înainte să ajungă la stația dumneavoastră Ignorare date de ieșire la distanță sau AO:** Această funcție permite unui proces care generează date de ieșire să ruleze până la finalizare, fără trimiterea datelor de ieșire către stația dumneavoastră de lucru. Această funcție înlătură o ieșire sistem-sistem deja produsă care încă nu a fost afișată pe stația de lucru.
- **Curățare cale de date dintre sistemul dumneavoastră și server Curățare cale de date sau SYNCH:** Această funcție ignoră toate caracterele (cu excepția comenzilor Telnet) dintre sistemul dumneavoastră și 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 oprește sesiunea Telnet și închide conexiunea TCP/IP la sistem (sistem 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.
- **Utilizare tastă Attn pentru opțiunea gazdă la distanță Tasta ATTN pentru gazdă la distanță:** Apăsați tasta Attn pentru afișarea meniului Funcții control Telnet.

#### Note:

1. Această opțiune se aplică doar pentru modul 5250.
2. Dacă rulați în modul VTxxx (VT100 sau VT220), atunci mai sunt două selecții suplimentare în acest meniu:
  - Pentru sesiuni VT100, opțiunea 6 (Modificare mapare de tastatură primară VT100) și opțiunea 7 (Modificare mapare de tastatură alternativă VT100).
  - Pentru sesiuni VT220, opțiunea 8 (Modificare mapare de tastatură primară VT220) și opțiunea 9 (Modificare mapare de tastatură alternativă VT220).

#### Concepte înrudite

“Pornirea unei sesiuni client Telnet”

Ar trebui să cunoașteți numele sau adresa Internet al sistemului la distanță cu care doriți să începeți sesiunea Telnet.

“Pornirea unei sesiuni client 3270 Telnet” la pagina 51

Când porniți o sesiune client Telnet prin folosirea emulării 3270, aplicația de sistem la distanță vă controlează stația de afișare. Primiți aceleași afișări și introduceți date în același fel în care o faceți pentru alte dispozitive 3270 atașate local la sistemul de la distanță.

“Pornirea unei sesiuni client VTxxx” la pagina 57

Puteți porni o sesiune client Telnet prin folosirea emulării VTxxx. Trebuie să porniți serverul Telnet de pe sistemul la distanță (sistemul la care doriți să vă conectați prin Telnet).

## Sesiunile client Telnet 5250

Puteți folosi acest tip de emulare pentru a vă semna și folosi aplicații pe un sistem la distanță care are o aplicație server Telnet.

Suportul client Telnet 5250 permite utilizatorilor să se semneze pe alte sisteme și să acceseze aplicații tot-ecranul 5250. Suportul tot-ecranul 5250 poate fi negociat doar cu o aplicație server Telnet care rulează pe un sistem de operare i5/OS sau un sistem care suportă serverul Telnet 5250. Negocierea suportului stație de lucru 525x cu aplicația server Telnet la distanță activează suportul tot-ecranul 5250.

### Pornirea unei sesiuni client Telnet

Ar trebui să cunoașteți numele sau adresa Internet al sistemului la distanță cu care doriți să începeți sesiunea Telnet.

Pentru a începe o sesiune Telnet cu un sistem la distanță, urmați acești pași:

1. Porniți Navigator System i și expandați **sistemul dumneavoastră** → **Rețea**.



2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele Internet și numele gazdă.
1. Tastați comanda STRTCPTELN (Start TCP/IP TELNET - pornire TCP/IP Telnet), sau tastați TELNET în linia de comandă și apăsați Enter.
2. Tastați numele sistemului la distanță. Dacă doriți 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 doriți 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)
  - Criptare parolă la distanță (RMTPWDENC)
  - Program inițial la distanță (RMTINLPGM)
  - Meniu inițial la distanță (RMTINLMNU)
  - Bibliotecă 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 ecranul de semnare pentru sistemul la distanță.

#### Note:

1. Ecranul de semnare este afișat doar dacă nici unul dintre parametrii Semnare automată nu este introdus în comanda STRTCPTELN (RMTUSER, RMTPWD, RMTPWDENC) sau dacă apare o problemă când acești parametrii sunt introduși. Dacă aceste valori sunt introduse corect, nu este afișat nici un ecran de semnare. Utilizatorul este semnat automat și este afișat, oricare ar fi, panoul inițial definit pentru utilizator.
2. În plus, următoarele condiții sunt adevărate:
  - Dacă comanda STRTCPTELN furnizează parametrii corecți RMTUSER, RMTPWD, and RMTPWDENC, și un parametru corect MTINLPGM este de asemenea furnizat, atunci utilizatorul este semnat. De asemenea, programul inițial furnizat rulează.
  - Totuși, dacă parametrul RMTINLPGM nu este valid, utilizatorul este semnat, dar se afișează mesajul **jobul s-a terminat anormal**. Aceleași acțiuni sunt adevărate și pentru parametrul RMTINLMNU.
3. Pentru parametrul RMTCURLIB, o valoare corectă are drept consecință semnarea utilizatorului. De asemenea, va fi rulat orice program sau meniu inițial sau ambele, după cum a fost definit fie în profilul utilizatorilor, fie în comanda STRTCPTELN. În plus, biblioteca curentă este setată la valoarea parametrului. Dacă va fi furnizată o valoare nevalidă a parametrului RMTCURLIB, atunci se va afișa un panou de semnare cu un mesaj care va afirma că valoarea bibliotecii curente este nevalidă.
4. De asemenea, pentru toate elementele anterioare, dacă parametrii RMTKBDTYPE sau RMTCHRSET sau RMTCODPAG sunt furnizați cu valori valide, au avut efect pentru încercările reușite de semnare automată. Aceștia nu au efect pentru încercările invalide de semnare.

**Notă:** Dacă sistemul nu găsește sau nu configurează un server SOCKS sau dacă survin erori în timpul utilizării serverului SOCKS, atunci este stabilită o conexiune directă.



## 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.

### Referințe înrudite

“Controlarea funcțiilor server Telnet de la client” la pagina 48

Puteți folosi clientul Telnet pentru a controla procesarea stației de lucru de pe serverul Telnet când vă aflați într-o sesiune client.

“Stabilirea unei sesiuni cascadeate Telnet” la pagina 80

Puteți stabili o altă sesiune Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați stabilit o sesiune cascadeată, vă puteți deplasa între diferitele sisteme.

## Sesiunile client Telnet 3270

Tipul de emulare 3270 vă permite să accesați un sistem la distanță care are o aplicație server Telnet.

Deoarece fluxurile de date 3270 sunt traduse în fluxuri de date 5250, dispozitivele stație de lucru funcționează ca o stație de afișare 5251 la distanță pentru platforma System i și programele de aplicație.

**Notă:** Folosind exemplele de cod, sunteți de acord cu termenii din “Informații referitoare la licența de cod și declinarea responsabilității” la pagina 97.

### Concepte înrudite

“Configurare server Telnet pentru modul tot-ecranul 3270” la pagina 25

Utilizatorii client Telnet se pot înscrie și rula aplicații tot-ecranul 5250 prin folosirea modului tot-ecranul 3270.

## Pornirea unei sesiuni client 3270 Telnet

Când porniți o sesiune client Telnet prin folosirea emulării 3270, aplicația de sistem la distanță vă controlează stația de afișare. Primiți aceleași afișări și introduceți date în același fel în care o faceți pentru alte dispozitive 3270 atașate local la sistemul de la distanță.

Când clientul Telnet negociază suport stație de lucru 327x cu aplicația Telnet la distanță, sistemul activează modul tot-ecranul 3270. Clientul negociază suport 3270 tot-ecranul cu orice aplicație server Telnet care suportă aplicații 3270 (în locul celor 5250) tot-ecranul.

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 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 System i și expandați *sistemul dumneavoastră* → **Rețea**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele Internet și numele gazdă.
1. Tastați comanda STRTCPTELN (Start TCP/IP TELNET - pornire TCP/IP Telnet), sau tastați TELNET în linia de comandă și apăsați Enter.
2. Tastați numele sistemului la distanță. Dacă doriți să folosiți parametrii opționali, apăsați F10; altfel, apăsați Enter. Dacă tastați \*INTERNETADR pentru numele **Sistem la distanță** și apăsați Enter, serverul vă promtează câmpul **Adresă Internet**.
3. Tastați adresa Internet a sistemului la distanță. Pentru a folosi 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. Conexiune la serverul Telnet pornește.
5. În tipul unei sesiuni 3270 tot-ecranul, se pot aplica 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 ecranul de semnare pentru sistemul la distanță.

#### **Concepte înrudite**

“Maparea tastaturii 3270 pentru serverele Telnet” la pagina 55

Subiectul conține informații despre maparea tastaturii pentru suport al emulării 3270.

“Considerente pentru 3270 tot-ecranul”

Trebuie să țineți cont de dimensiunea ecranului 3270, tasta selectare cursor, mesaje de eroare și caractere nule la folosirea emulării 3270.

#### **Referințe înrudite**

“Controlarea funcțiilor server Telnet de la client” la pagina 48

Puteți folosi clientul Telnet pentru a controla procesarea stației de lucru de pe serverul Telnet când vă aflați într-o sesiune client.

## **Considerente pentru 3270 tot-ecranul**

Trebuie să țineți cont de dimensiunea ecranului 3270, tasta selectare cursor, mesaje de eroare și caractere nule la folosirea emulării 3270.

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

## **Dimensiunea ecranului TN3270**

Cerințele modului Telnet 3270 tot-ecranul:

- Dacă tipul de dispozitiv 3270 negociat necesită 1920 de caractere, codul clientului Telnet rulează cu orice tip de dispozitiv 5250 ca și terminalul client.
- Dacă tipul de dispozitiv 3270 negociat necesită 3564 de caractere, codul clientului Telnet necesită un tip de dispozitiv 5250 FW Model 3180; Model 3197 D1, D2, W1, W2; Model 3477 FA, FC, FD, FE, FG; ca terminal client.
- Există un ecran de 27x132 la negocierea unui tip de dispozitiv FW Model 2 3180; Model 3197 D1, D2, W1, W2; Model 3477 FA, FC, FD, FE, FG. În versiunile anterioare, era necesară o zonă de date pentru a obține acest suport.
- Pentru a obține un ecran de 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 parametri pentru comanda STRTCPTLN veți emula tasta de selectare cursor:

Tabela 11. Parametri de emulare tasta de selectare cursor

Parametru	Valoare
Tasta Page Up (Roll Down)	*CSRSLT
Tasta Page Down (Roll Up)	*CSRSLT
Tasta de selectare cursor	Tasta *F (specificați o tastă funcțională de la *F1 la *F24)

## Mesajele TN3270

Când utilizați modul Telnet 3270 tot-ecranul, se pot afișa mai multe tipuri de mesaje de eroare.

- 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 de sistem includ mesaje Telnet și sunt emise din sistem.
- Pentru informații despre mesajele care sunt trimise de pe sistemul la distanță, vedeți documentația referitoare la sistemul la distanță.

## TN3270 - Tratarea caracterelor nule

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

Modifică caracterele nule de început și înglobate în blancuri. Aceasta este valoarea implicită. Caracterele nule de coadă sunt întotdeauna înlăturate pentru ambele valori. Aceasta este valoarea implicită. De exemplu, presupuneți că datele constau din următorul cod (0 indică un nul) :

```
0x0yz000
```

Fluxul de date trimis de la o stație de afișare 5250 care rulează Telnet 3270 tot-ecranul cu valoarea implicită \*BLANK conține codul următor:

```
bxbyz
```

Fluxul de date trimis de la o stație de afișare 3270 sau de la o stație de afișare 5250 care rulează o sesiune Telnet 3270 tot-ecranul când valoarea \*REMOVE este specificată ar conține codul următor:

```
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

### Concepte înrudite

“Pornirea unei sesiuni client 3270 Telnet” la pagina 51

Când porniți o sesiune client Telnet prin folosirea emulării 3270, aplicația de sistem la distanță vă controlează stația de afișare. Primiți aceleași afișări și introduceți date în același fel în care o faceți pentru alte dispozitive 3270 atașate local la sistemul de la distanță.

## Folosirea unei stații de afișare

Aici găsiți diferențele de tastatură și afișare la folosirea unei stații de afișare în timpul unei sesiuni tot-ecranul Telnet 3270 . Alte considerații speciale pentru modul 3270 Telnet includ numărul de câmpuri de intrare, mesaje de eroare și terminarea unei sesiuni.

## Specificarea tastaturii și a seturilor de caractere

Tipul de limbă pentru tastatură pe care o specificați pentru stația dumneavoastră de lucru, prin folosirea parametrului tip de limbă pentru tastatură în comanda STRTCPTLN, trebuie să fie același cu parametrul tip de limbă pentru tastatură al stației de lucru atșată 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 clientul Telnet care operează într-un mod 3270 tot-ecranul, funcția Curățare 3270 poate fi apelată în mod implicit prin succesiunea de taste Shift-Cmd-Backspace.

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

- Tastatura IBM îmbunătățită
- Tastatura tip mașină de scris cu 122 taste
- Tastatura 5250
- Tastatura tip calculator pentru PC sau PC IBM AT
- Tastatură tip 5250 pentru PC sau PC AT
- Tastatura IBM îmbunătățită PC

## Tastaturile PC

Dacă calculatorul dumneavoastră personal folosește WSF-ul (Workstation Function) System i Access pentru Windows, puteți afișa disponerea tastaturii dumneavoastră 5250 prin folosirea comenzii WSFKEYS (Work Station Function Keys - taste funcționale stație de lucru). Puteți modifica stilul utilizând comanda CFGWSF (Configure Work Station Function). Aceste comenzi sunt explicate în cartea 'Client Access/400 for DOS with Extended Memory Setup'. Dacă PC-ul dumneavoastră nu utilizează funcția stație de lucru, referiți-vă la documentația corespunzătoare pentru emulatorul dumneavoastră (de exemplu, OS/2 CM/2) pentru vizualizarea sau modificarea stilului tastaturii.

## TN3270-Semnul minus

Dacă ați specificat valoarea \*YES pentru parametrul blocare numerică a tastaturii din comanda STRTCPTLN, dacă utilizați o tastatură pentru introducerea datelor și dacă cursorul se află într-un câmp doar-numeric, atunci parcurgeți aceste operații pentru afișarea unui semn minus 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 alocă, 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

Subiectul conține informații despre maparea tastaturii pentru suport al emulării 3270.

Următoarea tabelă arată alocările 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 6 (Afișare mapare de tastatură 3270) în meniul Configurare TCP/IP Telnet, în timp ce terminalul dumneavoastră este în modul de emulare 3270.

Tabela 12. Alocările implicite pentru tastele PF

Tastă funcțională 5250	Taste 3270 implicite pentru selectarea funcției
Help	PF1
Ajutorul 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
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 (control language) setează mapare tastaturii pentru o stație de lucru de tip 327x care folosește Telnet pentru a ajunge la o platformă System i. Acest program mapează tastele funcționale i5/OS la tastele funcționale echivalente acestora 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 mesajului, restul programului este nefolosit în aceste circumstanțe.

**Notă:** Folosind exemplele de cod, sunteți de acord cu termenii din “Informații referitoare la licența de cod și declinarea responsabilității” la pagina 97.

```
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
```

Prin memorarea acestei surse CL ca o parte a fișierului QCLSRC în biblioteca TCPLIB ca membru CHGKBD, puteți crea programul CL CHGKBD (Change Keyboard Map) în biblioteca TCPLIB prin folosirea următoarei comenzi CL:  
CRTCLPGM PGM(TCPLIB/CHGKBD) SRCFILE(TCPLIB/QCLSRC)  
TEXT('Modifică maparea tastaturii pentru terminale 327x')

Programul CHGKBD poate fi apoi apelat de către oricine care folosește Telnet pe o platformă System i. Poate să fie apelat și automat la momentul de semnare prin specificarea programului CHGKBD în parametrul Program inițial în comanda CHGUSRPRF (Change User Profile - modificare profil utilizator), sau programul CHGKBD poate fi apelat de către programul inițial al profilului.

## Tastele 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 plănuți să începeți o sesiune fără să schimbați maparea de tastatură. Ar trebui să consultați documentația emulatorului pentru tastele sau apăsările 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. Aceste secvențe de tast sunt după cum urmează:

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

Funcția Tasta de ieșire câmp 5250 este realizată pe o tastatură 3270, prin folosirea tastei Ștergere EOF și apoi a tastei Tab.

## Circumstanțe speciale

Când folosiți modul tot-ecranul Telnet 3270 de la terminalul 3270 și înainte ca maparea implicită a terminalului să fie modificată, tastele de la PF1 la PF12 pot fi emulate de secvența de taste PA1 PFx. Prin urmare, instrucțiuni precum Apasă PF3 sau Apasă PF4 se vor citi: Apasă PA1 PF3 și Apasă PA1 PF4, înainte de crearea unei hărți noi de tastatură.

În funcție de instalarea clientului Telnet pentru gazdă (de exemplu, un client Telnet VM (virtual machine - mașină virtuală)), când apăsați PA1, utilizatorul se poate să primească instrucțiunea **TELNET command:** pe linia de jos a afișajului. Dacă sistemul afișează această instrucțiunea, tastați PA1, apăsați tasta Enter, mutați cursorul pe linia de comandă; și apăsați tasta PF necesară.

**Notă:** *HCF (Host Command Facility)* este o caracteristică disponibilă în sisteme gazdă System/370, 43xx și 30xx. Această caracteristică permite unui utilizator de pe sistemul gazdă să folosească aplicații pe o platformă System i. Dacă folosiți HCF pentru a vă conecta la o platformă System i și apoi folosiți Telnet pentru a vă semna pe o altă platformă System i de pe acea platformă, vă aflați într-o sesiune de mod tot-ecranul 3270. Tastatura este mapată de două ori, o dată pentru sesiunea inițială HCF și o dată pentru sesiunea Telnet. Pentru a vă folosi tastele PF așa cum le folosiți în mod normal, este nevoie să modificați maparea de tastatură pe ambele platforme. Asigurați-vă că folosiți aceeași mapare de tastatură pe fiecare platformă.

### Concepte înrudite

“Pornirea unei sesiuni client 3270 Telnet” la pagina 51

Când porniți o sesiune client Telnet prin folosirea emulării 3270, aplicația de sistem la distanță vă controlează stația de afișare. Primiți aceleași afișări și introduceți date în același fel în care o faceți pentru alte dispozitive 3270 atașate local la sistemul de la distanță.

“Configurare server Telnet pentru modul tot-ecranul 3270” la pagina 25

Utilizatorii client Telnet se pot înscrie și rula aplicații tot-ecranul 5250 prin folosirea modului tot-ecranul 3270.

## Sesiuni client Telnet VT<sub>xxx</sub>

Sesiunile client Telnet VT<sub>xxx</sub> furnizează informații despre folosirea acestui tip de emulare pentru înscrierea și folosirea aplicațiilor pe un sistem la distanță care are o aplicație server Telnet. Această secțiune furnizează de asemenea informații suplimentare despre emularea VT<sub>xxx</sub>.

Suportul Telnet VT<sub>xxx</sub> permite utilizatorilor să se înscrie pe platforme, altele decât platforma System i, ca și cum ar fi pe un terminal VT<sub>xxx</sub> atașat local sistemului. Suportul client VT<sub>xxx</sub> permite utilizatorilor să se înscrie pe orice sistem la distanță într-o rețea TCP/IP care suportă fluxul de octeți VT<sub>xxx</sub>. Ca utilizator Telnet, ar trebui să Țineți cont de diferențele fizice și operaționale dintre sesiunile VT<sub>xxx</sub> și 5250.

### Concepte Țnrudite

“Configurare server Telnet pentru mod tot-ecranul VT<sub>xxx</sub>” la pagina 27

Suportul pentru server VT<sub>xxx</sub> permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacȃ suportul tot-ecranul VT<sub>xxx</sub> este negociat.

## Pornirea unei sesiuni client VT<sub>xxx</sub>

Puteți porni o sesiune client Telnet prin folosirea emulării VT<sub>xxx</sub>. Trebuie să porniți serverul Telnet de pe sistemul la distanță (sistemul la care doriți să vă conectați prin Telnet).

Ar trebui să cunoașteți numele sau adresa Internet a sistemului la distanță cu care doriți să porniți sesiunea Telnet.

Pentru a porni o sesiune VT<sub>xxx</sub> Telnet la sistemul la distanță, urmați acești pași:

1. Porniți Navigator System i și expandați **sistemul dumneavoastrȃ** → **Rețea**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și faceți clic pe **Tabela de gazde** pentru a afișa adresele Internet și numele gazdȃ.
3. Tastați comanda STRTCPTELN (Start TCP/IP TELNET - pornire TCP/IP Telnet), sau tastați TELNET Țn linia de comandȃ și apăsați Enter.
4. Tastați numele sistemului la distanță sau tastați \*INTERNETADR dacȃ preferați să utilizați adresa Internet. Dacȃ doriți să vedeți parametrii opționali, apăsați F10; altfel, apăsați Enter.

Dacȃ ați tastat \*INTERNETADR Țn câmpul **Sistem la distanță**, serverul vă promtează câmpul **Adresȃ Internet**.

5. Tastați adresa Internet a sistemului la distanță. Pentru a folosi parametrii opționali, apăsați F10; altfel, apăsați Enter. Ecranul afișează valori ale parametrilor opționali și informațiile privind adresa Internet.
6. Pentru a folosi valorile implicite ale parametrilor, apăsați Enter.
7. Țn timpul unei sesiuni Țn mod tot-ecranul VT<sub>xxx</sub>, următorii parametrii opționali sunt de asemenea aplicabili:

- Tabela de traducere ASCII de intrare (TBLVTIN)
- Tabela de traducere ASCII de ieșire (TBLVTOU)
- Tabelȃ specialȃ ieșire (TBLVTDRWO)
- Tabelȃ specialȃ intrare (TBLVTDRWI)
- Opțiuni selectate (VTOPT)
- Afișare atributele caracterului (DSPCHRATTR)
- Caracteristica defilare paginȃ (PAGESEROLL)
- Caracteristica de rȃspuns (ANSWERBACK)
- Stopuri Tab (TABSTOP)
- Timp de așteptare pentru gazdȃ (INZWAIT)
- Identificator set de caractere codate (CCSID)
- Mod de operare ASCII (ASCOPRMOD)-- se aplicȃ doar la inițializarea unei sesiuni VT220 (nu are nici un efect asupra negocierilor)
- Numȃrul portului aplicației server gazdȃ la distanță (PORT)
- Caractere de control (CTLCHAR)



**Notă:** Este posibil să apară caractere neașteptate din cauza configurării incorecte a sistemului la distanță. Dacă aceasta se întâmplă, verificați dacă valoarea tip stație de lucru este o valoare corespunzătoare pentru o stație de lucru în mod tot-ecranul VTxxx. De asemenea, puteți utiliza comanda setare termen pentru modificarea modului tot-ecranul al conexiunii.

Următorul ecran este ecranul de semnare pentru sistemul la distanță.

#### **Concepte înrudite**

“Considerente tot-ecranul VTxxx”

Ca pentru orice tip de emulare, trebuie să țineți cont de anumite considerente înainte de a utiliza modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet. Aceste considerații includ probleme de securitate, precum și condiții de eroare posibile și indicatoare luminoase. Puteți să înțelegeți mai bine cum să folosiți modul tot-ecranul VTxxx dacă vă familiarizați cu aceste considerente.

#### **Referințe înrudite**

“Controlarea funcțiilor server Telnet de la client” la pagina 48

Puteți folosi clientul Telnet pentru a controla procesarea stației de lucru de pe serverul Telnet când vă aflați într-o sesiune client.

“Valori cheie VTxxx” la pagina 63

Valori cheie VTxxx furnizează mapare de tastatură pentru suport al emulării VTxxx. Suportul sesiunii client pentru ambele moduri VT100 și VT220 oferă o mapare primară și alternativă de tastatură.

“Mod național VTxxx” la pagina 69

Modul național VTxxx suportă setul de caractere de înlocuire naționale, care este un grup de seturi de caractere pe 7 biți.

### **Considerente tot-ecranul VTxxx**

Ca pentru orice tip de emulare, trebuie să țineți cont de anumite considerente înainte de a utiliza modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet. Aceste considerații includ probleme de securitate, precum și condiții de eroare posibile și indicatoare luminoase. Puteți să înțelegeți mai bine cum să folosiți modul tot-ecranul VTxxx dacă vă familiarizați cu aceste considerente.

În plus față de preocupările de securitate, mai sunt multe alte preocupări de luat în considerare înainte de a folosi modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet. Când folosiți modul tot-ecranul VTxxx, trebuie să fiți conștienți de următoarele preocupări:

- “Considerente de securitate pentru modul tot-ecranul VTxxx”
- “Considerente pass-through Telnet și SNA 5250 pentru modul tot-ecranul VTxxx” la pagina 59
- “Procesarea cerere sistem pentru sesiuni VTxxx” la pagina 59
- “Condițiile de eroare la tastatura 5250” la pagina 59
- “Afișare suport pentru stații și VTxxx” la pagina 59
- “Diferențe operaționale între terminale VTxxx și 5250.” la pagina 60
- “Caracteristicile tastaturii” la pagina 60
- “Caracteristicile ecranului” la pagina 61
- “Dimensiunea ecranului VTxxx” la pagina 61
- “Atribute de caracter VTxxx” la pagina 61

### **Considerente de securitate pentru modul tot-ecranul VTxxx**

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.



## Considerente pass-through Telnet și SNA 5250 pentru modul tot-ecranul VT<sub>xxx</sub>

Platforma System i suportă pass-through 5250. Pass-through-ul 5250 este similar cu cel de la Telnet, dar rulează pe o rețea cu protocol SNA (Systems Network Architecture) mai degrabă decât pe o rețea IP. 5250 Pass-through folosește dispozitive virtuale pentru afișarea directă la dispozitivele fizice la fel cum face Telnet. În pass-through-ul 5250, sistemul crează automat dispozitive virtuale în același mod în care o face pentru Telnet. Prin urmare, valoarea de sistem dispozitive controlează numărul de dispozitive virtuale configurate automat pentru ambele pass-through-uri 5250 și Telnet.

### Procesarea cerere sistem pentru sesiuni VT<sub>xxx</sub>

Procesarea de cerere sistem pentru sesiuni VT<sub>xxx</sub> este puțin diferită decât cea a unei stații normale de lucru 5250.

Când se apasă tasta Cerere sistem la o stație de lucru 5250, o linie de comandă de cerere sistem apare în partea de jos a ecranului. Dacă apăsați tasta Enter, apare meniul Cerere sistem.

Pentru sesiuni VT<sub>xxx</sub> când apelați funcția cerere sistem, meniul Cerere sistem este afișat imediat.

### Condițiile 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 VT<sub>xxx</sub>, aceste erori produc un sunet de clopot în stația de lucru VT<sub>xxx</sub> și fac ca tastatura să rămână blocată.

Anumite aplicații i5/OS de asemea blochează tastatura 5250 și aprind indicatorul de inhibare intrare 5250. Utilizatorul trebuie să apese tasta de resetare eroare (Error Reset) înainte de a debloca tastatura. Pentru sesiuni VT<sub>xxx</sub>, blocarea tastaturii 5250 produce un sunet de clopot la terminalul VT<sub>xxx</sub> de fiecare dată când se apasă o tastă. Pentru a debloca tastatura, tasta VT<sub>xxx</sub> care este mapată pentru tasta Restare eroare trebuie apăsată. La maparea implicită de tastatură VT<sub>xxx</sub>, tasta CTL-R mapează la tasta Restare eroare.

### Afișare suport pentru stații și VT<sub>xxx</sub>

Când sistemul negociază suportul VT<sub>xxx</sub>, serverul Telnet transmite afișaje care sunt de un maxim de 24 de linii și 80 de coloane. Sistemul client VT<sub>xxx</sub> vede aceste afișaje în mare parte în același mod în care apar la 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 server VT<sub>xxx</sub> emulează indicatorul Sistem disponibil prin punerea unui asterisc la coloana 80 a linie 9. Pentru Așteptare mesaj, Mod inserare și indicatori inhibare intrare, asteriscul apare în coloana 80 la liniile 11, 13 sau 15. Când apare asteriscul, el este scris peste caracterul care era afișat anterior în acea locație a ecranului. Implicit, serverul VT<sub>xxx</sub> 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.

#### Note:

- La folosirea unui client VT<sub>xxx</sub> pentru a-l atașa la serverul Telnet, luați la cunoștință că indicatoarele Mod inserare și Inhibare intrare s-ar putea să nu fie afișate așa cum s-a descris mai sus. 5250 suportă atașamentul ca pe o funcție locală în timp ce VT<sub>xxx</sub> nu are o astfel de facilitare. Indicatorii Sistem disponibil și Așteptare mesaj, totuși, sunt afișați corect.
- Un ecran 5251 suportă un atribut de ecran cunoscut sub numele de separator de coloane. Separatorul de coloană este o linie verticală afișată între caractere. Această linie nu ocupă spațiul unui caracter. VT<sub>xxx</sub> nu

suportă un astfel de atribut. Dacă o aplicație i5/OS generează un afișaj care folosește atributul de separator coloană, ecranul este afișat pe sistemul client VTxxx cu separatorul de coloană mapat la atributul linie de subliniere VTxxx.

## Diferențe operaționale între terminale VTxxx și 5250.

Ca utilizator Telnet, ar trebui să Țineți cont de diferențele fizice și operaționale dintre terminalele VTxxx și 5250.

5250 este un terminal orientat bloc. Datele tastate pe un 5250 sunt acumulate într-un buffer și sunt trimise doar către platforma System i când este apăsată o tastă AID (attention identifier). Tasta AID pe o tastatură 5250 este tasta care inițiază o funcție. Lista următoare prezintă tastele 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 într-un mod 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 câte un caracter pe rând, iar dumneavoastră vedeți datele care sosesc sub forma unor fluxuri de caractere. La 5250, sistemul scrie datele în blocuri și tot sau doar o parte din ecran, se schimbă odată.

## Caracteristicile tastaturii

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

De exemplu, folosirea Telnet pentru sistemul System p și obținerea emulării VT220, comanda SMIT (System Management Interface Tool - unealta interfață gestionare sistem) furnizează o interfață de tip meniu la AIX. Aici tastele funcționale asociate cu cuvintele cheie \*CSRxx se comportă așa cum vă așteptați să o facă tastele de deplasare cursor. Totuși, tastele de mutare a cursorului 5250, în timp ce mișcă fizic cursorul în josul ecranului și selectează opțiunea SMIT, nu produce evidențierea (highlight) opțiunii selectate. Evidențierea în imagine inversată rămâne prima opțiune a meniului SMIT, indiferent de poziția tastelor.

Tastarea unui caracter de control la o tastatură este diferită de tastarea unui caracter de control la un terminal real VTxxx. La un terminal VTxxx, apăsați și Țineți apăsată tasta de control în timp ce apăsați caracterul asociat funcției de control.

La folosirea suportului Telnet, echivalentul se obține prin tastarea a unui indicator de control de 2 caractere, urmat de apăsarea tastei funcționale asociată cu funcția implicită \*SENDWOCR (Send without Carriage Return - trimitere fără început de linie) (tasta F11). De exemplu, dacă maparea implicită de tastatură și parametrii implicați ai comenzii STRTCPTELN sunt în efect, funcția Control-C VTxxx poate fi introdusă prin tastarea &C urmată de apăsarea tastei F11. <F12> poate de asemenea să introducă această funcție, prin folosirea mapării implicite de tastatură. În cazul în care folosiți o aplicație unde <F12> este remapat, acest exemplu este inclus și ilustrează principiul 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 ultimele caractere introduse înaintea apăsării tastei

funcționale \*SENDWOCR, dacă nu, caracterul &C nu este interpretat drept un caracter de control. Un caracter de control se transmite doar atunci când tasta funcțională \*SENDWOCR este apăsată. Puteți asigna caractere de control VTxxx des folosite 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 System p, sistemul de obicei negociază emularea VT220. Succesiunea Ctrl-C este una importantă în AIX pentru terminarea comenzilor care rulează timp îndelungat, precum PING. Este important ca dumneavoastră să știți cum să faceți asta înainte de a emite orice comandă System p. Implicit secvența este &C<F11>. Luați aminte că trebuie să introduceți rapid aceste taste, și ar putea să fie nevoie de mai multe încercări înainte ca taskulSystem p să accepte intrarea.

Dacă nu doriți să afișați caractere tastate, apăsați tasta funcțională care este asociată funcției \*HIDE (F6 în maparea implicită a tastaturii). 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 platforma System i, F9 deseori asigură această funcție. Pe AIX, aceasta poate fi activată prin tastarea comenzii `set -o vi` și apoi apăsarea Enter. După aceasta, puteți începe să găsiți comenzi cu secvența Esc-K. Pentru a realiza această secvență prin folosirea mapării implicite de tastatură în timpul unei emulări VTxxx, ar trebui să folosiți secvența <F5>k<F11>. Caracterul Esc începe căutarea comenzii. Apoi folosiți litera k pentru a extrage comenzi ulterioare. 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> dezactivează această funcție.

## Caracteristicile ecranului

Caracterul de pe poziția imediat din-naintea poziției cursorului este mereu blank. 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 linia 1, coloana 1 a ecranului nu funcționează la fel când se folosește suportul client Telnet. Majoritatea stațiilor de afișare de tipul 5250 nu permit intrări la linia 1, coloana 1. Dacă aplicații VTxxx poziționează cursorul pe linia 1, coloana 1, sistemul pune automat cursorul pe linia 1, 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 tot-ecranul VTxxx Telnet suportă următoarele dimensiuni de ecran:

- Pe stațiile de afișare 3180:
  - Ecranele 24 x 80 VTxxx ar trebui să afișeze ca 24 x 80.
  - Ecranele 24 x 132 VTxxx ar trebui să afișeze ca 24 x 132.
- Pe stațiile de afișare 5250:
  - Ecranele 24 x 80 VTxxx ar trebui să afișeze ca 24 x 80.
  - Ecranele 24 x 132 au nevoie ca tasta funcțională alocată pentru \*SHIFTDSP (F10 pe maparea implicită de tastatură) să deplaseze informațiile despre ecran la dreapta sau la stânga.

## Atribute de 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 astfel că o stație de afișare 5250 poate 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 inversare imagine 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. Subliniere și inversare imagine 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 se primesc date VTxxx care vor fi afișate cu atribute de caracter, octetul de atribut 5250 suprapune poziția înaintea 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 se poate aplica pentru ecranele care suportă atribute extinse precum ecranul 3477.

## Indicatorul de tastatură VT100

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

### Concepte înrudite

“Pornirea unei sesiuni client VTxxx” la pagina 57

Puteți porni o sesiune client Telnet prin folosirea emulării VTxxx. Trebuie să porniți serverul Telnet de pe sistemul la distanță (sistemul la care doriți să vă conectați prin Telnet).

“Determinarea problemelor cu Telnet” la pagina 82

Aveți nevoie de informații de diagnostic pentru a depana Telnet, inclusiv o diagramă pentru analiza problemelor de sistem, și aveți nevoie de o listă de materiale când raportați probleme Telnet.

## Opțiuni de emulare VTxxx

Când folosiți modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet, sunt câteva proceduri opționale pe care le puteți aplica pentru a personaliza tipul de emulare. Puteți să afișați maparea curentă de tastatură și apoi să vă decideți dacă doriți să o modificați. Puteți de asemenea să modificați caracterele de control când folosiți modul tot-ecranul VT220.

## Afișarea unei mapări de tastatură VTxxx

Pentru a afișa maparea curentă de tastatură, folosiți comanda DSPVTMAPT (Display VT Keyboard Map - afișare mapare de tastatură VT). Această comandă nu are parametri. Vă sunt arătate tastele VTxxx care sunt mapate funcțiilor i5/OS.

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

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 și prin utilizarea opțiunii 5 (Setare mapare de tastatură VT) din meniul 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 i5/OS.

## Modificarea unei mapări de tastatură VT<sub>xxx</sub>

Ca și SETVTMAP, comanda CHGVMTMAP (Change VT Keyboard Map - modificare mapare de tastatură VT) vă permite să personalizați maparea de tastatură când sunteți conectat la un server Telnet în modul VT<sub>xxx</sub>. În timp ce parametrii pentru comanda CHGVMTMAP sunt, implicit, valorile setate în acel moment. Exceptând această diferență, cele două comenzi sunt identice.

## Wrap automat VT<sub>xxx</sub>

Serverul VT<sub>xxx</sub> are nevoie ca clientul VT<sub>xxx</sub> să aibe pornită opțiunea de wrap automat (autowrap). Când autowrap este pornit, un caracter scris pe coloana 80 a VT<sub>xxx</sub> mută cursorul la coloana 1 a liniei următoare. Consultați documentația de client VT<sub>xxx</sub> pentru detalii despre cum să setați această opțiune.

## Caracterele 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 avea drept consecință interpretarea de către sistem a caracterelor succesive dintr-un flux de date drept date în legătură cu aceste caractere. Dacă sistemul negociază VT220 7-biți sau VT100, atunci intervalul întreg de caractere de la X'80' la X'F' este disponibil pentru translatare de caractere. 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, este posibil ca emularea VT220 pe 8 biți să nu funcționeze așa cum v-ați aștepta.

### Concepte înrudite

“Configurare server Telnet pentru mod tot-ecranul VT<sub>xxx</sub>” la pagina 27

Suportul pentru server VT<sub>xxx</sub> permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacă suportul tot-ecranul VT<sub>xxx</sub> este negociat.

### Referințe înrudite

“Valori cheie VT<sub>xxx</sub>”

Valori cheie VT<sub>xxx</sub> furnizează mapare de tastatură pentru suport al emulării VT<sub>xxx</sub>. Suportul sesiunii client pentru ambele moduri VT100 și VT220 oferă o mapare primară și alternativă de tastatură.

## Valori cheie VT<sub>xxx</sub>

Valori cheie VT<sub>xxx</sub> furnizează mapare de tastatură pentru suport al emulării VT<sub>xxx</sub>. Suportul sesiunii client pentru ambele moduri VT100 și VT220 oferă o mapare primară și alternativă de tastatură.

Pentru a adapta capabilitățile blocului de taste (keypad) VT220, puteți să vă salvați maparea tastaturii. Prin folosirea tastei F6 din ecranul Modificare Mapare tastatură VT<sub>xxx</sub>, puteți salva toate modificările aduse acestor mapări de tastatură pentru sesiuni ulterioare. Datele sunt salvate în profilul utilizator, și vor fi aplicate automat data următoare când emularea Telnet VT<sub>xxx</sub> este activată.

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 VT<sub>xxx</sub> care corespund tastei 5250 AID. Lista următoare dă numărul opțiunii și figurile corespunzătoare :

- Figurile Figura 1 la pagina 64 și Figura 2 la pagina 64 prezintă opțiunea 6 (Modificarea mapării de tastatură primară VT100).
- Figura 3 la pagina 65 și Figura 4 la pagina 65 prezintă opțiunea 7 (Modificarea mapării de tastatură alternativă VT100).
- Figura 5 la pagina 66 și Figura 6 la pagina 66 prezintă opțiunea 8 (Modificarea mapării de tastatură primară VT220).
- Figura 7 la pagina 67 și Figura 8 la pagina 67 prezintă opțiunea 9 (Modificarea mapării de tastatură alternativă VT220).

Nivelul de suport negociat între platforma System i și serverul Telnet determină care opțiuni sunt afișate în meniul Trimitere funcții de control Telnet. 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 nici o diferență între valorile implicite ale mapărilor de tastatură VT100 primară și alternativă.

Următoarele figuri arată mapările implicite ale tastaturii. Puteți schimba oricare dintre valori. Dacă apăsați tasta Enter, modificările dumneavoastră sunt salvate doar pentru sesiunea curentă. Dacă apăsați F6 (Salvare), modificările dumneavoastră sunt salvate permanent și au efect începând cu următoarea dată când porniți o sesiune Telnet VTxxx.

```
Modificarea mapării de tastatură primară VT100
Tastați modificările, apăsați Enter:
Tastă 5250          Funcție VT100
Tasta funcțională 1 . . . *PF1
Tasta funcțională 2 . . . *PF2
Tasta funcțională 3 . . . *PF3
Tasta funcțională 4 . . . *PF4
Tasta funcțională 5 . . . *ESC
Tasta funcțională 6 . . . *HIDE
Tasta funcțională 7 . . . *TAB
Tasta funcțională 8 . . . *CTLA
Tasta funcțională 9 . . . *CTLB
Tasta funcțională 10 . . *SHIFTDSP
Tasta funcțională 11 . . *SENDWOCR
Tasta funcțională 12 . . *CTLC
Tasta funcțională 13 . . *CSRUP
Tasta funcțională 14 . . *CSRDOWN
Tasta funcțională 15 . . *CSRRIGHT
Tasta funcțională 16 . . *CSRLEFT

More...

F3=Ieșire  F6=Salvare  F12=Anulare
```

Figura 1. Modificarea mapării de tastatură primară VT100 (Ecran 1)

```
Modificarea mapării de tastatură primară VT100
Tastați modificările, apăsați Enter:
Tastă 5250          funcție VT100
Tasta funcțională 17 . . *CTLD
Tasta funcțională 18 . . *CTLE
Tasta funcțională 19 . . *CTLF
Tasta funcțională 20 . . *CTLG
Tasta funcțională 21 . . *CTLH
Tasta funcțională 22 . . *CTLI
Tasta funcțională 23 . . *CTLJ
Tasta funcțională 24 . . *CTLK
Tasta rollup . . . . . *CTLL
Tasta rolldown . . . . . *CTLM

Bottom

F3=Ieșire  F6=Salvare  F12=Anulare
```

Figura 2. Modificarea mapării de tastatură primară VT100 (Ecran 2)

```

                                Modificarea mapării de tastatură alternativă VT100
Tastați modificările, apăsați Enter:
Tastă 5250                      funcție VT100
Tasta funcțională 1 . . .      *PF1
Tasta funcțională 2 . . .      *PF2
Tasta funcțională 3 . . .      *PF3
Tasta funcțională 4 . . .      *PF4
Tasta funcțională 5 . . .      *ESC
Tasta funcțională 6 . . .      *HIDE
Tasta funcțională 7 . . .      *TAB
Tasta funcțională 8 . . .      *CTLA
Tasta funcțională 9 . . .      *CTLB
Tasta funcțională 10 . . .     *SHIFTDSP
Tasta funcțională 11 . . .     *SENDWOCR
Tasta funcțională 12 . . .     *CTLC
Tasta funcțională 13 . . .     *CSRUP
Tasta funcțională 14 . . .     *CSRDOWN
Tasta funcțională 15 . . .     *CSRRIGHT
Tasta funcțională 16 . . .     *CSRLEFT

                                More...

F3=Ieșire  F6=Salvare  F12=Anulare

```

Figura 3. Modificarea mapării de tastatură alternativă VT100 (Ecranul 1)

```

                                Modificarea mapării de tastatură alternativă VT100
Tastați modificările, apăsați Enter:
Tastă 5250                      funcție VT100
Tasta funcțională 17 . . .     *CTLD
Tasta funcțională 18 . . .     *CTLE
Tasta funcțională 19 . . .     *CTLF
Tasta funcțională 20 . . .     *CTLG
Tasta funcțională 21 . . .     *CTLH
Tasta funcțională 22 . . .     *CTLI
Tasta funcțională 23 . . .     *CTLJ
Tasta funcțională 24 . . .     *CTLK
Tasta rollup . . . . .         *CTLL
Tasta rolldown . . . . .       *CTLM

                                Bott

F3=Ieșire  F6=Salvare  F12=Anulare

```

Figura 4. Modificarea mapării de tastatură primară VT100 (Ecranul 2)

Puteți comuta între mapările primară și alternativă în timpul unei sesiuni VTxxx prin folosirea tastei funcționale asignată cuvintelor cheie \*KEYPRI și \*KEYALT. Puteți alocă aceste cuvinte cheie oricăror taste funcționale 5250 disponibile. Este recomandat să alocați \*KEYPRI la tasta funcțională 5250 Page Up și \*KEYALT la tasta funcțională 5250 Page Down pentru ambele mapări de tastatură: principală și alternativă.

```
Modificarea mapării de tastatură primară VT220
Tastați modificările, apăsați Enter:
Tastă 5250          funcție VT220
Tasta funcțională 1 . . . *PF1
Tasta funcțională 2 . . . *PF2
Tasta funcțională 3 . . . *PF3
Tasta funcțională 4 . . . *PF4
Tasta funcțională 5 . . . *ESC
Tasta funcțională 6 . . . *HIDE
Tasta funcțională 7 . . . *TAB
Tasta funcțională 8 . . . *CTLA
Tasta funcțională 9 . . . *CTLB
Tasta funcțională 10 . . *SHIFTDSP
Tasta funcțională 11 . . *SENDWOCR
Tasta funcțională 12 . . *CTLC
Tasta funcțională 13 . . *CSRUP
Tasta funcțională 14 . . *CSRDOWN
Tasta funcțională 15 . . *CSRRIGHT
Tasta funcțională 16 . . *CSRLEFT

More...

F3=Ieșire  F6=Salvare  F12=Anulare
```

Figura 5. Modificarea mapării de tastatură VT220 (Ecranul 1)

```
Modificarea mapării de tastatură primară VT220
Tastați modificările, apăsați Enter:
Tastă 5250          funcție VT220
Tasta funcțională 17 . . *CTLD
Tasta funcțională 18 . . *CTLE
Tasta funcțională 19 . . *CTLF
Tasta funcțională 20 . . *CTLG
Tasta funcțională 21 . . *CTLH
Tasta funcțională 22 . . *CTLI
Tasta funcțională 23 . . *CTLJ
Tasta funcțională 24 . . *CTLK
Page up (rolldown) . *KEYPRI
Page down (rollup) . *KEYALT

Bottom

F3=Ieșire  F6=Salvare  F12=Anulare
```

Figura 6. Modificarea mapării de tastatură VT220 (Ecranul 2)



```

Modificarea mapării de tastatură alternativă VT220
Tastați modificările, apăsați Enter:
Tastă 5250                funcție VT220
Tasta funcțională 1 . . . *PF1
Tasta funcțională 2 . . . *PF2
Tasta funcțională 3 . . . *PF3
Tasta funcțională 4 . . . *PF4
Tasta funcțională 5 . . . *ESC
Tasta funcțională 6 . . . *HIDE
Tasta funcțională 7 . . . *TAB
Tasta funcțională 8 . . . *CTLA
Tasta funcțională 9 . . . *CTLB
Tasta funcțională 10 . . . *SHIFTDSP
Tasta funcțională 11 . . . *SENDWOCR
Tasta funcțională 12 . . . *CTLC
Tasta funcțională 13 . . . *CSRUP
Tasta funcțională 14 . . . *CSRDOWN
Tasta funcțională 15 . . . *CSRRIGHT
Tasta funcțională 16 . . . *CSRLEFT

More...

F3=Ieșire  F6=Salvare  F12=Anulare

```

Figura 7. Modificarea mapării de tastatură alternativă VT220 (Ecranul 1)

```

Modificarea mapării de tastatură alternativă VT220
Tastați modificările, apăsați Enter:
Tastă 5250                funcție VT220
Tasta funcțională 17 . . *CTLD
Tasta funcțională 18 . . *FINDKEY
Tasta funcțională 19 . . *INSERTKEY
Tasta funcțională 20 . . *REMOVEKEY
Tasta funcțională 21 . . *SELECTKEY
Tasta funcțională 22 . . *PREVSCN
Tasta funcțională 23 . . *NEXTSCN
Tasta funcțională 24 . . *CTLK
Tasta rollup . . . . . *KEYPRI
Tasta rolldown . . . . . *KEYALT

Bottom

F3=Ieșire  F6=Salvare  F12=Anulare

```

Figura 8. Modificarea mapării de tastatură alternativă VT220 (Ecranul 2)

Puteți introduce mai multe tipuri de informații VTxxx pentru a modifica maparea tastaturii. Mai jos sunt câteva exemple:

**Date character:** Puteți alocă un șir de caractere la o tastă funcțională. De exemplu, presupuneți că vă aflați pe un model System i și folosiți Telenet pentru a stabili o conexiune cu un sistem System p. Pentru a alocă șirul de caractere `set term=vt100` următoarei taste funcționale:

```
Tasta funcțională 24 .. *CTLK
```

Din sistem puteți tasta:

```
Tasta funcțională 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 asociat acelei taste funcționale transmite către sistemul de la distanță cu caracterele începutul de linie, linie nouă 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 alocați șirul de caractere corespunzător unei comenzi des folosite la o tastă funcțională. Datele de caracter pe care le tastați sunt mapate din EBCDIC în ASCII, înainte de transmisia către sistemul la distanță.

**Cuvinte cheie tastă de control:** Puteți asigna o apăsare de tastă de control VTxxx unei taste funcționale prin folosirea unui cuvânt cheie definit. De exemplu, dacă ați vrut să asignați o altă apăsare de tastă de control VTxxx următoarelor taste funcționale:

Tasta funcțională 24 . . \*CTLK

Puteți tasta:

Tasta funcțională 24 . . \*CTLZ

Când apăsați tasta funcțională, noul caracter de control alocat 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 alocă 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 alocă un șir hexazecimal, tastați X urmat de un șir de caractere hexazecimale între apostrofuri, de exemplu, X'IAIA'. Datele hexazecimale nu sunt mapate înainte de a fi trimise sistemului la distanță.

**Funcții de control i5/OS locale:** Puteți asigna un cuvânt cheie pentru a fi tratat local în cadrul sesiunii de client Telnet. Este posibil ca aceste alocări sau mapări să nu aibă ca rezultat transmiterea traficului de flux de date ASCII către sesiunea serverului Telnet la distanță. Aceste funcții de control local sunt \*HIDE, \*SHIFTDSP, \*KEYPRI și \*KEYALT. Funcția de trimis fără CR (\*SENDWOCR) este, de asemenea, o funcție locală, dar în acest caz, fluxurile de date ASCII sunt transmise sesiunii server Telnet la distanță.

#### Concepte înrudite

“Pornirea unei sesiuni client VTxxx” la pagina 57

Puteți porni o sesiune client Telnet prin folosirea emulării VTxxx. Trebuie să porniți serverul Telnet de pe sistemul la distanță (sistemul la care doriți să vă conectați prin Telnet).

#### Referințe înrudite

“Opțiuni de emulare VTxxx” la pagina 62

Când folosiți modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet, sunt câteva proceduri opționale pe care le puteți aplica pentru a personaliza tipul de emulare. Puteți să afișați maparea curentă de tastatură și apoi să vă decideți dacă doriți să o modificați. Puteți de asemenea să modificați caracterele de control când folosiți modul tot-ecranul VT220.

#### Suport limbă națională VTxxx:

Suportul NLS (national language support) VTxxx oferă metode alternative de selectare a mapărilor de caractere între client și sistemele cu emulare VTxxx.

Aceste metode sunt:

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

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

**Notă:** Suportul VTxxx este limitat la un subset de limbi SBCS (single-byte character set). O listă cu limbile suportate se găsește mai târziu în acest subiect. Oricare dintre aceste tabele suportate de traducere limbă pe un singur

octet poate fi modificată pentru maparea oricărei limbi pe un singur octet care este preferată, apoi identificată în parametrul corespunzător pentru pornirea Clientului 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.

### **Modul multinațional VT<sub>xxx</sub>**

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.

### **Mod național VT<sub>xxx</sub>:**

Modul național VT<sub>xxx</sub> suportă setul de caractere de înlocuire naționale, 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
- Engleza S.U.A.

Pentru a folosi modul național, sistemul necesită tabele de mapare pentru a mapa datele ASCII de intrare în EBCDIC (Extended Binary Coded Decimal Interchange Code) și datele EBCDIC de ieșire în ASCII când se lucrează în modul tot-ecranul VT<sub>xxx</sub>.

Folosiți parametrul CCSID (coded character set identifier) în comanda Telnet pentru a selecta un mod național, care este o tabelă NLS de mapare.

Introducerea unei valori numerice care reprezintă o valoare CCSID înregistrată în intervalul de la 1 la 65 553 este o metodă de identificare a tabelii de mapare corespunzătoare. Cartea AS/400 International Application Development

V4R2  conține detalii de CCSID-uri 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 bază de 7 biți, pot conține doar caracterele unice dintr-o regiune. 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 de sistem se află în biblioteca QUSRSYS.

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

Aici sunt indicațiile pentru tabela de ieșire (EBCDIC-în-ASCII):

- ID-ul paginii de cod DE LA este luat de la ID-ul paginii de cod din QCHRID al descrierii de mesaj CPX8416 (folosiți WRKMSGD CPX8416 pentru a afișa), 37 în figura următoare de la un sistem bazat pe engleza americană.
- Setul de caractere și pagina de cod LA sunt derivate din parametrul CCSID folosit cu comanda Telnet.

Aici sunt indicațiile pentru tabela de intrare (ASCII-în-EBCDIC):

- ID-ul paginii de cod DE LA este derivat din parametrul CCSID folosit cu comanda Telnet.
- Setul caractere și pagina de cod LA sunt luate de la ID-ul setului de caractere și ID-ul paginii de cod din QCHRID al descrierii de mesaj CPX8416 (folosiți WRKMSGD CPX8416 pentru a afișa), 697 și 37 în figura următoare de la un sistem bazat pe engleza americană.

```

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
    
```

Figura 9. Exemplu mesaj CPX8416

CCSID	ID real set de caractere	ID tabelă set de caractere	ID real pagină de cod	ID real pagină de cod
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 un QCHRID de 697 285 (setul de caractere 697 pagina de cod 285) în mesajul CPX8416 care utilizează Telnet cu CCSID(\*BRITISH), tabellele vor purta numele următoare:

- Ieșire (EBCDIC-la-ASCII) Q285A06A5V

- Intrare (ASCII-la-EBCDIC) QA5V697285

### Tabelele de mapare definite de 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 (TBLVTOU) și intrare ASCII-la-EBCDIC (TBLVTIN) ai comenzii STRTCPTLN. Puteți să specificați o tabelă de mapare definită de utilizator fie pentru tabela de mapare de ieșire, fie pentru tabela de mapare de intrare, iar apoi să utilizați valoarea sistem implicită pentru cealaltă.

#### Concepte înrudite

“Pornirea unei sesiuni client VTxxx” la pagina 57

Puteți porni o sesiune client Telnet prin folosirea emulării VTxxx. Trebuie să porniți serverul Telnet de pe sistemul la distanță (sistemul la care doriți să vă conectați prin Telnet).

#### Tastatura numerică:

Aici sunt tastele din blocul auxiliar de taste care în mod normal transmit codurile pentru zecimale, punct zecimal, semne minus și virgule.

Tabela 13. Taste de pe blocul de taste auxiliar

Cuvânt cheie	Mod	Caracter hexazecimal transmis	Descrierea caracterelor de control
*NUM0	Mod VT52	X'30' sau X'1B3F70 <sup>1</sup>	Tasta 0 a tastaturii numerice
*NUM0	Modul pe 7 biți VT100 sau VT220	X'30' sau X'1B4F70 <sup>1</sup>	Tasta 0 a tastaturii numerice
*NUM0	Modul pe 8 biți VT220	X'30' sau X'8F70 <sup>2</sup>	Tasta 0 a tastaturii numerice
*NUM1	Mod VT52	X'31' sau X'1B3F71 <sup>1</sup>	Tasta 1 a tastaturii numerice
*NUM1	Modul pe 7 biți VT100 sau VT220	X'31' sau X'1B4F71 <sup>1</sup>	Tasta 1 a tastaturii numerice
*NUM1	Modul pe 8 biți VT220	X'31' sau X'8F71 <sup>2</sup>	Tasta 1 a tastaturii numerice
*NUM2	Mod VT52	X'32' sau X'1B3F72 <sup>1</sup>	Tasta 2 a tastaturii numerice
*NUM2	Modul pe 7 biți VT100 sau VT220	X'32' sau X'1B4F72 <sup>1</sup>	Tasta 2 a tastaturii numerice
*NUM2	Modul pe 8 biți VT220	X'32' sau X'8F72 <sup>2</sup>	Tasta 2 a tastaturii numerice
*NUM3	Mod VT52	X'33' sau X'1B3F73 <sup>1</sup>	Tasta 3 a tastaturii numerice
*NUM3	Modul pe 7 biți VT100 sau VT220	X'33' sau X'1B4F73 <sup>1</sup>	Tasta 3 a tastaturii numerice
*NUM3	Modul pe 8 biți VT220	X'33' sau X'8F73 <sup>2</sup>	Tasta 3 a tastaturii numerice
*NUM4	Mod VT52	X'34' sau X'1B3F74 <sup>1</sup>	Tasta 4 a tastaturii numerice
*NUM4	Modul pe 7 biți VT100 sau VT220	X'34' sau X'1B4F74 <sup>1</sup>	Tasta 4 a tastaturii numerice
*NUM4	Modul pe 8 biți VT220	X'34' sau X'8F74 <sup>2</sup>	Tasta 4 a tastaturii numerice
*NUM5	Mod VT52	X'35' sau X'1B3F75 <sup>1</sup>	Tasta 5 a tastaturii numerice
*NUM5	Modul pe 7 biți VT100 sau VT220	X'35' sau X'1B4F75 <sup>1</sup>	Tasta 5 a tastaturii numerice
*NUM5	Modul pe 8 biți VT220	X'35' sau X'8F75 <sup>2</sup>	Tasta 5 a tastaturii numerice
*NUM6	Mod VT52	X'36' sau X'1B3F76 <sup>1</sup>	Tasta 6 a tastaturii numerice

Tabela 13. Taste de pe blocul de taste auxiliar (continuare)

Cuvânt cheie	Mod	Caracter hexazecimal transmis	Descrierea caracterelor de control
*NUM6	Modul pe 7 biți VT100 sau VT220	X'36' sau X'1B4F76' <sup>1</sup>	Tasta 6 a tastaturii numerice
*NUM6	Modul pe 8 biți VT220	X'36' sau X'8F76' <sup>2</sup>	Tasta 6 a tastaturii numerice
*NUM7	Mod VT52	X'37' sau X'1B3F77' <sup>1</sup>	Tasta 7 a tastaturii numerice
*NUM7	Modul pe 7 biți VT100 sau VT220	X'37' sau X'1B4F77' <sup>1</sup>	Tasta 7 a tastaturii numerice
*NUM7	Modul pe 8 biți VT220	X'37' sau X'8F77' <sup>2</sup>	Tasta 7 a tastaturii numerice
*NUM8	Mod VT52	X'38' sau X'1B3F78' <sup>1</sup>	Tasta 8 a tastaturii numerice
*NUM8	Modul pe 7 biți VT100 sau VT220	X'38' sau X'1B4F78' <sup>1</sup>	Tasta 8 a tastaturii numerice
*NUM8	Modul pe 8 biți VT220	X'38' sau X'8F78' <sup>2</sup>	Tasta 8 a tastaturii numerice
*NUM9	Mod VT52	X'39' sau X'1B3F79' <sup>1</sup>	Tasta 9 a tastaturii numerice
*NUM9	Modul pe 7 biți VT100 sau VT220	X'39' sau X'1B4F79' <sup>1</sup>	Tasta 9 a tastaturii numerice
*NUM9	Modul pe 8 biți VT220	X'39' sau X'8F79' <sup>2</sup>	Tasta 9 a tastaturii numerice
*NUMMINUS	Mod VT52	X'2D' sau X'1B3F6D' <sup>1</sup>	Tasta minus a tastaturii numerice
*NUMMINUS	Modul pe 7 biți VT100 sau VT220	X'2D' sau X'1B4F6D' <sup>1</sup>	Tasta minus a tastaturii numerice
*NUMMINUS	Modul pe 8 biți VT220	X'2D' sau X'8F6D' <sup>2</sup>	Tasta minus a tastaturii numerice
*NUMCOMMA	Mod VT52	X'2C' sau X'1B3F6C' <sup>1</sup>	Tasta virgulă a tastaturii numerice
*NUMCOMMA	Modul pe 7 biți VT100 sau VT220	X'2C' sau X'1B4F6C' <sup>1</sup>	Tasta virgulă a tastaturii numerice
*NUMCOMMA	Modul pe 8 biți VT220	X'2C' sau X'8F6C' <sup>2</sup>	Tasta virgulă a tastaturii numerice
*NUMPERIOD	Mod VT52	X'2E' sau X'1B3F6E' <sup>1</sup>	Tasta punct a tastaturii numerice
*NUMPERIOD	Modul pe 7 biți VT100 sau VT220	X'2E' sau X'1B4F6E' <sup>1</sup>	Tasta punct a tastaturii numerice
*NUMPERIOD	Modul pe 8 biți VT220	X'2E' sau X'8F6E' <sup>2</sup>	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' <sup>2</sup>	Tasta PF1 a tastaturii numerice
*PF2	Mod VT52	X'1B51'	Tasta PF2 a tastaturii numerice
*PF2	Modul pe 7 biți VT100 sau VT220	X'1B4F51'	Tasta PF2 a tastaturii numerice
*PF2	Modul pe 8 biți VT220	X'8F51' <sup>2</sup>	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

Tabela 13. Taste de pe blocul de taste auxiliar (continuare)

Cuvânt cheie	Mod	Caracter hexazecimal transmis	Descrierea caracterelor de control
*PF3	Modul pe 8 biți VT220	X'8F52' <sup>2</sup>	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' <sup>2</sup>	Tasta PF4 a tastaturii numerice

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

<sup>2</sup>- Această secvență este o versiune scurtată a secvenței pe 7 biți. Fie este prezentat când operați în modul de 8-biți, care poate fi apelat de către serverul sau gazda la distanță VT220, sau îl puteți specifica în parametrul ASCOPRMOD al comenzii STRTCPTLN (Start TCP/IP TELNET - pornire TCP/IP Telnet).

#### Concepte înrudite

“Configurare server Telnet pentru mod tot-ecranul VTxxx” la pagina 27

Suportul pentru server VTxxx permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacă suportul tot-ecranul VTxxx este negociat.

#### Editarea blocului de taste (keypad):

Tabela arată tastele care transmit coduri pentru tasta editare bloc de taste.

Tabela 14. Tastele care transmit coduri pentru tastele din blocul de taste de editat

Cuvânt cheie	Mod	Caracter hexazecimal 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



Tabela 14. Tastele care transmit coduri pentru tastele din blocul de taste de editat (continuare)

Cuvânt cheie	Mod	Caracter hexazecimal transmis	Descrierea caracterelor de control
*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
*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 Find a tastaturii numerice
*FINDKEY	Modul pe 8 biți VT220	X'9B317E' <sup>1</sup>	Editarea tastei Find a tastaturii numerice
*INSERTKEY	Modul pe 7 biți VT220	X'1B5B327E'	Editarea tastei Insert Here a tastaturii numerice
*INSERTKEY	Modul pe 8 biți VT220	X'9B327E' <sup>1</sup>	Editarea tastei Insert Here a tastaturii numerice
*REMOVEKEY	Modul pe 7 biți VT220	X'1B5B337E'	Editarea tastei Remove a tastaturii numerice
*REMOVEKEY	Modul pe 8 biți VT220	X'9B337E' <sup>1</sup>	Editarea tastei Remove a tastaturii numerice
*SELECTKEY	Modul pe 7 biți VT220	X'1B5B347E'	Editarea tastei Select a tastaturii numerice
*SELECTKEY	Modul pe 8 biți VT220	X'9B347E' <sup>1</sup>	Editarea tastei Select a tastaturii numerice
*PREVSCN	Modul pe 7 biți VT220	X'1B5B357E'	Editarea tastei Prev Screen a tastaturii numerice
*PREVSCN	Modul pe 8 biți VT220	X'9B357E' <sup>1</sup>	Editarea tastei Prev Screen a tastaturii numerice
*NEXTSCN	Modul pe 7 biți VT220	X'1B5B367E'	Editarea tastei Next Screen a tastaturii numerice
*NEXTSCN	Modul pe 8 biți VT220	X'9B367E' <sup>1</sup>	Editarea tastei Next Screen a tastaturii numerice

**Notă:** Această secvență reprezintă o versiune scurtată a secvenței pe 7 biți. Este prezentat doar când operați în modul de 8-biți, care poate fi apelat de către serverul sau gazda la distanță VT220, sau îl puteți specifica în parametrul ASCOPRMOD al comenzii STRTCPTLN (Start TCP/IP TELNET - pornire TCP/IP Telnet).

#### Concepte înrudite

“Configurare server Telnet pentru mod tot-ecranul VTxxx” la pagina 27

Suportul pentru server VTxxx permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacă suportul tot-ecranul VTxxx este negociat.

### Valori de taste VTxxx prin funcție 5250:

Tabela descrie valoarea tastei VTxxx prin funcția 5250.

Tabela 15. Valori de taste VTxxx prin funcție 5250

Funcția 5250 implicită	Valoarea specială	Taste VTxxx	Valoarea hexazecimală <sup>1</sup>
Attn	*CTLA	<CTRL-A>	X'01'
Attn	*ESCA	<ESC><A>	X'1B41'
Backspace	*BACKSPC	<Backspace sau CTRL-H>	X'08'
Curățare ecran	*ESCC	<ESC><C>	X'1B43'
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 <sup>2</sup>
Ștergere	*RMV	<Înlăturare>	X'9B337E <sup>3</sup>
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 la câmp	*TAB	<TAB sau CTRL-I>	X'09'
Înapoi la 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 câmp	*ESCM	<ESC><M>	X'1B4D'
Ajutor	*CTLQST	<CTRL-Question Mark>	X'1F'
Ajutor	*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 <sup>2</sup>
Inserare	*INS	<Inserează aici>	X'9B327E <sup>3</sup>
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 <sup>2</sup>

Tabela 15. Valori de taste VTxxx prin funcție 5250 (continuare)

Funcția 5250 implicită	Valoarea specială	Taste VTxxx	Valoarea hexazecimală <sup>1</sup>
Page Down (Roll Up)	*NXTSCR	<Ecranul următor>	X'9B367E' <sup>3</sup>
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' <sup>2</sup>
Page Up (Roll Down)	*PRVSCR	<Ecranul precedent>	X'9B357E' <sup>3</sup>
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'
Cerere test	*CTLT	<CTRL-T>	X'14'
Comutare indicatoare luminoase	*ESCT	<ESC><T>	X'1B54'
F1	*ESC1	<ESC><1>	X'1B31'
F1	*F1	<F1> <sup>5</sup>	X'1B5B31317E' <sup>2</sup>
F1	*F1	<F1> <sup>5</sup>	X'9B31317E' <sup>3</sup>
F1	*PF1	<PF1>	X'1B4F50' <sup>2</sup>
F1	*PF1	<PF1>	X'8F50' <sup>3</sup>
F2	*ESC2	<ESC><2>	X'1B32'
F2	*F2	<F2> <sup>5</sup>	X'1B5B31327E' <sup>2</sup>
F2	*F2	<F2> <sup>5</sup>	X'9B31327E' <sup>3</sup>
F2	*PF2	<PF2>	X'1B4F51' <sup>2</sup>
F2	*PF2	<PF2>	X'8F51' <sup>3</sup>
F3	*ESC3	<ESC><3>	X'1B33'
F3	*F3	<F3> <sup>5</sup>	X'1B5B31337E' <sup>2</sup>
F3	*F3	<F3> <sup>5</sup>	X'9B31337E' <sup>3</sup>
F3	*PF3	<PF3>	X'1B4F52' <sup>2</sup>
F3	*PF3	<PF3>	X'8F52' <sup>3</sup>
F4	*ESC4	<ESC><4>	X'1B34'
F4	*F4	<F4> <sup>5</sup>	X'1B5B31347E' <sup>2</sup>
F4	*F4	<F4> <sup>5</sup>	X'9B31347E' <sup>3</sup>
F4	*PF4	<PF4>	X'1B4F53' <sup>2</sup>
F4	*PF4	<PF4>	X'8F53' <sup>3</sup>
F5	*ESC5	<ESC><5>	X'1B35'
F5	*F5	<F5> <sup>5</sup>	X'1B5B31357E' <sup>2</sup>
F5	*F5	<F5> <sup>5</sup>	X'9B31357E' <sup>3</sup>
F6	*ESC6	<ESC><6>	X'1B36'
F6	*F6	<F6>	X'1B5B31377E' <sup>2</sup>
F6	*F6	<F6>	X'9B31377E' <sup>3</sup>

Tabela 15. Valori de taste VTxxx prin funcție 5250 (continuare)

Funcția 5250 implicită	Valoarea specială	Taste VTxxx	Valoarea hexazecimală <sup>1</sup>
F7	*ESC7	<ESC><7>	X'1B37'
F7	*F7	<F7>	X'1B5B31387E <sup>2</sup>
F7	*F7	<F7>	X'9B31387E <sup>3</sup>
F8	*ESC8	<ESC><8>	X'1B38'
F8	*F8	<F8>	X'1B5B31397E <sup>2</sup>
F8	*F8	<F8>	X'9B31397E <sup>3</sup>
F9	*ESC9	<ESC><9>	X'1B39'
F9	*F9	<F9>	X'1B5B32307E <sup>2</sup>
F9	*F9	<F9>	X'9B32307E <sup>3</sup>
F10	*ESC0	<ESC><0>	X'1B30'
F10	*F10	<F10>	X'1B5B32317E <sup>2</sup>
F10	*F10	<F10>	X'9B32317E <sup>3</sup>
F11	*ESCMINUS	<ESC><Minus>	X'1B2D'
F11	*F11	<F11>	X'1B5B32337E <sup>2</sup>
F11	*F11	<F11>	X'9B32337E <sup>3</sup>
F12	*ESCEQ	<ESC><Egal>	X'1B3D'
F12	*F12	<F12>	X'1B5B32347E <sup>2</sup>
F12	*F12	<F12>	X'9B32347E <sup>3</sup>
F13	*ESCEXCL	<ESC><Exclamație>	X'1B21'
F13	*F13	<F13>	X'1B5B32357E <sup>2</sup>
F13	*F13	<F13>	X'9B32357E <sup>3</sup>
F14	*ESCAT	<ESC><semnul at (@)>	X'1B40'
F14	*F14	<F14>	X'1B5B32367E <sup>2</sup>
F14	*F14	<F14>	X'9B32367E <sup>3</sup>
F15	*ESCPOUND	<ESC><Liră sterlină>	X'1B23'
F15	*F15	<F15>	X'1B5B32387E <sup>2</sup>
F15	*F15	<F15>	X'9B32387E <sup>3</sup>
F16	*ESCDOLLAR	<ESC><Dollar>	X'1B24'
F16	*F16	<F16>	X'1B5B32397E <sup>2</sup>
F16	*F16	<F16>	X'9B32397E <sup>3</sup>
F17	*ESCPCT	<ESC><Procent>	X'1B25'
F17	*F17	<F17>	X'1B5B33317E <sup>2</sup>
F17	*F17	<F17>	X'9B33317E <sup>3</sup>
F18	*ESCCFX	<ESC><Accent circumflex>	X'1B5E <sup>1</sup>
F18	*F18	<F18>	X'1B5B33327E <sup>2</sup>
F18	*F18	<F18>	X'9B33327E <sup>3</sup>
F19	*ESCAMP	<ESC><Ampersand>	X'1B26'
F19	*F19	<F19>	X'1B5B33337E <sup>2</sup>
F19	*F19	<F19>	X'9B33337E <sup>3</sup>
F20	*ESCAST	<ESC><Asterisc>	X'1B2A'

Tabela 15. Valori de taste VTxxx prin funcție 5250 (continuare)

Funcția 5250 implicită	Valoarea specială	Taste VTxxx	Valoarea hexazecimală <sup>1</sup>
F20	*F20	<F20>	X'1B5B33347E' <sup>2</sup>
F20	*F20	<F20>	X'9B33347E' <sup>3</sup>
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	<Find>	X'1B5B317E'
Vezi nota 4	*FIND	<Find>	X'9B317E'
Vezi nota 4	*SELECT	<Select>	X'1B5B347E'
Vezi nota 4	*SELECT	<Select>	X'9B347E'

**Note:**

- <sup>1</sup> - Doar dacă nu este identificată valoarea hexazecimală este în modul VT100.
- <sup>2</sup> - Mod de control VT220 pe 7 biți.
- <sup>3</sup> - Nu este nici o tastă funcțională 5250 care mapează această tastă VT.
- <sup>4</sup> - 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.

**Concepte înrudite**

“Configurare server Telnet pentru mod tot-ecranul VTxxx” la pagina 27

Suportul pentru server VTxxx permite utilizatorilor client Telnet să se logheze și să ruleze aplicații tot-ecranul 5250, chiar dacă suportul tot-ecranul VTxxx este negociat.

**Moduri de operare ale stațiilor de lucru VT220:**

Mai multe moduri de operare sunt suportate în timp ce sistemul negociază tipul de stație de lucru VT220.

Aceste moduri de operare sunt după cum urmează:

- 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 națională (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, un mod inițial de operare pentru clientul Telnet este selectat prin folosirea parametrului ASCOPRMODE (ASCII operating mode - mod de operare ASCII al comenzii STRTCPTLN (start TCP/IP Telnet - pornire TCP/IP Telnet) sau TELNET.

**Tastele funcționale din linia de sus la VT220:**

Tabela descrie tastele care transmit codurile pentru tastele funcționale din rândul de sus al tastaturii VT220 în modul 7-biți.

*Tabela 16. Tastele funcționale din linia de sus la VT220*

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'

Tabela descrie tastele care transmit codurile pentru tastele funcționale din rândul de sus al tastaturii VT220 în modul 8-biți.

*Tabela 17. Taste funcționale din rândul de sus VT220 în modul 8-biți*

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

**Cuvintele cheie pentru caracterele de control VT100 și VT220:**

Cuvintele cheie pentru caracterele de control VT100 și VT220 sunt listate în tabelă.

Tabela 18. Cuvintele cheie pentru caracterele de control VT100 și VT220

Descrierea caracterelor de control	Tastă+CTRL	Cuvânt cheie	Caracter hexazecimal 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'
Interogare	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'
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 cascadeate Telnet

Puteți stabili o altă sesiune Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați stabilit o sesiune cascadeată, vă puteți deplasa între diferitele sisteme.



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.

## Pornirea unei sesiuni cascadeate

Pentru a porni sesiunea dumneavoastră cascadeată, semnați-vă la sistemul gazdă, apoi parcurgeți pașii pentru stabilirea unei sesiuni client. Repetați pașii pentru fiecare sistem la care doriți să vă conectați.

## Întoarcerea la sistem

Comanda SIGNOFF încheie sesiunea și vă întoarce la ecranul de semnare al sistemului. Când sunteți semnat în sistem, comanda SIGNOFF încheie jobul curent de server și vă întoarce la ecranul de semnare al sistemului.

Puteți folosi parametrul ENDCNN (end connection - terminare conexiune) al comenzii SIGNOFF pentru a vă anula semnarea în sistem și să opriți conexiune 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.

### Note:

1. Nu există nici o limitare pentru numărul de sisteme cu care puteți stabili o sesiune Telnet.
2. Sistemul gazdă interceptează opțiunile 13 și 14 din Cererea Sistem dacă sunt introduse la linia de intrare a Cererii Sistem. Această funcție s-ar putea dovedi utilă dacă stabiliți o sesiune Telnet cu un sistem la care nu puteți să vă semnați. În acest caz, puteți termina o sesiune la sistemul respectiv prin parcurgerea pașilor următori:
  - 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.

### Concepte înrudite

“Scenariu Telnet: Sesiuni Telnet în cascadă” la pagina 3

Scenariul demonstrează abilitatea de a pornit sesiuni Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați fost conectat, puteți comuta între sisteme prin folosirea valori de cerere sistem.

“Pornirea unei sesiuni client Telnet” la pagina 49

Ar trebui să cunoașteți numele sau adresa Internet al sistemului la distanță cu care doriți să începeți sesiunea Telnet.

## Mutarea între sesiuni cascadeate Telnet

După ce ați pornit o sesiune cascadeată Telnet, apăsați tasta SysRq, și apăsați Enter pentru a afișa meniul Cerere sistem.

Meniul Cerere sistem vă oferă următoarele funcții.

Opțiune Cerere sistem	Acțiunea	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 dintr-un sistem intermediar sau terminal la meniul Cerere sistem din sistemul de bază
14	Transferul la sistemul de bază	Vă duce dintr-un sistem intermediar sau terminal la jobul alternativ de pe sistemul de bază
15	Transferul la sistemul terminal	Vă duce de la un sistem intermediar sau gazdă la sistemul terminal

Pentru a ocoli meniul Cerere sistem, apăsați tasta SysReq și tastați 10 în linia de comandă. Această scurtătură se poate aplica doar între platformele System i.

## Pentru clienții telnet non-IBM

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 opțiunea 11 din Cerere sistem pentru a vă deplasa înapoi din sistem în sistem până ajungeți la sistemul gazdă. Sistemul gazdă este primul sistem la care clientul dumneavoastră Telnet este conectat la începutul sesiunii.
2. De la sistemul gazdă, folosiți opțiunea 1 din Cerere sistem pentru a vă deplasa de la un sistem la altul.

### Concepte înrudite

“Scenariu Telnet: Sesiuni Telnet în cascadă” la pagina 3

Scenariul demonstrează abilitatea de a porni sesiuni Telnet în timp ce vă aflați într-o sesiune Telnet. După ce ați fost conectat, puteți comuta între sisteme prin folosirea valori de cerere sistem.

## Terminarea unei sesiuni client Telnet

Când sunteți conectat la o platformă System i, deconectarea nu închide în mod necesar sesiunea server 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. Apoi puteți tasta comanda pentru a încheia sesiunea.

- Din sistemul de operare i5/OS, apăsați tasta Atenție iar apoi selectați opțiunea 99 (Terminare sesiune TELNET - IEȘIRE).
- 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).

---

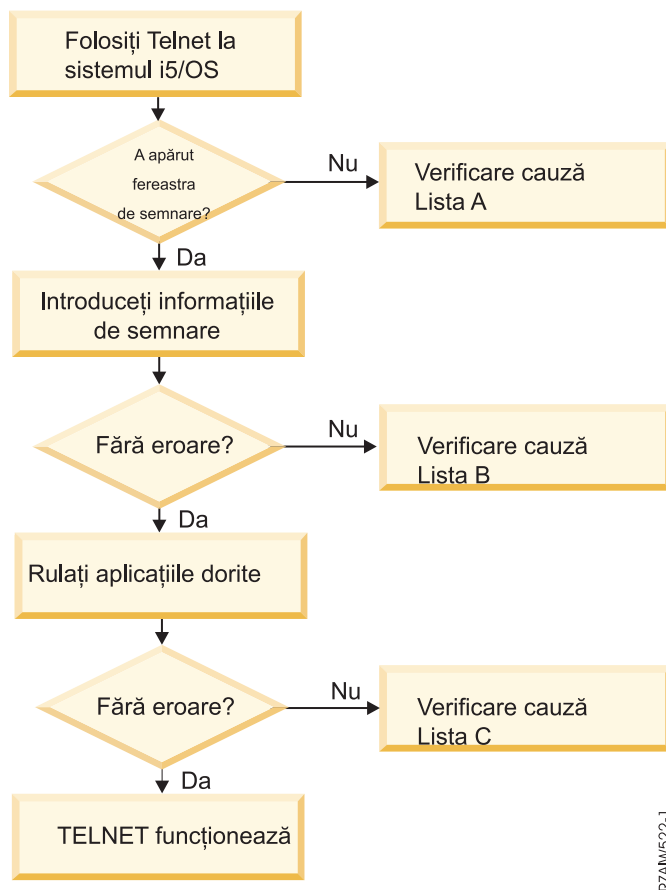
## Depanarea problemelor Telnet

Acest subiect conține informații despre depanarea și corectarea problemelor cu Telnet.

## Determinarea problemelor cu Telnet

Aveți nevoie de informații de diagnostic pentru a depana Telnet, inclusiv o diagramă pentru analiza problemelor de sistem, și aveți nevoie de o listă de materiale când raportați probleme Telnet.

Utilizați această diagramă după folosirea diagramei pentru probleme generale legate de TCP/IP. Dacă este detectată o problemă la folosirea serverului Telnet, folosiți diagrama pentru a identifica acea cauză. Listele de cauze care urmează după diagramă ar putea fi de folos la identificarea potențialelor probleme.



## Lista de cauze A

1. Verificați dacă joburile serverului Telnet sunt active și dacă serviciul Telnet este alocat unui port valid nerestricționat.
  - a. Pentru a verifica dacă joburile QTVTELNET și QTVDEVICE sunt active în subsistemul QSYSWRK, parcurgeți pașii următori:
    - 1) Porniți Navigator System i și expandați *sistemul dumneavoastră* → **Control funcționare**.
    - 2) Faceți clic dreapta pe **Joburi active** și uitați-vă dacă sunt active QTVTELNET și QTVDEVICE. Dacă sunt active, continuați cu pasul 1c.
  - b. Dacă aceste joburi nu sunt active, parcurgeți pașii următori pentru a porni aceste joburi:
    - 1) Porniți Navigator System i și expandați *sistemul dumneavoastră* → **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 System i și expandați *sistemul dumneavoastră* → **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 de porturi mergând în meniul CFGTCP și selectând opțiunea 4 (Lucrul cu restricțiile de porturi TCP/IP).
2. Verificați dacă valoarea de sistem dispozitive din sistem este setată corespunzător pentru a permite serverului Telnet pentru a crea automat dispozitive virtuale.
3. Verificați dacă conexiune rețelei dintre sistem și clientul Telnet este activ prin folosirea funcției Ping în Navigator System i. În cazul în care conexiunea nu este activă, consultați administratorul rețelei dumneavoastră.

4. Verificați dacă dispozitivele virtuale din sistem care sunt folosite de Telnet sunt definite unui subsistem sub care joburile interactive Telnet ar trebui să ruleze.
  - a. Pentru a vedea care intrări de stație de lucru sunt definite la un subsistem, parcurgeți pașii următori:
    - 1) Porniți Navigator System i și expandați **sistemul dumneavoastră** → **Control funcționare**.
    - 2) Faceți dublu clic pe **Subsisteme** și selectați **Deschidere**.
  - b. Utilizați comanda ADDWSE (Add Work Station Entry - Adăugare intrare stație de lucru) pentru definirea stațiilor de lucru la un subsistem. De exemplu, ați putea utiliza 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 nu sunt complete dacă subsistemul interactiv nu este activ. 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 System i și expandați **sistemul dumneavoastră** → **Control funcționare**.
  - b. Faceți dublu clic pe **Subsisteme** și selectați **Deschidere**.
  - c. Verificați dacă subsistemul este activ.
6. Dacă lucrați în modul ecran-întreg VTxxx, verificați dacă configurația de client local VTxxx specifică autowrap. Când autowrap este activat, 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 determinarea portului la care este alocat serviciul Telnet, parcurgeți pașii următori:

  - a. Porniți Navigator System i și expandați **sistemul dumneavoastră** → **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 job QTVTELNET pentru mesaje care indică dacă portul pe care încercați să-l folosiți nu este restricționat.
10. Când încercați să vă conectați prin folosirea Telnet SSL, asigurați-vă că aveți instalat DCM-ul (Digital Certificate Manager). Aceasta este în plus față de cele enumerate mai sus. De asemenea, asigurați-vă că un certificat valid, neexpirat este alocat 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 înregistrați în platforma System i, nu aveți autorizație pentru dispozitivul virtual de afișare. Când serverul Telnet crează dispozitive virtuale, valoare de sistem QCRTAUT este folosită pentru a determina autorizația 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. Dacă întâmpinați probleme la folosirea comenzii WRKFLR (Work with Folders - lucru cu foldere), s-ar putea să fiți nevoiți să vă modificați configurația astfel încât Office Adapted Editor este folosit în loc de Standard Editor. Pentru aceasta, rugați administratorul de sistem să vă schimbe alegerea procesorului de cuvinte din informațiile de mediu asociate cu ID-ul dumneavoastră de utilizator office.

2. Dacă lucrați în modul ecran-întreg VTxxx, verificați dacă configurația de client local VTxxx specifică autowrap. Când autowrap este activat, sistemul va face wrap automat la coloana 80.
3. Dacă nu sunt afișate corect caracterele pentru sesiunea dumneavoastră VTxxx, verificați dacă sunt folosite tabelele de mapare corecte pentru sesiune.
4. Dacă clientul dumneavoastră VTxxx dă bipuri de fiecare dată când apăsați o tastă, s-ar putea ca tastatura dumneavoastră să fie blocată.
5. Verificați istoricul de job QTVTELNET și istoricul de job QTVDEVICE pentru mesaje de eroare în sistem.

### Concepte înrudite

Valori de sistem: Privire generală dispozitive

“Considerente tot-ecranul VTxxx” la pagina 58

Ca pentru orice tip de emulare, trebuie să țineți cont de anumite considerente înainte de a utiliza modul tot-ecranul VTxxx cu serverul dumneavoastră Telnet. Aceste considerații includ probleme de securitate, precum și condiții de eroare posibile și indicatoare luminoase. Puteți să înțelegeți mai bine cum să folosiți modul tot-ecranul VTxxx dacă vă familiarizați cu aceste considerente.

## Descriere: Tabelul de analiză pentru probleme Telnet

Urmați acești pași pentru a determina ce listă de cauze să folosiți:

1. Telnet la sistemul de operare i5/OS.
2. V-a fost afișat un ecran de semnare? Dacă Da, continuați. Dacă Nu, consultați Lista de cauze A.
3. Introduceți informațiile de semnare.
4. Semnarea s-a făcut cu succes? Dacă Da, continuați. Dacă Nu, consultați Lista de cauze B.
5. Rulați aplicațiile necesare.
6. Aplicațiile au avut succes? Dacă Da, continuați. Dacă Nu, consultați Lista de cauze C.
7. Telnet funcționează.

## A face ping serverului dumneavoastră gazdă

Puteți folosi funcția Ping în Navigator System i pentru a testa conexiunea dumneavoastră TCP/IP.

Pentru a face ping sistemului dumneavoastră, completați următorii pași:

1. Porniți Navigator System i și expandați *sistemul dumneavoastră* → **Rețea**.
2. Faceți clic dreapta pe **Configurare TCP/IP** și selectați **Utilitare**.
3. Faceți clic pe **Ping** pentru a afișa caseta de dialog **Ping**.
4. Tastați nume gazdei dumneavoastră în caseta **Ping** (de exemplu, numecompanie.com).
5. Apăsați **Ping acum**.

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

### Operații înrudite

“Verificarea stării sistemului” la pagina 88

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

## Tipuri de depanare emulare

Când dezvoltați un client Telnet, este important să negociați tipul corect de stație de lucru de emulare. Funcțiile permise variază o dată cu tipul stației de lucru. Următorul ghid vă ajută să înțelegeți tipul de stație de lucru și capacitățile funcționale ale acelei stații de lucru.

## Negocierile și mapările tipului de 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 în partea de sus. Acesta este numele dispozitivului virtual de afișare asociat cu jobul dumneavoastră Implicit, convenția de numire este QPADEVxxxx, unde xxxx sunt caractere alfanumerice.

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 19. Mapările imprimantei și stației 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
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) <sup>2</sup>	3487 (HG) <sup>2</sup> 3487 (HW) <sup>2</sup>	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) <sup>2</sup>		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.

Tabela 19. Mapările imprimantei și stației de lucru (continuare)

Stația de lucru suportată și (model)	Tipul echivalent și (model)	Specificația Internet	Descriere
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) <sup>3</sup>	3277 (DHCF)	IBM-3277-2	Monitor monocrom 24 X 80
3277 (0) <sup>3,4</sup>	3278 (DHCF)	IBM-3278-2	Monitor monocrom 24 X 80
3278 (0) <sup>3</sup>		IBM-3278-2-E <sup>5</sup>	Monitor monocrom 24 x 80
3278 (0) <sup>3</sup>		IBM-3278-3	Monitor monocrom 24 x 80
3278 (0) <sup>3</sup>		IBM-3278-4	Monitor monocrom 24 x 80
3278 (0) <sup>3</sup>		IBM-3278-5	Monitor monocrom 24 x 80
3279 (0) <sup>3</sup>	3279 (DHCF)	IBM-3279-2 IBM-3279-2-E <sup>5</sup>	Monitor monocrom 24 X 80
3279 (0) <sup>3</sup>		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) <sup>6</sup>		DEC-VT100 VT100(7) VT102 DEC-VT102 DEC-VT200 DEC-VT220 VT200(7) VT220(7)	Monitor monocrom ASCII 24 x 80

**Considerente:**

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

<sup>2</sup> Această stație de lucru poate fi configurată fie 24 x 80, fie 27 x 132. Trebuie să stabiliți modul stației de lucru înainte de setarea valorii parametrului tip de stație de lucru.

<sup>3</sup> Sistemul suportă doar ecrane de 24 X 80 în stații de lucru 327x de la distanță. Stațiile de lucru 3277 de la distanță (atât DHCF-uri (distributed host command facility) cât și obișnuite) sunt mapate pe IBM-3277-2. Stațiile de la distanță 3278 sunt mapate pe IBM-3278-2. Stațiile de lucru la distanță 3279 sunt mapate la IBM-3279-2.

<sup>4</sup> Unele pachete de emulare tot-ecranul Telnet 3270 (TN3270) sau 3278-2 nu suportă corect câmpuri cu structură scrisă. Din această cauză, dispozitivele de tipul 3278-2 sunt mapate pe dispozitive 3277-2 de către implementarea serverului Telnet pentru a permite sistemului să lucreze cu acele implementări TN3270.

<sup>5</sup> Este suportată evidențierea atributelor extinse. Sublinierea, clipirea și imaginea inversată sunt incluse. De asemenea, este suportată și procesarea 3270 DBCS.



<sup>6</sup> Dispozitivul virtual VT100 suportă dispozitive VT220.

<sup>7</sup> VT100, VT200 și VT220 nu reprezintă nume oficiale pentru tipurile de terminal. Totuși, câteva implementări negociază folosind aceste nume ca valoare pentru tipul de terminal.

#### **Referințe înrudite**

“INIT0100: Formatul informației de descriere a conexiunii” la pagina 45

Acest subiect conține informații despre conexiune client pe care programul de ieșire o poate folosi.

## **Depanarea serverului dumneavoastră SSL Telnet**

Aici sunt pașii detaliați pentru depanarea serverului SSL (Secure Sockets Layer) inclusiv coduri de retur sistem SSL și o listă cu problemelor SSL obișnuite.

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

1. Controlați starea sistemului dumneavoastră pentru a verifica dacă a fost 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 activ, utilizând comanda NETSTAT \*CNN.
5. Examinați istoricul jobului Telnet pentru a găsi codul de retur SSL.
6. Căutați în Probleme SSL și coduri de retur pentru sugestii în rezolvarea problemei.

Certificatele digitale incorecte pot provoca multe probleme cu SSL. DCM-ul (Digital Certificate Manager) va permite să vă modificați CA-ul (certificate authority) sau certificate de sistem. Pentru a confirma că aveți un certificat valid de sistem, citiți despre cum să porniți DCM (Digital Certificate Manager) iar apoi vedeți certificatul de sistem.

#### **Concepte înrudite**

“Securizare Telnet cu SSL” la pagina 30

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

Conceptele DCM

Pornire Digital Certificate Manager

#### **Operații înrudite**

“Configurarea SSL pe serverul Telnet” la pagina 30

Cel mai important factor de luat în considerare când activați SSL pe serverul Telnet este sensibilitatea informației care este implicată în sesiunile client. Dacă informațiile sunt sensibile, sau private, atunci este recomandată securizarea serverului Telnet cu SSL.

## **Verificarea stării sistemului**

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

1. Verificați că aveți instalat software-ul corespunzător pentru a suporta Telnet SSL și pentru a gestiona certificate:
  - IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1)
  - Manager de certificat digital
  - IBM HTTP Server for i5/OS (5761-DG1)
  - IBM Developer Kit for Java (5761-JV1)
2. Verificați dacă aveți un server Telnet sigur prin asocierea unui certificat cu aplicația server Telnet QIBM\_QTV\_TELNET\_SERVER.
3. Dați un ping sistemului 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.

#### **Operații înrudite**

“Asignarea unui certificat la serverul Telnet” la pagina 31

Când activați serverul Telnet în sistemul dumneavoastră să folosească SSL (Secure Sockets Layer), puteți stabili conexiuni securizate Telnet către sistemul dumneavoastră de la System i Access pentru Windows sau de la oricare alți clienți Telnet SSL-activi, cum ar fi un emulator Comunicații personale.

“A face ping serverului dumneavoastră gazdă” la pagina 85

Puteți folosi funcția Ping în Navigator System i pentru a testa conexiunea dumneavoastră TCP/IP.

“Pornirea serverului Telnet” la pagina 19

Serverul Telnet activ are una sau mai multe instanțe de aceste joburi care rulează în subsistemul QSYSWRK: QTVTELNET și QTVDEVICE.

“Configurarea SSL pe serverul Telnet” la pagina 30

Cel mai important factor de luat în considerare când activați SSL pe serverul Telnet este sensibilitatea informației care este implicată în sesiunile client. Dacă informațiile sunt sensibile, sau private, atunci este recomandată securizarea serverului Telnet cu SSL.

### Referințe înrudite

“Coduri de retur SSL” la pagina 90

Subiectul listează codurile de retur SSL (Secure Sockets Layer) pentru cele mai obișnuite probleme care ar putea apărea în timpul inițializării SSL sau în timpul dialogului de confirmare SSL.

## Căutarea unui ascultător SSL activ

Folosiți această procedură pentru a verifica dacă există un ascultător SSL (Secure Sockets Layer) activ. Serverul Telnet trebuie să fie activ și pregătit să primească încercări de conexiune.

Pentru a căuta un ascultător SSL activ, urmați acești pași:

1. În interfața pe bază de caractere, tastați NETSTAT \*CNN pentru a afișa ecranul Stare lucru cu conexiune TCP/IP.
2. În coloana **Port local**, găsiți eticheta telnet- pentru telnet-ssl. Puteți vedea doar telnet- deoarece câmpul nu este destul de lung în ecran.
  - Folosiți tasta F22 pentru a afișa complet câmpul Port local.
  - Folosiți tasta F14 pentru a vedea numerele de port. Intrarea telnet-ssl este port 992.

Inițializarea SSL eșuează dacă nu găsiți telnet-ssl în coloana Port local. Pentru a rezolva problema, verificați mesajul de diagnostic SSL în istoricul de job QTVTELNET care rulează în subsistemul QSYSWRK. Doar un singur job QTVTELNET va rula după o eroare de inițializare SSL.

### Operații înrudite

“Verificarea istoricului de joburi Telnet”

Când inițializarea și dialogul de confirmare SSL (Secure Socket Layer) eșuează, serverul Telnet trimite un mesaj de diagnostic CPDBC *nn* la jobul QTVTELNET.

## Verificarea istoricului de joburi Telnet

Când inițializarea și dialogul de confirmare SSL (Secure Socket Layer) eșuează, serverul Telnet trimite un mesaj de diagnostic CPDBC *nn* la jobul QTVTELNET.

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

1. În Navigator System i, expandați *sistemul dumneavoastră* → **rețea** → **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. Expandați **Gestiune Job** → **Joburi Server**.
5. Apăsăți butonul drept al mouse-ului pe **QTVTELNET** din coloana Nume job.
6. Selectați **Istoric job**.
7. Căutați mesajul CPDBC*nn* 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.

#### Concepte înrudite

“Inițializare și dialog de confirmare (handshake) SSL” la pagina 35

Aici sunt detaliile despre interacțiunile dintre servere Telnet, clienți și SSL (Secure Sockets Layer).

#### Operații înrudite

“Căutarea unui ascultător SSL activ” la pagina 89

Folosiți această procedură pentru a verifica dacă există un ascultător SSL (Secure Sockets Layer) activ. Serverul Telnet trebuie să fie activ și pregătit să primească încercări de conexiune.

## Coduri de retur SSL

Subiectul listează codurile de retur SSL (Secure Sockets Layer) pentru cele mai obișnuite probleme care ar putea apărea în timpul inițializării SSL sau în timpul dialogului de confirmare SSL.

Este nesar să parcurgeți acești pași înainte de a utiliza următoarele tabele de coduri de retur:

- Trebuie să aflați codul retur SSL în istoricul jobului QTVTELNET.
- În unele cazuri, este nevoie să lucrați cu configurația DCM (Digital Certificate Manager) pentru a rezolva problemele cu certificatele CA (certificate authority) sau certificate de sistem.
- La copierea informațiilor din certificatele CA pentru clientul Telnet SSL, nu uitați să copiați liniile ce includ cuvintele BEGIN CERTIFICATE și END CERTIFICATE.

Tabela 20. Codurile obișnuite de retur

Cod de retur	Descriere
-2	<p><b>Nu este disponibil nici un certificat sistem pentru procesarea SSL.</b> Serverul Telnet inițializează cu succes SSL, dar dialogul de confirmare (handshake) SSL eșuează. Nu există nici un panou de semnare în fereastra client Telnet SSL. Aplicația QIBM_QTV_TELNET_SERVER nu are alocată un certificat sistem.</p> <p>Vizualizați certificatul sistem și verificați dacă apare valoarea Da (Yes) în coloana Certificat alocat. Dacă valoarea este Nu, creați un certificat sistem pentru aplicația QIBM_QTV_TELNET_SERVER.</p>
-4	<p><b>Certificatul CA sau certificatul sistem este viciat.</b> Certificatul sistem nu este privat sau de încredere. Câmpurile Cheie privată și De încredere din certificatul de pe server sunt incorecte. Fereastra client SSL Telnet nu are nici un panou de semnare.</p> <p>Adăugați informații CA în clientul dumneavoastră SSL Telnet. Dacă folosiți System i Access pentru Windows ca client SSL Telnet, vedeți Gestionare certificate publice Internet pentru sesiunii de comunicație SSL. În caz contrar, vedeți pentru instrucțiuni Obținerea unei copii a certificatului CA privat.</p>
-16	<p><b>Sistemul peer nu este recunoscut.</b> 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 la clientul dumneavoastră SSL Telnet.</p>
-18	<p><b>Certificatul sistem este auto-semnat, iar serverul îl utilizează drept certificat CA.</b> Certificatul sistem alocat 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.</p>

Tabela 20. Codurile obișnuite de retur (continuare)

Cod de retur	Descriere
-23	<b>Certificatul sistem nu este semnat de către o autoritate de certificare de încredere.</b> Certificatul sistem alocat aplicației QIBM_QTV_TELNET_SERVER trebuie să fie de încredere, semnat de o autoritate de certificate și folosit în perioada de validitate.  Modificați certificat CA la De încredere. Pentru instrucțiuni, vedeți Gestionarea aplicațiilor în DCM.
-24	<b>Perioada validă de timp a certificatului CA a expirat.</b> Utilizați un certificat expirat. Fereastra client Telnet SSL nu are nici un panou de semnare în sistem.  Reînnoiți certificatul CA care a fost utilizat pentru a construi certificatul sistem.
-93	<b>SSL nu este disponibil pentru utilizare.</b> Clienții Telnet SSL nu se pot conecta la o gazdă deoarece nu există nici un ascultător SSL activ.  Instalați necesarul software care să sigure suportul pentru Telnet SSL și pentru administrarea certificatelor. Pentru instrucțiuni, vedeți Verificarea stării sistemului.

### Alte coduri de retur SSL

Pentru codurile de retur SSL din tabela următoare, folosiți DCM pentru a verifica dacă certificatele digitale îndeplinesc aceste cerințe:

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

Tabela 21. Alte coduri de retur SSL

Cod de retur	Descriere
-1	Nu sunt disponibile sau specificate cifruri
-6	Sistemul de operare i5/OS nu suportă tipul de certificat
-10	A intervenit o eroare în procesarea SSL. În istoricul de joburi, verificați mesajul CPExxxx unde xxxx este valoarea erorii de socket
-11	SSL a primit un mesaj formatat greșit
-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 nu este valid sau este respins de programul de ieșire
-94	SSL_Init() nu a fost invocat anterior pentru job

Tabela 21. Alte coduri de retur SSL (continuare)

Cod de retur	Descriere
-95	Nu există inel de chei pentru inițializarea 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

### Operații înrudite

Configurare DCM

Gestionarea asignarea certificatului pentru o aplicație

Gestionarea certificatelor publice Internet pentru sesiuni de comunicații SSL

Crearea și operare unui CA local

Gestionarea aplicațiilor în DCM

“Verificarea stări sistemului” la pagina 88

Este nevoie să confirmați că Telnet-ul dumneavoastră este pregătit pentru sesiuni SSL (Secure Sockets Layer).

### Referințe înrudite

Obținerea unei copii a certificatului privat CA

## Ieșiri ale programului serviciu TRCTCPAPP

Puteți rula o urmărire de componentă VCM (Virtual Terminal Manager - Manager de terminal virtual) cu câmpul de date utilizator setat la Telnet.

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 la QTVnnnnnn.

Iată un exemplu cu ce vedeți în istoricul dumneavoastră de job interactiv când realizați o apelare TRCTCPAPP \*OFF.

```

Introducere comenzi                                SYSNAM03
Nivel cerere: 1
Toate mesajele și comenzile anterioare:
> trctcpapp *telnet *off
Fișier imprimantă spool 1 deschis pentru ieșire.
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 un exemplu cu ce vedeți în coada implicită de ieșiri.

Lucru cu toate fişierele spool  
 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 User Data	Sts	Total Pages	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 fişier cu numele VTMTRACE. Dacă modul Telnet SSL este operaţional pe server, s-ar putea să aveţi unul sau mai multe fişiere QTOCTTRC.

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

```

                                Afişare fişier spool
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
  00FF0000 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:
qvtvtnet: 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 QTVTELNET 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 fişier QTOCTTRC. Acesta este un fişier spool manager de dispozitiv, opus jobului de server QTVTELNET.



```

                                Afişare fişier spool
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 5FFFFFFE4 | .....y..U| Byte 48
  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:
qvtvncsh: >>>> 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
qvtvncsh: Program QTVTNCSSH dated 04 December 1998 running
qvtvncsh: iActiveLogLevel: 0
qvtvncsh: Source file: qvtvncsh.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

```

### Concepte înrudite

“Materialele necesare pentru raportarea problemelor Telnet”

S-ar putea să fie nevoie să furnizați reprezentantului service aceste informații când raportați o problemă Telnet.

## Materialele necesare pentru raportarea problemelor Telnet

S-ar putea să fie nevoie să furnizați reprezentantului service aceste informații când raportați o problemă Telnet.

- Istoricul jobului server Telnet:
  - Istoric job QTVTELNET
  - Istoric job QTVDEVICE

- Câteva detalii despre scenariul problemei. De exemplu:
  - Tipul de gazdă la distanță pe care o folosiți pentru Telnet de la sau către, cum ar fi System i, System z, sau System p. Acesta este util în mod special dacă realizați funcții Telnet cascade.
  - Tipul de client care încearcă să se conecteze la serverul Telnet, cum ar fi IBM Personal Communications și System i Access pentru Windows.
- Istoricul jobului interactiv care rulează clientul Telnet (când clientul Telnet este sub investigație).
- 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 dumneavoastră de service vă poate îndruma să includeți mesaje de difuzare în această urmărire. În plus, ar trebui să filtrați această urmărire pe o adresă IP specifică dacă aveți o cantitate mare de trafic în rețeaua dumneavoastră și cunoașteți adresa IP a clientului care eșuează.
- Orice istorice pentru codul intern licențiat (LIC) cu codul major 0700 și codul minor 005x din timpul eșecului. În plus, ar putea exista istorice informative de LIC pentru codul major 0701 și pentru codul minor 005x, care pot fi utile, dar nu 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 detalii complete despre utilizarea comenzii TRCTCPAPP (Trace TCP/IP application - Urmărire aplicație TCP/IP), vedeți descrierea comenzii TRCTCPAPP.

Când rulează urmărirea VTM LIC se simte asupra performanței. Câteva 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(ume\_dispozitiv)
- Pentru a urmări activitatea pe un dispozitiv anume, când cunoașteți adresa clientului:  
TRCTCPAPP APP(\*TELNET) SET(\*ON) RMTNETADR(\*INET'www.xxx.yyy.zzz')
- Pentru oprirea urmăririi și generarea unui fișier spool de ieșire:  
TRCTCPAPP APP(\*TELNET) SET(\*OFF)

**Notă:** Ar trebui să primiți de la reprezentantul dumneavoastră de service detalii specifice despre ce parametri de urmărire să utilizați pentru problema dumneavoastră înainte de rularea acestei comenzi. Aceasta asigură strângerea de informații corecte despre problema dumneavoastră.

### Concepte înrudite

“Ieșiri ale programului serviciu TRCTCPAPP” la pagina 92

Puteți rula o urmărire de componentă VCM (Virtual Terminal Manager - Manager de terminal virtual) cu câmpul de date utilizator setat la Telnet.

## Informații de diagnoză generate automat

Unele erori de server Telnet generează automat informații de diagnoză. Acest subiect descrie cum se pot extrage acele informații.

S-ar putea să se producă unele informații de diagnoză generate automat la apariția anumitor erori în cadrul serverului Telnet. Exită momente când reprezentantul dumneavoastră de service va avea nevoie de informațiile de diagnoză pentru a putea analiza corespunzător o problemă de server 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. Unul este provocat de apelul DSPJOB \*PRINT și DSPJOBLOG \*PRINT îl provoacă pe celălalt. În acest fel,

obțineți în dump atât istoricul jobului, cât și atributele de rulare ale jobului și aveți ieșirea de la grupul de date al utilizatorului împreună cu un identificator de număr de job. Apoi, puteți să o comparați cu ieșirea oricărei componente VTM de urmărire.

Puteți observa nu 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 următoare:

```
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
      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
```

## Informațiile înrudite pentru Telnet

Publicațiile IBM Redbooks și siteurile web conțin informații înrudite cu colecția de subiecte Telnet. Puteți vedea sau tipări oricare din fișierele PDF.

### IBM Redbooks

**V4 TCP/IP pentru AS/400: Mai multe lucruri interesante ca niciodată**  (aproximativ 10 035 KB)

Această publicație furnizează informații extinse despre TCP/IP, inclusiv exemple de scenarii care demonstrează soluții obișnuite cu exemple de configurații.

### Situri Web

- **Internet Assigned Numbers Authority (IANA)**  ([www.iana.org](http://www.iana.org))

Găsiți informații despre asignarea comună a numerelor de port.

- **The Internet Engineering Task Force (IETF)**  ([www.ietf.org](http://www.ietf.org))

RFC (Request for Comments), cum sunt Îmbunătățiri Telnet 5250 RFC 4777 .

#### Referințe înrudite

“Fișier PDF pentru Telnet” la pagina 1

Puteți vizualiza și tipări un fișier PDF cu aceste informații.

## Informații referitoare la licența de cod și declinarea responsabilității

IBM vă acordă o licență de copyright neexclusivă pentru utilizarea tuturor exemplurilor de cod de programare din care puteți genera funcții similare, adaptate propriilor nevoi specifice.

CU EXCEPȚIA GARANȚIILOR LEGALE CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII SĂI DE PROGRAME ȘI FURNIZORII SĂI NU ACORDĂ NICI O GARANȚIE SAU CLAUZĂ, EXPLICITĂ SAU IMPLICITĂ, INCLUSIV DAR FĂRĂ A SE LIMITA LA GARANȚIILE SAU CLAUZELE IMPLICITE DE VANDABILITATE, DE CONCORDANȚĂ CU UN ANUMIT SCOP ȘI DE NEÎNCĂLCARE A LEGII, PRIVIND PROGRAMUL SAU SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII SĂI NU VOR FI ÎN NICI O ÎMPREJURARE RĂSPUNZĂTORI PENTRU ORICARE DINTRE URMĂTOARELE, CHIAZ DACĂ AU FOST INFORMAȚI CU PRIVIRE LA POSIBILITATEA PRODUCERII ACESTORA:

1. PIERDERE SAU DETERIORARE A DATELOR;
2. PAGUBE DIRECTE, SPECIFICE, ACCIDENTALE SAU INDIRECTE, SAU PENTRU ORICE PAGUBE ECONOMICE SURVENITE DREPT CONSECINȚĂ; SAU
3. PIERDERI DE PROFIT, DE VENITURI, PIERDERI COMERCIALE SAU PIERDERI PRIVIND REPUTAȚIA SAU ECONOMIILE SCANTATE.

ANUMITE JURISDICȚII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR DIRECTE, ACCIDENTALE SAU A CELOR SURVENITE DREPT CONSECINȚĂ, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU SE APLICE ÎN CAZUL DUMNEAVOASTRĂ.

---

## Anexa. Observații

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

Este posibil ca IBM 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 disponibile în prezent în zona dumneavoastră. Orice referință la un produs, program sau serviciu IBM nu intenționează să declare sau să sugereze că se poate utiliza doar acel produs, program sau serviciu IBM. Se poate folosi în schimb orice produs, program sau serviciu echivalent din punct de vedere funcțional și care nu încalcă vreun drept 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 deține brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Furnizarea acestui document nu vă acordă nici o licență asupra acestor brevete. 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), contactați Departamentul de proprietate intelectuală al IBM 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, EXPRIMATĂ SAU PRESUPUSĂ, 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 notificare.

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 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 față de 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 YBWA  
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 acest document și toate produsele cu licență disponibile pentru acesta sunt furnizate de către IBM sub termenii Contractului IBM cu Clientul, Contractului IBM de licență internațională a programului,
- | Contractului IBM de licență pentru cod mașină sau orice contract echivalent între noi.

Informațiile privind produsele non-IBM au fost obținute de la furnizorii acestor produse, din anunțurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse și nu poate confirma acuratețea performanțelor, compatibilitatea sau orice alte pretenții legate de produsele non-IBM. Întrebările legate de capacitățile produselor non-IBM vor fi adresate furnizorilor acestor produse.

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.

---

## | Informații despre interfața de programare

Această publicare Telnet documentează anumite Interfețe de programare care permit clientului să scrie programe care obțin servicii de la IBM i5/OS.

---

## Mărci comerciale

Următorii termeni sunt mărci comerciale deținute de International Business Machines Corporation în Statele Unite, în alte țări sau ambele:

AIX  
AS/400  
i5/OS  
IBM  
IBM (logo)  
OS/2  
OS/400  
Redbooks  
System i  
System p  
System z  
System/370

- | Adobe, logo-ul Adobe, PostScript și logo-ul PostScript sunt fie mărci comerciale înregistrate fie mărci comerciale ale Adobe Systems Incorporated în Statele Unite, și/sau alte țări.

Microsoft, Windows, Windows NT și logo-ul Windows sunt mărci comerciale ale corporației Microsoft din Statele Unite, din 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, produse sau servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

---

## Termenii și condițiile

Permisunile pentru utilizarea acestor publicații sunt acordate în conformitate cu următorii termeni și condiții.

**Utilizare personală:** Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți distribui, afișa sau realiza obiecte derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

**Utilizare comercială:** Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit al IBM.

Cu excepția a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licențe sau drepturi, explicit sau implicit, pentru Publicații sau alte informații, date, software sau altă proprietate intelectuală conțină în acestea.

IBM își rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicațiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât în deplină conformitate cu legile și regulamentele aplicabile, inclusiv toate legile și regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICI O GARANȚIE PENTRU CONȚINUTUL ACESTOR PUBLICAȚII. ACESTE PUBLICAȚII SUNT FURNIZATE "CA ATARE", FĂRĂ NICI UN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ȘI DE POTRIVIRE PENTRU UN ANUMIT SCOP.









Tipărit în S.U.A.